УДК 681.3

ВИЗНАЧЕННЯ ЗАЛИШКОВОГО РИЗИКУ ПРИ ОЦІНЦІ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО – ОБЧИСЛЮВАЛЬНИХ СИСТЕМАХ

Микола Будько
Відкрите акціонерне товариство "КП ОТІ"

Анотація: **Для оцінки захищеності інформації автоматизованих систем запропоновано моделі відповідних систем захисту інформації та застосування ймовірностей подолання порушником засобів захисту тих чи інших властивостей захищеності – величин залишкового ризику; наведені вирази для їх розрахунків.**
Summary: **For estimation of protected of information of the automated systems the models of the proper systems of defence of information and application of probabilities of overcoming by the violator of facilities of defence of those or other properties of protected are offered − sizes of remaining risk, resulted expressions for their calculations.**
Ключові слова: **Загроза, конфіденційність інформації, цілісність інформації, доступність інформації, засоби захисту, залишковий ризик, модель захисту.**

I Вступ

На сучасному етапі розвитку інформаційно − обчислювальних систем та мереж (ОС) для захисту їх ресурсів, насамперед інформації, розробляються системи захисту, які мають забезпечити потрібний рівень захищеності інформації ОС – рівень захищеності її конфіденційності, цілісності, та доступності [1 – 3]. Одним із етапів оцінки рівня захищеності, що досягається при розробці чи виборі для використання систем захисту, є етап аналізу загроз (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків) і визначення переліку суттєвих загроз. Для оцінки ефективності та ступеню захищеності ОС використовують якісні чи кількісні показники. Одним із таких кількісних показників може бути введена в [4] шкода, яка завдається чи власнику ОС, чи власнику інформації ОС у разі подолання порушником системи захисту цієї інформації. Для обчислення шкоди необхідно знати величини збитків, які зазнає власник ресурсу в разі подолання засобів захисту конфіденційності, цілісності та доступності інформації ОС та при простої системи під час контролю. В багатьох випадках інформація про такі збитки або відсутня цілком, або уявлення про їх розмір є занадто загальним. Звернемо наразі увагу на те, що величина шкоди визначається також через ймовірності подолання засобів захисту конфіденційності, цілісності та доступності інформації ОС, визначення яких є менш складним. Тому як кількісні показники для оцінки захищеності систем в [5] запропоновано залишкові ризики у формі ймовірностей подолання порушниками засобів захисту конфіденційності, цілісності та доступності інформації ОС та наведені формульні вирази для їх обчислення. Вид формульних виразів для розрахунку залишкового ризику залежить, зрозуміло, від складу та порядку використання засобів захисту, тобто від застосованих моделей систем захисту відповідних функціональних властивостей захищеності інформаційних ресурсів. В даній статті пропонуються деякі уточнення моделей систем захисту та відповідних виразів для визначення залишкового ризику, а також пропонується варіант узагальненої моделі системи захисту.

II Залишкові ризики для оцінки конфіденційності, цілісності та доступності

За **величину залишкового ризику** пропонується використовувати ймовірності порушення: конфіденційності – $q_{пк}$, цілісності – $q_{пц}$, доступності – $q_{пд}$ та подолання, злому комплексної системи захисту – q.

Для їх оцінки ОС вважається складною, ієрархічною, розподіленою інформаційно – обчислювальною системою, елементами якої є ЛОМ, елементи різних рівнів якої пов'язані засобами телекомунікаційної мережі (ТКМ). Нехай узагальнена модель загроз інформаційному об'єкту ЛОМ має вигляд, наданий на рис. 1. Нехай також об'єктом захисту є інформаційні ресурси ЛОМ, а засоби технічного захисту ресурсів певної ЛОМ складаються із засобів організаційного обмеження доступу, охоронної сигналізації, адміністрування доступу – внутрішньомережних засобів управління доступом до ресурсів ЛОМ, зовнішньомережних засобів управління доступом до ресурсів даної ЛОМ (із ТКМ), засобів захисту від витоків інформації технічними каналами, засобів захисту від спеціальних впливів на інформацію технічними каналами та засобів антивірусного захисту і забезпечують реалізацію певного набору функцій з обслуговування множини запитів.

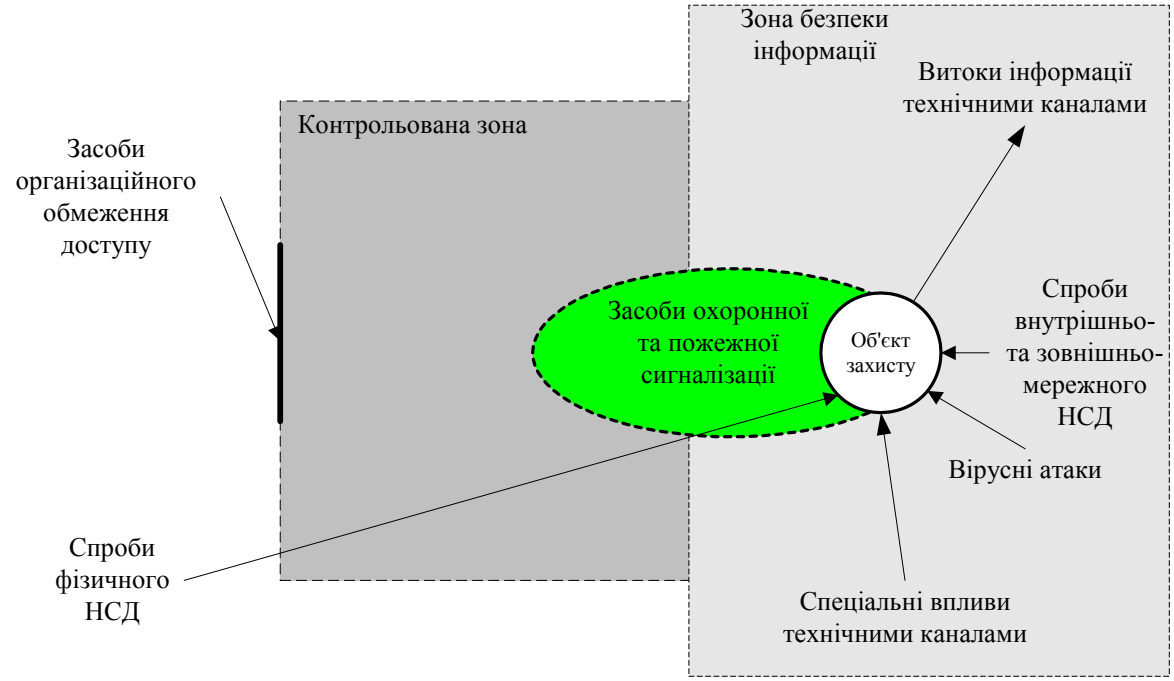

Рисунок 1 – Узагальнена модель загроз інформаційному об’єкту ЛОМ

Модель взаємодії засобів реалізації атак з засобами протидії загрозам – засобами забезпечення конфіденційності інформації, представлена на рис. 2. На цьому рисунку ЗК – загрози конфіденційності.

Як виплиає з моделі, несанкціоноване отримання користувачем інформації тим чи іншим чином є можливим при умові подолання неавторизованим користувачем засобів захисту у складі:

1. Організаційного обмеження доступу (контроль доступу та управління доступом до приміщень організаційними засобами, наприклад, реалізацією перепускного режиму до будівель чи окремих приміщень та таке інше). Такі дії слід очікувати, скоріше за все, від "терплячих зловмисників" – авторизованих користувачів, які мають атрибути легального доступу до певних приміщень ОС (наприклад, перепустки чи їх еквіваленти), або від "рішучих зловмисників", які вимушено використовують підроблені атрибути легального доступу до приміщень ОС;
2. Охоронної сигналізації (тобто шляхом "обходу" засобів організаційного обмеження доступом. Такі дії слід очікувати, скоріше за все, від "рішучих зловмисників", які мають на меті будь-що порушити ту чи іншу властивість захищеної інформації;
3. Управління доступу, включаючи засоби управління фізичним доступом (дозвіл чи блокування доступу до приміщень, терміналів, системних блоків, клавіатури та інших фізичних засобів) та адміністрування доступу (адміністрування суб’єктів, об’єктів, побудови і реалізації моделі захищеної системи, розмежування доступу тощо). Такі дії слід очікувати, скоріше за все, від "терплячих зловмисників", які порушують політику безпеки даної послуги навмисно, але без рішучих дій, маскуючись, шляхом підбору атрибутів доступу інших користувачів з метою прихованого подолання засобів управління (адміністрування) доступом до інформації, або від "випадкових порушників" – авторизованих користувачів, які порушують конфіденційність не навмисно, а помилково – шляхом випадкового подолання засобів управління (адміністрування) доступом до об’єкту захисту, виконання непередбачених дій відносно цього інформаційного об’єкту та т. п.;
4. Засобів канального захисту в ТКМ (засобів захисту від несанкціонованого доступу з телекомунікаційної мережі до ресурсів даної ЛОМ);
5. Засобів захисту від вірусних атак (засобів антивірусного захисту).

При цьому ймовірність подолання засобів управління доступом q_1 можна визначити з виразу

$$q_1 = q_{уд} \cdot [1-(1-q_{оод}) \cdot (1-q_{ос})],$$

де: $q_{уд}$ – ймовірність подолання засобів управління доступом; $q_{оод}$ – ймовірність подолання засобів організаційного обмеження доступу; $q_{ос}$ – ймовірність подолання засобів охоронної сигналізації.

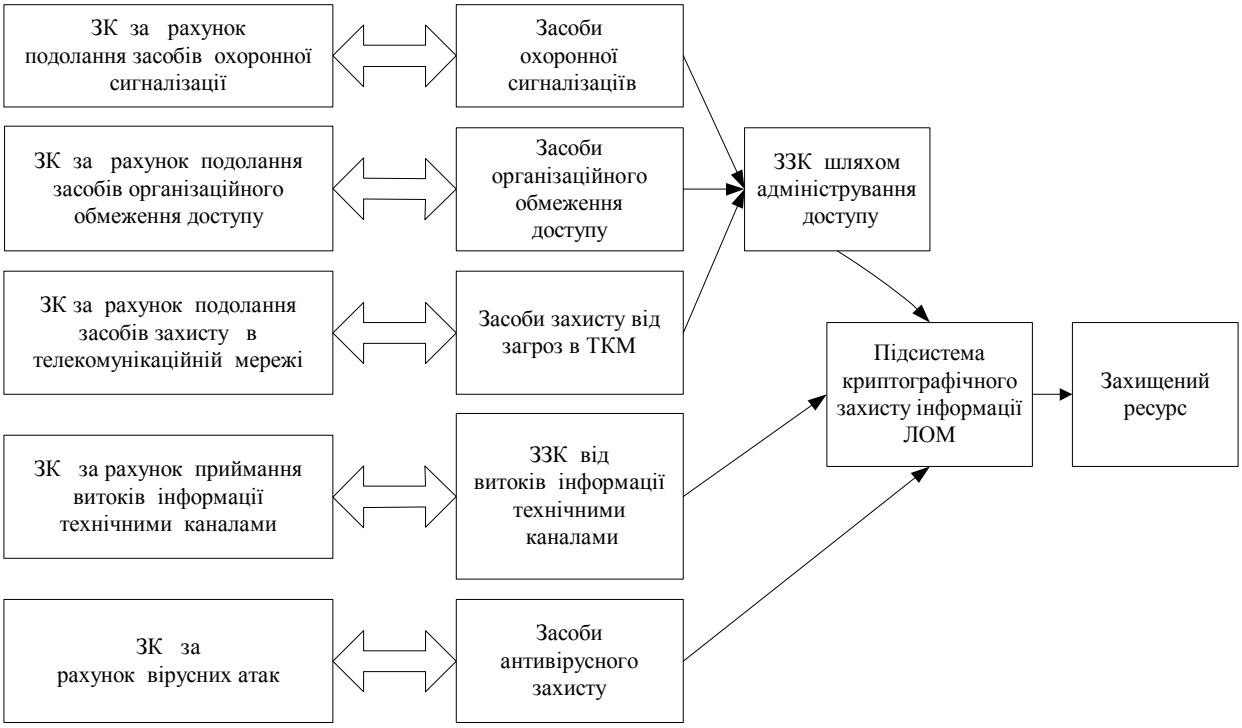

Рисунок 2 – Модель взаємодії засобів реалізації атак з засобами протидії загрозам – засобами забезпечення конфіденційності інформації

***Примітка* 1.** Тут і надалі при відсутності того чи іншого виду захисту ймовірність його подолання вважається такою, що дорівнює одиниці.

В свою чергу, ймовірність $q_{уд}$ подолання засобів управління доступом є також ймовірністю складної події, яка полягає в подоланні порушником як засобів управління фізичним доступом, так і засобів адміністрування доступом з використанням механізмів базового та прикладного програмного забезпечення. Якщо позначити ці ймовірності через $q_{уфд}$ і $q_{ад}$ відповідно, то

$$q_{уд} = q_{уфд} \cdot q_{ад}.$$

Тоді, зрозуміло,

$$q_1 = q_{уфд} \cdot q_{ад} \cdot [1-(1-q_{оод}) \cdot (1-q_{ос})].$$

Окрім того, несанкціоноване отримання користувачем інформації є можливим і через засоби віддаленого доступу до інформаційних об’єктів, використовуючи витоки інформації технічними каналами, засоби телекомунікаційної мережі та вірусні атаки при умові подолання неавторизованим користувачем відповідних засобів захисту. Нехай ймовірність подолання засобів захисту від витоків інформації технічними каналами дорівнює $q_{зві}$, ймовірність подолання засобів антивірусного захисту – $q_{ав1}$, а ймовірність подолання засобів захисту конфіденційності інформацій в телекомутаційних мережах – $q_{кткм}$.

Після отримання ІзОД тим чи іншим шляхом порушнику необхідно здійснити розкриття її змісту. Подія, яка полягає в тому, що порушник може розкрити зміст ІзОД (при умові подолання системи захисту даного інформаційного об’єкту) є також складною і складається з трьох подій: першої – порушник знає мову, якою інформація представляється; другої – порушник знає і може застосувати програмні засоби або апаратуру для криптографічного перетворення (для дешифрування закритої інформації); третьої – має необхідні ключі (ключові набори) для такого перетворення. Ймовірності цих подій $P_{зм}$, $P_{зкп}$, $P_{кн}$ відповідно.

При цьому $P_{кзі}$ – ймовірність подолання неавторизованим користувачем засобів криптозахисту (можливість розкрити зміст ІзОД) інформації можна визначити з виразу

$$q_{кзі} = P_{зм} \cdot P_{зкп} \cdot P_{кн}.$$

Тоді вираз для розрахунку ймовірності $q_{пк}$ порушення конфіденційності інформації з подоланням розглянутих засобів захисту можна записати у вигляді

$$q_{пк} = q_{кзі} \cdot [1-(1-q_1) \cdot (1-q_{зві}) \cdot (1-q_{ав1}) \cdot (1-q_{кткм})].$$

На рис. 3 представлена модель взаємодії атак з засобами протидії атакам - засобами забезпечення

цілісності (на цьому рис. ЗЦ - загрози цілісності).

При цьому, як і для моделі взаємодії засобів реалізації загроз конфіденційності інформації та засобів протидії цим загрозам, подолання неавторизованим користувачем системи захисту з імовірністю $q_{пц}$ можливе, якщо:

1. Подолано засоби охоронної сигналізації або засоби організаційного обмеження доступу та (і) засоби управління доступом, включаючи засоби управління фізичним доступом (дозвіл чи блокування доступу до приміщень, терміналів, системних блоків, клавіатури та інших фізичних засобів) та адміністрування доступу (адміністрування суб'єктів, об'єктів, побудови і реалізації моделі захищеної системи, розмежування доступу тощо). Ймовірність такої події q_1 уже визначена раніше.
2. З імовірністю $q_{цткм}$ подолано засоби захисту цілісності від загроз в ТКМ;
3. З імовірністю $q_{св}$ подолано засоби захисту від спеціальних впливів на інформацію по технічним каналам;
4. З імовірністю $q_{ав}2$ подолано засоби антивірусного захисту;
5. З імовірністю $q_{кц}$ подолано засоби контролю та поновлення цілісності інформації.

Тоді, з використанням застосованих вище підходів ймовірність порушення цілісності $q_{пц}$ можна знайти з виразу

$$q_{пц} = q_{кц} \cdot [1-(1-q_1)\cdot(1-q_{св})\cdot(1-q_{цткм})\,(1-q_{ав2})].$$

Розглянута в методиці модель дозволяє зробити, по-перше, висновок про те, що для забезпечення цілісності за рахунок унеможливлення доступу до інформації та модифікації неавторизованим користувачем змісту інформаційного об'єкту необхідно застосовувати засоби (апаратурні чи програмні) адміністрування доступу, контролю цілісності, управління фізичним доступом, охоронної сигналізації та організаційного обмеження доступом.

По-друге, з останнього виплиає необхідність, на відміну від моделі взаємодії засобів реалізації загроз та засобів забезпечення конфіденційності, застосування для забезпечення цілісності інформаційних об'єктів засобів з відповідними механізмами контролю цілісності та замість засобів захисту від витоків – засобів захисту від спеціального впливу. Окрім того, для унеможливлення порушення цілісності за рахунок отримання неавторизованим користувачем доступу до інформації з обмеженим доступом слід застосовувати такі ж засоби управління доступом (апаратурні чи програмні), як і для забезпечення конфіденційності.

Примітка 2. Звернемо увагу на те, що із наведеного вище визначення цілісності, як функціональної властивості захищеності інформації, не витікає ніяких часових обмежень щодо тривалості процесу поновлення цілісності в разі виявлення засобами контролю наявності її порушення. Це дає змогу для забезпеченні цілісності використовувати і ручні методи, наприклад, поновлення з застосуванням резервних копій інформаційних об'єктів чи шляхом забезпечення відкату процесів у разі виявлення порушення цілісності.

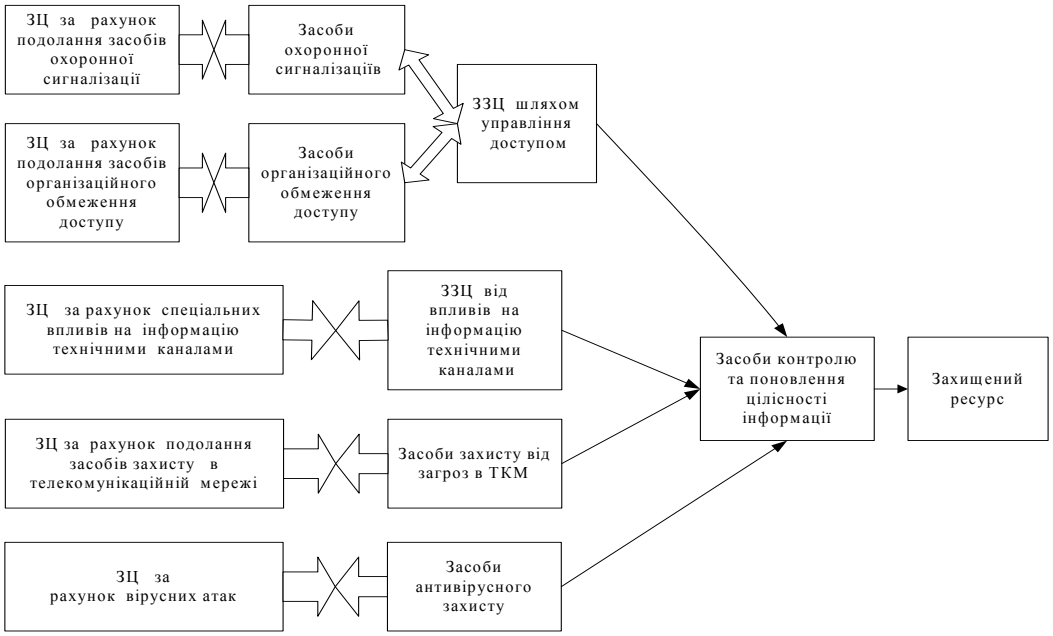

Рисунок 3 – Модель взаємодії засобів реалізації атак з засобами протидії загрозам – засобами забезпечення цілісності інформації

Виходячи із визначення функціональної властивості доступності інформації подію, пов'язану з її порушенням, слід розглядати як наслідок впливу на інформаційний об'єкт загроз, найбільш суттєвими з яких є:

1. Несанкціонована модифікація інформаційного ресурсу (порушення цілісності – вигляду ресурсу, необхідного користувачеві), включаючи зміни режимів його функціонування, місця зберігання, необхідного чи заданого користувачем, що потребує поновлення цілісності ресурсу шляхом, наприклад, використання його резервної копії. Така подія передбачає можливість фізичного доступу до джерел чи носіїв інформаційних ресурсів, наявність реалізованої спроби несанкціонованого доступу до інформаційного ресурсу, в тому числі каналами ТКМ та каналами спеціального впливу (порушник зумів здійснити маскування під авторизованого користувача чи модифікація не виявлена засобами контролю цілісності);

2. Перевід ресурсу в режим штучної відмови шляхом:

несанкціонованого використання інформаційного ресурсу в той час, коли ресурс є необхідним користувачеві, та протягом часу довше заданого (малого) проміжку – шляхом захоплення ресурсів (неконтрольованого використання, утримання, занадто тривалого використання) і створенню таким чином перешкод іншим користувачам в використання цих ресурсів;

постійного використання ресурсу, наприклад, шляхом генерації потоку заважаючих запитів (несправжніх запитів на обслуговування, несправжніх пакетів вхідної інформації, спроб підбору паролів та т. п. – завад процесу обслуговування справжніх запитів) з такою інтенсивністю, коли їх період (середня тривалість проміжку часу між двома сусідніми запитами) не перевищує тривалості обслуговування кожного з таких запитів, тобто такого потоку, коли захищений ресурс призначається для обслуговування лише заважаючих запитів;

постійного порушення цілісності з періодичністю меншою, ніж час відновлення інформаційного ресурсу. Така подія передбачає наявність порушень цілісності за рахунок впливу природних факторів (збої, відмови), а також наявність реалізованих спроб несанкціонованого доступу до інформаційного ресурсу каналами спеціального впливу (без спроб маскування).

Ймовірність першої з цих подій визначено вище (з використанням моделі, представленої на рис. 3) і вона дорівнює $q_{пц}$.

Для оцінки ймовірності порушення доступності шляхом переводу ресурсу в режим штучної відмови необхідно визначити інтенсивність потоку впливів на ресурс, що захищається. В [4] показано, що на інформаційні ресурси ОС можуть впливати як спроби несанкціонованого доступу, при умові подолання систем управління доступом та фільтрації, так і безпосередньо природні впливи. Інтенсивність внутрішніх штучних впливів в3наслідок відсіву (фільтрації) внутрішніх впливів системою управління доступом на її виході буде дорівнювати $\lambda_{шв} \cdot q_1$, якщо стійкість (в розумінні імовірності не подолання) системи управління доступом $p_д = 1 - q_1$. Інтенсивність зовнішніх штучних впливів (від елементів розподіленої обчислювальної мережі через засоби телекомунікаційної мережі), які впливають на дану ЛОМ, знижується за рахунок їх фільтрації (засобами фільтрації типу міжмережних екранів (firewall, брандмауерів), сервісів – посередників (proxyservices) та т. п.). Якщо стійкість таких засобів (в розумінні імовірності не подолання) дорівнює $p_ф = 1 - q_ф$, то на виході системи фільтрації інтенсивність завад буде дорівнювати $\lambda_{шз} \cdot q_{фі}$, а інтенсивність $\lambda_р$ штучних впливів, які не відфільтровані системами управління доступом та фільтрації, складе:

$$\lambda_{рш} = \lambda_{шв} \cdot q_1 + \lambda_{шз} \cdot q_ф + \lambda.$$

З урахуванням інтенсивності справжніх запитів $\lambda_{сз}$ загальна інтенсивність $\lambda_з$ впливів дорівнює

$$\lambda_з = \lambda_{сз} + \lambda_{шв} \cdot q_1 + \lambda_{шз} \cdot q_ф + \lambda.$$

При середній тривалості обслуговування в ОС одного запиту (середньому значення часу використання ресурсу $t_{вр}$) і пуассонівському законі розподілу ймовірностей впливу ймовірність того, що під час звернення до ресурсу він уже використовується (ймовірність звернення до ресурсу на даному інтервалі $t_{вр}$ більше ніж однієї заявки – ймовірність порушення доступності шляхом переводу ресурсу в режим штучної відмови) дорівнює

$$q_{пз} = 1 - p_0 = 1 - \exp\{-t_{вр} \cdot \lambda_з\},$$

де p_0 – ймовірність відсутності впливів (ймовірність того, що на даному часовому інтервалі виникне рівно нуль впливів), а отже ймовірність порушення доступності ресурсу

$$q_{пд} = 1 - (1 - q_{пз}) \cdot (1 - q_{пц}).$$

Змінну $t_{вр}$ при цьому слід розглядати як середній час використання захищеного ресурсу в умовах обслуговування автоматизованою системою усіх можливих запитів (для інформаційних об'єктів це – контроль цілісності, при необхідності її поновлення, виконання програмного засобу, читання чи запис

інформації та все таке інше). Визначення величини $t_{вр}$ виходить за рамки даної роботи, хоча як перше, грубе, наближення можна використати значення $t_{вр} = (T_{ki} - \Delta T_{ki})/n_{io}$, де: n_{io} – кількість інформаційних об'єктів, що потребують використання на інтервалі часу $(T_{ki} - \Delta T_{ki})$, T_{ki}, ΔT_{ki} – періодичність та тривалість контролю відповідно [4]. При цьому, якщо середнє значення часу використання ресурсу перевищить середнє значення часового інтервалу між сусідніми запитами (інтенсивність запитів перевищує інтенсивність обслуговування), то кількість будь-яких запитів у черзі на використання ресурсу буде зростати до нескінченості, що є ознакою штучної відмови захищеного ресурсу. Тобто умову, коли $1/\lambda_з \leq t_{вр}$ слід розглядати як умову переходу захищеного ресурсу в режим штучної відмови.

III Залишковий ризик для оцінки загальної стійкості системи захисту інформації

Із розгляду представлених моделей взаємодії засобів реалізації атак з засобами забезпечення кожної з функціональних властивостей захищеності ОС можна зробити висновок про те, що для унеможливлення подолання неавторизованим користувачем системи захисту даного інформаційного об'єкту необхідно застосовувати:

- організаційні заходи (організація зовнішньої охорони, перепускного режиму – унеможливлення проникнення через перепускні пункти, унеможливлення крадіжок носіїв ІзОД, зберігання в таємниці ідентифікаторів та паролів користувачів та інше);
- первинні технічні заходи (блокування витоків інформації чи блокування спеціального впливу на неї технічними каналами, унеможливлення фізичного доступу до ресурсів ОС та доступу до носіїв інформації носіїв ІзОД, в тому числі через елементи будівельних конструкцій – наявність надійних стін, дверей, віконних ґрат, охоронної сигналізації та т. п.);
- основні технічні заходи (засоби адміністрування чи управління доступом, засоби контролю чи контролю та поновлення цілісності, засоби антивірусного захисту та засоби криптографічного захисту інформації в відокремлених терміналах та їх мережах, в тому числі в розподілених мережах тощо).

Це дозволяє побудувати загальну модель взаємодії атак та засобів захисту ресурсів ОС (рис. 4) і отримати узагальнені кількісні характеристики системи захисту.

При побудові загальної моделі системи захисту інформації враховано:

1) функціональну близькість, схожість, інколи навіть єдність, деяких із засобів захисту, тобто їх здатність виконувати однакові функції захисту, хоча, можливо, і в різних умовах у складі різних моделей забезпечення функціональних властивостей захищеної системи.

2) можливість об'єднати в деяких засобах певну множину близьких чи однотипних функцій, наприклад, в засобах управління доступом – функції адміністрування доступом, контролю та поновлення цілісності, фільтрації пакетів, блокування засобів генерації безперервних запитів та т. п.

3) здатність інших засобів захисту виконувати функції захисту від однотипних загроз різним функціональним властивостям захищених ресурсів.

Це надає змогу об'єднувати різні засоби протидії певним загрозам чи, навпаки, відокремлювати окремі з них у відповідні підсистеми, в наслідок чого у складі комплексної системи технічного захисту можна вичленити її підсистеми, які виконують свої функції в різних середовищах чи по відношенню до достатньо характерних лише для них загроз.

1. Підсистему контролю доступу і захисту інформації з функціями побудови моделі захищеної системи, побудови і реалізації правил розмежування доступу до ресурсів АС, управління фізичним доступом, контролю та поновлення цілісності, криптографічного захисту інформації, фільтрації пакетів, блокування спроб підбору паролів тощо.
2. Підсистему захисту інформації від витоків інформації технічними каналами та спеціального впливу на неї.

Звернемо увагу на те, що на рис. 4 не наведено засобів забезпечення спостереженості за подіями в захищеній системі, які є пов'язаними з усіма процесами використання інформації та її захисту. Це не означає приниження їх значення в процесі захисту ресурсів, а лише ілюструє те, що ці засоби не виконують функцій безпосереднього захисту ресурсів ОС. Але відсутність засобів забезпечення спостереженості чи їх подолання порушниками фактично означає наявність змоги доступу цих порушників до ресурсів ОС і, в цьому сенсі, засоби забезпечення спостереженості відіграють таку ж роль, як і засоби забезпечення інших властивостей захищеності ресурсів ОС.

Звернемо увагу також на те, що до складу моделі взаємодії атак та засобів захисту ресурсів ОС входять засоби захисту відповідних властивостей захищеності інформаційних ресурсів ОС *в телекомунікаційних мережах* ОС (і, зрозуміло, в засобах обміну інформацією локальних обчислювальних мереж, як елементів таких ОС). Це означає суттєву вразливість стану захищеності ОС як раз через мережі, канали обміну інформацією та через їх елементи. Наслідком цього є, принаймні, відокремлення цих засобів захисту в

підсистему захисту інформації в ТКМ.

Останнє дозволяє зробити висновок про *актуальність та* важливість досліджень та розробок щодо методів, способів, засобів та методик забезпечення властивостей захищеності інформації *в мережах, каналах обміну інформацією та їх елементах.*

Неважко показати, що величину **загального залишкового ризику** у вигляді ймовірності порушення (подолання, злому) комплексної системи захисту можна при цьому розрахувати з виразу

$$q = 1 - (1 - q_{пк}) \cdot (1 - q_{пц}) \cdot (1 - q_{пд}),$$

що добре узгоджується з близькими за змістом виразами з [6].

Таким чином, розглянутий підхід дозволяє отримати вирази для визначення показників захищеності інформації по кожній з функціональних послуг захисту від можливих загроз у вигляді залишкового ризику – ймовірності порушення захисту від загроз відповідного типу, та побудувати загальну модель системи захисту в частині забезпечення необхідних властивостей захищеності і, за умовою оптимізації параметрів та характеристик згідно з [5], може бути використаним при проектуванні ефективних систем технічного захисту інформації взагалі та їх складових зокрема.

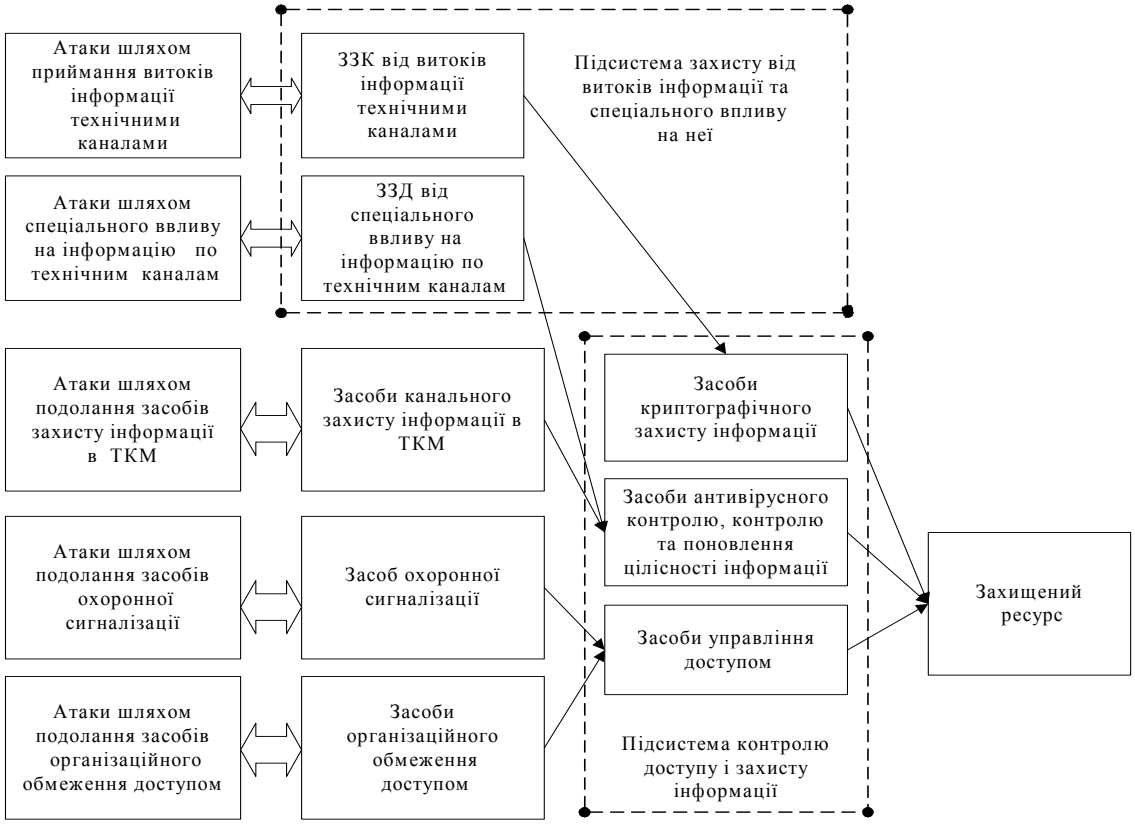

Рисунок 4 – Загальна модель взаємодії засобів реалізації атак з засобами системи захисту ресурсів ОС

*Література: **1.** Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 1.1 – 002 – 99); **2.** Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" (НД ТЗІ 2.5 – 004 – 99); **3.** Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (НД ТЗІ 2.5 – 005 – 99); **4.** Будько М. М., Василенко В. С., Короленко М. П. Варіант формалізації процесу захисту інформації в комп'ютерних системах та оптимізації його цільової функції // Реєстрація, зберігання і обробка даних. - 2000. - № 2, т. 2. с. 73 - 84. **5.** Будько М. М., Василенко В. С. Оцінка залишкового ризику при застосуванні засобів захисту інформації від НСД в корпоративних системах. К.: Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова, Матеріали науково – практичної конференції "Інформаційні технології в енергетиці", 2002, с. 29 – 39. **6.** Антонюк А. А., Волощук А. Г., Заславская Е. А., Суслов В. Ю. Об одном подходе в моделировании защиты информации. Перша міжнародна науково - практична конференція з програмування УкрПРОГ, 1998, с. 505 - 510.*