УДК 004.681

Шорошев В.В.,Чирков Д.В.

ФОРМУВАННЯ ПОЛІТИКИ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ

Під політикою безпеки (Policy of safety, PS) комп'ютерної системи (надалі КС) розуміється низка законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки, захисту та поширення інформації і спрямовані на захист інформації від певних загроз. Політика безпеки передбачає також захист і ресурсів КС від цих загроз. Політика безпеки повинна містити, насамперед, перелік та опис послуг безпеки, що надаються комплексом засобів захисту (КЗЗ) - ядром безпеки обчислювальної системи КС, а також перелік та опис послуг безпеки, що надаються комплексною системою захисту Інформації (КСЗІ) - ядром безпеки усієї КС.

Термін "політика безпеки" може бути застосовано щодо: певного об'єкту інформаційної діяльності (ОІД), наприклад: установи, міністерства, відомства, організації тощо; автоматизованої системи (АС); комп'ютерної системи (КС); обчислювальної системи (ОБС) АС, КС; а також стосовно окремої послуги безпеки, яка реалізується цими системами чи набором функціональних (Services of safety functional, SSF-послуг) та гарантійних (Services of safety guaranty, SSG - послуг) послуг безпеки тощо. Чим дрібніше об'єкт, відносно якого застосовується даний термін, тим конкретнішими і формальніше визначаються правила реалізації політики безпеки (Rules of realization of policy (politics) of safety, RPS- правила). Далі для скорочення замість словосполучення "політика безпеки інформації і ресурсів" використовується словосполучення "політика безпеки" (або скорочення RS-політика), а замість словосполучення "політика безпеки інформації, що реалізується послугою" - "політика безпеки послуги" (Policy of Service of safety, PSS - політика).

Політика безпеки інформації в КС є частиною загальної політики безпеки об'єкта інформаційної діяльності, на якому функціонує захищена КС (КС державної чи комерційної структури) і може успадковувати також специфічні вимоги безпеки структури та окремі положення державної політики у галузі захисту інформації.

Основними складовими політики безпеки комп'ютерної системи визначаються: загальні положення щодо формування політики безпеки, методичні основи формування складових і концептів політики безпеки, політика дотримання системних основ забезпечення політики безпеки, політика постійного моніторингу порушень і забезпечення політики безпеки. Вони визначені на інформаційно-логічній моделі політики безпеки комп'ютерної системи, наведеної на рис. 1.

Політика безпеки КС має бути також гармонізована з основними положеннями Конвенції Ради Європи про кіберзлочинність, яка у 2001 році підписана Україною для її виконання у рамках міжнародного співробітництва щодо здійснення контролю за суспільно небезпечними діями з комп'ютерними даними та системами [1].

Політика постійного моніторингу порушень і забезпечення політики безпеки передбачає: своєчасне виявлення порушень політики безпеки категорій 1, 2, 3, 4; документування порушень, їх насідків, їх аналіз для попередження у подальшому; *показ* фактичного надання певної послуги безпеки (послуга є чи ні); *демонстрація* фактичного надання певної послуги безпеки (послуга функціонує чи ні); *доказ* надання послуги безпеки (послуга ефективна чи ні).

Як найбільш *практично важливі* складові частини PS - політики (політики безпеки інформації в КС) визначаються також уніфіковані (стандартні, обов'язкові) політики надання наступних послуг: а) функціональних послуг безпеки (Policy safety services functional, PSSF - політика) - *конфіденційності* інформації (Policy confidentiality information, PSCI - політика); *цілісності* інформації (Policy integrity information, PSII - політика); *доступності* інформації (Policy availabity information, PSAI- політика); *спостереженості* інформації (Policy management information, Policy accountability information, PSMI -

політика); б) гарантійних послуг безпеки інформації (Policy safety infrmation, PSGG - політика) на рівнях Г-1...Г-7.

Вимоги до функціональних послуг безпеки спостереженості інформації та до гарантійних послуг безпеки рівнів Г-2, Г-3 визначаються як обов'язкові та необхідні умови для реалізації політик конфіденційності, цілісності і доступності інформації.

Найбільш практично важливою складовою щодо реалізації обраної політики безпеки визначається політика надання профільних послуг безпеки, тобто послуг стандартних профілів захищеності інформації (Standard structures of security of the information, PSSS - політика, СПЗІ - політика). Профілі захищеності складають ядро політики безпеки (Nucleus policy safety, PSNS-політика) КС тому, що вибір їх складу та їх реалізація забезпечує поступове нарощування до належного стану захищеності інформації шляхом надання двох базових видів послуг безпеки: *функціональних SSF-* послуг (захист від загроз конфіденційності, цілісності, доступності і спостереженості оброблюваної інформації КС) та *гарантійних SSG* - послуг (гарантії безпеки інформації і ресурсів КС рівнів Г-1, ... , Г-7).
Нарешті, політика *персональної відповідальності* (Policy of the personal responsibity, PSPR - політика) та постійного моніторингу (Policy monitoring conditional safety, PSMS - політика) щодо належного стану безпеки інформації і ресурсів КС також визначається базовою складовою політики безпеки. Відповідальність персоналу за постійне дотримання положень політики безпеки має бути персоніфікована і підконтрольна адміністратором безпеки КС.

Частина політики безпеки, яка регламентує правила доступу користувачів і процесів до інформації і ресурсів КС, складає правила розмежування доступу (Rules of differentiation of access, RDA-правила, ПРД, RDA - політика, ПРД -політика).

Політики безпеки інформації, що реалізуються різними КС, будуть відрізнятися не тільки тим, що реалізовані в них функції захисту, складові та концепти політики безпеки можуть забезпечувати захист від різних типів загроз, різних об'єктів КС, але і в зв'язку з тим, що ресурси КС можуть істотно відрізнятись. Так, якщо операційна система оперує файлами, то система управління базами даних (СУБД) має справу із записами, розподіленими в різних файлах, аналогічно щодо КС різних класів та підкласів тощо. Тому, у самому повному варіанті формування політики безпеки з урахуванням специфічних особливостей КС, додатково, рішенням Замовника ЗКС (захищених КС), повинні визначатись усі складові політики безпеки щодо усіх елементів конфігурації таких захищених КС, які підлягають захисту від загроз НСД, витоку інформації, деструктивних впливів специфічних для даної ЗКС реальних і перспективних (при необхідності) загроз тощо.

Формулювання політики безпеки КС може здійснюватись за двома базовими варіантами — спрощеним (правило ПБ-1) або повним (правило ПБ-2).

Правило ПБ-1. Для якого класу і підкласу КС, для яких її об'єктів, від яких загроз, з використанням (шляхом надання) яких функціональних і гарантійних послуг безпеки стандартних профілів захищеності інформації здійснити належний захист інформації і ресурсів КС.

Таким чином, модель політики безпеки (sequrity policy model, SPM-модель) – найбільш суттєва складова політики безпеки КС і являє собою абстрактний формалізований чи неформалізований опис у довільній формі її складових і концептів та шляхів їх реалізації та аудиту. Вона розробляється після формування політики безпеки КС. Формалізовано-описовий варіант моделі політики безпеки КС надається на рис.1.

Визначення послуг безпеки стандартних профілів захищеності інформації здійснюється з дотриманням вимог НД ТЗІ 2.5-005-99 та інших нормативних чи розпорядчих документів (відомчих, Власника КС, Замовника КС тощо).

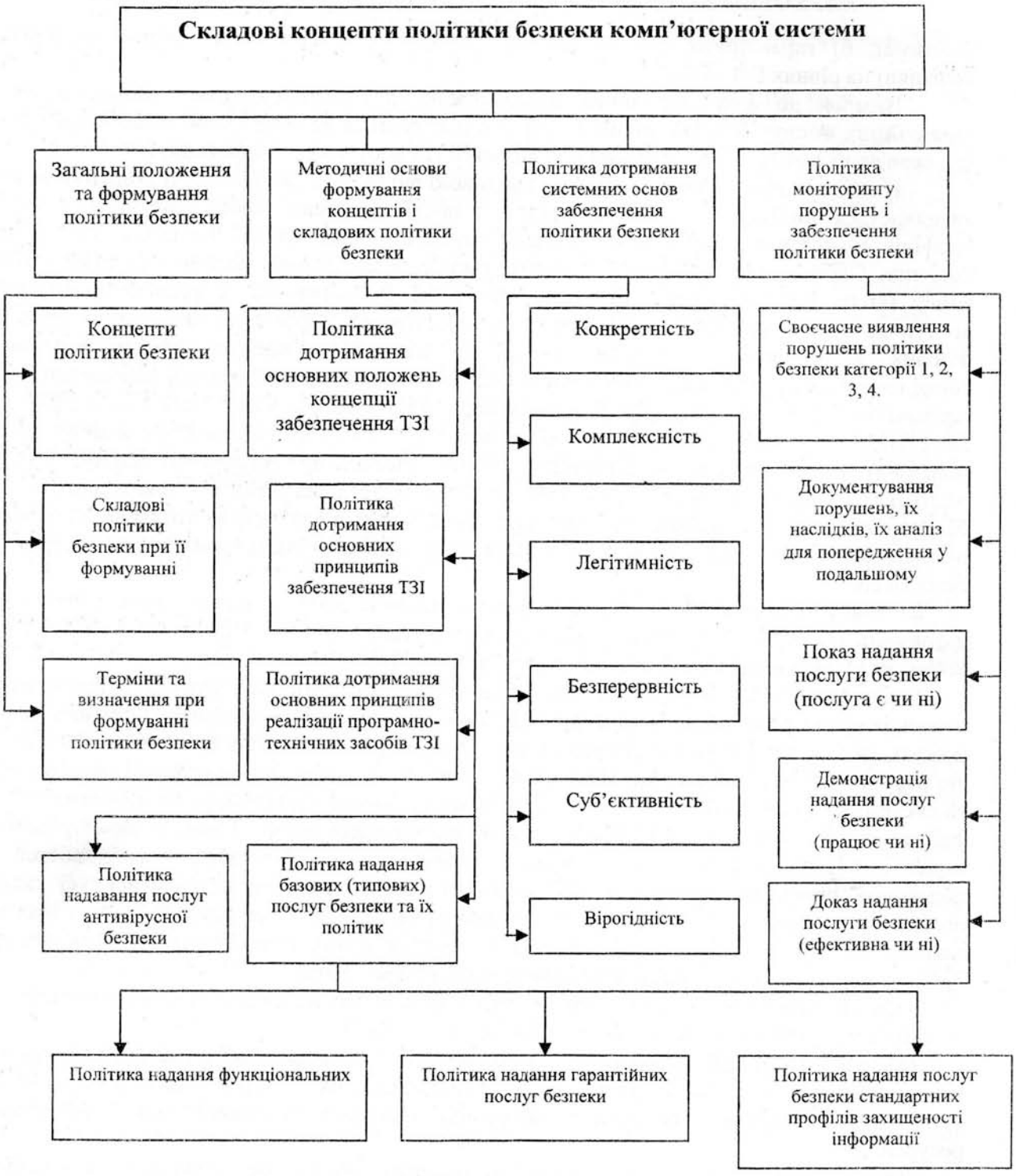

Рис 1. Базова модель політики безпеки комп'ютерної системи

Визначення політики дотримання системних основ формування і забезпечення політики безпеки здійснюється за принципами комплексності, конкретності, легітимності, безперервності, суб'єктивності та вірогідності [5].

Визначення політики дотримання постійного моніторингу порушень і забезпечення політики безпеки здійснюється за концептами згідно моделі потенційного порушника та категорії порушень політики безпеки КС (рис.3), а також згідно вимог НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99 та інших нормативних чи розпорядчих документів (відомчих, Власника КС, Замовника КС тощо).

Загрозами інформації визначаються будь-які обставини чи події, що можуть призвести до порушення політики її безпеки і/або нанесення збитків КС.

Інформація в КС існує у вигляді даних, тобто представляється у формалізованому вигляді, придатному для її обробки в ОБС. Тут і далі під обробкою розуміється як власна обробка, так і введення, виведення, зберігання, передача тощо (ДСТУ 2226-93). Далі термін «інформація» і «дані» використовуються як синоніми.

Інформація для свого існування завжди вимагає наявності носія. Як носій інформації може виступати поле або речовина. В деяких випадках у вигляді носія інформації може розглядатися людина. Втрата інформацією своєї цінності, наприклад, може статися внаслідок переміщення інформації або зміни фізичних властивостей її носія.

При аналізі проблеми захисту від загроз НСД до інформації, яка може циркулювати в обчислювальній системі (ОБС), розглядаються, як правило, лише об'єкти КС, що служать приймальника/джерела інформації, та інформаційні потоки (порції інформації, що пересилаються між об'єктами) безвідносно до фізичних характеристик їх носіїв.

Загрози оброблюваній в КС інформації залежать від характеристик, фізичного середовища, властивостей оброблюваної інформації і персоналу. Загрози можуть мати або об'єктивну природу, наприклад, помилки персоналу чи дії порушника. Загрози, що мають суб'єктивну природу, можуть бути випадковими або навмисними. Спроба реалізації загрози визначається атакою.

Із всієї множини способів кваліфікації загроз найпридатнішою для формування політики безпеки є класифікація загроз за результатом їх впливу на властивості інформації та за нормативними засадами захисту від них. На цій основі визначаються потенційні загрози [2–7], що призводять до порушення конфіденційності, цілісності, доступності, спостереженості в гарантії безпеки КС, а також відповідна модель потенційних загроз та послуг безпеки для захисту від них (рис.2).

Порушення конфіденційності інформації. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Порушення цілісності інформації. Інформація зберігає цілісність, якщо дотримуються встановлені правила її *модифікації* (видалення).

Порушення доступності інформації. Інформація зберігає доступність, якщо зберігається можливість ознайомлення з нею або її модифікації відповідно до встановлених правил упродовж будь-якого певного (малого) проміжку часу.

Порушення спостереженості. Ідентифікація і контроль за діями користувачів, керованість інформацією і ресурсами КС становлять предмет послуг спостереженості. Спостереженість від загроз не порушується, якщо КЗЗ продовжує надавати послуги щодо забезпечення відповідальності користувача КС за свої дії і щодо підтримки спроможності КЗЗ виконувати свої функції. Спостережність забезпечується в КС такими послугами безпеки: реєстрація (аудит), ідентифікація й автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація й автентифікація при обміні, автентифікація відправника (невідмова від авторства), автентифікація одержувача (невідмова від одержання).

Порушення гарантії безпеки. Запобігання порушень (умовно "загроз") гарантії безпеки при формуванні політики безпеки визначаються найбільш складними.

Це обумовлено тим, що порушення гарантії безпеки виникають та передбачають їх постійний моніторинг й аудит на всіх етапах життєвого циклу КС (від проектування (розробки) і виробництва до впровадження, експлуатації, удосконалення та виведення з експлуатації). Упевненість у відсутності порушень гарантії безпеки у Експерта, Адміністратора безпеки (Адміністратора), Власника, Розробника чи Користувача КС забезпечується в основному контролем та оцінкою ступеню дотримання вимог гарантії безпеки двох видів: вимог до функцій (послуг) забезпечення безпеки; вимог до рівня гарантій.

Виконання вимог першого виду забезпечується Розробником в процесі проектування (розробки) і перевіряється Експертною комісією (Експертом) в процесі оцінки. Виконання вимог другого виду забезпечується як діями Розробника, проте вже на всіх стадіях життєвого циклу КС, так і спільними діями Розробника і Експертної комісії (Експерта) в процесі оцінки. Наведені в критеріях гарантії безпеки вимоги [2] регламентують передусім дії Розробника. Дії Експертної комісії (Експерта) регламентуються іншими документами [1 7 17].

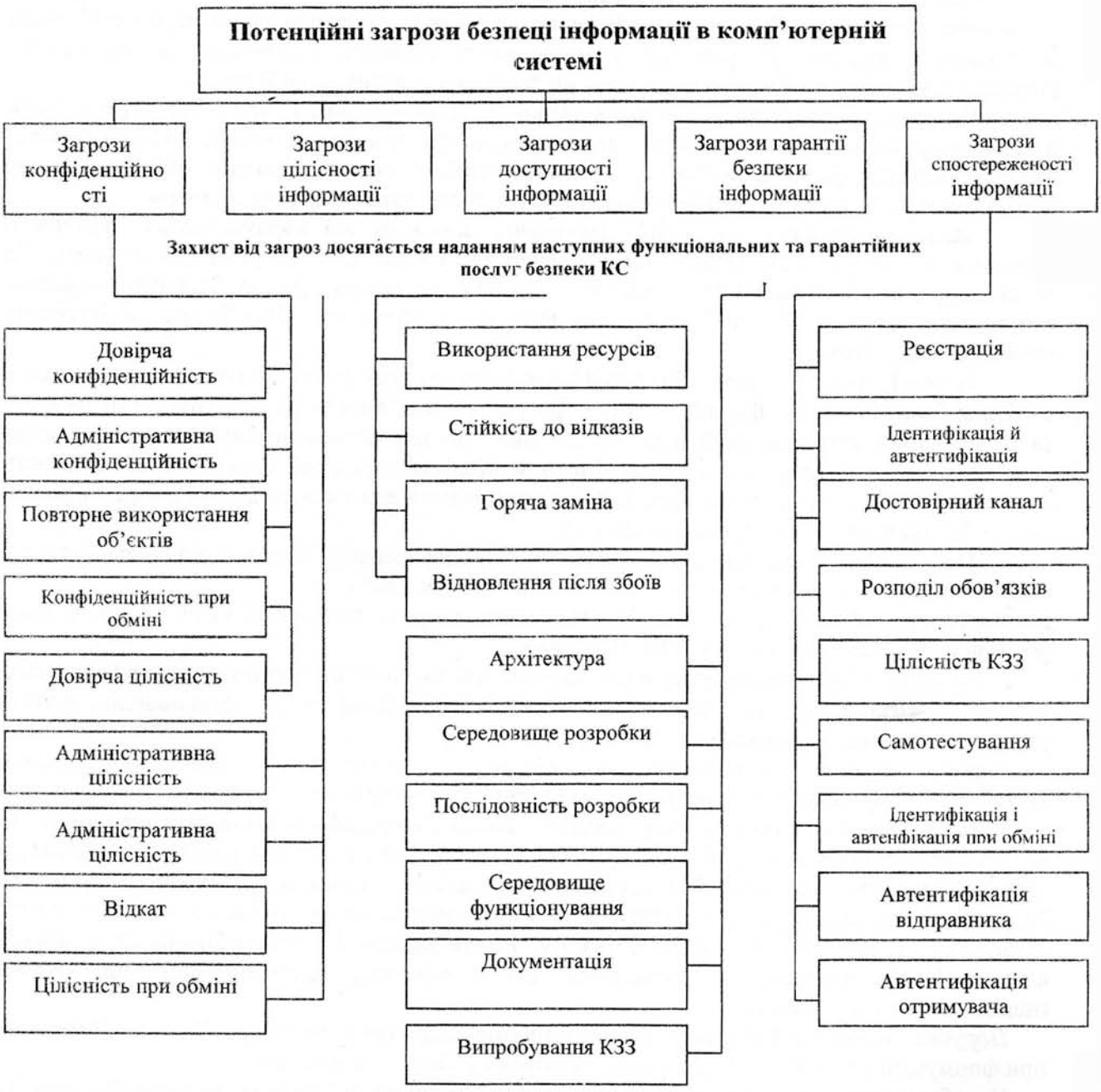

Рис.2. Модель потенційних загроз інформації в КС та базових послуг безпеки для захисту від них

Більшість з вимог критеріїв гарантії являють собою конкретизацію вимог щодо створення КЗЗ КС стандартів серії ДСТУ ISO 9000 і для їх викладення використовується термінологія з області керування якістю продукції (ДСТУ 3230-95).

Гарантії безпеки від загроз не порушуються, якщо в КС на усіх етапах її життєвого циклу дотримувались, а при експлуатації продовжують дотримуватись вимог до архітектури

КЗЗ, середовища розробки, послідовності розробки, випробування КЗЗ, середовища функціонування й експлуатаційної документації. Визначаються сім рівнів гарантії (Г-1,...,Г-7), які є ієрархічними

. Ієрархія рівнів гарантії відбиває поступово наростаючу міру певності у тому, що реалізовані в КС послуги безпеки дозволяють протистояти певним загрозам, що механізми, які їх реалізують, в свою чергу коректно реалізовані і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації.

Загрози, реалізація яких призводить до порушення якої-небудь з властивостей інформації або ресурсу КС чи надання функціональних і гарантійних послуг безпеки КС при формулюванні політики безпеки визначаються потенційними загрозами конфіденційності, цілісності, доступності, спостереженості та гарантії безпеки інформації і ресурсів КС.

Визначення потенційних загроз для об'єктів захисту КС здійснюється з дотриманням вимог НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99 та їх деталізації згідно вимог інших нормативних чи розпорядчих документів (відомчих, Власника КС, Замовника КС тощо). Згідно Закону про основи національної безпеки України [7] в інформаційній та науково-технологічній сферах (ст.ст. 2, 7) необхідно, крім потенційних загроз визначати та описувати і реальні загрози безпеці (з урахуванням специфічних особливостей обчислювальної системи, фізичного середовища, персоналу й оброблюваної інформації КС).

Окремим видом дуже небезпечної перспективної загрози слід вважати так звані радіочастотні засоби електромагнітного ураження (засоби РЧЕМУ) - засоби, які забезпечують ураження напівпровідникової елементної бази за рахунок надпотужної енергетичної дії електромагнітних випромінювань радіочастотного діапазону, що може призвести до повної або тимчасової відмови в роботі КС у найбільш відповідальних оперативних ситуаціях (порушення роботи КС силових структур в антитерористичних операціях чи заходах, КС банківських систем тощо).

Щодо моделі потенційного порушника та категорій порушень політики безпеки доцільно надати наступні рекомендації (рис.3).

Як порушник політики безпеки розглядається особа, яка може одержати несанкціонований чи санкціонований доступ до роботи з включеними до складу КС засобами та який призвів до зниження належного стану безпеки нанесення збитків. Формалізований опис моделі порушника політики безпеки надається на рис. 3.

Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами КС. Визначаються чотири рівні цих можливостей. Класифікація є ієрархічною та об'єктно-орієнтованою, тобто кожний наступний рівень включає в себе функціональні можливості попереднього, а саме:

- *перший* рівень визначає найнижчий рівень можливостей проведення діалогу з КС — можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
- *другий* рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;
- *третій* рівень визначається можливістю управління функціонуванням КС, тобто впливом на базове програмне забезпечення системи та на склад і конфігурацію її устаткування;
- *четвертий* рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів КС, аж до включення до складу КС власних засобів з новими функціями обробки інформації.

Загроза безпеці КС від потенційних порушників визначається максимальною тому, що порушник політики безпеки кожного рівня - це фахівець вищої кваліфікації, який має повну інформацію про КС; її конфігурацію, обчислювальну систему ОБС, комплекс засобів захисту КЗЗ та комплексну систему захисту інформації КСЗІ.

Доцільно розглянути ще один підхід до моделі потенційного порушника ТЗІ [в].

Оскільки час та місце факту навмисної загрози НСД передбачити неможливо, доцільно прогнозувати узагальнену інформаційно-аналітичну модель поведінки потенційного порушника ТЗІ в найбільш загрозливих ситуаціях, а саме:

1) порушник може з'явитися в будь-який час та в будь-якому місці периметру безпеки КС;

2) кваліфікація та освіченість порушника ТЗІ можуть перебувати на рівні розробника даної системи;

3) інформація щодо принципів роботи системи, у тому числі і таємна, порушнику ТЗІ відома;

4) для досягнення своєї мети порушник ТЗІ вибиратиме найбільш слабкішу ланку в захисті;

5) порушником ТЗІ може бути не тільки стороння особа, але і санкціонований користувач системи;

6) порушник діє один.

Дана формалізована інформаційно-описова модель порушника ТЗІ дозволяє визначитись з вихідними даними для організаційно-технічних заходів захисту, накреслити концептуальні основи для їх експертної оцінки і подальшої реалізації.

Згідно з п.1 необхідно створити навколо об'єкта захисту постійно діючий замкнений контур або оболонку захисту у вигляді деякої низки перешкод ТЗІ.

Згідно з п.2 властивості перешкоди ТЗІ, що являє собою механізм або засіб захисту, повинен за можливістю бути відповідним очікуваній кваліфікації та освіченості порушника ТЗІ;

Згідно з п.3 для входу в ІС санкціонованого користувача необхідна мінлива таємна інформація, яка відома тільки йому.

Згідно з п.4 підсумкова стійкість захисного контуру (оболонки) ТЗІ визначається їх найслабкішою ланкою.

Згідно з п.5 за наявності декількох санкціонованих користувачів доцільно забезпечити розмежування їх доступу до інформації у відповідності з повноваженнями та виконуваними функціями. Тим самим забезпечується реалізація основного концептуального принципу найменшої освіченості користувача КС з метою скорочення втрати, якщо матиме місце безвідповідальність (халатна помилка) одного з них. Звідси також випливає, що розрахунок стійкості захисту повинен здійснюватись для двох можливих вихідних позицій порушника ТЗІ: за межами контрольованої території та в її межах.

Згідно з п.6 як вихідною передумовою також вважаємо, що порушник ТЗІ діє один, оскільки захист від групи порушників - завдання окремого етапу досліджень. Але це не виключає можливості захисту запропонованими методами та засобами і від такого роду ситуацій, хоча подібне завдання значно складніша. При цьому під групою порушників ТЗІ слід розуміти групу фахівців, які виконують єдине завдання ТЗІ під загальним керівництвом.

Але для різних за призначенням і принципами роботи КС, видів і обмеженості оброблюваної в них інформації найбільш "загрозлива" модель поведінки потенційного порушника ТЗІ також може бути різною. Наприклад, для військових систем (систем національної гвардії, цивільної оборони) це рівень розвідника-професіонала, для комерційних - рівень кваліфікованого користувача, для інформаційних систем органів МВС - це рівень кваліфікованого стороннього або санкціонованого порушника ТЗІ тощо. Очевидно, що для захисту інформації від кваліфікованішого і освіченішого (проінформованого) порушника ТЗІ потрібно буде розглянути більшу кількість потенційних каналів НСД та використати більшу кількість засобів захисту з найвищими показниками стійкості ТЗІ.

Для вибору вихідної моделі поведінки потенційного порушника ТЗІ найбільш доцільно використовувати диференційований підхід, який буде враховувати гриф захищуваної інформації. Оскільки кваліфікація порушника ТЗІ

- поняття досить відносне і приблизне, доцільно прийняти за основу наступні чотири рівня стійкості захисту або класи безпеки стосовно порушників ТЗІ:

1-й клас рекомендується для захисту суттєво важливої інформації, витік, порушення або модифікація якої можуть призвести до великих втрат для санкціонованого користувача. Стійкість захисту повинна бути розрахована на порушника-професіонала;

2-й клас рекомендується використовувати для захисту важливої інформації при роботі декількох санкціонованих користувачів, які мають доступ до різних масивів даних або які формують свої файли, що недоступні іншим санкціонованим користувачам. Стійкість захисту повинна розраховуватись на порушника ТЗІ високої кваліфікації;

3-й клас рекомендується для захисту відносно цінної інформації, постійний несанкціонований доступ до якої шляхом її накопичення може призвести до витоку і більш цінної інформації. Стійкість захисту повинна розраховуватись на відносно кваліфікованого порушника-професіонала ТЗІ;

4-й клас рекомендується для захисту іншої інформації, яка для серйозних порушників ТЗІ не має цінності. Такий клас необхідний для додержання технологічної дисципліни обліку та обробки інформації службового користування і відкритої інформації КС з метою захисту її від випадкових порушень внаслідок помилок санкціонованих користувачів і деякої підстраховки від випадків цілеспрямованих загроз НСД.

Рис.3. Модель потенційного порушника та категорій порушень політики безпеки КС.

Реалізація вищевказаних рівнів безпеки КС від загроз НСД згідно з класифікацією порушників ТЗІ повинна узгоджуватись з низкою відповідних організаційно-технічних заходів та засобів захисту, але з обов'язковою передумовою перекриття всіх можливих каналів НСД з урахуванням грифу та ступеня важливості захищуваної інформації в КС.

Рівень безпеки захисту для кожного класу забезпечується експертною оцінкою та моніторингом стану безпеки КС від атак НСД за певними методиками [6, 7].

Висновок

Викладені рекомендації можуть бути корисними для формування політики безпеки КС - найбільш суттєвої і ще мало визначеної складової при створенні, експлуатації та забезпеченні безпеки інформації в захищених КС.

Список літератури

1. *В.В.Шорошев, Близнюк І.Л.* Огляд способів вчинення комп'ютерних злочинів. Бизнес и безопасность № 2, 2004. С.44-50.

2. *НД ТЗІ 1.4-004-99.* Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБУ, 1999.

3. *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.

4. *НД ТЗІ 2.5-010-2003.* Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. ДСТСЗІ СБУ, 2003.

5. *А.Ю. Ільніцький, В.В.Шорошев, І.Л.Близнюк.* Монографія "Базова модель експертної системи оцінки безпеки інформації в комп'ютерних система органів внутрішніх справ України" (шифр "Торсіон-1 ").

- К.: Видавництво НАВСУ, 2003р. - 316с.

6. *Зегжда Д.П., Ивашко А.М.* Основи безопасности информационних систем. - М: Горячая линия - Телеком, 2000. - 452 с. 15.

7. *НД ТЗІ 1.4-004-99.* Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБУ, 1999

Надійшла 12.11.2007р.

УДК 681.3.06 **Терейковський І.А.**

ПЕРСПЕКТИВИ ПРАКТИЧНОГО ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ В ЗАДАЧАХ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Використання нейронних мереж (НМ) в галузі комп'ютерного забезпечення технічних та економічних систем триває вже декілька десятиліть. Розроблені належні теоретичні та практичні рекомендації в яких наведена досить чітка методика визначення відповідності архітектури мережі з характером прикладної задачі. На цьому фоні за останні декілька років помітно зріс інтерес до застосування НМ при вирішенні задач захисту програмного забезпечення інформації. Відомі дослідження в яких показано методику вирішення окремих задач за допомогою НМ. Разом з тим, коло практичних задач захисту інформації (ЗЗІ) розв'язувати які доцільно за допомогою НМ окреслено не достатньо чітко. Крім того, відсутня загальна методика визначення відповідності архітектури та характеру застосування НМ до прикладної ЗЗІ. По цим причинам метою даної статі є – визначення кола практичних задач захисту програмного забезпечення які доцільно вирішувати за допомогою НМ та формування рекомендацій що до застосування конкретного типу мережі.

Передумови застосування штучних нейронних мереж

Під терміном штучні НМ розуміють мережу елементів (штучних нейронів), пов'язаних між собою синаптичними зв'язками [1, 2]. Нейрони та зв'язки між ними