НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

На правах рукопису

Прус Руслана Богданівна

УДК 004.056.5:519.8(043.5)

МЕТОДИ ТА МОДЕЛІ ДИНАМІЧНОГО УПРАВЛІННЯ РЕСУРСАМИ ЗАХИСТУ ІНФОРМАЦІЇ

21.05.01 – інформаційна безпека держави

Дисертація на здобуття наукового ступеня
кандидата технічних наук

Науковий керівник:
Швець Валеріян Анатолійович
кандидат технічних наук, доцент

Київ – 2014

ЗМІСТ

ВСТУП

Актуальність теми. Розвиток інформаційної сфери та відповідне зростання її обсягів і вартості супроводжується впровадженням передових інформаційних технологій у всі сфери суспільного життя держави, що зумовлює збільшення частоти нападів і потенційних збитків від витоку інформації. Як результат – ускладнення систем захисту і збільшення їх вартості. В цих умовах задача ефективного розподілу обмежених фінансових ресурсів на захист інформації суб'єктів господарської діяльності стає дедалі більш важливою і в значній мірі визначає рівень інформаційної безпеки держави. Особливої актуальності набуває розробка питань оптимізації показників системи захисту інформації в умовах динамічного протистояння. Такими показниками можуть бути величина завданої шкоди від реалізації загроз інформації, яка визначає ефективність системи захисту, прибуток від внесення інвестицій в захист інформації, їх рентабельність тощо.

Вирішення поставленої задачі має цілу низку аспектів. По-перше, необхідно визначити загальну кількість ресурсів захисту, яка мінімізує сумарні втрати від можливого витоку інформації. По-друге, оптимальним чином розподілити ресурси між об'єктами, які містять різну частку інформації і відрізняються природною захищеністю, динамічною уразливістю, імовірністю нападу з виділенням певної кількості ресурсів. Третій аспект полягає у визначенні оптимального моменту внесення ресурсів захисту – після того, як будуть з'ясовані направленість і інтенсивність нападів та, відповідно, можливий рівень збитків. Невизначеність умов протистояння, характерна для конкурентної боротьби, приводить до того, що першим етапом в спробах здобуття інформації іноді стає розвідка, направлена на виявлення слабких місць в системі захисту. При цьому виникає питання оптимізації розподілу ресурсів між розвідкою і отриманням інформації. В умовах комплексного протистояння, коли кожна з сторін прагне захистити свою інформацію і здобути інформацію суперника, в коло показників, що підлягають оптимізації, включають

співвідношення між кількістю ресурсів, направлених на захист власної інформації і на отримання інформації суперника.

Завдання ускладнюється тим, що пошук оптимальних рішень ведеться в умовах невизначеності, коли дії суперника невідомі і можуть бути оцінені лише з певною імовірністю. Визначення параметрів і функціональних залежностей, що входять до математичної моделі, доводиться проводити на основі експертних оцінок, оскільки застосування статистичного методу ускладнене через недостатність статистичних даних про результати конкурентної боротьби.

Проблемам теоретичного та методологічного розвитку технологій побудови та застосування оптимальних систем захисту інформації присвячені роботи вітчизняних вчених В.А. Герасименка, В.К. Задіраки, О.Г. Корченка, О.К. Юдіна, О.Є. Архипова, Є.Г. Левченка, О.М. Новікова, Г.Ф. Конаховича, В.О. Хорошка, Б.Є. Журиленка та закордонних науковців Л. Гордона, М. Лоеба, К. Хуана, В. Лью, Р. Бьоме, Т. Мура, К.Мацури. Аналіз наукових робіт з моделювання оптимальних систем захисту інформації показав, що основні зусилля зосереджені на визначенні оптимального обсягу інвестицій у захист. Питанням розподілу цих інвестицій між об'єктами захисту присвячені одиничні роботи. Крім того, існуючі розробки не враховують вплив можливих дій зловмисника та їх наслідків на зміну показників та характеристик системи.

Тому виникла нагальна потреба в розробці моделей управління ресурсами захисту інформації та методу оптимізації показників систем захисту в умовах динамічного протистояння. Дисертаційна робота присвячена розв'язанню актуальної науково-технічної задачі – забезпеченню необхідного рівня захищеності інформаційних систем за рахунок оптимального розподілу ресурсів захисту інформації між елементами систем із врахуванням часової зміни умов протистояння. Розв'язок цієї задачі направлений на підвищення інформаційної безпеки підприємств та організацій, що є складовою інформаційної безпеки держави.

Зв'язок роботи з науковими програмами, планами, темами. Отримані результати дисертаційної роботи реалізовано в НДР №77/14.01.04 «Методи і

моделі управління ресурсами захисту інформації» (номер державної реєстрації 0113U006543) кафедри засобів захисту інформації Національного авіаційного університету.

Мета і завдання дослідженя. Метою дослідження є підвищення рівня захищеності інформаційних систем за рахунок оптимального розподілу ресурсів захисту інформації між об’єктами захисту із врахуванням дій зловмисника.

Для досягення поставленої мети в дисертації необхідно вирішити такі задачі:

1. Провести аналіз існуючих математичних моделей управління ресурсами захисту інформації, теоретико-ігрових методів оптимізації та обґрунтувати задачі дослідження.

2. Розробити математичну модель та інвестиційний метод для підвищення ефективності використання ресурсів захисту інформації в багаторубіжних системах за рахунок оптимального розподілу ресурсів між окремими елементами захисту.

3. Розробити метод пошуку оптимальних рішень в умовах динамічного протистояння з врахуванням зміни параметрів та характеристик процесу нападу і захисту.

4. Розробити модель реалізації процесів різнонаправленого протистояння, коли кожна з сторін захищає свою інформацію і одночасно прагне здобути інформацію суперника, на основі розрахунку станів інформаційної безпеки з врахуванням часової зміни умов протистояння.

5. Розробити методику аналізу та оцінки ефективності використання запропонованого інвестиційного методу.

6. На основі розробленої методики оцінки ефективності використання запропонованого інвестиційного методу створити програмний апарат комплексної реалізації процесу оптимізації розподілу ресурсів в складних інформаційних системах в динамічному режимі.

Об’єктом дослідження є процес динамічного управління ресурсами захисту інформації в багаторубіжних системах захисту з врахуванням уразливості об’єктів.

Предметом дослідження є методи та моделі управління ресурсами при побудові системи захисту інформації.

Методи дослідження. В роботі використані аналітичні і графічні методи, що застосовуються в оптимізаційних задачах дослідження операцій, зокрема, методи дробово-лінійного і дробово-нелінійного програмування, метод динамічного програмування Белмана – для знаходження оптимальних ресурсів; методи теорії дискретних та неперервних марковських ланцюгів – для визначення станів інформаційної безпеки.

Для математичного моделювання використано пакети прикладних програм – MathLab, MathCAD.

Наукова новизна одержаних результатів:

1. Вперше на базі запропонованої цільової функції розроблено математичну модель та сформовано інвестиційний метод, що за рахунок використання нових функціональних залежностей дає можливість виявити вплив внесених інвестицій на значення частки очікуваних втрат інформації та обгрунтувати рішення щодо оптимального розподілу ресурсів.

2. Вперше запропоновано метод удосконалення технології динамічного регулювання розподілу ресурсів захисту, який, базуючись на математичному апараті теорії ігор та розробленій моделі реалізації процесу пошуку оптимальних рішень, враховує на відміну від існуючих вплив зміни націленості атак зловмисника на значення параметрів та характеристик систем.

3. Вперше запропоновано модель реалізації процесів різнонаправленого протистояння, яка враховує часові зміни умов протистояння, і надає можливість створити інструментарій оцінки рівня інформаційної безпеки та визначити стан безпеки у конкретний момент часу.

Практичне значення отриманих результатів:

1. Запропоновано методику проведення імітаційного моделювання наслідків почергового прийняття рішень сторонами нападу і захисту у динамічному режимі, що дозволяє сформулювати рекомендації щодо оптимізації розподілу ресурсів та оцінити розмір очікуваних втрат інформації.

2. Сформульовано практичні рекомендації щодо використання розробленої моделі реалізації процесів різнонаправленого протистояння конкуруючих сторін для дослідження динаміки зміни стану інформаційної безпеки та завдяки розрахунку моменту часу, коли імовірність успішної атаки найвища, нейтралізувати загрозу.

3. Сформульовано рекомендації щодо проведення аналізу ефективності використання інвестиційного методу, що дозволяє оцінити гарантованість інформаційної безпеки.

4. Розроблено програмний комплекс, який дозволяє автоматизувати процес динамічного управління ресурсами.

Практичні результати досліджень, отримані у дисертації, впроваджено на ПрАТ «Волиньхолдінг» (акт впровадження від 22.07.14 р.), ТзОВ «ЖИТЛОБУД-2» (акт впровадження від 22.07.14 р.), ТзОВ «Західелектромонтаж» (акт впровадження від 21.07.14 р.), СП «ЗД Україна» (акт впровадження від 22.07.14р.) та в навчальному процесі Національного авіаційного університету (акт від 26.05.14 р.).

Особистий внесок здобувача. В опублікованих разом зі співавторами наукових працях за темою дисертації особисто здобувачем отримані аналітичні моделі та формули, зроблено моделювання, на підставі яких отримані нові наукові та прикладні результати. Особистий внесок здобувача полягає у наступному: [100,103,105,111,113,114] – на основі теоретико-ігрових методів сформовано математичний апарат для пошуку оптимального розподілу ресурсів між об’єктами захисту за відсутності інформації про дії нападу; [101,106,115,117] – розроблено математичну модель, яка дозволяє підвищити ефективність захисту інформації в багаторубіжних системах за рахунок

оптимального розподілу ресурсів захисту інформації; [102,116] – розроблено алгоритм для автоматизації процесу оптимізації розподілу ресурсів в складних інформаційних системах в динамічному режимі; [104] – розраховано показники системи захисту інформації залежно від схеми розташування засобів захисту, розроблено методику побудування оптимальних схем; [107] – проведено дослідження розробленої моделі із використанням методів безумовної і умовної оптимізації; [108] – проведено аналіз функцій динамічної уразливості та імовірності нападу і їх вплив на продуктивності витрат; [109] – розроблено методику розрахунку станів інформаційної безпеки в динамічному режимі з врахуванням зміни умов протистояння з часом та визначено оптимальний момент інвестування ресурсів; [110,112] – визначено умови існування сідлової точки цільової функції при протистоянні двох сторін в залежності від характеристик складних інформаційних структур.

Апробація результатів дисертації. Результати досліджень оприлюднені та обговорювались на 5 конференціях: Міжнародній науково-практичній конференції «Інтегровані інтелектуальні роботехнічні комплекси» (Київ, НАУ, 2008 р.); Науково-практичній конференції «Інформаційна безпека» (Київ, ДУІКТ), 2009 р.); Науково-практичній конференції «Захист інформації в інформаційно-комунікаційних системах» (Київ, НАУ, 2009 р.); IV всесвітньому конгресі «Авіація в XXI ст.» (Київ, НАУ, 2010 р.); II міжнародній науково-практичній конференції «Комплексне забезпечення якості технологічних процесів та систем» (Чернігів, ЧДТУ, 2012 р.).

Публікації. Основні наукові положення, висновки та результати дисертаційного дослідження знайшли відображення у 18-ти опублікованих працях, із них: статей у виданнях, що входять до переліку фахових видань України, – 11 (у тому числі 2 праці без співавторів, 5 статей у спеціалізованих наукових журналах, що входять до міжнародних наукометричних баз), тез доповідей на конференціях – 5 (3 праці без співавторства).

РОЗДІЛ 1
АНАЛІЗ ТА ПОСТАНОВКА ЗАДАЧ ДОСЛІДЖЕННЯ

1.1. Аналіз моделей інформаційної безпеки

Серед моделей інформаційної безпеки найбільш грунтовною і поширеною є модель Гордона-Лоеба (ГЛ) [89]. Метою цієї моделі є рішення першої з поставлених задач – визначення оптимальної кількості інвестицій в захист інформації. Ключовий момент в моделі ГЛ – введення і розробка функції уразливості, котра визначає рівень інформаційної безпеки. Інформаційний об'єкт може мати різні форми – список користувачів, бухгалтерська книга рахунків, стратегічний план розвитку, вебсайт тощо. Підвищення безпеки може відбуватися в напрямку захисту конфіденційності, цілісності, аутентичності, безвідмовності, доступності до авторизації користувачів і т.ін.

Модель за своєю структурою є статичною – рішення і результат настають одночасно, а динамічні ефекти, в тому числі залежність грошей від часу, не враховується.

Для характеристики інформаційного об'єкта введено такі параметри:

λ – потенційні збитки від витоку інформації;

t – імовірність нападу, $t \in [0,1]$;

v – уразливість інформації, під котрою розуміють імовірність того, що при відсутності інвестицій атака буде успішною, що завдасть збитки λ; $0 \le v \le 1$;

z – витрати на захист інформації.

В моделі прийнято, що $\lambda = const$, хоча на практиці зазвичай $\lambda = \lambda(t)$. Величина t відноситься до одиночного нападу (одночасне настання кількох нападів не розглядається).

До розгляду прийнято також величини:

vt – імовірність збитків в результаті атаки;

$L = t\lambda$ – потенційні збитки при відсутності інвестицій;

$S(z,v)$ – імовірність порушення безпеки.

Враховуючи природу уразливості інформації та інформаційної безпеки, можна зробити такі припущення відносно функції $S(z,v)$:

$S(z,0)=0$ для всіх z ($v=0$ – інформація абсолютно неуразлива);

$S(0,v)=v$ для всіх v;

$S_z'(z,v)<0$ і $S_z''(z,v)>0$ для всіх v і всіх z: при збільшенні інвестицій інформаційна безпека зростає, але зі спадаючим темпом, $\lim\limits_{z\to\infty} S(z,v)=0$.

При виборі критерія оптимальності вважається, що керівництво фірми нейтральне до ризику, а в якості показників ефективності внесення інвестицій розглядаються величини:

$EBIS(z)=[v-S(z,v)]L$ – зменшення топенційних втрат завдяки додатковим витратам на безпеку [expected benefits of an investment in information security];

$ENBIS(z)=[v-S(z,v)]L-z$ – очікуваний чистий прибуток від інвестування у безпеку.

Оптимальним вважається значення z^*, за якого $ENBIS(z)$ досягає максимального значення.

Ключовим питанням в застосуванні моделі ГЛ є визначення форми залежності $S(z,v)$. В [89] запропоновано два широких класи функцій, які можна використовувати в якості функцій уразливості. Перший клас формують показникові функції

$$S^I(z,v)=\frac{v}{(\alpha z+1)^\beta}, \qquad (1.1)$$

де параметри $\alpha>0$, $\beta\geq 1$ характеризують економічну доцільність інвестицій (при заданих v і z імовірність порушення безпеки зі зростанням α і β зменшується). З умови $ENBIS_z'(z^*)=0$ знаходиться вираз для оптимального розміру інвестицій:

$$z^*(v) = \frac{(v\alpha\beta L)^{1/(\beta+1)}}{\alpha}. \qquad (1.2)$$

З (1.2) випливає, що $z^*(v) = 0$ при $0 \le v \le \frac{1}{\alpha\beta L}$. Таким чином, оптимальні інвестиції для першого класу при низькій уразливості залишаються рівними нулю до того моменту, коли v не зросте до значення $v = \frac{1}{\alpha\beta L}$. При подальшому збільшенні v величина z^*, відповідно до (1.1), зростає зі спадаючою швидкістю. Отже, якщо уразливість описується функцією (1.1), то інвестування в захист недоцільне при малих значеннях v: витрати на захист при низькій уразливості не дадуть бажаного ефекту. При високій уразливості інвестування доцільне, проте потребує великих витрат. Цей висновок не завжди справедливий для функцій II класу.

Другий клас формують функції

$$S^{II}(z, v) = v^{\alpha z + 1}, \qquad (1.3)$$

де параметр $\alpha > 0$ – економічна доцільність витрат на безпеку.

З умови $ENBIS_z'(z^*) = 0$ отримано

$$z^{II*}(v) = \frac{\ln\left(1/(-\alpha v L(\ln v))\right)}{\alpha \ln v}.$$

З цього виразу випливає, що для II класу функцій $S(z, v)$ оптимальний розмір ресурсів захисту при малих значеннях уразливості v дорівнює нулю (так, як і для функцій $S^I(z, v)$), при збільшенні v зростає, при певному значенні v досягає максимума, а потім стрімко зменшується і дорівнює нулю при $v \to 1$.

Оптимальне значення ресурсів залежить не тільки від уразливості системи, але й від вартості інформації, котра підлягає захисту. Аналіз ГЛ показує, що величина z^* обмежена зверху: $z^* < \frac{1}{e} vL$, тобто оптимальний об'єм інвестицій в захист не перевищує 36,8% від можливих втрат за відсутності інвестицій. Реальні значення z^* значно менші. В [89] наведено числовий приклад: при $\beta = 1$, $\alpha = 10^{-5}$, $v = 1$, $L = 400000$ USD маємо $z^*_{\max} = 0{,}25$.

Враховуючи, що інвестиції в захист неефективні при досить малих і досить великих значеннях уразливості, автори [89] вважають першим завданням менеджменту поділ об'єктів на низький, середній і високий рівень уразливості.

Автори моделі ГЛ [88,89] відзначили її недоліки:

1. Не існує простої процедури визначення імовірності нападу і уразливості.
2. Проблематичне визначення потенційних втрат від порушення безпеки.
3. Складність реалізації результатів дослідження на конкретному об'єкті.
4. Не враховано, як зловмисник буде міняти свою стратегію при внесенні додаткових інвестицій для захисту, тобто відсутній аналіз протистояння в динамічному режимі.

Не дивлячись на те, що модель ГЛ знайшла широке визнання і одержала свій розвиток в багатьох роботах на протязі десяти років з часу її опублікування, більша частина поставлених питань до сьогоднішнього дня не вирішена. Беззаперечною заслугою авторів моделі є те, що вони вперше ґрунтовно розглянули проблему і визначили функцію уразливості, що є ключовим при розгляді протистояння в інформаційній сфері. Визначення форми функції, яка виражає уразливість динамічної системи, є ключовим завданням при математичному моделюванні інформаційного протистояння.

В роботі **В.К. Задіраки та співавторів** [37] цільова функція $S(i, y)$ визначає суму втрат $i(y)$ від витоку інформації та витрат на її захист: $S(i, y) = i(y) + y$.

Функція $i(y)$ - спадаюча, тобто $i'(y) < 0$. Припускається, що $i'(y) = -cy^n$, де c і n - параметри. Мінімум цільової функції $S(i, y)$ досягається за умови $S_y'(i, y^0) = 0$, яка приводить до квадратного рівняння відносно шуканої величини y^0. Розв'язок цього рівняння дає змогу одержати таблицю значень y^0 для різних величин c і n. Умова $i'(y) = -cy^n$ виконується при дробово-лінійній формі функції $i(y)$:

$$i(y) = \frac{1}{1 + cy^n}$$

Ця функція використовується в роботі, що дає змогу порівняти одержані результати з [37].

Якщо звернутись до історії питання, то протистояння двох сторін вперше ґрунтовно розглянуто спеціалістами фірми RAND Corporation наприкінці другої світової війни при розробці математичних основ військового планування. Основною відмінністю в постановці цих задач від нашої є те, що елементи військової системи (винищувачі, бомбардувальники, зенітні комплекси) являють собою активні об'єкти, призначені для нападу на об'єкти суперника. Кількість індивідуальних протистоянь становить значну величину $2m_1 \cdot m_2$, де $m_1 \cdot m_2$ – кількість об'єктів суперників. Це є однією з причин того, що на першому етапі розглядались, в основному, однорідні системи, в котрих об'єкти кожної з сторін однакові – це суттєво спрощує обчислювальну процедуру. Моделлю протистояння двох сторін, розробленою в рамках фірми RAND, є **модель Гроса** [61,65,73], призначена для імітації тактичних військових операцій. Відповідно до цієї моделі, конфліктуючі сторони володіють ресурсами X та Y, а результат їхнього протистояння визначається цільовою

функцією, яка лінійно залежить від різниці вкладених ресурсів і приводить до задачі лінійного програмування:

$$i(x,y)=\sum_{k=1}^{l} i_k(x_k y_k)=\sum_{k=1}^{l} g_k \max(x_k - y_k,0),$$

де k – номер об'єкта, x_k і y_k – ресурси нападу і захисту на k-му об'єкті, g_k – ваговий коефіцієнт, котрий виражає важливість об'єктів або їх уразливість.

Величина $\max(x_k - y_k,0)$, значенням якої є більше з двох чисел $x_k - y_k$ та 0, являє собою ту частину підрозділу x_k, котра здатна проникнути через оборону до об'єкта. Таким чином, величина $g_k \max(x_k - y_k,0)$ кількісно характеризує успіх нападу на k-й об'єкт. В застосуванні до задач інформаційної безпеки g_k виражає відносну цінність інформації на k-му об'єкті, а $g_k \max(x_k - y_k,0)$ – завдану шкоду від витоку інформації. Оскільки завдана шкода не може бути більшою за її вартість, то слід покласти $i(x,y)=1$ при $x-y\geq 1$. Отже, функція $i(x,y)$ має кусочно-лінійний характер. Весь інтервал зміни x при сталому y можна поділити на три зони, обмежені двома граничними значеннями x_1 і x_2: при $x<x_1$ маємо $i(x,y)=0$, при $x>x_2$ – $i(x,y)=1$, при $x_1<x<x_2$ – функція $i(x,y)$ зростає лінійно з кутовим коефіцієнтом g. З врахуванням приведених міркувань цільова функція, яка виражає завдану шкоду від витоку інформації, приймає вигляд [51,102]:

$$i(x,y)=\sum_{k=1}^{l} g_k(x_k - y_k),$$

де

$$x_k - y_k=\begin{cases} 0 & при \quad x_k - y_k \leq 0 \\ x_k - y_k & при \quad 0<x_k - y_k \leq 1 \\ 1 & при \quad x_k - y_k>1. \end{cases}$$

Задача Гроса, яка виникла при плануванні військових операцій, має низку відмінностей від розглянутих задач. По-перше, цільова функція має дискретний характер, оскільки визначає кількість одиниць, які прорвались через оборону або які знищили напад чи оборона. По-друге, ці одиниці в кожному епізоді протиборства однакові для нападу і, відповідно, для оборони. Однотипність об'єктів суттєво спрощує рішення задачі, проте обмежує умови протиборства. Однак, основний недолік моделі Гроса – кусочно-лінійний характер її цільової функції, котрий, звичайно, не може відповідати реальним умовам. З цієї причини модель Гроса, враховуючи її простоту, використано лише для апроксимації цільової функції і одержання результатів у першому наближенні [54,102,108].

Ще однією математичною моделлю, яка дає можливість розрахувати рівень збитків внаслідок реалізації загроз, що залежить від обсягу витрат на захист інформації є модель **Б.Є. Журиленко.**

Метою досліджень Б.Є. Журиленко є оцінка стійкості комплексу технічного захисту інформації (ТЗІ) в часі з використанням відомих розподілів ймовірностей [34, 35].

Імовірнісна надійність комплексу технічного захисту інформації виначається за виразом:

$$P_i(X_i) = \left(\frac{X_i^{X_i}}{(1+X_i)^{1+X_{i_i}}} \right)^{\beta_s},$$

де $X_i = {x_i}/{H_i}$ - фінансові інвестиції у захист;

x_i - фінансові затрати на створення даного ТЗІ;

H_i - початкові фінансові втрати за відсутності захисту;

β_i - ефективність захисту залежно від фінансування.

Для визначення ефективності технічного захисту інформації необхідні експериментальні, сертифіковані або статистичні дані імовірності зламу даної системи захисту і час, коли настала така імовірність.

Імовірність зламу в часі визначається за формулою:

$$P_i(t) = \left(\left(\frac{t_{0i}}{t_{0i} + t} \right)^{\frac{t_{0i}}{t}} \left(\frac{t}{t_{0i} + t} \right)^{\gamma_s} \right),$$

де t_{0i} - часовий параметр, властивий даній системі захисту, і який може бути визначений лише внаслідок реальних результатів порушення безпеки;

t - поточна координата часу;

γ_i - визначає ефективність захисту в часі.

За відсутності фінансових інвестицій у захист або його модернізацію імовірність надійності захищеності рівна нулю незалежно від часу. Дана модель дає змогу встановити залежність імовірності захищеності від максимально ефективного фінансування.

Основні труднощі при побудові моделі пов’язані із збором статистичних даних про результати зламу (і необхідність факту самого зламу захисту), оскільки така система захисту після цього не може використовуватись в подальшому. У зв’язку з цим автором розроблено метод для визначення імовірнісної надійності ТЗІ на основі реальних спробах зламу, який дозволяє оцінити імовірнісну надійність одиничних систем захисту і при її встановленні на кількох об’єктах (наприклад, встановлення антивірусної програми на кількох комп’ютерах дозволяє передбачити не лише спробу, але й час, при якому імовірний злам на інших комп’ютерах) [36]. Недоліком цього методу є необхідність знання ефективності ТЗІ, яка у даному випадку отримується в результаті аналізу наслідків реального зламу системи.

В результаті проведених досліджень показано, що t_0 - параметр, що визначає властивості ТЗІ, може бути не лише сталою величиною, а й функцією,

що залежить від спроб зламу і від часу, коли такі спроби мають місце. На основі досліджень отримано функції, що дають можливість розрахувати частоту спроб зламу.

Модель Глушака-Новікова [21] направлена на оптимальне розміщення механізмів захисту між компонентами (об'єктами) системи, що забезпечить максимальний рівень захищеності.

Пошук оптимального набору механізмів захисту, який забезпечує мінімум ризику втрат інформації, проводиться на прикладі системи районних відділень банку. Обсяг інформації в кожному відділенні пропорційний потенційній кількості клієнтів, тобто чисельності жителів району. Імовірність реалізації окремих загроз, а також вартість і ефективність кожного з механізмів захисту визначається методом експертної оцінки. При цьому припускається, що імовірність реалізації загрози проти кожного об'єкта однакова і залежить тільки від виду загрози. Розглядаючи різні комбінації елементів захисту для кожного з відділень, розраховується сумарний збиток для всієї системи (який і характеризує ступінь ризику) і оптимальний набір елементів захисту для кожного відділення за умови введення обмеження на загальну вартість системи захисту. При розрахунку повного ризику залишається відкритим питання про величину перехресних членів, котрі виражають розмір завданої шкоди від реалізації різних видів загроз (ці події вважаються сумісними).

Питанням застосування **економіко-вартісних моделей «атака-захист»** для оцінювання ризиків та дослідження ефективності інвестицій в інформаційну безпеку присвячені роботи **О.Є. Архипова** [4, 5].

Для визначення імовірнісних параметрів ризику в цих моделях використовуються певні характеристики мотиваційно-вартісних та економіко-фінансових відносин, характерних для ситуації «атака-захист» в інформаційній сфері. Зокрема, розглянуто ситуацію, що виникає при реалізації атакуючою стороною A (зловмисник) загрози T відносно деякого інформаційного ресурсу I, який належить стороні B. Для опису ситуації введено наступні позначення:

D – загальна вартість витрат зловмисника A на реалізацію загрози T;

g – отриманий «виграш» зловмисника, величина якого обумовлюється цінністю ресурсу I для зловмисника;

q – збитки, яких зазнала в цій ситуації сторона B, тобто вартість критичної інформації з точки зору її власника;

c – загальна вартість реалізованого в інформаційній системі комплексу захисних заходів.

Чистий прибуток зловмисника в разі успішної реалізації загрози T визначається за формулою:

$$Q = g - D.$$

Виходячи з мотиваційних характеристик зловмисника, який діє виключно за принципом економічної доцільності, можливі такі варіанти:

1) якщо $g>>D$, вважається, що ймовірність P_t виникнення загрози T буде практично дорівнювати 1, тобто зловмисник спробує використати будь-які шанси для реалізації цієї загрози;

2) для малих значень g економічні мотиви виникнення загрози T практично відсутні: при $Q=0$ (або $g=D$) атака ресурсу I стає недоцільною, в цьому випадку $P_t=0$;

3) для $g<D$ спроба реалізації загрози T втрачає будь-який економічний сенс.

Виходячи з цих міркувань, для оцінювання значень імовірності виникнення загрози T запропоновано співвідношення:

$$P_t = \frac{Q}{g} = 1 - \frac{D}{g}.$$

Для оцінки імовірності P_t виникнення загрози T враховуючи рівень індивідуальних мотиваційних характеристик зловмисника використано формулу:

$$P_t = \frac{\gamma g - D}{\gamma g} = 1 - \frac{D}{\gamma g},$$

де коефіцієнт мотивації γ відображає ступінь впливу величини «виграшу» g на дії зловмисника. Для впевненого в собі зловмисника $\gamma > 1$, і $\gamma < 1$ – для обережного.

Імовірність P_v успішного проведення комплексу атак, породжених існуванням сукупності уразливостей інформаційної системи (включно із уразливостями самої системи захисту інформації), залежить від ступеню захищеності інформаційної системи, який в свою чергу зумовлюється обсягом інвестувань в систему захисту інформації (величиною c), і визначається співвідношенням:

$$P_v = \frac{q}{q + sc},$$

де s – коефіцієнт, діапазон значень якого пов'язаний із залежністю між рівнем інвестицій c та цінністю критичної інформації (наприклад, для комерційної таємниці прийнято $c = (0{,}05 \div 0{,}20)q$, $s \geq 10 \div 45$).

Наведені вище формули автор пропонує застосовувати безпосередньо для обчислення ризиків будь-якої конкретної організації за умов, що існує реальна змога проаналізувати та кількісно оцінити економіко-вартісні характеристики реалізації загрози інформації. Вихідні данні для цих оцінок можна отримати, виконавши обстеження (аудит) стану інформаційної безпеки організації відповідно з настановами та рекомендаціями стандартів менеджменту ризиків за наявності певної додаткової інформації, статичні у часі

оцінки можна розвинути у динамічні, що змінюють свої значення у часі відповідно до прийнятих економіко-вартісних сценаріїв розвитку атак [5].

Економіко-вартісні моделі «атака – захист» також дають можливість на основі конкретної інформації про реальну організацію перевірити, чи достатні за обсягом кошти, інвестовані у інформаційну безпеку цієї організації.

Дослідженню кібератак на інформаційні системи присвячені роботи **Хорошка В.О. та Хохлачової Ю.Є**. Оцінка можливостей зловмисника при кібератаках проводиться із використанням ігрових методів аналізу кібератак [25].

Авторами розглянуто безкоаліційну кібератаку A n гравців кібернападу на інформаційну сферу:

$$A = \langle N, \{x_i\}_{i \in N}, \{f_i(x)_{i \in N}\} \rangle,$$

де n – кількість гравців кібернападу, яка визначена на множині N, $n \in N$, $N = \{1,2,...,n\}$;

i – номер гравця кібернападу, $i \in N$;

x_i – стратегія i-го гравця кібернападу, $x_i \in X_i$;

$f_i(x)$ – плата i-го гравця кібернападу в кібератаці A при виборі n гравцями власних стратегій x кібернападу. У кібератаці A кожен i-й гравець кібернападу використовує довільну стратегію кібернападу. Тоді в результаті реалізації кібератаки A формується ситуація $x = \{x_i, x_2, ..., x_n\} \in X = \prod_{i \in N} X_i$.

Плата за успішну кібератаку i-го гравця кібернападу має вигляд квадратичної функції

$$f_i(x) = xM^{(i)}x^T,$$

де $M^{(i)}$ – симетрична скалярна квадратична матриця, x^T – вектор стовпець.

Метою кібернападу для *i*-го гравця в кібератаці є вибір такої стратегії $x_i \in X_i$, щоб в ситуації *x*, яка склалася, успіх від її реалізації був найбільшим, тобто:

$$f_i(x) \to \max$$

При формалізації оптимального циклу в кібератаці *A* на інформаційну сферу передбачається оперуванням поняття рівноваги за Нешем. В [25] розглянуто та проаналізовано можливі кібератаки та підатаки на інформаційну сферу при формалізації оптимального циклу.

У даній моделі не враховано вплив інвестицій на вибір оптимального рішення, однак, дослідники демонструють як розроблені ігрові методи аналізу дозволяють оцінювати як поодинокі, так і групові кібератаки. Це дозволяє отримувати гарантовані й достовірні оцінки рівня захищеності інформації від кібератак на інформаційну сферу.

Аналіз наукових робіт з математичного моделювання систем захисту інформації показав, що основні зусилля зосереджені на визначенні обсягу інвестицій у захист (Табл. 1.1). Питанням розподілу цих інвестицій між об’єктами захисту присвячені одиничні роботи. Крім того, існуючі розробки рідко враховують вплив можливих дій зловмисника та їх наслідків на зміну показників та характеристик системи.

Таблиця 1.1.

Порівняльна характеристика математичних моделей інформаційної безпеки

Критерії порівняння / Моделі	Враховано ресурси захисту	Враховано ресурси нападу	Враховано вартість окремого засобу захисту	Враховано уразливості об’єктів	Оптимізація розподілу ресурсів між об’єктами захисту	Розрахунок опьтимального рішення в динамічному режимі
Модель Гроса	+	+	-	-	+	-
Модель Гордона-Лоеба	+	-	-	+	-	-
Модель Задіраки	+	-	-	-	-	-
Модель Глушака-Новікова	+	-	+	-	+	-
Модель Журиленка	+	-	-	+	-	+
Модель Архипова	+	+	+	+	-	+
Модель Хорошка-Хохлачової	-	-	-	+	-	+
Розроблена модель	+	+	-	+	+	+

В результаті аналізу приведених вище наукових робіт, задача ефективного використання обмежених фінансових ресурсів на захист інформації суб'єктів господарської діяльності стає дедалі більш важливою і в значній мірі визначає рівень інформаційної безпеки держави [45,46,92,95]. Окрім того, в умовах невизначеності, коли дії суперника можна передбачити лише з певною імовірністю, пошук оптимального розподілу обмежених ресурсів між об'єктами захисту інформації за рахунок використання теоретико-ігрових методів та врахування динаміки зміни умов протистояння дозволить звести фінансові втрати від витоку інформації до мінімуму.

1.2 Аналіз сучасних математичних методів динамічного управління ресурсами

Розвиток економічних відносин та інформаційної сфери приводить до посилення конкурентної боротьби, збільшення обсягів і вартості інформації, а також потенційних збитків від її витоку, кількості інформаційних об'єктів, частоти нападів. При цьому умови протистояння постійно змінюються, відображаючи динамічну взаємодію двох протилежних сторін. Зміни спричиняють постійні напади, котрі, з одного боку, виявляють наміри суперника, з другого, вказують на слабкі місця захисту, куди, як правило, направлений напад. Іншими причинами змін можуть бути «старіння» інформації, введення нової інформації та додаткових ресурсів, перерозподіл їх між об'єктами, поява нових зв'язків між ними.

Антагоністичне протистояння двох сторін в інформаційній сфері характеризується тим, що захист, зазвичай, знаходиться у невизначеності щодо дій суперника, а напад має певне уявлення про структуру системи захисту і направляє свої зусилля в ту ланку системи безпеки, котра може принести найбільший ефект. Розподіл ресурсів захисту на блокування різного типу загроз може вестись як в активному режимі – випереджаючи дії суперника, так і в адаптивному, з затримкою інвестування, коли виявляється напрямок атак.

Необхідність динамічного управління ресурсами обумовлена такими причинами:

- невизначеністю відносно дій суперника, а саме направленістю його зусиль по здобуттю інформації і масштабом цих зусиль;
- зміною з часом як внутрішніх, так і зовнішніх умов протистояння – вартості інформації, її розподілу між об'єктами, направленості атак суперника, появою нових суперників;
- зміною стану інформаційної системи, зокрема, зміною її найслабшої ланки після виявлення націленості атак і прийняття відповідних заходів з боку захисту.

При використанні адаптивного режиму інвестування поряд з двома основними величинами, котрі підлягають оптимізації – загальній кількості ресурсів Y^0 і їх розподілу $\{y_k^0\}$ між об'єктами – виникає необхідність визначення оптимального моменту t^0 інвестування. Існування оптимуму відносно моменту розподілу коштів можна пояснити наступними міркуваннями. Затримка в інвестуванні в умовах послідовних атак, звичайно, приведе до певних втрат. Проте попередній розподіл ресурсів, коли ще не проявилась націленість суперника, може виявитись неефективним і привести до ще більших втрат. Тому настає момент t^0, який визначається пороговим значенням допустимої завданої шкоди від реалізації загроз інформації, при настанні якого стає доцільним виділення певної кількості ресурсів на захист і їх розподілу між об'єктами. Оптимальні значення зазначених величин можна знайти з умови досягнення оптимуму цільової функції, котра, наприклад, визначає прибуток від внесених інвестицій.

Аналізу поставленої задачі присвячена низка робіт [86,90,99]. В [86] використовується модель Гордона-Лоеба і послідовні атаки розглядаються як гаусівський випадковий процес. Цільова функція визначає прибуток від інвестицій, тобто різницю між вартістю захищеної в результаті внесення інвестицій інформації та втратами – завданому збитку від витоку інформації і вартістю витрат на її захист. Розглянуто 25 типів загроз, і метою аналізу є

визначення оптимальної кількості загроз, на які слід направити ресурси захисту. Ця величина визначається в динаміці в залежності від параметрів, які характеризують: σ – рівень невизначеності, λ – безповоротні втрати, ρ – коефіцієнт кореляції захисту від різних загроз, μ – очікуваний темп зростання потенційних втрат. Вартість активів з часом не накопичується. Вартість атаки x_m для m-ї загрози моделюється як гаусівська випадкова величина з середнім значенням $\overline{x_m}$ і стандартним відхиленням σ_m. Значення $\overline{x_m}$ залишається незмінним з часом, а величина σ_m може коригуватись. В цільову функцію входять також параметри, котрі характеризують інформаційну систему: v – уразливість системи, α – продуктивність інвестицій.

В моделі припускається, що ефективність (рентабельність) всіх загроз для нападу однакова. Атакуючий направляє свої зусилля на об'єкт, котрий приносить йому максимум прибутку, тобто максимум величини $z \cdot a - x_i$, де a – вартість інформації, z – імовірність успішності атаки, x_i – вартість атаки на i-й об'єкт.

Автори [86] вважають, що при повній невизначеності логічно всі ресурси захисту розподілити рівномірно між об'єктами. Проте при обмежених ресурсах, виділених на захист, розмір коштів, які припадають на один об'єкт, можуть виявитись недостатніми для захисту і виникає дилема: взагалі відмовитись від захисту, вважаючи, що втрати від витоку будуть меншими від втрат на захист, чи розподілити ресурси між меншою кількістю об'єктів з метою більш надійного захисту. В останньому випадку виникає задача визначення оптимальної кількості m^0 захищених об'єктів.

Ця задача розглянута в [86] для наступного прикладу.

Загальна вартість активів комерційного підприємства $a = 1000$ (всі розрахунки – в тисячах доларів). Кожен рік рентабельність активів становить $r = 5\%$. Кількість загроз (які розглянуто як кількість об'єктів захисту) складає $n = 25$. В разі успішної атаки підприємство витрачає $z = 2{,}5\%$ вартості своїх активів, тобто 25 тисяч доларів. Середня вартість успішної атаки становить 15

тисяч доларів, тобто $\bar{x} = 15$. Ціна кожної наступної атаки зростає на 1 тисячу доларів, отже градієнт ціни атаки $\Delta x = 1$. Невизначеність протистояння представляється як відхилення ціни атаки від її середнього значення. При цьому $\sigma = 0$ означає, що всі напади передбачені ідеально, при $\sigma = 1$ правильно передбачені 96% атак, при $\sigma = 16$ – 65%.

Після кожної атаки напад змінює її направленість. На одне коло повторюваної гри захист витрачає на кожний об'єкт 1 тисячу доларів. Кореляція додаткових витрат виражається коефіцієнтом $\rho = 0{,}1$. В розрахунок вводиться також параметр управління – неповоротні витрати λ. Це вартість оновлення захисту, котра розглядається як часткова вартість активів.

Результати досліджень [86] можна коротко викласти наступним чином. В статичному випадку, коли ресурси вносяться відразу і їх розподіл надалі не коригується, оптимальна кількість об'єктів, на котрі направляються ресурси захисту становить: $\sigma = 0$ $m^0 = 11$, при $\sigma = 1$ $m^0 = 12$, при $\sigma = 2$ $m^0 = 13$, а при $\sigma \geq 4$ $m^0 = 0$, тобто ресурси слід розподіляти на велику кількість об'єктів і захист стає неефективним. При всіх значеннях σ і $m \geq 23$ прибуток від інвестування є від'ємним.

При роботі в динамічному режимі досягаються два позитивні ефекти: по-перше, зменшується невизначеність, оскільки виявляється націленість атак суперника (зменшується σ), по-друге, проявляються слабкі місця захисту, куди, як правило, направляє свої зусилля суперник, прагнучи досягти максимального прибутку від нападу. Після нападу з'являється можливість коригування системи захисту і підвищення її показників. Очевидно, що при повній визначеності ($\sigma = 0$) дані динамічного режиму співпадають з результатами статичного – $m^0 = 11$. Але при зростанні невизначеності оптимальні стратегії динамічного і статичного підходів до інвестування починають відрізнятися. При цьому значення m^0 змінюються, і розподіл ресурсів між об'єктами стає ефективним в ширшому інтервалі величин σ: при $\sigma = 2$ $m^0 = 9$, при $\sigma = 4$ $m^0 = 11$, при $\sigma = 8$ $m^0 = 4$ і лише при досягненні межі $\sigma \geq 16$ одержуємо $m^0 = 0$. Ці дані ілюструють той висновок, що переваги

динамічного режиму в більшій степені проявляються при значній невизначеності.

В [86] досліджено також вплив величини неповоротних активів на вибір оптимальної стратегії при різних рівнях невизначеності. Показано, що цей вплив зростає зі збільшенням невизначеності.

В [86] наведено емпіричні докази ефективності вживаного підходу і висловлено міркування щодо сфери його застосування. Як приклад, розглянуто роботу комп'ютера, підключеного до Інернету. Зловмисники користуються тим, що цей комп'ютер може «спілкуватися» з будь-яким іншим комп'ютером. Це дає змогу їм будувати мережі компрометуючих пристроїв (бот-мережі), що атакують законних користувачів, розсилаючи спам, поширюючи шкідливе програмне забезпечення та здійснюючи фішинг-атаку. Великі компанії мають технічний персонал, котрий виявляє та очищає заражені машини, в той час, як звичайні користувачі іноді не можуть навіть зафіксувати момент атаки, не говорячи вже про вжиття заходів по виправленню становища. На цих користувачів і направлені в першу чергу зусилля зловмисників. При зміні становища вони перенацілюють свої атаки в бік найслабшої ланки. Інформація про напрямок атак дає можливість адаптуватися до загроз і зменшити втрати від реалізації нападів. Наведено приклад, коли застосування засобів захисту у Великобританії зменшило річні втрати з 2003 по 2007 рік з 0,18% до 0,10% від річного обороту.

Визначенню оптимального моменту інвестування в інформаційну безпеку присвячена також робота [99]. Наведено результати розрахунків оптимального розміру z^0 інвестицій та імовірних втрат T від ступеня невизначеності σ і уразливості v для обох видів функцій $S(z,v)$. При збільшенні σ обидві величини – z^0 і T – зростають по нелінійному закону, причому в залежності $z^0(\sigma)$ нелінійність виражена несуттєво, а в залежності $T(\sigma)$ – досить виразно. Залежності $z^0(v)$ і $T(v)$ при різних формах $S(z,v)$ носять суттєво відмінний характер, підкреслюючи той факт, що визначення форми функції $S(z,v)$ є

найважливішою задачею, оскільки терміни і оптимальна сума інвестиційних витрат залежать в найбільшій степені саме від уразливості.

В [17] розглянута доцільність динамічного управління ресурсами захисту в інформаційних системах в умовах, котрі відрізняються загальною кількістю об’єктів і кількістю об’єктів, на які здійснюється напад, частотою атак і розподілом інформації по об’єктах.

1.3. Обґрунтування та постановка задач роботи

Сучасні системи захисту інформації являють собою досить складні структури, які можуть містити велику кількість об’єктів, захищених багаторубіжними перешкодами [18,21,32,35]. Дослідження таких систем представляє складну задачу, котру розглядають зазвичай з допомогою математичної моделі. Це абстрактний образ реальної фізичної системи, котрий повинен відповідати двом суперечливим величинам: в найбільшій степені відображати властивості системи, уникаючи при цьому зайвої деталізації, котра може ускладнити одержання кінцевих результатів. Інтерес до математичного моделювання в сфері інформаційної безпеки зростає з часом з огляду на збільшення обсягів і цінності інформації, масовості нападів, розширення і вдосконалення засобів отримання несанкціонованого доступу до інформації та засобів захисту інформації; збільшення вартості інформації [5,21,36,41,71]. Ускладнення схем протистояння відбивається на структурі математичних моделей, які повинні відображати нові умови і виникаючі ситуації.

Основним завданням менеджменту інформаційної безпеки є оптимізація її технічних і економічних показників. Формування оптимізаційних задач і розробка методів їх рішення має багатовікову історію. На цій основі виникла нова галузь математики – дослідження операцій, що базується на єдності математичних моделей і методів рішення оптимізаційних задач в різних галузях людської діяльності [13,64,74,75].

До цієї галузі відноситься і один з важливих напрямків менеджменту інформаційної безпеки – оптимізація ресурсів, виділених на захист інформації. Цей напрямок має декілька аспектів, в яких оптимізації підлягають:

- загальна кількість ресурсів Y захисту;

- їх розподіл $\{y_k\}$ між окремими об'єктами (k - номер об'єкта);

- момент t^0 інвестування.

Критерієм оптимальності може бути один (або декілька) [84] показників інформаційної безпеки – величина завданої шкоди від реалізації загроз інформації, загальні витрати, котрі включають збиток від витоку інформації і витрати на її захист; прибуток від внесення інвестицій в захист інформації, їх рентабельність тощо.

Рішення поставлених задач ускладнюється низкою причин. Головна з них обумовлена тим, що пошук оптимального рішення ведеться в умовах невизначеності [62,82,85], коли дії суперника можна передбачити лише з певною імовірністю, а іноді взагалі неможливо. Різноманітність засобів та засобів захисту, їх характеристик, різноманітність схем протистояння, неможливість точного визначення уразливостей окремих елементів системи захисту, відсутність статистичних даних по нашій країні [67].

Задачею роботи є пошук в динамічному режимі оптимального розподілу ресурсів в багаторубіжних системах та системах різнонаправленого протистояння, де кожна з сторін прагне зберегти свою інформацію і здобути інформацію суперника. Рішення цієї задачі для широкого класу систем з «прив'язкою» до конкретних об'єктів дасть можливість покращити економічні і технічні показники [45,58,77].

Побудову математичної моделі поділено на декілька етапів [3,9-10,26,48].

▪ Обрати показник, який визначає цільову функцію і підлягає оптимізації. Такими показниками можуть бути: надійність системи, збиток від витоку інформації, кількість ресурсів, виділених на захист інформації, їх розподіл між об'єктами, рентабельність інвестицій в захист інформації, сумарні втрати, котрі включають в себе збиток від витоку інформації і витрати на її захист тощо.

▪ Визначити параметри і характеристики системи, від яких залежить цільова функція.

▪ Зібрати відомості про систему захисту і можливі умови протистояння (розподіл інформації по об’єктах, залежність уразливості об’єктів від умов протистояння, імовірності нападів на окремі об’єкти, імовірності виділення певної кількості ресурсів нападу на об’єкти тощо).

▪ Встановити вид залежності цільової функції від параметрів і характеристик системи захисту, а також від умов протистояння, тобто форму цільової функції.

▪ Обрати критерій оптимальності (сумарний збиток від витоку інформації, його середнє значення по об’єктах, максимально допустиме значення для кожного з об’єктів і т.п.).

Організація розрахунків передбачає операції.

- вибір методу розв’язку задачі;
- складання і налагодження програми для комп’ютера;
- проведення розрахунків;
- представлення результатів у найбільш виразній формі;
- формулювання висновків і рекомендацій.

Висновки до 1 розділу

1. Аналіз існуючих моделей оптимізації систем захисту інформації показав, що метою багатьох моделей є оптимізація сумарних витрат на захист інформації (модель Гордона-Лоеба, модель В.К. Задіраки), і лише одиничні моделі направлені на пошук оптимального розподілу коштів між об’єктами захисту інформації (модель О.М. Новікова).

2. Аналіз моделі Гордона-Лоеба, яка має емпіричне підтвердження, показав, що основну роль при розрахунку оптимальних витрат на систему захисту відіграє уразливість об’єктів. На жаль, модель по своїй структурі є статичною – рішення і результат настають одночасно; не враховано, як напад буде міняти свою стратегію при внесенні в захист додаткових інвестицій, тобто відсутній аналіз протистояння в динамічному режимі, що є суттєвим недоліком в умовах постійних атак.

3. Сучасні системи захисту інформації являють собою складні структури, які містять велику кількість об’єктів, для захисту яких може бути використано широкий спектр методів та засобів захисту. Дослідження інформаційних структур, що потребують захисту, ведеться шляхом математичного моделювання. З огляду на збільшення обсягів і цінності інформації, масовості нападів, розширення і вдосконалення засобів здобуття і захисту інформації та відповідне збільшення її вартості процес протистояння ускладнюється, що відбивається на структурі математичних моделей, які повинні відображати нові умови і виникаючі ситуації. Перспективним при моделюванні є використання функції уразливості об’єктів, що залежить від кількості вкладених як ресурсів нападу, так і ресурсів захисту, та може описувати різні системи.

4. В умовах невизначеності, коли дії суперника можна передбачити лише з певною імовірністю, пошук оптимального розподілу обмежених ресурсів між об’єктами захисту інформації за рахунок використання теоретико-ігрових методів та врахування динаміки зміни умов протистояння дозволить звести величину завдоної шкоди від реалізації загроз інформації до мінімуму.

РОЗДІЛ 2
ОПТИМІЗАЦІЯ РОЗПОДІЛУ РЕСУРСІВ МІЖ ОБ'ЄКТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ МОДЕЛЮВАННІ ПРОЦЕСІВ НАПАДУ НА ІНФОРМАЦІЮ ТА ЇЇ ЗАХИСТУ

2.1. Моделювання протистояння двох сторін у сфері захисту інформації на основі теоретико-ігрових методів

Для побудови ефективної системи захисту в умовах невизначеності важливою проблемою є дослідження можливих варіантів розподілу ресурсів між об'єктами захисту та вибір серед них оптимального. Метою сторони захисту являється мінімізація ймовірності реалізації загроз. Сторона нападу переслідує прямо протилежні цілі: розподіл своїх ресурсів, який створює максимальні можливості для реалізації інформаційних загроз. Таке протистояння двох сторін є типовою задачею теорії ігор [12,24,29,33,43,47,50,62,65,71]. Виграш кожної із сторін залежить від стратегій суперника і визначається цільовою функцією $i(x, y)$.

Така постановка задачі відповідає несиметричній грі з нульовою сумою: виграти може тільки перший гравець (сторона нападу), причому його виграш, що оцінюється вартістю критичної інформації, дорівнює програшу другого (сторони захисту).

У теорії ігор припускається, що кожний гравець знає свою функцію виграшу та набір стратегій, які є в його розпорядженні, а також функції виграшів і стратегії інших гравців, і діятиме у відповідності з цією інформацією.

Для досягнення поставлених цілей у розпорядженні сторони нападу є X ресурсів та у сторони захисту Y ресурсів. Ці ресурси, звичайно, є обмеженими і можуть бути направлені на різні об'єкти.

Стратегія першого гравця полягає в розподілі своїх ресурсів між об'єктами у різних співвідношеннях:

$$\{x_{ik}\}=(x_1, x_2,..., x_l),\ \sum_{k=1}^{l} x_k = X, x_k \geq 0,$$

де k – номер об'єкта захисту ($k=\overline{1,l}$), x_k – витрати (ресурси) для реалізації загроз на k-му об'єкті.

Другий гравець використовує свою стратегію розподілу ресурсів:

$$\{y_{jk}\}=(y_1, y_2,..., y_l),\ \sum_{k=1}^{l} y_k = Y, y_k \geq 0,$$

де y_k – витрати на захист k-го об'єкту.

Оскільки нападник намагається завдати максимальної шкоди супернику, цільова функція сторони нападу має вигляд:

$$i(x_k, y_k) \to \max.$$

Величина завданої шкоди $i(x_k.y_k)$ оцінюється вартістю критичної інформації і залежить від розподілу ресурсів x_k, y_k між об'єктами захисту.

Сторона захисту переслідує протилежні цілі – мінімізувати розмір завданої шкоди в результаті реалізації загроз, тому цільова функція для сторони захисту записується наступним чином:

$$i(x_k, y_k) \to \min,$$

Використовуючи теоретико-ігровий підхід, на наступному етапі будується матриця виграшів для функції $i(x_k, y_k)$, в якій стовпчики відповідають варіантам розподілу $\{y_{jk}\}$ ресурсів захисту, а рядки – імовірним варіантам розподілу $\{x_{ik}\}$ ресурсів нападу:

$$i = \begin{pmatrix} i_{11} & i_{12} & ... & i_{1n} \\ i_{21} & i_{22} & ... & i_{2n} \\ ... & ... & ... & ... \\ i_{m1} & i_{m2} & ... & i_{mn} \end{pmatrix},$$

де i_{ij} – розмір завданої шкоди від реалізації загроз у результаті застосування гравцями своїх $\{x_i\}$ та $\{y_j\}$ чистих стратегій ($i=(\overline{1,m})$, $j=(\overline{1,n})$).

Шукана стратегія цієї матричної гри є оптимальним розподілом ресурсів захисту, який знаходять по одному з відомих критеріїв.

При пошуку оптимальної стратегії, перший гравець (сторона нападу) розглядає і-й рядок, припускаючи, що другий гравець (сторона захисту) обирає j-й стовпчик. При цьому виграшем буде елемент i_{ij}. Інтереси гравців протилежні, тому перший гравець прагне максимізувати виграш i_{ij}, у той же час другий гравець навпаки, обиратиме таку стратегію, що мінімізує програш i_{ij}. Жоден з них не знає напевно, якою буде стратегія суперника, що ускладнює прийняття рішення.

Якщо кожен з гравців обирає однозначно з ймовірністю 1 деяку стратегію, то вважають, що він використовує чисту стратегію. У такому випадку рішення гри знаходиться в чистих стратегіях. Рішення гри полягає у визначенні оптимальної стратегії кожного гравця.

Стратегія гравця є оптимальною, якщо застосування цієї стратегії забезпечить йому найбільший гарантований виграш при усіх можливих стратегіях іншого гравця. Виходячи із цих міркувань, нападник досліджує матрицю виграшів i наступним чином.

У кожному *i*-му рядку ($i=\overline{1,m}$) визначається мінімальне значення виграшу i_{ij} в залежності від вибору стратегій захисту - $\min\limits_{j} i_{ij}$, тобто визначається мінімальне значення завданої шкоди від реалізації загроз (виграш) при застосуванні нападником своєї *i*-тої чистої стратегії. Серед цих мінімальних виграшів $\min\limits_{j} i_{ij}$ шукається така *i*-та стратегія, за якої цей мінімальний виграш буде максимальним, тобто знаходиться:

$$\alpha = \max_{i} \min_{j} i_{ij}.$$

Число α є нижньою ціною гри і показує, яку мінімальну частку вилученої інформації i_{ij} може гарантувати собі нападник, застосовуючи свої чисті стратегії при усіх можливих діях захисту.

Сторона захисту за своєї оптимальної поведінки намагається за рахунок своїх стратегій максимально зменшити збитки i_{ij}. Тому для сторони захисту у

кожному *j*-му стовпчику знаходиться $\max_i i_{ij}$, тобто визначається максимальний виграш нападника при застосуванні стороною захисту свєї *j*-тої чистої стратегії, після чого знаходиться така *j*-та стратегія захисту, за якої нападник завдасть мінімальної шкоди, тобто знаходиться:

$$\beta = \min_j \max_i i_{ij}.$$

Число β є верхньою ціною гри і показує, якої максимальної шкоди завдасть нападник у разі реалізації загроз. Іншими словами, сторона захисту обирає таку чисту стратегію, яка гарантує, що величина завданої шкоди *i* у результаті будь-яких дій нападника не перевищить значення β.

Якщо у грі з матрицею *i* нижня та верхня ціни гри співпадають, тобто $\max_i \min_j i_{ij} = \min_j \max_i i_{ij} = v$, то гра має сідлову точку, а величина *v* становить ціну гри. У такому випадку чисті стратегії гравців, які забезпечують $\max_i \min_j i_{ij}$ для нападника та $\min_j \max_i i_{ij}$ для захисту є оптимальними. При відхиленні стратегії нападника від оптимальної його виграш буде зменшуватись, і відповідно при відхиленні сторони захисту від своєї оптимальної стратегії буде збільшуватись величина завданої шкоди внаслідок реалізації загроз.

Якщо сідлової точки немає, то знайдені значення нижньої і верхньої ціни гри вказують, що програш сторони захисту не перевищить верхню ціну гри і щонайменше дорівнюватиме нижній ціні гри. Оскільки жодна з чистих стратегій гравців не забезпечує оптимальний результат, теорія ігор пропонує застосовувати змішані стратегії.

Змішані стратегії сторони нападу задаються набором імовірностей S_X^0=(P_1, … , P_m), з якими гравець застосовує свої початкові чисті стратегії $\{x_i\}$ ($i = \overline{(1,m)}$), причому:

$$\sum_{i=1}^{m} P_i = 1,\ P_i \geq 0,\ i = \overline{(1,m)}.$$

Аналогічно змішані стратегії сторони захисту задаються набором ймовірностей S_Y^0=(Q_1, … , Q_n):

$$\sum_{j=1}^{n} Q_j = 1,\ Q_j \geq 0,\ \ j = \overline{(1,n)}.$$

Програш сторони захисту (виграш сторони нападу) при використанні змішаних стратегій визначається як математичне очікування завданої шкоди:

$$i^0 = \sum_i \sum_j P_i i_{ij} Q_j .$$

Знаходження рішення гри відбувається за допомогою зведення її до задачі лінійного програмування.

Оптимальна змішана стратегія S_Y^0 має таку властивість, що програш захисту не перевищить значення ціни гри v за будь-якої поведінки нападу та дорівнюватиме v при оптимальній поведінці нападу. Значення ціни гри v поки не відоме, але можна вважати, що $v>0$ (для цього достатньо, щоб всі елементи i_{ij} були додатніми).

Припускаючи, що захист використовує змішану стратегію, а напад свою i-ту чисту стратегію. Тоді математичне очікування завданої шкоди становитиме:

$$i_i = i_{i1} Q_1 + i_{i2} Q_2 + ... + i_{in} Q_n .$$

Враховуючи властивість оптимальних змішаних стратегій, жодне з чисел i_i не перевищить значення v. Таким чином, записано ряд лінійних обмежень:

$$\begin{cases} Q_1 + Q_2 + Q_3 = 1 \\ i_{11} Q_1 + i_{12} Q_2 + i_{13} Q_3 \leq v; \\ i_{21} Q_1 + i_{22} Q_2 + i_{23} Q_3 \leq v; \\ i_{31} Q_1 + i_{32} Q_2 + i_{33} Q_3 \leq v \end{cases}$$

Така задача теорії ігор зводиться до задачі лінійного програмування, для рішення якої використовується симплекс-метод.

Для пошуку розв’язку сформульованої задачі необхідно записати цільову функцію $i(x_k, y_k)$, яка визначає розмір завданої шкоди від реалізації загроз в залежності від розподілів ресурсів обох сторін.

2.2. Формування цільової функції моделі пошуку оптимального розподілу між об’єктами захисту інформації

При розробці математичної моделі певної інформаційної системи необхідно встановити значення параметрів і форму залежностей, які входять у цільову функцію. На основі проведеного аналізу існуючих моделей інформаційної безпеки з метою усунення виявлених недоліків і найповнішого використання останніх досягнень у галузі моделювання систем захисту інформації визначено основні складові цільової функції [55]. Для обраної моделі цільова функція виражає завдану шкоду від реалізації загроз і має вигляд:

$$i(x_k, y_k) = \sum_{k=1}^{l} i_k(x_k, y_k) = \sum_{k=1}^{l} g_k p_k f_k(x_k, y_k), \qquad (2.1)$$

де $k = \overline{1, l}$ – номер об’єкта;

x_k і y_k – ресурси нападу і, відповідно, захисту;

g_k – відносна цінність інформації на k-му об’єкті;

p_k – імовірність нападу на об’єкт;

$f_k(x_k, y_k)$ – уразливість k-го об’єкту, яка залежить від співвідношення ресурсів нападу і захисту.

Величини $i(x, y)$, $i_k(x, y)$ та g_k віднесені до всієї вартості інформації, $f_k(x, y)$ - до вартості інформації на об’єкті.

Розглядається протистояння в умовах невизначеності, коли оцінити імовірність нападу p_k неможливо. Тому покладено $p_k = 1$ (напад відбувся).

Уразливість $f(x, y)$ об’єкта розглядається як імовірність успішної атаки, що залежить від витрат x на здійснення атаки та витрат y на захист об’єкта.

При застосуванні моделі [55] на першому етапі слід знайти значення параметрів і форму залежностей, котрі входять в цільову функцію. Відносна

цінність g_k інформації на об'єктах може бути визначена досить точно. Визначення імовірностей нападу p_k на об'єкти і форми залежності $f(x, y)$ являє собою більш серйозну задачу, котра ускладнюється невизначеністю дій суперника.

Постановка задачі йде по двох напрямках.

1. Введення показників системи захисту інформації:

1) кількість об'єктів захисту;

2) відносна цінність g_k інформації на об'єктах;

3) початкова уразливість $f(x,0)$ об'єкта, котра визначається його природною захищеністю;

4) загальна кількість $Y = \sum_{k=1}^{l} y_k$ ресурсів захисту;

5) залишковий ризик.

2. Оцінка дій суперника:

1) характер атак (їх націленість і інтенсивність);

2) імовірності нападу p_k на об'єкти;

3) загальна кількість $X = \sum_{k=1}^{l} x_k$ ресурсів нападу;

4) імовірний розподіл $\{x_k\}$ ресурсів по об'єктах.

Модель [55] не обмежується описаним варіантом. Цільова функція може виражати не тільки завдану шкоду від реалізації загроз, а й інші величини: сумарні втрати, прибуток від внесення інвестицій в захист, їх рентабельність. Можливі варіанти щодо критерія оптимальності для функції (2.1). Можуть бути введені додаткові умови, зокрема, обмеження по Y, по $i(x, y)$, по $i_k(x, y)$ [3, 15].

При встановленні залежностей $f(x, y)$ враховано такі міркування. Імовірність успішної атаки прямо-пропорційно залежить від витрат x на здійснення атаки та обернено-пропорційно від витрат y на захист об'єкта [2,22]. Тому змінні x, y входять у $f(x, y)$ у вигляді відношення x/y. Для

скорочення запису в окремих випадках покладено $y = const$ і розглянуто залежності $f(x)$, розуміючи під x відносну величину.

Залежності $f(x, y)$ повинні задовольняти умовам: при $x/y \to 0$ $f(x, y) \to 0$, при $x/y \to \infty$ $f(x, y) \to 1$. Цим умовам задовольняють степеневі функції виду:

$$f(x, y) = \frac{\left(x/y\right)^n}{\left(x/y\right)^n + c} \tag{2.2}$$

і показникові

$$f(x, y) = 1 - e^{-m\left(x/y\right)^n}, \tag{2.3}$$

де константи c, n, m визначають положення і форму кривих (рис.1.2). Враховуючи, що обидві залежності схожі за формою, оскільки задовольняють наведеним вище умовам, надалі використано більш просту дробово-степеневу функцію. При $n = 1$ вона виражає дробово-лінійну залежність, при $n > 1$ – дробово-нелінійну.

Для скорочення запису у (2.2) позначено $\tilde{x} = x/y$:

$$f(\tilde{x}) = \frac{(\tilde{x})^n}{(\tilde{x})^n + c}. \tag{2.4}$$

Оскільки основним завданням менеджменту інформаційної безпеки є розробка оптимального варіанту дій захисту, функції уразливості (2.2) розглянуто також у формі:

$$f(\tilde{y}) = \frac{1}{1 + c\tilde{y}^n}, \tag{2.5}$$

де $\tilde{y} = y/x$. Залежності (2.4) та (2.5) показані на рис. 1.2.

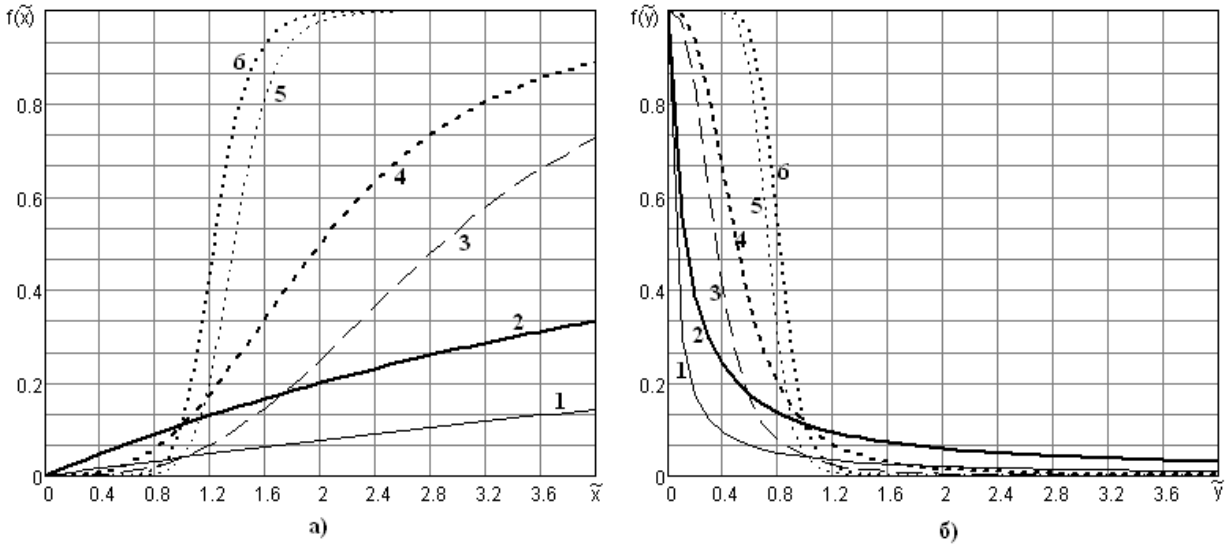


Рис.1.2. Функції уразливості у формі (2.4) (рис.1.2,а) і у формі (2.5) (рис.1.2,б) при різних значеннях n і c: криві **1,2** – $n=1$, **3,4** – $n=3$, **5,6** – $n=10$, криві **1,3,5** – $c=24$, **2,4,6** – $c=8$

При $\tilde{x}\to\infty$ показники n і c слабо впливають на форму кривої, оскільки вона асимптотично наближається до одиниці при будь-яких n і c. При $0<\tilde{x}<1$ величина n впливає, в основному, на форму опуклості, а c – на висоту підйому кривої над віссю абсцис.

Вплив параметрів n і c на форму залежностей (2.5) показано на рис.1.2,б. Вплив параметра n проявляється, в основному, в початковій області $y<1$: при $n\le 1$ опуклість кривих направлена донизу, при $n>1$ – догори. Параметр c впливає на висоту підйому кривих над віссю абсцис: зі зростанням c уразливість зменшується, і криві опускаються донизу.

Дробово-лінійні ($n=1$, криві 1, 2) функції (2.2) описують уразливість інформації, що зберігається на матеріальних носіях, де початкові внески в захист ($y\approx 0$) (на організаційні та інженерно-технічні заходи та засоби захисту) приводить до монотонного, майже пропорційного зменшення уразливості і як результат – зменшення завданої шкоди, а при подальшому збільшенні їх ефективність зменшується, що відповідає економічному закону про граничну норму прибутку. Дробово-нелінійні ($n>1$, криві 3-6) функції відображають властивості інформації, що циркулює у комп'ютерних системах, де для

подолання перешкоди потрібно витратити значні ресурси. При зростанні нелінійності за рахунок збільшення показника n у (2.2) крива $f(x,y)$ по формі наближається до ступінчастої. Така залежність спостерігається при використанні шифрування даних, коли для зламу системи необхідно витратити значні ресурси, після чого величина завданої шкоди від реалізації загроз інформації зростає стрибкоподібно.

При $0<n<1$ функції (2.2) описують схильність інформації до впливу ненавмисних загроз, таких як, наприклад, некомпетентність персоналу або збій у роботі обладнання, коли власнику інформації завдано шкоди без затрат ресурсів з боку зловмисника.

Вибір параметрів c, n, m для кожної системи є ключовим завданням дослідження. Задача встановлення форми залежності імовірності успішної атаки від співвідношення ресурсів нападу і захисту є досить складною і вирішується окремо для кожної конкретної системи. Явний вид залежності (2.2) встановлюється на основі експертної оцінки (наприклад, з допомогою методики [53]), або на основі статистичних даних [96-98].

Можливість знаходження величин c і n продемонстровано, використовуючи результати моделювання стійкості мережевих систем [94]. Хрестиками на рис.2.2 показані точки, одержані в припущенні, що уразливість $f(y)$ є величиною, оберненою до стійкості, нормованої до одиниці (по осі абсцис відкладена величина інвестицій y, віднесена до вартості інформації).

Плавна крива проведена за умови, що сумарне лінійне відхилення від реперних точок, позначених хрестиками, дорівнює нулю. Порівняння форми кривої 2 з кривими на рис.1.2,б свідчить про те, що уразливість можна апроксимувати функцією (2.5) з $n=1$. Параметр c знаходимо, задовольняючи рівність (2.5) для кожної реперної точки і усереднюючи одержані значення c_i за умови мінімізації сумарного відхилення. Цю процедуру можна здійснити і для середньоквадратичного відхилення. Одержане значення $c=1500$ дозволяє сформувати функцію уразливості:

$$f(\tilde{y}) = \frac{1}{1+1500\,\tilde{y}}.$$

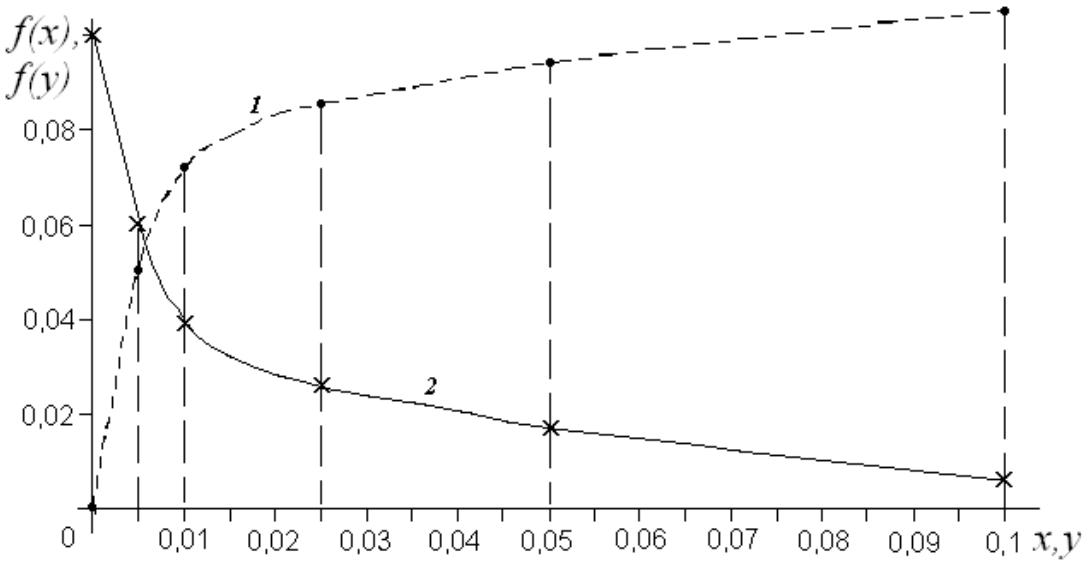


Рис. 2.2. Стійкість $f(x)$ системи (крива **1** – [14]) та її уразливість $f(y)$ (крива **2**), x, y – у відсотках до g

Важливе значення має питання чутливості оптимального рішення задачі до вибору параметрів, котрі входять в (2.2) та (2.3) і визначають динамічну уразливість об'єктів.

Чутливість оптимального рішення досліджено на прикладі системи, яка містить три об'єкти з обсягами інформації, розподіленими у пропорції $g_1 : g_2 : g_3 = 0{,}5 : 0{,}3 : 0{,}2$. Напад здійснюється на всі три об'єкти, уразливості об'єктів однакові. При аналізі використаємо 6 форм функцій уразливості $f(x,y)$, а також усереднену форму $\overline{f}(x,y)$ (рис.2.3) [108].

Основну увагу зосереджено на впливі параметрів n, c в степеневих функціях (2.2). З цією метою покладено в (2.2) $a = b = 1$. Для порівняння наведено також показникову функцію (крива 2 на рис.2.3), а також лінійну функцію (крива 3). Результати розрахунків – оптимальні розподіли ресурсів захисту $\{y_k\}$ і відповідні значення $i^0(x,y)$, одержані з допомогою методу Белмана [7].

Величини, які входять до складу цільової функції (2.1), визначаються на основі статистичних даних або в результаті експертної оцінки. Інтерес до складових цільової функції викликаний тим, що протистояння нападу і захисту відбувається в умовах невизначеності. В цьому випадку особливе значення має питання чутливості оптимального значення цільової функції $i^0(x,y)=i(x,y^0)$ до зміни величин, які входять до її правої частини.

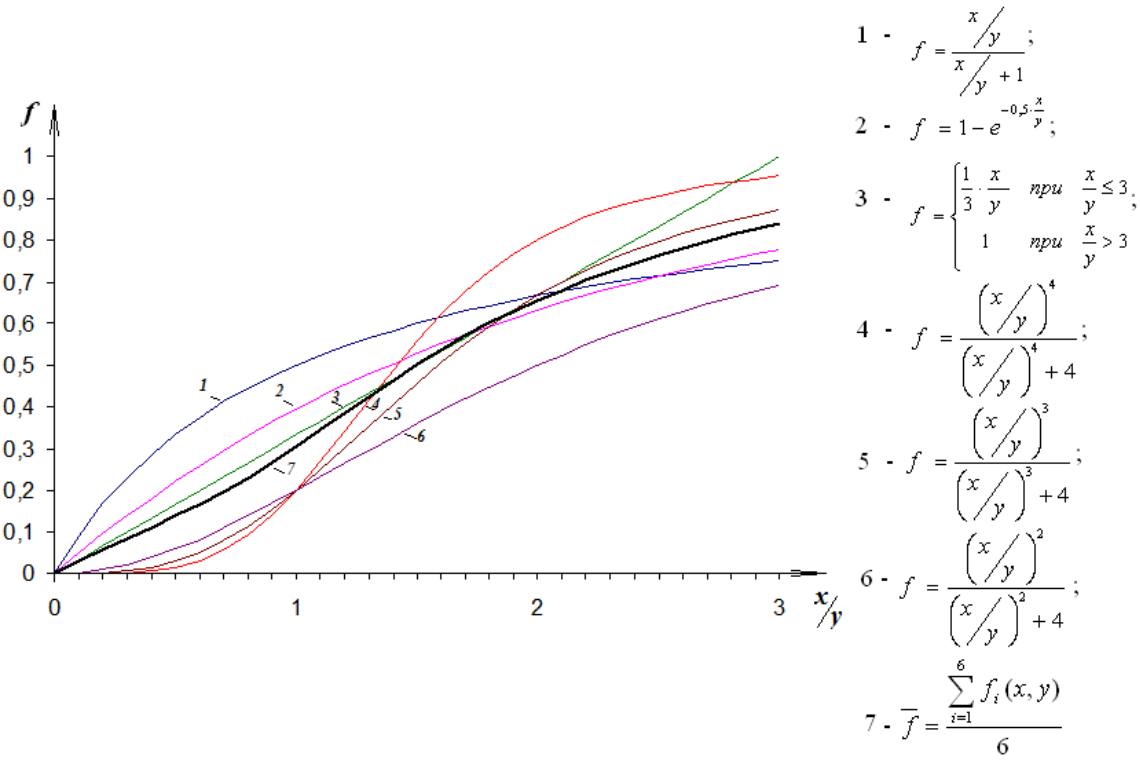


Рис.2.3. Залежності величини завданої шкоди від реалізації загроз від вкладених ресурсів для різних функцій уразливості $f(x,y)$

Дослідження розпочато із аналізу чутливості функції $i(x,y)$ до залежності $f(x,y)$. З цією метою розглянуто деякі залежності $f_t(x,y)$ (t - номер залежності) та прослідковується, як змінюється оптимальний розподіл ресурсів та відповідні втрати інформації при використанні кожної залежності $f_t(x,y)$.

При встановленні виду залежності $f(x,y)$ враховано такі міркування: при $x/y \to 0$ $f(x,y)\to 0$, при $x/y \to \infty$ $f(x,y)\to 1$. Розглянуто декілька функцій, що відповідають даним умовам (рис.2.3). Також побудовано усереднену функцію (крива 7), при цьому використано підхід Бернуллі-Лапласа, вважаючи всі

варіанти залежностей $f_t(x, y)$ рівноімовірними за браком статистичної інформації.

Застосовуючи метод Белмана [7], знайдено оптимальні розподіли $\{y_k^0\}$ ресурсів для сторони захисту та відповідні значення величини завданої шкоди від реалізації загроз інформації i^0 для системи з трьох об'єктів у випадку, коли напад здійснюється на всі три об'єкти з ваговими коефіцієнтами $g_1 = 0{,}5$, $g_2 = 0{,}3$, $g_3 = 0{,}2$.

В табл. 2.1 приведені оптимальні розподіли $\{y_k^0\}$ для різних функцій $f(x, y)$ та різних значень $Z = \frac{X}{Y}$. Ці розподіли відповідають сідловим точкам, тобто забезпечують виконання рівності $\min_j \max_i i(x, y) = \max_i \min_j i(x, y)$, де i та j - відповідно варіанти розподілу ресурсів нападу та ресурсів захисту.

Таблиця 2.1

Оптимальні стратегії захисту при різних функціях уразливості

Номер функції $f(x, y)$	Оптимальні стратегії	Z=0,5	Z=1	Z=1,5	Z=2	Z=2,5	Z=3
1	$y_1^0 : y_2^0 : y_3^0$	0,5:0,3:0,2					
	i^0	0,329	0,5	0,599	0,667	0,714	0,75
2	$y_1^0 : y_2^0 : y_3^0$	0,5:0,3:0,2					
	i^0	0,22	0,393	0,527	0,632	0,713	0,777
3	$y_1^0 : y_2^0 : y_3^0$	0,98:0,01:0,01					
	i^0	0,218	0,303	0,383	0,473	0,558	0,643
4	$y_1^0 : y_2^0 : y_3^0$	0,42:0,34:0,24	0,5:0,3:0,2	0,62:0,25:0,13	0,48:0,35:0,17	0,48:0,35:0,17	0,5:0,28:0,22
	i^0	0,167	0,4	0,566	0,795	0,905	0,952
5	$y_1^0 : y_2^0 : y_3^0$	0,43:0,33:0,24	0,5:0,3:0,2	0,59:0,26:0,15	0,52:0,33:0,15	0,51:0,31:0,18	0,49:0,33:0,18
	i^0	0,141	0,333	0,474	0,665	0,794	0,87
6	$y_1^0 : y_2^0 : y_3^0$	0,5:0,3:0,2					
	i^0	0,114	0,25	0,374	0,5	0,609	0,692
7	$y_1^0 : y_2^0 : y_3^0$	0,5:0,33:0,17	0,53:0,3:0,17	0,53:0,32:0,15	0,5:0,3:0,2	0,8:0,1:0,1	0,8:0,1:0,1
	i^0	0,178	0,345	0,504	0,655	0,739	0,796

Як видно з табл. 2.1, при використанні лінійної функції f_3 оптимальним варіантом для захисту при будь-яких значеннях Z являється зосередження своїх ресурсів на найбільш важливому першому об'єкті. Якщо функції f_1, f_2,

f_6 дають однаковий результат, а саме: оптимальним являється розподіл $\{y_k^0\} = (0{,}5;0{,}3;0{,}2)$, то при використанні функцій f_4 та f_5 спостерігається деяке відхилення від зазначеного варіанту залежно від значення *Z*. Наприклад, при *Z*=0,5 оптимальним варіантом являється розподіл ресурсів захисту у співвідношенні $\{y_k^0\} = (0{,}42;0{,}34;0{,}24)$ (функція f_4) та $\{y_k^0\} = (0{,}43;0{,}33;0{,}24)$ (функція f_5), при *Z*=1,5 оптимальний розподіл при використанні функції f_4 - $\{y_k^0\} = (0{,}62;0{,}25;0{,}13)$ та при функції f_5 - $\{y_k^0\} = (0{,}59;0{,}26;0{,}15)$.

Отримані результати проаналізовано з врахуванням виду залежностей $f_t(x, y)$ (рис.2.3). При функціях f_1, f_2, f_6 втрати інформації монотонно зростають на всьому проміжку Z від 0 до 3 і досягають значення 0,7-0,75. Плавний хід кривих є причиною того, що оптимальний розподіл ресурсів захисту залишається незмінним при будь-яких значеннях Z.

Функції f_4 і f_5 мають дещо інший характер. При $Z \le 0{,}5$ $f = 0{,}167$, а на проміжку від $Z = 0{,}5$ до $Z = 2{,}5$ втрати інформації різко зростають до значення $f = 0{,}8...0{,}9$, після чого f плавно наближається до 1. Тому на цих трьох відрізках оптимальний розподіл ресурсів захисту відрізнятиметься.

Розглядаючи степеневі функції f_4, f_5, f_6, зазначено, що оптимальний розподіл ресурсів не залежить від Z при степені $n = 2$, а для випадку n>2 він змінюється, досягаючи максимальної концентрації ресурсів на першому об'єкті при $Z = 1{,}5$ - в області найбільшої крутизни залежностей $f_t(x, y)$.

У ході дослідження усереднювалась не лише функція $f(x, y)$, за якою знаходиться кінцевий результат, а самі кінцеві результати, тобто $\{y_k^0\}$ і i_t^0, причому це усереднення проведено як по функціях $f_t(x, y)$, так і по значенням Z.

Щоб провести усереднення по Z, обрано деякі нормовані коефіцієнти c_Z ($\sum c_Z = 1$), вважаючи, що імовірність виділення нападом ресурсів $Z = 2$ є найвищою. Усереднений розподіл обчислено наступним чином:

$$(y_k^0)_Z = c_{0,5} \cdot y_k + c_1 \cdot y_k + c_{1,5} \cdot y_k + c_2 \cdot y_k + c_{2,5} \cdot y_k + c_3 \cdot y_k,$$

$$(y_1^0)_Z = 0{,}05 \cdot 0{,}5 + 0{,}15 \cdot 0{,}53 + 0{,}2 \cdot 0{,}53 + 0{,}25 \cdot 0{,}5 + 0{,}2 \cdot 0{,}8 + 0{,}15 \cdot 0{,}8 \approx 0{,}62.$$

Результати розрахунків приведені у табл. 2.2.

Таблиця 2.2

Оптимальні розподіли ресурсів та відповідні втрати інформації за різних варіантів усереднення

Z	Усереднення по значеннях f		Усереднення по значеннях $\{y_k^0\}$	
	$\{y_k^0\}$	i^0	$\{y_k^0\}$	i^0
0,5	0,5:0,33:0,17	0,178	0,55:0,27:0,18	0,210
1	0,53:0,3:0,17	0,345	0,58:0,25:0,17	0,370
1,5	0,53:0,32:0,15	0,504	0,61:0,24:0,15	0,513
2	0,5:0,3:0,2	0,655	0,58:0,27:0,15	0,658
2,5	0,8:0,1:0,1	0,739	0,58:0,26:0,16	0,764
3	0,8:0,1:0,1	0,796	0,58:0,25:0,17	0,825
Усереднення по Z	0,62:0,23:0,15	0,531	0,58:0,26:0,16	0,614

За результатами табл. 2.2 зроблено висновок, що усереднюючи значення $\{y_k^0\}$, отримано оптимальний розподіл практично однаковий при всіх значеннях Z - $\{y_k^0\} = (0{,}58 : 0{,}25 : 0{,}17)$ (із незначним відхиленням максимума на $0{,}03$), тоді як оптимальний розподіл, знайдений з використанням усередненої функції $\overline{f}(x, y)$, різко відрізняється при найбільших із приведених значеннях $Z = 2{,}5$ та $Z = 3$ у бік зосередження значної частки ресурсів ($y_1 = 0{,}8$) на першому об'єкті, де частка інформації найбільша. Однак, при такому варіанті усереднення очікувані втрати інформації менші, ніж у випадку усереднення $\{y_k^0\}$.

Усереднення по Z також дає змогу порівняти обидва підходи. Отримані при цьому розподіли містять лише незначні відмінності, тому будь-який із методів може бути використаний при пошуку оптимального розподілу ресурсів.

Підводячи підсумок, зазначено, що із використанням усередненої функції $\overline{f}(x, y)$ знайдений оптимальний розподіл ресурсів мало відрізняється від усередненого оптимального розподілу, однак такий метод потребує меншої кількості обчислювальних процедур. Тому для дослідження впливу інших

складових цільової функції на оптимальний результат використано усереднену функцією $\overline{f}(x, y)$.

Звертаючись до інших величин в (2.1) та вважаючи, що величини g, p, q, f є незалежними змінними, на основі теореми Тейлора:

$$\nabla i^0(g, p, q, f) = \nabla_g i^0 \partial g + \nabla_p i^0 \partial p + \nabla_q i^0 \partial q + \nabla_f i^0 \partial f$$

і визначено коефіцієнти чутливості функції $i^0(x, y)$ до цих величин:

$$\alpha_g = \frac{\partial i^0}{\partial g} = \nabla_g i^0;\ \alpha_p = \frac{\partial i^0}{\partial p} = \nabla_p i^0;\ \alpha_q = \frac{\partial i^0}{\partial q} = \nabla_q i^0;\ \alpha_f = \frac{\partial i^0}{\partial f} = \nabla_f i^0.$$

Для прикладу розглянуто величину g. Коефіцієнт α_g показує, як зміниться величина втрат інформації при оптимальному розподілі ресурсів захисту, якщо фактичне значення g відрізнятиметься від прийнятого. Якщо $\Delta g = 0{,}1$ при $Z = 1$ $\Delta i^0 = 0{,}057$, при $Z = 2$ $\Delta i^0 = 0{,}065$, при $Z = 3$ $\Delta i^0 = 0{,}080$.

Чутливість оптимального розв'язку зростає зі збільшенням $Z = \frac{X}{Y}$. Аналогічні висновки зроблено щодо інших величин. Оскільки швидкість зміни частинної похідної лінійної функції по незалежній змінній c_s виражається значенням цієї функції при $c_s = 1$ (а саме добутком всіх інших змінних), чутливість α_{c_s} буде тим більшою, чим більше значення $i^0(g, p, q, f)|_{c_s=1}$ в точці стаціонарності.

Використовуючи метод Белмана та цільову функцію (2.1) знайдено оптимальний варіант розподілу ресурсів захисту в умовах невизначеності. Зважаючи на труднощі встановлення виду залежності $f(x, y)$ від вкладених ресурсів, розглянуто різні методи усереднення – самих залежностей $f(x, y)$, а також усереднення отриманих результатів $\{y_k^0\}$. У результаті проведених досліджень обгрунтовано доцільність використання усередненої функції $\overline{f}(x, y)$.

На основі аналізу коефіцієнтів чутливості цільової функції до вхідних даних зроблено висновок, що розглянута модель може бути використана при пошуку оптимального рішення, при цьому відхилення від очікуваних втрат являється припустимим в умовах невизначеності.

У ході проведених досліджень виявлено певні закономірності впливу параметрів цільової функції на оптимальний розподіл ресурсів та відповідне значення величини завданої шкоди від реалізації загроз інформації. На основі аналізу виявлених взаємозв'язків за аналогією з моделю Гордона-Лоеба для характеристики ефективності використання внесених коштів введено поняття продуктивності витрат, яке кількісно виражається двома показниками – продуктивністю зменшення уразливості (ПЗУ) і продуктивністю зменшення загрози (ПЗЗ). Перший з цих показників виражається параметрами n і c функції уразливості $f(x, y)$, другий – параметром h функції розподілу $q(x, y)$.

2.3. Визначення показників економічної доцільності витрат на захист інформації

Розвиток інформаційної сфери проявляється, з одного боку, в зростанні обсягів інформації і її комерційної вартості, з другого – в збільшенні кількості нападів і, відповідно, зростанні збитків від реалізації загроз. Виникає необхідність постійного удосконалення систем захисту, що супроводжується збільшенням їх вартості. При цьому зростають вимоги до ефективності використання ресурсів захисту, показником якої є економічна доцільність витрат.

Поняття економічної доцільності витрат введене в моделі Гордона – Лоеба (ГЛ). Відповідно до цієї моделі імовірність порушення безпеки описується функцією $S(y,v)$, де y - інвестиції в захист, а v - початкова уразливість інформації (при $y = 0$).

Функція $S(y,v)$ може приймати дві форми (1.1) і (1.3), де параметри $\alpha > 0$ і $\beta \geq 1$ виражають міру економічної доцільності витрат на захист, тобто ступінь зменшення імовірності реалізації загроз $S(y,v)$ при внесенні інвестицій y.

Цільова функція в [89] виражає прибуток $b(y)$, котрий визначається як зменшення шкоди від реалізації загроз за рахунок внесення коштів y в захист інформації за відрахуванням величини y:

$$b(y) = [v - S(y,v)]L - y, \qquad (2.6)$$

де L - потенційні збитки від витоку інформації.

Модель ГЛ знайшла свій розвиток в багатьох роботах і стала найбільш відомою моделлю економічного менеджменту інформаційної безпеки. Зокрема, в [93] економічна доцільність витрат на захист інформації поділяється на два показники: продуктивність зменшення уразливості (ПЗУ) і продуктивність зменшення загрози (ПЗЗ). Перший з цих показників визначається виразом $v^{\alpha y+1}$, а другий — $t\beta y+1$, де t - імовірність загрози, а α і β - міри продуктивності обох типів. Таким чином, внесені в захист інвестиції y впливають і на зменшення уразливостей, і на зменшення загрози. Ступінь цього впливу при заданій величині y залежить в першому випадку – від початкової уразливості, а в другому – від імовірності нападу. Введені показники продуктивності формують двомірний простір продуктивності, котрий, в залежності від значень v і y, можна поділити на 3 зони:

1) зона низької продуктивності при малих інвестиціях, коли обидві продуктивності малі;

2) зона середньої уразливості, де ПЗУ висока, а ПЗЗ низька;

3) зона високої уразливості, де ПЗЗ висока.

Звичайно, цей поділ носить приблизний характер, границі зон не можуть бути окреслені точно, і дослідження зон може надати лише якісні висновки щодо величин v і y. Розмір y^0 оптимальних інвестицій, при якому прибуток від інвестування досягає максимуму дає рішення оптимізаційної задачі. Одним з результатів такого дослідження є визначення інтервалів значень α і β, в якому $y^0 = 0$ - інвестування недоцільне, оскільки витрати перевищують вартість захищеної інформації.

Цільова функція $i(x,y)$ (2.1) у запропонованій моделі виражає відносну величину завдоної шкоди від реалізації загроз інформації і визначається через співвідношення ресурсів нападу і захисту - x і, відповідно, y.

У функції (2.1) залежність $f(x,y)$ представляє динамічну уразливість на відміну від статичної уразливості $f(x,0)$. Наслідуючи [93], вважається, що $f'_y(x,y)$ визначає продуктивність зменшення уразливості при внесенні інвестицій y в захист, а імовірнісна функція $q'_y(x,y)$ - продуктивність зменшення загрози. Міри обох продуктивностей визначаються параметрами, які входять в ці функції.

Оскільки, припускається, що функції, які входять в (2.1), залежать від співвідношення x і y, в цих виразах достатньо залишити одну змінну. Розглядаючи дії захисту і покладаючи $x=1$, в якості такої змінної оберемо y. В [55] запропоновані два види функції $f(y)$ – степеневі і показникові. Враховуючи, що вони мають схожі форми, обмежимось розглядом степеневої функції (2.5)

Параметри n, c в (2.5) можна розглядати як міри продуктивності зменшення уразливості.

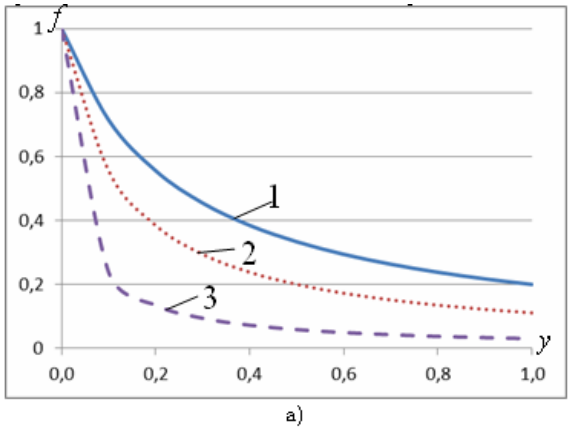
Використовуючи модель [55], в [48] здійснено першу спробу проаналізувати положення різних зон у просторі продуктивності при різних варіантах функцій $f(y)$.

Метою даного етапу роботи є дослідження функцій уразливості та визначення на їх основі продуктивності витрат.

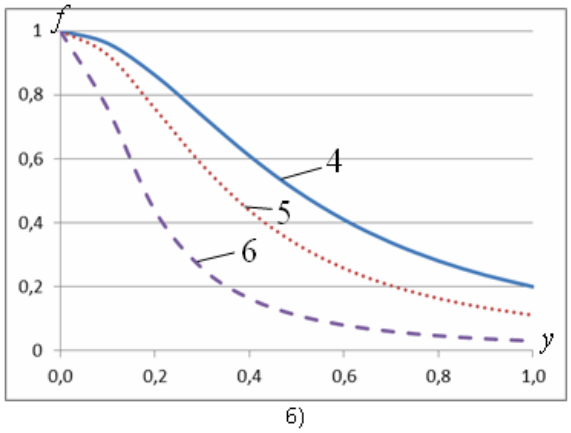
На рис. 2.4, 2.5 показано хід залежностей $f(y)=\frac{1}{1+cy^n}$ при різних n і c. На рис. 2.4 результати скомпоновані так, щоб показати вплив параметра c при різних n, а на рис.2.5 – вплив параметра n при різних c. Видно, наскільки зменшуються значення $f(y)$ при збільшенні c і сталому y і зростають при збільшенні n. Вважається, що $y<1$ — для зламу системи необхідно виділити більше коштів, ніж внесено в захист. Враховуючи, що зменшення $f(y)$ означає зменшення уразливості, можемо оцінити ступінь зростання ПЗУ при збільшенні c і зменшенні n. Цим підкреслюється важливість встановлення значень n і c, котрі відображають об’єктивні характеристики інформаційної системи.

Залежність ПЗУ від розміру інвестицій y визначається крутизною кривої $f(y)$. При дробово-лінійних залежностях зона високої продуктивності обмежується низькими значеннями y (рис. 2.4а). Цим відображається той факт, що в фізичних системах необхідні певні початкові заходи, які не потребують великих витрат, проте можуть суттєво зменшити уразливість. При зростанні розміру інвестицій їх ефективність зменшується, що відповідає відомому економічному закону про зменшення граничної норми прибутку.

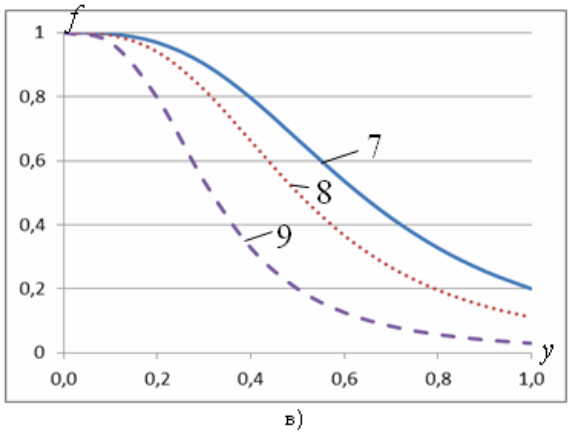
При дробово-нелінійних залежностях $f(y)$ (рис. 2.4б-в) зона високої продуктивності ПЗУ відповідає середнім значенням y. При високому рівні нелінійності ($n \geq 3$) в початковій області $y \geq 0$ з'являється «поличка» (рис. 2.4в), яка свідчить про те, що існує певний мінімальний рівень витрат, котрий приносить відчутний ефект у зменшенні уразливості. Це відповідає висновку [93] про наявність зони низької продуктивності, в якій $y^0 = 0$.



а)

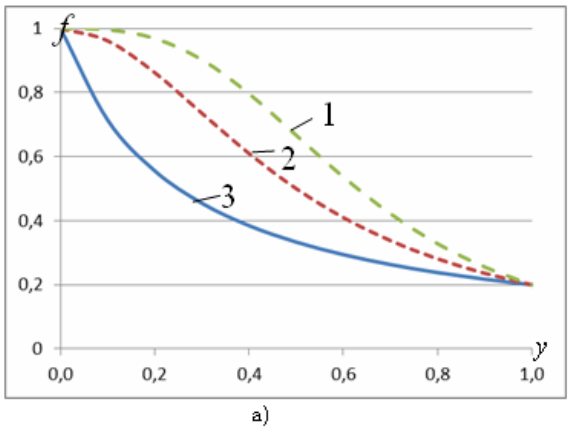


б)

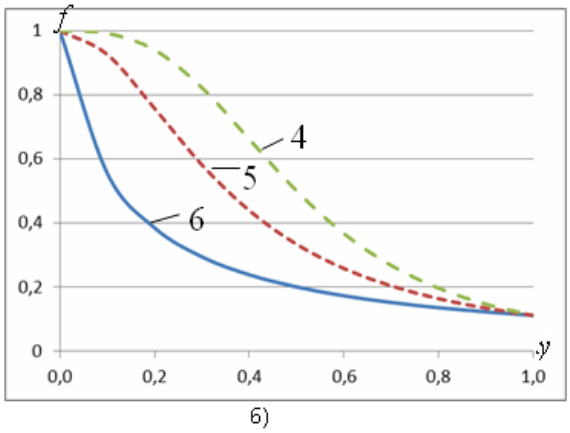


в)

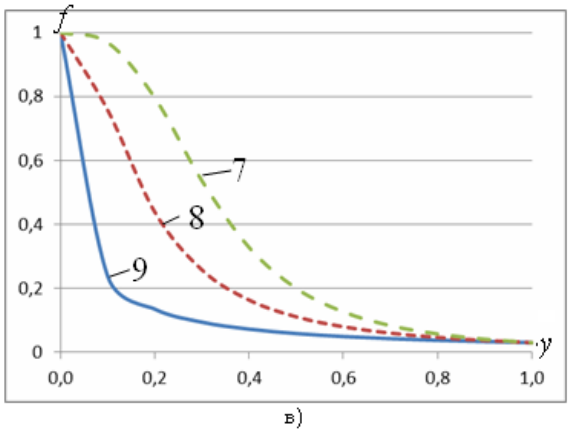
Рис.2.4. Вплив параметра c в залежностях $f(y)=\frac{1}{1+cy^n}$ при різних n: а) $n=1$; б) $n=2$; в) $n=3$; **1, 4, 7** — $c=4$; **2, 5, 8** — $c=8$; **3, 6, 9** — $c=32$



а)



б)



в)

Рис.2.5. Вплив параметра n в залежностях $f(y)=\frac{1}{1+cy^n}$ при різних c: а) $c=4$; б) $c=8$; в) $c=32$; **1, 4, 7** — $n=4$; **2, 5, 8** — $n=8$; **3, 6, 9** — $n=32$

На рис. 2.6, 2.7 показано хід похідних $f'(y)$ при різних значеннях n і c.

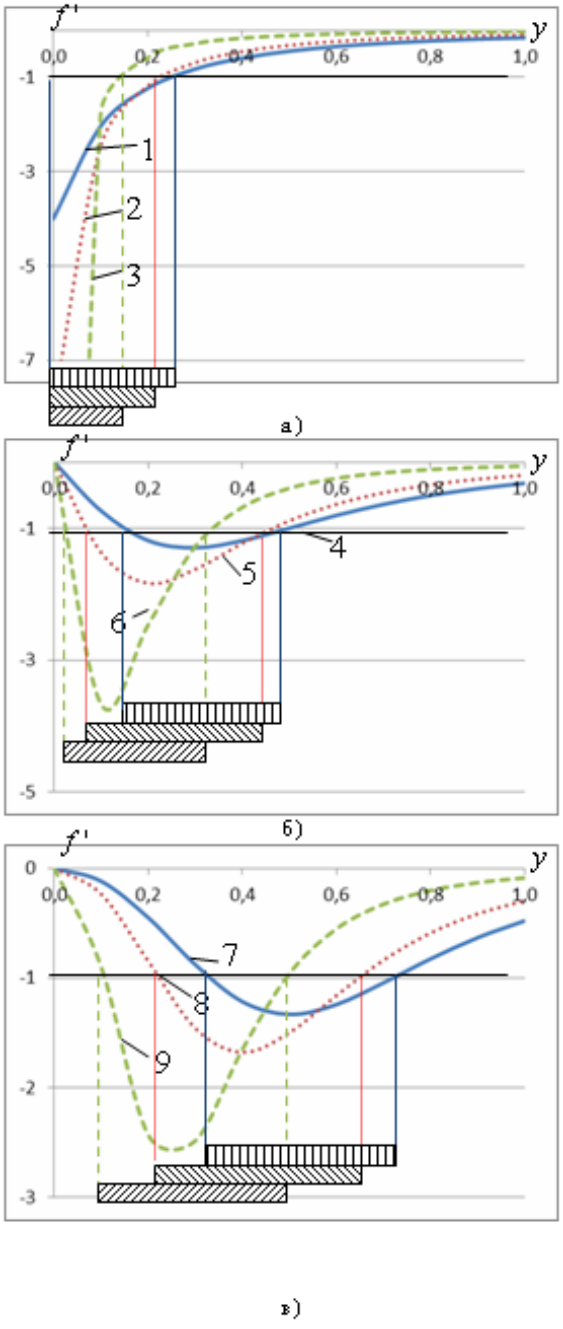


Рис.2.6. Крутизна функцій $f'(y)$ в залежності від c при різних n: а) $n=1$; б) $n=2$; в) $n=3$; **1, 4, 7** — $c=4$; **2, 5, 8** — $c=8$; **3, 6, 9** — $c=32$

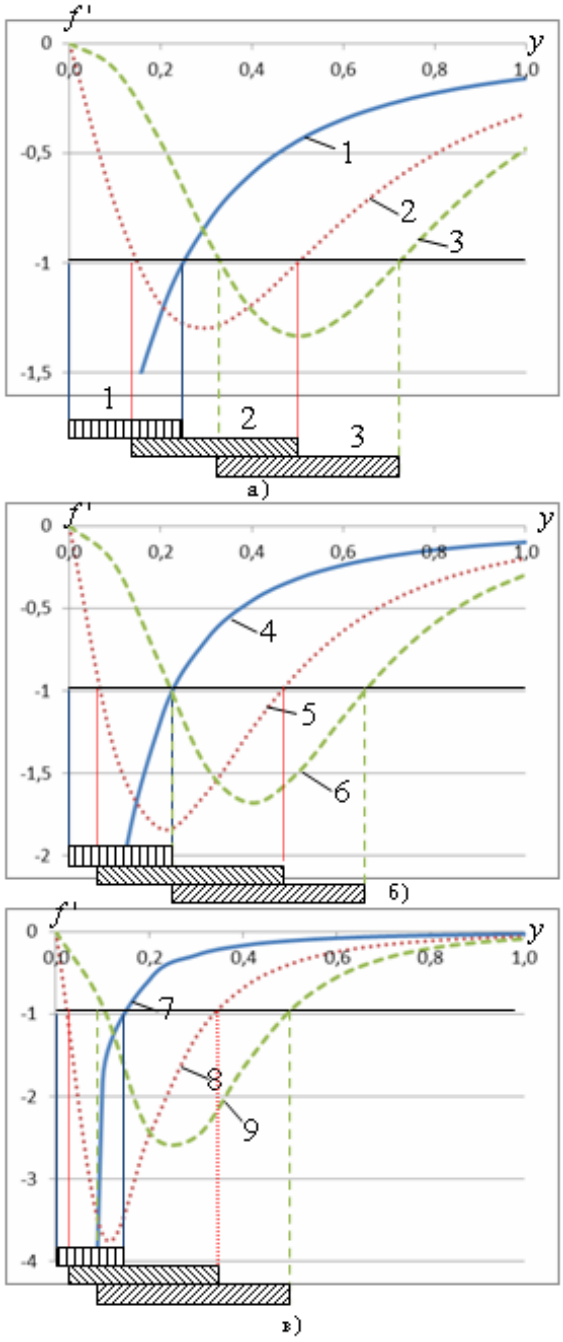


Рис.2.7. Крутизна функцій $f'(y)$ в залежності від n при різних c: а) $c=4$; б) $c=8$; в) $c=32$; **1, 4, 7** — $n=4$; **2, 5, 8** — $n=8$; **3, 6, 9** — $n=32$

За даними цих рисунків визначено зони високої ПЗУ, границі яких встановлено значенням $f'(y)=-1$ (рис. 2.7а), де зони показані штриховкою.

Аналізуючи положення зон в залежності від параметрів n і c, відзначено такі закономірності.

При $n=1$ (зона 1) ліва границя співпадає зі значенням $y=0$. В цій точці крутизна $f'(y)$ і, відповідно, ПЗУ досягають найбільших значень, поступово зменшуючись і прямуючи до нуля при зростанні y.

При $n=2$ (зона 2) і $n=3$ (зона 3) ліва границя зміщується вправо, свідчачи про те, що при дробово-нелінійній формі динамічної уразливості невеликі за розміром інвестиції в захист неефективні. В тому ж напрямку зміщується права границя. Зміщення інтервалів зростає зі збільшенням n і зменшується при збільшенні c. Таким чином, можлива ситуація, коли зміщення інтервалів при одночасній зміні значень n і c буде частково компенсуватись за умови їх різнобічної зміни. Повна компенсація не може бути досягнута, оскільки ці параметри мають різний вплив на залежність $f(y)$: при збільшенні c значення $f(y)$ узгоджено зменшуються при всіх y (рис. 2.4), а при збільшенні n в початковій області значень y змінюється форма залежності – з'являється «поличка» (рис. 2.5). Найбільші значення ПЗУ слабо залежать від n і суттєво – від c: при збільшенні $n \geq 2$ максимальне значення $|f'(y)|$ залишається майже незмінним (рис. 2.7), а при збільшенні c значно зростає, хоча це зростання зменшується при збільшенні n (рис. 2.6).

Розрахунок ПЗУ дозволяє визначити вплив внесення інвестицій на показники ефективності систем захисту.

В системі, яка містить декілька об'єктів з різними характеристиками $f_k(x,y)$ (k - номер об'єкта) на ПЗУ буде впливати також відносна цінність інформації на об'єктах [113]. У випадку двох об'єктів цільова функція, яка визначає розмір завданої шкоди від реалізації загроз інформації, має вигляд: $i(y_1,y_2)=g_1 f_1(y_1)+g_2 f_2(y_2)$.

Цю функцію можна представити у вигляді просторової фігури (рис. 2.8) [30]. Види функціональних залежностей на цьому рисунку вибрані довільно, оскільки він має лише ілюстративний характер. Улоговина просторової фігури

визначає мінімальні значення $i_{\min}(y_1, y_2)$ при різних величинах сумарного ресурсу захисту $y_1 + y_2 = Y$ і одночасно дозволяє знайти оптимальний розподіл (y_1^0, y_2^0) для кожного значення Y та напрямок зміни цього розподілу при збільшенні Y, котрий, в свою чергу, визначає ПЗУ. Вона показана на рис. 2.8 жирною лінією. Це лінія найшвидшого спуску, котру можна поділити на 3 дільниці:

1 — всі кошти вкладають в перший об'єкт, $y_2 = 0$;

2 — y_1 зменшується, а y_2 зростає (перерозподіл ресурсів);

3 — y_1 та y_2 зростають.

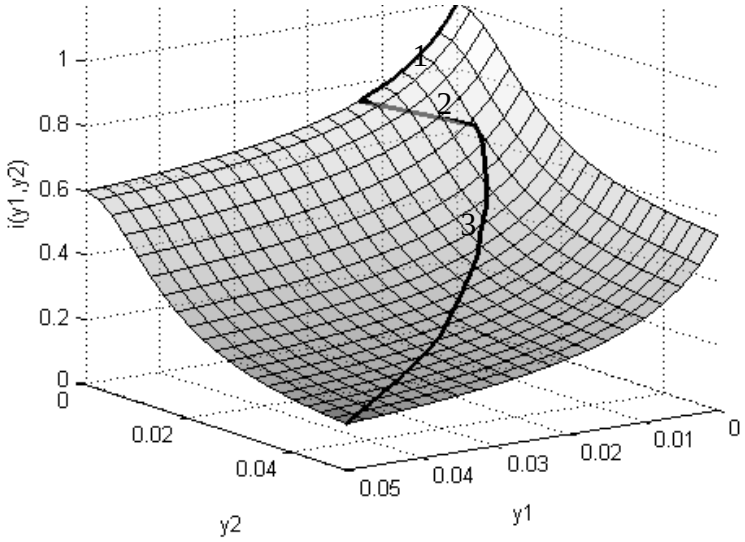


Рис. 2.8. Вид залежності $i(y_1, y_2)$ при $g_1 = g_2 = 0{,}5$, $f_1(y_1) = \dfrac{1}{1+16y_1}$, $f_2(y_2) = \dfrac{1}{1+16y_2^2}$.

В загальному випадку цільова функція для системи з двох об'єктів має вигляд:

$$i(y_1, y_2) = g_1 f_1(y_1) + g_2 f_2(y_2).$$

Оптимальний розподіл ресурсів $\{y_1^0, y_2^0\}$ визначається умовою: продуктивність зменшення завданої шкоди, тобто величина $di(y_1^0, y_2^0)$ повинна бути максимальною порівняно з усіма іншими розподілами.

Прибуток від внесення інвестицій визначається виразом

$$b(y) = 1 - i(y) - y = j(y) - y,$$

де $i(0) = 1$ - розмір завданої шкоди від реалізації загроз при відсутності інвестицій, $j(y)$ - відносна вартість захищеної інформації. Оскільки $b'(y) = |i'(y)| - 1$, то продуктивність зменшення втрат визначає також продуктивність збільшення прибутку.

Ще один показник – рентабельність інвестицій $R(y) = \frac{b(y)}{y}$. Продуктивність цього показника: $R'(y) = \frac{b'(y)y - b(y)}{y^2}$. Вона також визначається похідною $b'(y)$.

Проведений аналіз висвітлює той факт, що в функції $f(x, y)$ переплелися два важливих поняття інформаційної безпеки – уразливість системи і продуктивність внесення ресурсів на її захист. Їх показники тісно пов’язані між собою. Перший з них визначається видом функціональної залежності – в степеневих функціях, в основному, значенням n, яке характеризує ступінь нелінійності. При заданому значенні n другий показник – коефіцієнт c, який впливає на кривизну залежності, не міняючи суттєво її форми. Значущість цих показників зростає в складних системах з великою кількістю об’єктів, котрі містять різні обсяги інформації, мають різні імовірності нападу і відрізняються уразливістю і продуктивністю витрат. Правильна оцінка значень n_k і c_k в таких системах може суттєво вплинути на прийняття рішення про розподіл ресурсів між об’єктами.

2.4. Пошук оптимального рішення задач умовної оптимізації в сфері інформаційної безпеки

Пошук оптимального значення цільової функції (2.1) ведеться в умовах обмежень, які накладаються на ресурси нападу і захисту: $\sum_{k=1}^{l} x_k = X$, $\sum_{k=1}^{l} y_k = Y$. Це задача умовної оптимізації.

Оптимізація функції $i(x, y)$ ведеться по одній із змінних – x або y – в залежності від того, для якої із сторін (нападу чи захисту) шукається розв'язок. Рішення знаходиться одним з аналітичних методів оптимізації [8,13,19,27,38,42-44,63,70,75,77,83]. В найпростіших випадках використовуються методи Якобі або Лагранжа, в більш складних – методи програмування.

Розглянуто систему, яка містить два об'єкти – в цьому випадку розв'язок можна проілюструвати графічно, що дасть можливість прояснити сутність задачі. Рішення шукається для сторони нападу, тобто знаходиться $\max_x i(x)$ при сталому значенні y. Ресурси нападу знаходяться в інтервалі $X \in [0,3]$, ресурси захисту розподілені між об'єктами рівномірно: $y_1 = y_2 = 1$, $Y = y_1 + y_2 = 2$.

Об'єкти мають однакову уразливість у формі $f(x) = \frac{x}{1+x}$ і відрізняються відносною цінністю інформації інформації: $g_1 \neq g_2$, $g_1 + g_2 = 1$. Предметом пошуку є розподіл $\{x_1, x_2\}$.

Цільова функція має вигляд

$$i(x_1, x_2) = g_1 \frac{x_1}{1+x_2} + g_2 \frac{x_2}{1+x_2}. \qquad (2.7)$$

Її оптимальне значення $i(x_1, x_2) \to \max$ (для функції $i(y)$ оптимумом буде $i(y_1, y_2) \to \min$) досягається в точці дотику лінії рівня $i(x_1, x_2) = C = const$, яка визначає величину завданої шкоди від реалізації загроз інформації на обох об'єктах при різних варіантах розподілу ресурсів нападу між об'єктами, і

обмежувальної прямої $H(x) = x_1 + x_2 = X$, яка визначається загальною величиною ресурсів нападу.

Залежність $i(x_1, x_2)$ зображена на рис.2.9. Фізичний зміст дана фігура має в першому октанті (на рисунку зображена суцільною лінією).

Нахил кривих 1 і 2 на рис.2.9 залежить не лише від значень x_1 та x_2, а й від відносної цінності інформації g_1 та g_2, оскільки розмір завданої шкоди від реалізації загроз на об'єкті, на якому відносна цінність інформації менша, зростатиме по відношенню до вкладених ресурсів нападу повільніше (рис.2.10).

Лінії рівня $i(x_1, x_2) = g_1 \frac{x_1}{1 + x_1} + g_2 \frac{x_2}{1 + x_2} = C$ отримано в результаті перерізу просторової фігури, зображеної на рис.2.9, площинами, паралельними площині $x_1 0 x_2$.

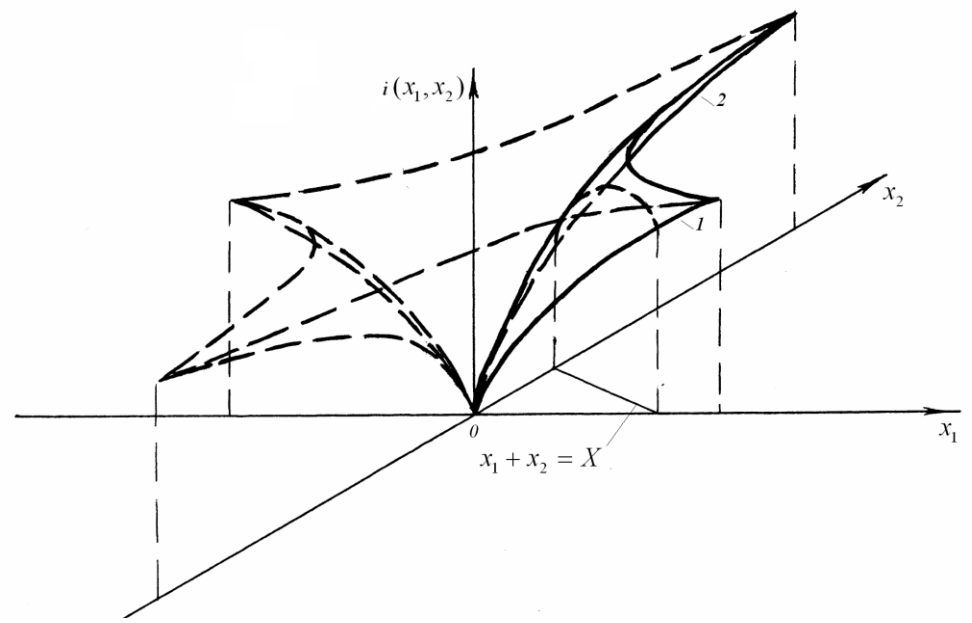


Рис.2.9. Залежність величини завданої шкоди від реалізації загроз інформації від розподілу ресурсів нападу між об'єктами

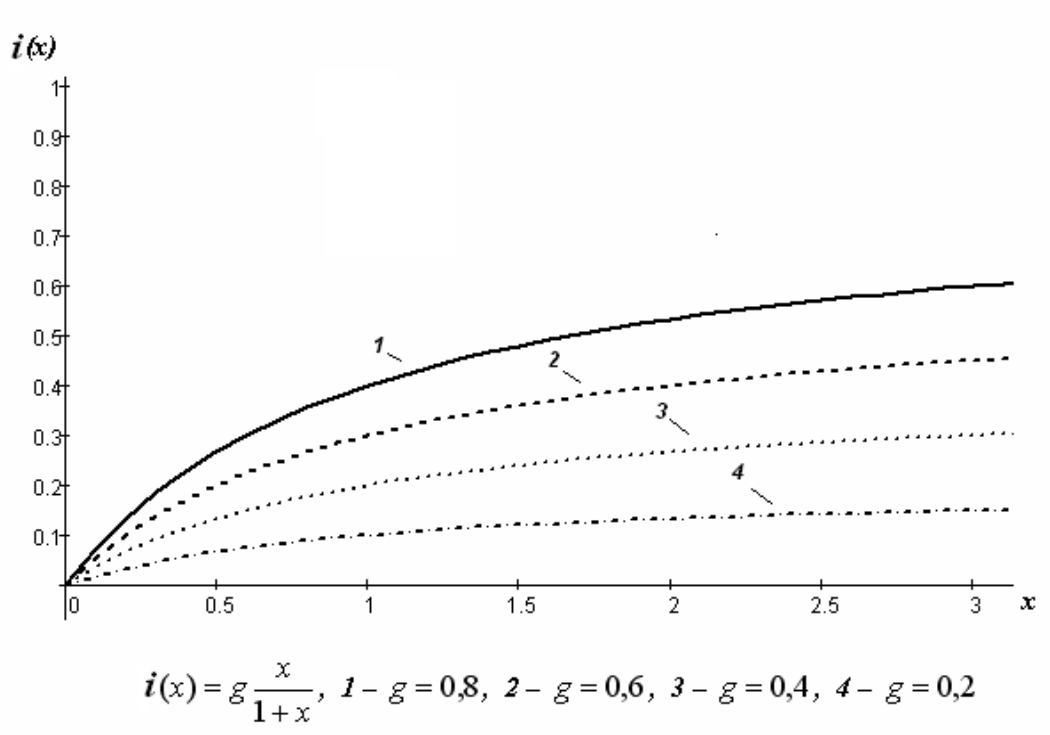


Рис.2.10. Залежність величини завданої шкоди від реалізації загроз інформації від ресурсів нападу при різних значеннях g

Дотик кривої $i(x_1, x_2) = C$ і прямої $H(x)$ досягається двома шляхами. Якщо в умові задано кількість ресурсів X, тобто положення прямої $H(x)$, то необхідно рухати лінію рівня $i(x_1, x_2) = C$ в напрямку прямої $H(x)$ до досягнення дотику. Точка дотику буде визначати максимальну величину завданої шкоди від реалізації загроз інформації при заданому значенні X. Якщо ж ставиться задача визначення необхідної кількості ресурсів для отримання несанкціонованого доступу до інформації (вона задається кривою $i(x_1, x_2) = C$), то лінія рівня залишається нерухомою, а пряму $H(x)$ слід рухати в напрямку кривої $i(x_1, x_2) = C$, і при дотику визначити величину необхідних ресурсів X.

На рис.2.11 зображено оптимальні розв'язки при обмеженні $X = x_1 + x_2 = 1$ залежно від відносної цінності інформації g_1 та g_2 на об'єктах.

З рис.2.11 видно, що оптимальне значення $i(x_1, x_2)$ для $\frac{g_1}{g_2} = \frac{0{,}8}{0{,}2}$ досягається при $x_1^{\,0} = 1$ та $x_2^{\,0} = 0$ (тобто напад вкладає всі ресурси в більш цінний обєкт), і як випливає з (2.7), становить 0,4 [109].

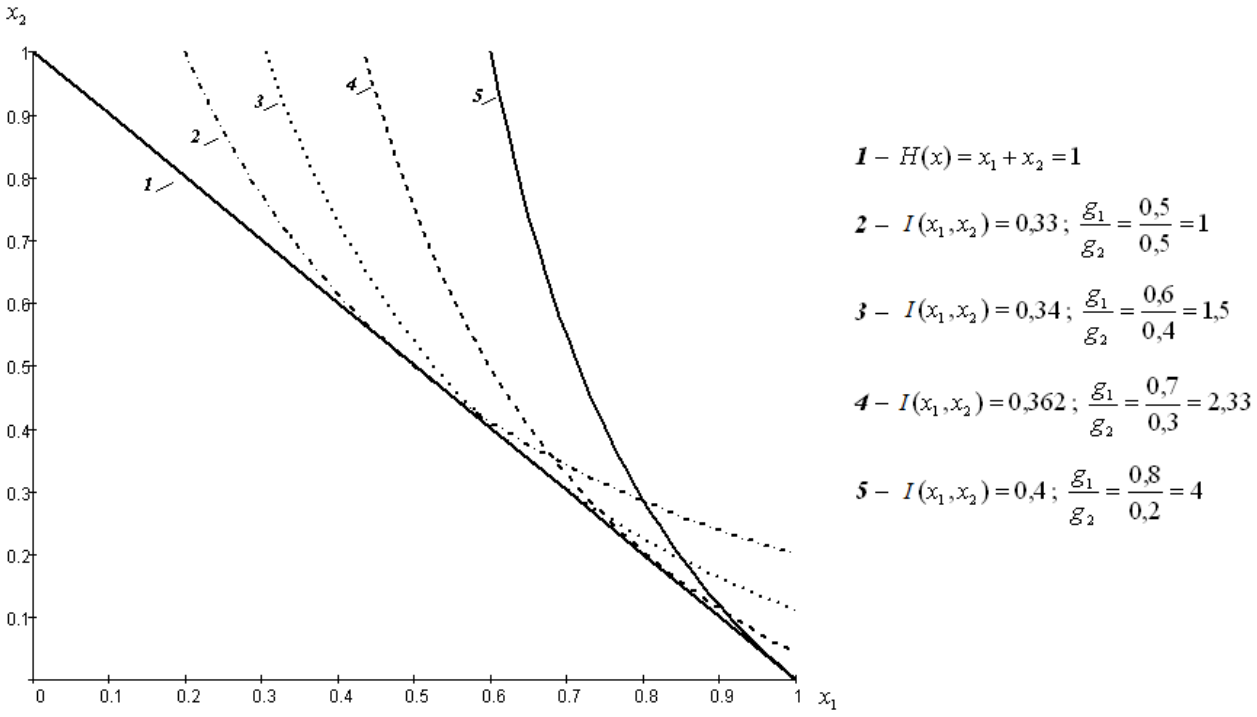


Рис.2.11. Геометрична інтерпретація досягнення оптимуму в системі з двох об’єктів при різних значеннях g_1, g_2

Один із аналітичних методів розв’язку поставленої задачі – метод Якобі – у випадку двох змінних дозволяє, використовуючи обмежувальне рівняння $x_1 + x_2 = X$, звести задачу на умовний екстремум функції двох змінних до задачі на безумовний екстремум функції однієї змінної:

$$i(x_1) = g_1 \frac{x_1 / y_1}{1 + x_1 / y_1} + g_2 \frac{(X - x_1) / y_2}{1 + (X - x_1) / y_2}.$$

Умовою оптимальності є $\frac{di(x_1)}{dx_1}=0$. Проте пошук значення $x_1^{\,0}$ приводить до необхідності розв'язку громіздкого алгебраїчного рівняння другого ступеня, при дробово-нелінійній формі функції $i(x, y)$ – алгебраїчного рівняння більш високого рівня. Таким чином, навіть у випадку двох об'єктів цей метод приводить до досить складної обчислювальної процедури.

Звертаючись до другого з аналітичних методів, методу множників Лагранжа, записано функцію

$$L(x_1, x_2, \lambda) = g_1 \frac{x_1 / y_1}{1 + x_1 / y_1} + g_2 \frac{x_2 / y_2}{1 + x_2 / y_2} + \lambda(x_1 + x_2 - X),$$

де введена третя змінна – невідомий множник Лагранжа λ.

$$\begin{cases} \dfrac{\partial L}{\partial x_1} = g_1 \dfrac{c_1 / y_1}{\left(x_1 / y_1 + c_1\right)^2} + \lambda = 0 \\ \dfrac{\partial L}{\partial x_1} = g_2 \dfrac{c_2 / y_2}{\left(x_2 / y_2 + c_2\right)^2} + \lambda = 0 \\ \dfrac{\partial L}{\partial \lambda} = x_1 + x_2 - X = 0 \end{cases}$$

Звідси отримано вирази для оптимальних значень x_1^0, x_2^0 і значення λ:

$$x_1^0 = \sqrt{\frac{c_1 g_1 y_1}{\lambda}} - c_1 y_1$$

$$x_2^0 = \sqrt{\frac{c_2 g_2 y_2}{\lambda}} - c_2 y_2$$

$$\lambda = \frac{\left(\sqrt{c_1 g_1 y_1} + \sqrt{c_2 g_2 y_2}\right)^2}{\left(X + c_1 y_1 + c_2 y_2\right)^2}$$

Наведені вирази легко розповсюдити на довільну кількість об'єктів.

При розгляді дій захисту метод Лагранжа приводить до аналогічних виразів, які в загальному випадку мають такий вигляд:

$$y_k^0 = \sqrt{\frac{g_k x_k}{\lambda c_k}} - \frac{x_k}{c_k};\ \lambda = \frac{\left(\sum_k \frac{g_k x_k}{c_k}\right)^2}{\left(\sum_k \left(x_k \middle/ c_k\right) + Y\right)^2}.$$

Приклад застосування методу Лагранжа.

Нехай $c_1 = c_2 = 1$, $y_1 = y_2 = 1$, $X = 1$. Знайти оптимальний розподіл ресурсів нападу в залежності від відносної цінності інформації на об'єктах.

I варіант

$g_1 = g_2 = 0{,}5$

Підставивши ці величини у вирази для оптимальних значень x_1^0, x_2^0 і значення λ, отримано:

$\lambda = 0{,}22$;

$x_1^0 = x_2^0 = 0{,}5$.

II варіант

$g_1 = 0{,}4$, $g_2 = 0{,}6$

$\lambda = 0{,}22$; $x_1^0 = 0{,}35$, $x_2^0 = 0{,}65$

III варіант

$g_1 = 0{,}2$, $g_2 = 0{,}8$

$\lambda = 0{,}2$; $x_1^0 = 0$, $x_2^0 = 1$

У перших двох варіантах ресурси захисту слід розподіляти між усіма об'єктами, а в третьому – зосередити на другому об'єкті. Перший варіант дає тривіальний результат і може розглядатись, як контрольний.

2.5. Застосування оптимальних змішаних стратегій

У попередньому параграфі розглянуто ситуацію, коли захист кожного каналу здійснюється автономно – засобами, які діють тільки в цьому каналі і нейтралізують загрози, характерні для цього каналу (комп'ютерні віруси – програмні засоби, акустичний канал – засоби зашумлення). Проте деякі заходи і

засоби діють одночасно в декількох каналах (контроль периметру, системи ідентифікації), що необхідно враховувати при оцінці їх ефективності і обґрунтованості витрат.

Цю ситуацію проілюстровано за допомогою табл. 2.3, де приведені імовірності p_{rs} блокування витоку інформації по s-му каналу при застосуванні r-го засобу захисту.

Таблиця 2.3

Імовірнісні характеристики засобів захисту

Стратегії захисту	Канали витоку (стратегії нападу)				$\min_s p_{rs}$
	акустичний, $(s=1)$	оптичний, $(s=2)$	радіотехнічний, $(s=3)$	електричний, $(s=4)$	
Контроль периметру $(r=1)$	0,36	0,5	0,55	0,4	0,36
Системи ідентифікації та аутентифікації $(r=2)$	0,4	0,6	0,35	0,7	0,35
Екранування обладнання $(r=3)$	0	0	0,9	0,4	0
Системи зашумлення $(r=4)$	0,8	0	0	0	0
$\max_r p_{rs}$	0,8	0,6	0,9	0,7	

За даними таблиці не можна однозначно сказати, які з технічних заходів слід використовувати. Якщо перші дві стратегії (контроль периметру $(r=1)$, системи ідентифікації та аутентифікації $(r=2)$) з певними ймовірностями можуть протидіяти усім загрозам, то використання спеціалізованого обладнання екранованого обладнання $(r=3)$, активних систем зашумлення $(r=4)$) направлено на блокування лише конкретних загроз, однак забезпечує їх нейтралізацію з вищою ймовірністю.

Проведені розрахунки показують, що $\max_r \min_s p_{rs} \neq \min_r \max_s p_{rs}$, тобто гра сідлової точки немає, і оптимальне рішення відповідає змішаній стратегії $S_Y^0 = (P_1, P_2, P_3, P_4)$, $\sum_{i=1}^{4} P_i = 1$. Суть такого рішення полягає у тому, що одночасно

застосовуються декілька запропонованих стратегій у певному співвідношенні. Наприклад, використовуючи декілька технічних засобів захисту інформації, направлених на нейтралізацію різних загроз, можна значно знизити величину завданої шкоди від реалізації загроз інформації, ніж у випадку застосування лише одного виду засобів. У такій постановці задачі, визначаються пропорції, в яких використовуються різні види засобів захисту [13].

Задача лінійного програмування для сторони захисту має вигляд:

$$\frac{1}{v} = a_1 + a_2 + a_3 + a_4 \to \max$$

$$\begin{cases} 0{,}36a_1 + 0{,}4a_2 + 0a_3 + 0{,}8a_4 \le 1 \\ 0{,}5a_1 + 0{,}6a_2 + 0a_3 + 0a_4 \le 1 \\ 0{,}55a_1 + 0{,}35a_2 + 0{,}9a_3 + 0a_4 \le 1 \\ 0{,}4a_1 + 0{,}7a_2 + 0{,}4a_3 + 0a_4 \le 1 \end{cases},$$

де $a_i = \frac{P_i}{v}$, v - ціна гри.

За допомогою симплекс-таблиць знаходяться оптимальні змішані стратегії сторін.

Для сторони захисту рішення гри: $S_Y^0 = (0{,}5;0{,}29;0{,}05;0{,}16)$.

Таким чином, прийнято наступні рекомендації: використовувати запропоновані технічні засоби у співвідношенні: 0,5:0,29:0,05:0,16. При цьому середня ймовірність нейтралізації загроз буде максимальна і становитиме 0,42.

Використання змішаних стратегій не веде до збільшення виграшу, оскільки змішана стратегія не може дати більше, ніж будь-яка чиста стратегія. Перевага використання змішаних стратегій у тому, що вони породжують невизначеність для суперника. Однак доцільність використання таких стратегій існує лише в разі можливості повторного вибору чистої стратегії при почерговому здісненні ходів обома сторонами.

Висновки до 2 розділу

1. У процесі проведення дослідження визначено, що використання розробленої математичної моделі багаторівневої багаторубіжної системи захисту інформації, дає можливість оптимізувати використання ресурсів захисту в складних інформаційних структурах, які відрізняються кількістю об’єктів, розташуванням перешкод, їх уразливістю, розподілом інформації по об’єктах при різних співвідношеннях ресурсів нападу і захисту.

2. В результаті досліджень обгрунтовано вибір цільової функції моделі та функціональних залежностей, що входять до складу цільової функції. Особливу увагу приділено функції динамічної уразливості об’єктів, що описує різні типи систем. Встановлено, що дробово-лінійні функції описують уразливість інформації, що зберігається на матеріальних носіях, де збільшення ресурсів захисту (на організаційні та інженерно-технічні заходи та засоби захисту) в початковій області значень y приводить до монотонного, майже пропорційного зменшення уразливості і як результат – зменшення величини завданої шкоди. Дробово-нелінійні функції відображають властивості інформації, що циркулює у комп’ютерних системах, де для подолання перешкоди потрібно витратити значні ресурси.

3. Визначення зон найбільшої продуктивності зменшення уразливості і продуктивності зменшення загрози в складних системах захисту інформації дозволяє розрахувати об’єм ресурсів, що забезпечують досягнення заданих значень продуктивностей та підвищення ефективності використання внесених коштів.

РОЗДІЛ 3
РОЗРОБКА МЕТОДІВ ДИНАМІЧНОГО УПРАВЛІННЯ РЕСУРСАМИ

3.1. Метод оптимального розподілу інвестицій між елементами систем захисту інформації

Комплексні системи захисту являють собою складні багаторівневі багаторубіжні структури. Як приклад розглянуто систему, котра містить декілька об'єктів, і в кожному з них може відбуватись витік по декількох каналах. Оптимізація розподілу ресурсів повинна вестись на двох рівнях: між окремими об'єктами і для кожного об'єкта – між окремими каналами. Цільова функція має вигляд:

$$i(x,y)=\sum_{k=1}^{l}\sum_{s=1}^{t} i_{ks}(x,y)=\sum_{k=1}^{l}\sum_{s=1}^{t} g_k p_{ks} f_{ks}(x_{ks},y_{ks}), \qquad (3.1)$$

де k – номер об'єкта, s – номер каналу. Для захисту метою є знаходження розподілу $\{y_{ks}\}$, який відповідає умові $\min\limits_{y} i(x,y)$ при будь-яких варіантах розподілу ресурсів нападу $\{x_{ks}\}$, $\sum\limits_{k=1}^{l}\sum\limits_{s=1}^{t} x_{ks}=X$.

Оскільки комплексні системи захисту інформації є багаторубіжними [32,35,106], то оптимізація розподілу ресурсів повинна вестись на кожному рівні. Методику пошуку оптимального розподілу ресурсів розглянуто на двох рівнях: між об'єктами захисту, а також між можливими каналами витоку на кожному об'єкті.

Якщо інформація вилучається по декількох каналах, то $i_k(x,y)=\sum\limits_{s=1}^{t} i_{ks}(x,y)$, де $s=\overline{1,t}$ - номер каналу. Серед величин, які стоять в правій частині виразу (3.1) з певною мірою точності можна розрахувати лише вагові коефіцієнти g_k, які

характеризують відносну цінність інформації на кожному з об'єктів [53]. Інші величини в умовах відсутності статистичної інформації можуть бути задані в розрахунок методом експертної оцінки. Ключовим моментом при цьому являється вибір залежностей $f_k(x, y)$, який суттєво впливає на результат розрахунку. Задача ускладнюється тим, що ці залежності для різних об'єктів захисту інформації (електронні системи, паперова документація, персонал) можуть мати різний характер, який визначається специфікою об'єкта (це справедливо і для каналів).

Метою дослідження є знаходження розподілу $\{y_{ks}\}$ ресурсів захисту $\sum_k \sum_s y_{ks} = Y$, який відповідає обраному критерію. При цьому необхідно врахувати всі можливі варіанти розподілу $\{x_{ks}\}$ ресурсів нападу в межах $\sum_k \sum_s x_{ks} \le X$.

Для прикладу розглянуто випадок, коли залежності величини завданої шкоди від реалізації загроз інформації від співвідношення ресурсів нападу і захисту відрізняються на різних об'єктах і різних каналах. В умовах невизначеності необхідно обрати критерій оптимальності по $i(x, y)$. При $Z >> 1$ напад здійснюється одночасно на декілька об'єктів, число можливих варіантів дій сторони нападу збільшується і розрахунки ускладнюються. У випадку, коли сідлова точка відсутня, оптимальний розподіл $\{y_k\}$ визначається відповідно до пріоритетів, які встановлює менеджмент.

Пошук оптимального рішення ведеться за допомогою методу динамічного програмування Р. Белмана [7,85,87], і процедуру розбито на два етапи. На першому знаходиться оптимальний розподіл $\{y_k\}$ між об'єктами, на другому – між каналами на кожному об'єкті. Опис методики проілюстровано на розгляді другого етапу.

Об'єкт має декілька каналів можливого витоку інформації, причому величина завданої шкоди від реалізації загроз інформації по s-му каналу

визначається залежністю $f_s(x, y)$. Для прикладу розглянуто три канали, для яких залежності $f_s(x, y)$, $s = \overline{1,3}$ мають вигляд (рис. 3.1).

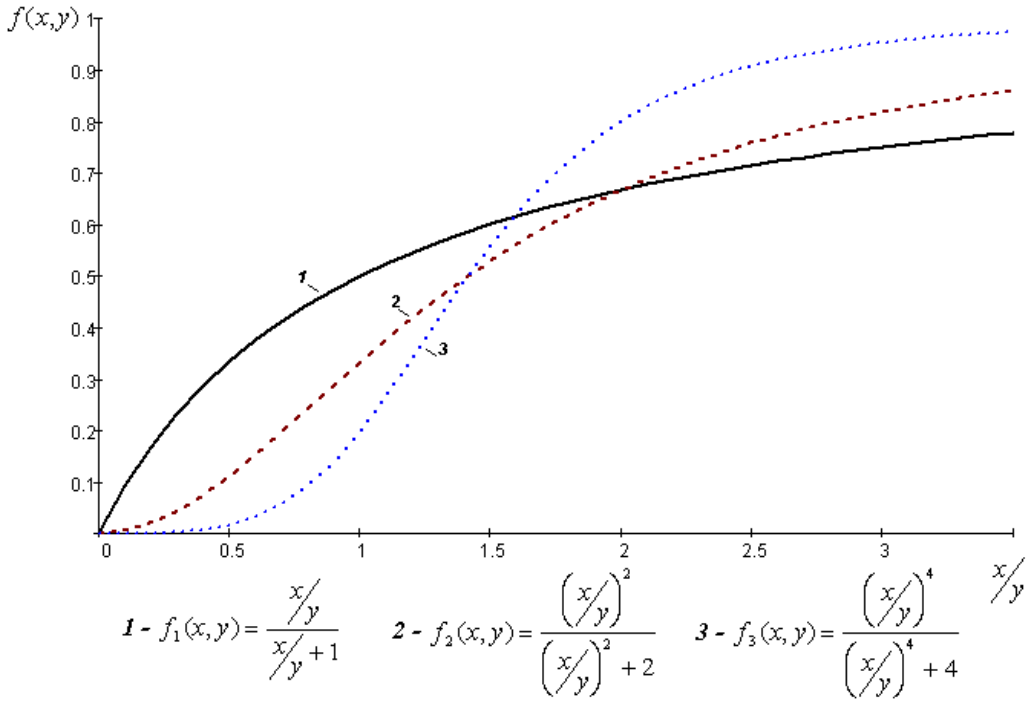


Рис.3.1. Залежність величини завданої шкоди від реалізації загроз інформації від співвідношення ресурсів для трьох каналів

Задача формулюється наступним чином: знайти $\min_y \sum_{s=1}^{t} i_s(x, y)$, $\sum_{s=1}^{t} x_s = X$. Алгоритм пошуку розподілу $\{y_s\}$ представлено у наступній послідовності [107]:

1. Розподіл $\{y_s\}$ ресурсів захисту приймається у такій пропорції: $\{y_s\} = 0{,}0167 : 0{,}0167 : 0{,}0167$ (рівномірний розподіл), $\sum_{s=1}^{t} y_s = Y = 0{,}05$, або 5% від вартості інформації [2,96-98].

2. Переходячи до дискретного програмування, розраховуються значення $f_s(x)$ для низки значень виділених ресурсів x_s нападу.

3. Користуючись методом Белмана для прийнятого розподілу $\{y_s\}$ ресурсів захисту, знаходиться оптимальний для нападу розподіл $\{x_s\}$,

послідовно максимізуючи величини завданої шкоди від реалізації загроз інформації $i_s(x)$ за зворотною схемою. Для цього записано рівняння станів:

$$d_{s-1} = d_s - x_s,$$

де s $(s = \overline{1,t})$ - номер кроку, що відповідає номеру каналу, d_s - параметр стану, що визначає кількість ресурсів, яка залишились після s-кроку, d_{s-1} - відповідно, кількість ресурсів, що може бути використана на s-му кроці. Управління на s-му кроці (вибір величини x_s) задовольняють умові $0 \le x_s \le d_{s-1}$.

За принципом оптимальності Белмана, нападу потрібно вибирати такі значення кількості ресурсів x_s, щоб для будь-яких можливих станів d_{s-1} отримати максимум цільової функції:

$$i^{(s)}(d_{s-1}) = \max_{0 \le x_s \le d_{s-1}} \left\{ f_s(x_s) + i^{(s+1)}(d_s - x_s) \right\}, \qquad (3.2)$$

де $i^{(s)}(d_{s-1})$ - максимальна величина завданої шкоди від реалізації загроз, яка може бути завдана при оптимальному розподілі d_{s-1} ресурсів на всіх кроках, включаючи s-й. Відповідне значення x_s, за якого досягається максимум функції (3.2), являється умовним оптимальним рішенням на s-му кроці і позначається $x_s^0(d_{s-1})$.

Рухаючись від останнього кроку, поступово знаходиться $i^{(1)}(d_0)$ - умовний максимум цільової функції за t кроків при різних значеннях d_0. Оптимальне значення шукається за формулою: $i_s^0 = \max_{0 \le d_0 \le X} \left\{ i^{(1)}(d_0) \right\}$, що визначає максимальну величину завданої шкоди від реалізації загроз при оптимальному розподілі ресурсів нападу між t каналами.

Оптимальний розподіл $x^0 = (x_1, x_2, ..., x_t)$ ресурсів нападу отримано за формулами: $x_1^0 = x_1^0(d_0)$, $x_s^0 = x_s^0(d_{s-1} - x_{s-1}^0)$, $x_t^0 = x_t^0(d_{s-1} - \sum_{s=1}^{t-1} x_s)$.

Для прикладу розглянуто три канали витоку інформації $s=\overline{1,t}=\overline{1,3}$, $X=1$, крок дискретних значень $\Delta x=0{,}005$ та записано задачу динамічного програмування: $\max\limits_{x_s}\{f_1(x_1)+f_2(x_2)+f_3(x_3)\}$, $x_1+x_2+x_3=1$, $x_s\in\{0;0{,}005;0{,}01;0{,}015;0{,}02;0{,}025;0{,}03;0{,}035;0{,}04;0{,}045;0{,}05\}$. Оптимальний розподіл $\{x_s\}$ ресурсів нападу знайдено згідно (3.2). Для цього заповнено табл. 3.1 та визначено максимальну величину завданої шкоди від реалізації загроз:

$$\max i_1(d_0)=\max\{0{,}054;0{,}052;0{,}053;0{,}056;0{,}062;0{,}079;0{,}103;0{,}132;0{,}165;0{,}197;0{,}229\}=0{,}229.$$

Таблиця 3.1

Пошук оптимального розподілу ресурсів за методом Белмана

d_{s-1}	x_s	d_s	$s=1$			$s=2$			$s=3$		
			$f_1(x_1)+i^{(2)}(d_1)$	$i^{(1)}(d_0)$	$x_1^0(d_0)$	$f_2(x_2)+i^{(3)}(d_2)$	$i^{(2)}(d_1)$	$x_2^0(d_1)$	$f_3(x_3)+i^{(4)}(d_3)$	$i^{(3)}(d_2)$	$x_3^0(d_2)$
0	0	0	0	0	0	0	0	0	0	0	0
0,005	0,005 0	0 0,005	0,0072+0=0,0072 0+0,0017=0,0017	0,0072	0,005	0,0017+0=0,0017 0+0,000042=0,00042	0,0017	0,005	0,00042+0=0,00042 0+0=0	0,00042	0,005
0,01	0,01 0,005 0	0 0,005 0,01	0,014+0=0,014 0,0072+0,0017=0,0089 0+0,0066=0,0066	0,014	0,01	0,0066+0=0,529 0,0017+0,00042=0,0021 0+0,0034=0,0034	0,0066	0,01	0,0034+0=0,0034 0,00042+0=0,00042 0+0=0	0,0034	0,01
…	…	…	…	…	…	…	…	…	…	…	…
0,05	0,05 0,045 0,04 0,035 0,03 0,025 0,02 0,015 0,01 0,005 0	0 0,005 0,01 0,015 0,02 0,025 0,03 0,035 0,4 0,045 0,05	0,0545+0=0,0545 0,0505+0,0017=0,0522 0,0462+0,0066=0,0528 0,0416+0,0145=0,0561 0,0367+0,0256=0,0623 0,0316+0,0477=0,0793 0,0261+0,0771=0,1032 0,0202+0,1122=0,1324 0,0140+0,1508=0,1648 0,0072+0,1904=0,1976 0+0,2288=0,2288	0,2288	0	0,1080+0=0,1080 0,0939+0,00042=0,0943 0,0794+0,0034=0,0828 0,0648+0,0111=0,0759 0,0505+0,0256=0,0761 0,0370+0,0477=0,0847 0,0247+0,0771=0,1018 0,0145+0,1122=0,1267 0,0066+0,1508=0,1574 0,0017+0,1904=0,1921 0+0,2288=0,2288	0,2288	0	0,2288+0=0,2288 0,1904+0=0,1904 0,1508+0=0,1508 0,1122+0=0,1122 0,0771+0=0,0771 0,0477+0=0,0477 0,0256+0=0,0256 0,0111+0=0,0111 0,0034+0=0,0034 0,00042+0=0,00042 0+0=0	0,2288	0,05

Оптимальний розподіл: $x_1^0=x_1^0(1)=0$,

$$x_2^0=x_2^0(0{,}05-x_1^0)=x_2^0(0{,}05-0)=x_2^0(0{,}05)=0,$$

$$x_3^0=x_3^0(0{,}05-x_1^0-x_2^0)=x_2^0(0{,}05-0-0)=0{,}05,$$

$$\{x_s^0\}=(0;0;0{,}05).$$

4. Враховуючи прийнятий розподіл $\{x_s^0\}$ ресурсів нападу, проводиться коригування розподілу $\{y_s\}$ ресурсів захисту, збільшуючи y_s найбільш

небезпечного каналу (третій канал), а залишок коштів розподіляючи порівну між двома іншими каналами. Наприклад, $\{y_s\} = 0{,}3;0{,}3;0{,}4$.

5. Описана процедура повторюється до моменту, коли $\max i_s(x)$ не стане мінімальним. Відповідний розподіл $\{y_s^0\}$ вважається оптимальним.

Задачу оптимального розподілу ресурсів між об'єктами інформаційної безпеки вирішується за таким же алгоритмом.

3.2. Метод удосконалення технології динамічного регулювання розподілу ресурсів захисту при зміні націленості атак зловмисника

Статистика показників протистояння в інформаційній сфері свідчить про те, що у зв'язку з постійним зростанням потоків інформації і їх важливості збільшується інтенсивність нападів, і їх можна розглядати як неперервний процес [18, 91]. Це викликає необхідність прийняття адекватних заходів з боку захисту інформації. Проте націленість атак з часом може змінюватись, супроводжуючись перерозподілом ресурсів нападу між об'єктами. Подібна ситуація виникає, зокрема, при проведенні розвідки, коли напад не має відомостей про розподіл інформації по об'єктах і в результаті розвідки має можливість спрямувати свої зусилля у вигідному для себе напрямку [31]. Перерозподіл ресурсів нападу викликає відповідну реакцію захисту, який також перерозподіляє свої ресурси. Одним з контрзаходів захисту є динамічне управління ресурсами, сутність якого полягає в тому, що розподіл ресурсів проводиться з затримкою – після того, як визначиться націленість атак [86]. Таким чином, постає проблема розробки методів динамічного управління ресурсами захисту, котре забезпечує досягнення оптимальних показників в ситуаціях, які постійно змінюються. В термінології теорії ігор це є позиційна гра [12, 62].

При цьому виникає низка питань:

1) за яких умов в цій грі існує сідлова точка для величини, яка визначається цільовою функцією і як на її положення впливають умови протистояння – відносна кількість $Z = X/Y$ ресурсів нападу (X) і захисту (Y), відносна цінність $\{g_k\}$ інформації на об'єктах (k - номер об'єкта), уразливості f_k об'єктів;

2) яким повинен бути розподіл $\{y_k\}$ ресурсів захисту в умовах невизначеності у випадку, коли сідлова точка відсутня;

3) яким чином в ситуації, коли націленість атак стає відомою, розподілити інформацію з різною цінністю $\{g_k\}$ між об'єктами з різною уразливістю так, щоб загальні втрати стали мінімальними;

4) як відрізняються алгоритми управління при використанні різних критеріїв оптимальності і різних цільових функцій, котрі визначають такі величини, як величина завданої шкоди від реалізації загроз інформації, прибуток від внесення інвестицій, їх рентабельність і яким буде результат при використанні багатоцільової функції;

5) яким буде алгоритм управління при комплексному протистоянні, коли кожна із сторін витрачає одну частину ресурсів на захист своєї інформації, а іншу на здобуття інформації суперника.

З метою дослідження процесів динамічного протистояння і розробки рекомендацій по розподілу ресурсів між об'єктами захисту в динамічному режимі розглянуто систему з декількох об'єктів, котрі відрізняються один від одного відносною цінністю інформації, уразливістю і продуктивністю витрат.

Цільова функція, котра визначає величину завданої шкоди від реалізації загроз інформації $i(x, y)$, має вигляд (2.1).

Умови динамічного протистояння визначимо наступним чином. Напад і захист роблять почергові "ходи", знаючи на даний момент розподіл ресурсів суперника і на цій основі перерозподіляючи свої ресурси. Захист припиняє гру, коли черговий хід є для нього невигідним або він несе загрозу наступного ходу суперника, котрий приведе до значних збитків [112].

Прийнято, що в інтервалі зміни x_k і $p_k = 1$ (напад відбувся). Розглядаючи дії захисту отримано замість (2.1) спрощений вираз:

$$i(x, y) = \sum_{k=1}^{l} g_k f_k(x, y) \qquad (3.3)$$

Варіанти розрахунків будуть відрізнятись відносною цінністю $\{g_k\}$ інформації на об'єктах, значеннями n_k, c_k (продуктивності витрат) у функціях уразливості $f(x, y) = \dfrac{\left(x/y\right)^n}{\left(x/y\right)^n + c}$, а також параметром $Z = X/Y$, де $X = \sum_{k=1}^{l} x_k$, $Y = \sum_{k=1}^{l} y_k$, який характеризує всю систему і визначає загальне співвідношення ресурсів нападу і захисту.

На першому етапі розглянуто систему з двох об'єктів, для якої

$$i(x, y) = g_1 f_1(x, y) + g_2 f_2(x, y).$$

Систему характеризують такі величини:

- співвідношення відносної вартості інформації на об'єктах g_1/g_2;
- динамічні уразливості об'єктів $f_1(x, y)$, $f_2(x, y)$;
- співвідношення ресурсів нападу і захисту $Z = X/Y$.

Основна мета динамічного управління – пошук сідлової точки, яка відповідає найбільш сприятливому для кожної сторони розподілу ресурсів і забезпечує таким чином стабільність ситуації. Існування сідлової точки залежить від приведених вище показників, зокрема від значення Z. В результаті розрахунківв встановлено, що якщо уразливості описуються дробово-лінійними функціями, то сідлова точка існує при всіх значеннях Z, якщо хоча б одна з функцій є більш складною (дробово-квадратичною, дробово-кубічною), то існує в певних інтервалах значень Z. На рис. 3.2

показано процес динамічного управління при різних Z в системі, де одна з залежностей $f_k(x,y)$ описується дробово-лінійною функцією, а друга – дробово-кубічною.

При $Z=1$ (рис. 3.2,а) спостерігається близький до коливального процес, при якому відбувається повна почергова перекачка з одного об'єкта на інший як ресурсів нападу, так і ресурсів захисту. Цей процес обумовлений обмеженістю коштів нападу ($Z=1$), за якої при концентрації ресурсів на одному з об'єктів напад завдає більшої шкоди, ніж при їх розподілі між об'єктами.

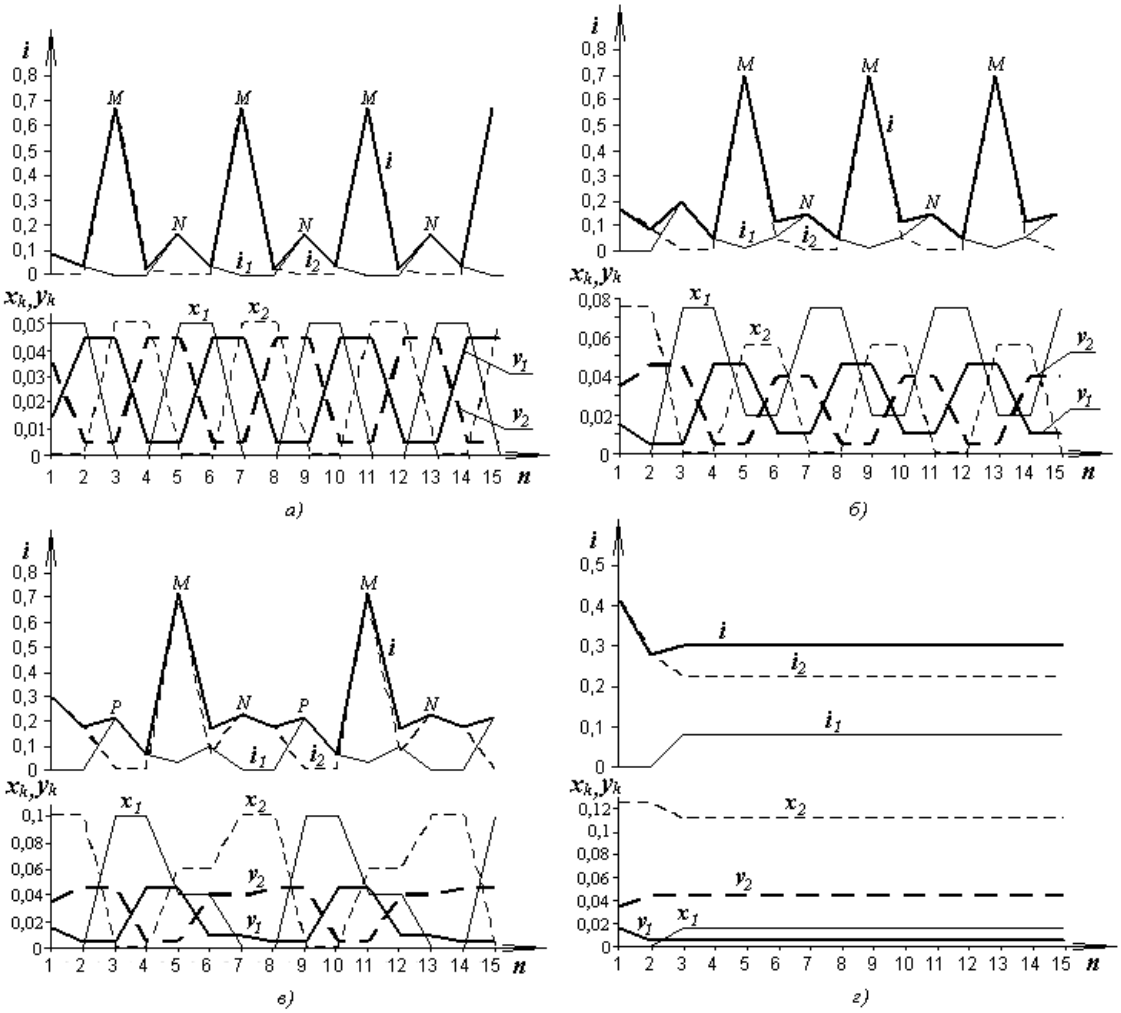


Рис. 3.2. Динамічний режим протистояння нападу і захисту при g_1=0,3; g_2=0,7; $f_1(x,y)=\frac{x/y}{x/y+8}$; $f_2(x,y)=\frac{(x/y)^3}{(x/y)^3+32}$ і різних Z: а) $Z=1$; б) $Z=1{,}5$; в) $Z=2$; г) $Z=2{,}5$

Захист відслідковує дії нападу і направляє свої ресурси на той об'єкт, де зосереджені ресурси нападу. Зубчаста лінія $i(n)$ на рис. 3.2,а показує, що після кожного кроку нападу зростає величина завданої шкоди від реалізації загроз інформації, а після наступного кроку захисту вона зменшується. В точках M величина завданої шкоди від реалізації загроз інформації значно більша, ніж в точках N, оскільки точки M відображають ситуацію, коли ресурси нападу направлені на другий об'єкт, де зосереджена інформації більшої цінності, а точки N – протилежну ситуацію.

При збільшенні Z (рис. 3.2,б) відбувається лише часткова перекачка ресурсів, оскільки їх вже достатньо для розподілу між обома об'єктами. Розрив між максимальним і мінімальним значеннями $i(n)$ зменшується.

З рис. 3.2,в видно, що при $Z = 2$ повна перекачка з одного об'єкта на інший відбувається не на кожному кроці. А період зміни величин збільшується від чотирьої кроків до шести.

При $Z = 2{,}5$ (рис. 3.2,г) досягається сідлова точка, в якій розподіли ресурсів стають оптимальними: $x_1^0 = 0{,}015$; $x_2^0 = 0{,}11$; $y_1^0 = 0{,}01$; $y_2^0 = 0{,}04$, а величина завданої шкоди від реалізації загроз інформації становить $i = 0{,}166$.

На рис. 3.2,в процес перерозподілу ресурсів схожий на субгармонійні коливання в нелінійних системах [78]. У ході проведених досліджень встановлено, що форми наведених на рис. 3.2 залежностей із збільшенням Z стають складнішими, а коливання – в більшій степені нелінійними при збільшенні нелінійності в функціях $f_k(x, y)$. Якщо $f_1(x, y)$ описується дробово-лінійною функцією, а $f_2(x, y)$ – дробово-квадратичною, від динамічного режиму із повною перекачкою ресурсів з одного об'єкту на інший ми одразу переходимо до режиму сідлової точки, минаючи режими, зображені на рис.3.1,б-в.

З метою детальнішого розгляду процесу досягнення сідлової точки в залежності від Z, побудовано матрицю рішень, враховуючи різні варіанти розподілу ресурсів нападу і захисту. Відповідні розрахунки значень цільової

функції (3.3) приведено у табл. 3.2, де стовпчики відповідають варіантам розподілу ресурсів нападу, а рядки – ресурсів захисту.

Праворуч приведені значення $\max\limits_{\{y_k\}} i$ для кожного рядка, тобто максимальне значення величини завданої шкоди від реалізації загроз інформації i для кожного варіанту розподілу ресурсів захисту. Ці значення зображені на рис.3.3,а у вигляді кривої 1. Нижній рядок таблиці містить значення $\min\limits_{\{x_k\}} i$ для кожного стовпчика, тобто мінімально досяжне значення величини завданої шкоди від реалізації загроз інформації i для кожного варіанту розподілу ресурсів нападу. На рис. 3.3,а значення $\max\limits_{\{y_k\}} i$ для кожного варіанту розподілу ресурсів захисту відображає крива 2. На осі абсцис приведено номери варіантів розподілу ресурсів нападу для кривої 1 та захисту для кривої 2.

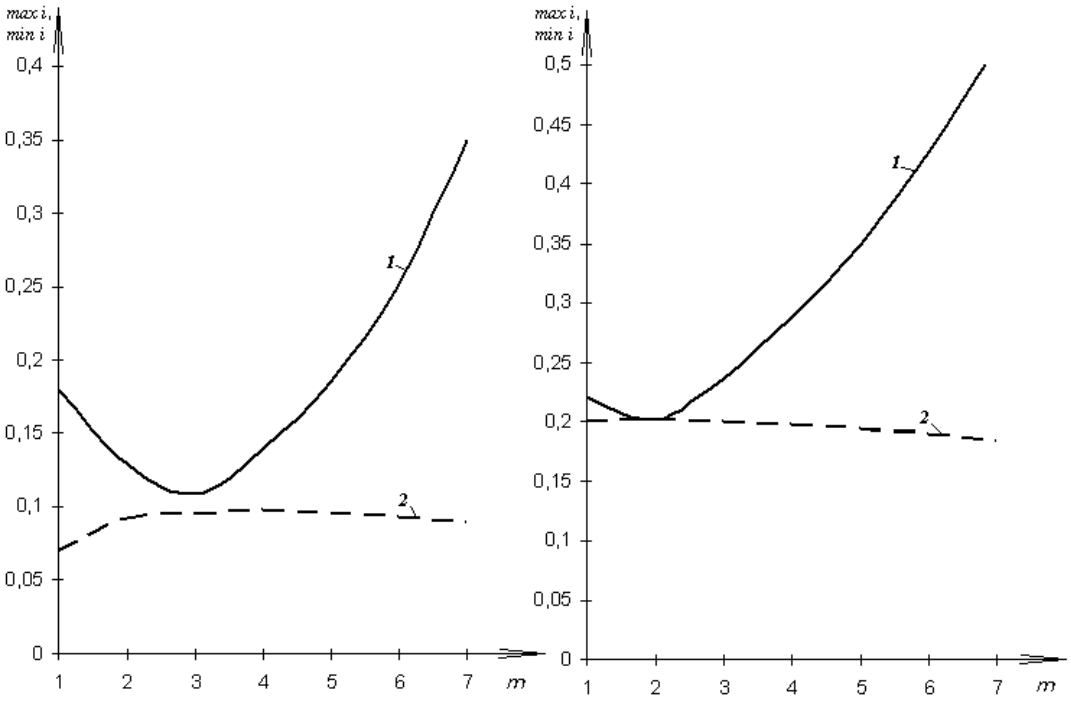
Таблиця 3.2

Матриця рішень сторін при g_1=0,3; g_2=0,7; $f_1(x,y)=\dfrac{x/y}{x/y+8}$; $f_2(x,y)=\dfrac{(x/y)^2}{(x/y)^2+16}$ і різних Z

	m	$Z=1,2$								$Z=2$							
	$\{x_k\}$ / $\{y_k\}$	0; 0,06	0,035; 0,025	0,04; 0,02	0,045; 0,015	0,05; 0,01	0,055; 0,005	0,06; 0	*max i*	0,01; 0,09	0,017 0,083	0,03 0,07	0,04 0,06	0,05 0,05	0,06 0,04	0,07 0,03	*max i*
i	0,005; 0,045	0,180	0,140	0,132	0,122	0,110	0,093	0,070	0,180	0,200	0,212	0,221	0,220	0,217	0,213	0,210	0,221
	0,01; 0,04	0,129	0,103	0,101	0,099	0,096	0,092	0,086	0,129	0,199	0,200	0,196	0,190	0,182	0,176	0,171	**0,200**
	0,015; 0,035	0,100	0,093	0,096	0,099	0,102	0,106	0,109	**0,109**	0,228	0,219	0,200	0,184	0,167	0,153	0,141	0,228
	0,02; 0,03	0,082	0,095	0,103	0,112	0,121	0,131	0,140	0,140	0,270	0,255	0,225	0,200	0,175	0,152	0,132	0,270
	0,025; 0,025	0,069	0,110	0,124	0,139	0,154	0,170	0,185	0,185	0,328	0,309	0,269	0,235	0,200	0,166	0,136	0,382
	0,03; 0,02	0,060	0,141	0,163	0,186	0,209	0,231	0,252	0,252	0,403	0,383	0,337	0,295	0,248	0,200	0,154	0,403
	0,035; 0,015	0,053	0,202	0,235	0,267	0,297	0,325	0,350	0,350	0,495	0,477	0,433	0,388	0,332	0,268	0,200	0,495
	min i	0,053	0,093	0,096	**0,099**	0,096	0,092	0,070		0,199	**0,200**	0,196	0,184	0,167	0,152	0,132	

З табл. 3.2 видно, що при $Z=1,2$ $\min\max i \neq \max\min i$ (ці значення виділено жирним шрифтом), при цьому криві 1 і 2 на рис. 3.3,а не дотикаються. При

збільшенні Z до $Z = 2$ (рис. 3.3,б) досягається сідлова точка, що відображається у правій частині таблиці та на рис. 3.3,б. Точка дотику і є сідловою точкою. У табл.3.2 ця точка відповідає значенню $\min\max i = \max\min i = 0{,}2$. Відхилення від неї небажане для кожної з сторін, оскільки веде до порушення її показників.



а) $Z = 1{,}2$ б) $Z = 2$

Рис. 3.3. Досягнення сідлової точки при g_1=0,3; g_2=0,7;

$f_1(x,y) = \dfrac{x/y}{x/y + 8}$; $f_2(x,y) = \dfrac{\left(x/y\right)^2}{\left(x/y\right)^2 + 16}$; 1 - $\max\limits_{\{y_k\}} i$, 2 - $\min\limits_{\{x_k\}} i$

Коливальний характер процесів перерозподілу ресурсів наводить на думку побудувати фізичну модель інформаційної системи [1,6,11]. Для процесів (рис. 3.2) механічною моделлю може бути пара пружно зв'язаних подвійних маятників (рис. 3.4). Жорсткий зв'язок між окремими кульками кожного з подвійних маятників виражає незмінність ресурсів як нападу, так і захисту: $x_1 + x_2 = X$, $y_1 + y_2 = Y$. Пружний зв'язок між подвійними маятниками забезпечує узгодженість їх коливань. При початкових умовах, що відповідають

умовам нашої системи, тобто при збудженні протифазних коливань в консервативній системі коливання будуть тривати необмежено довго [59].

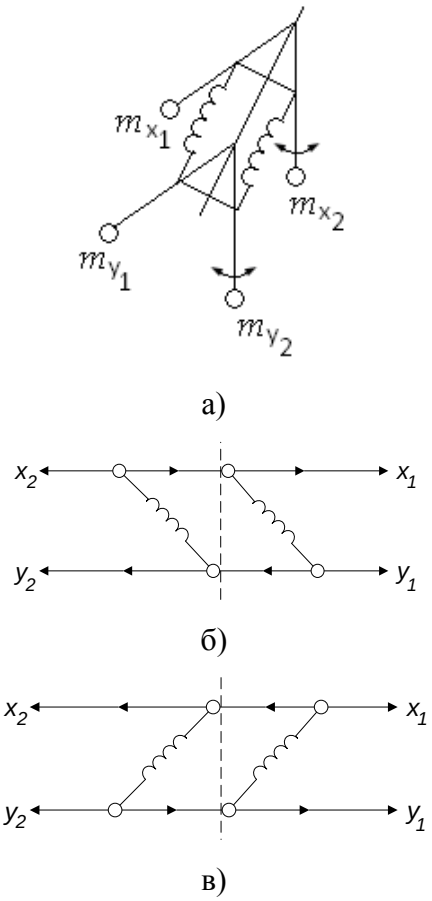


Рис. 3.4. Механічна модель системи, в котрій відбувається перерозподіл ресурсів

При $Z \neq 1$ симетрія картини порушується, оскільки $x_{\max} \neq y_{\max}$. На моделі це проявляється в тому, що маси кульок m_1 і m_2 перестають бути однаковими. При малих відхиленнях можна вважати, що $\frac{m_x}{m_y} = \frac{y_{\max}}{x_{\max}}$. При подальшому зростанні нелінійності (за рахунок показника n в функції $f(\tilde{y})$ та значення Z процеси перерозподілу ресурсів залишаються періодичними, але вже не можуть моделюватись вільними коливаннями.

Процеси на рис. 3.2,б можна розглядати як гармонічні коливання коло точки, яка не є точкою рівноваги, а процеси на рис. 3.2,в – як субгармонічні

коливання періоду $1/2$. Періодичну зміну величини $i(n)$ можна трактувати як вимушені коливання в дисипативному середовищі з субгармонійною зовнішньою силою.

Строго кажучи, процеси, зображені на рис. 3.2,а кусочно-лінійними відрізками, не є гармонічними, проте гармонічна модель в достатній степені відображає основні закономірності процесів. Більш того, в реальних умовах процес переходу з одного стану $\{x_k\}$ (чи $\{y_k\}$) в інший можна вважати миттєвим, і ці коливання наближаються до релаксаційних. Моделлю таких систем є релаксаційні генератори.

Відношення Z ресурсів нападу до ресурсів захисту відображають на еквівалентній схемі величиною зв'язку між коливальними системами (на механічній моделі – жорсткістю пружин, на електричній – величиною ємності зв'язку). Величина зв'язку впливає на швидкість перекачки ресурсів і їх величину. При малих Z зв'язок повинен бути більшим, ніж при великих. При $Z=1$ ресурси на кожному кроці повністю переводяться на інший об'єкт, що дозволяє потрапити на ділянку залежності $f(x,y)$ з високою крутизною для цього об'єкта і забезпечити максимальну завдану шкоду від реалізації загроз. На наступному кроці захист переводить на цей об'єкт всі свої ресурси. В результаті робоча точка переміщується на положисту ділянку залежності $f(x,y)$, де $x/y \geq 0,$ значення $i(x,y)$ зменшується, що примушує напад переводити свої ресурси на інший, незахищений об'єкт.

Запропонована модель пошуку оптимального рішення дозволяє надати рекомендації щодо оптимального розподілу ресурсів захисту інформації із врахуванням дій нападу. Проведені розрахунки показали, що існує вплив відносної кількості ресурсів нападу, уразливостей об'єктів та відносної цінності інформації на об'єктах на інтервали існування сідлової точки по *Z*, що є важливим фактором для побудови оптимальної системи захисту інформації.

3.3. Дослідження умов існування сідлової точки в багаторубіжних системах захисту інформації

Інформаційне протистояння відбувається частіше всього в умовах невизначеності, коли можливості, наміри, а іноді і дії суперника невідомі. В цій ситуації здається доцільним шукати таку стратегію поведінки, котра забезпечує певний результат при будь-яких діях суперника. Така ситуація спостерігається в сідловій точці цільової функції, де кожна з сторін досягає найкращого для себе результату і не зацікавлена в тому, щоб змінювати свою стратегію [13, 50, 83]. Стратегія кожної з сторін полягає в певному розподілі своїх ресурсів між об'єктами, які відрізняються часткою інформації, уразливістю та імовірністю нападу.

При визначенні умов існування сідлової точки в складних багаторубіжних системах, котрі відрізняються структурою, розподілом інформації між об'єктами, їх уразливістю та співвідношенням між кількістю ресурсів нападу і захисту, використаємо цільову функцію (2.1), яка визначає величину завданої шкоди від реалізації загроз інформації [55].

Величини, котрі входять в (2.1) – відносні. Величини $i(x,y)$, $i_k(x,y)$ та g_k віднесені до загальної вартості інформації, $f_k(x,y)$ - до вартості інформації на об'єкті. Останню величину розглянуто як динамічну уразливість об'єкта – імовірність втрати інформації при нападі на об'єкт. При $y=0$ маємо $f(x,0)$ - статичну уразливість, котра визначається початковою або природною уразливістю об'єкта.

Маючи на меті виявлення впливу характеристик системи, покладено $p_k=1$. Тоді (2.1) переходить в більш простий вираз:

$$i(x,y)=\sum_{k=1}^{l} g_k f_k(x,y). \qquad (3.4)$$

Вирази (2.1), (3.4) придатні для застосування до однорівневих систем. Найпростіша з таких систем зображена на рис. 3.5,а, де два об'єкти g_1 і g_2 захищені індивідуальними перешкодами 1 і 2. Однорівнева система (рис.3.5,б) містить три об'єкти з трьома індивідуальними перешкодами.

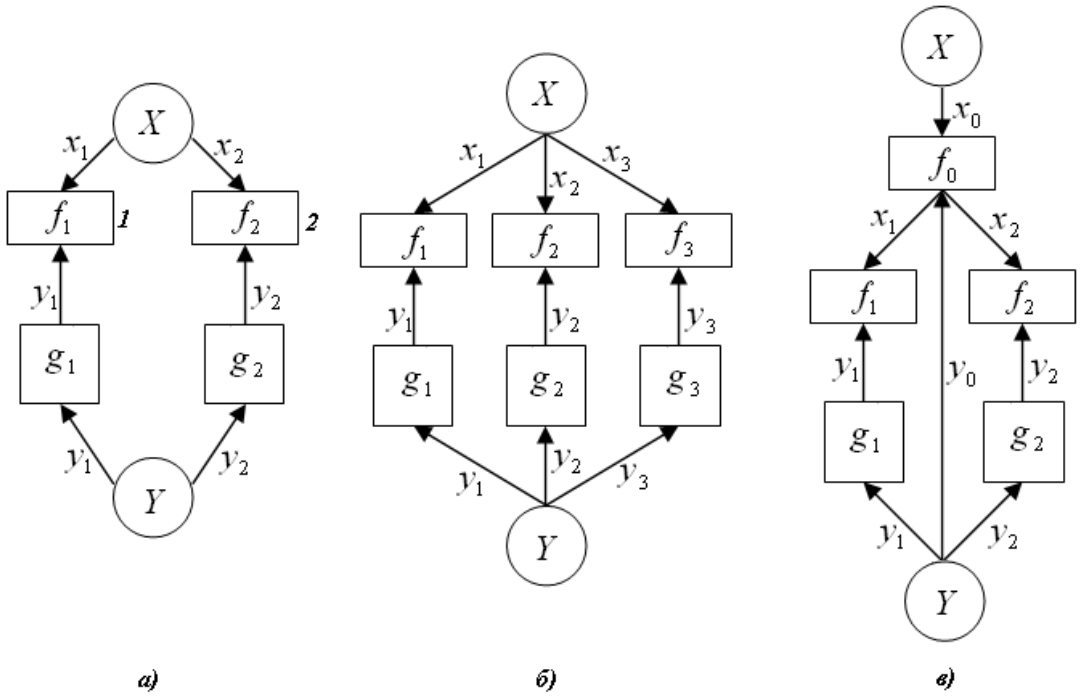


Рис. 3.5. Схеми однорівневих (а, б) та дворівневої (в) систем захисту

Ресурси y_k, котрі виділяються на захист об'єктів, витрачаються фактично на облаштування перешкод і визначають їх уразливості $f_k(x,y)$, які характеризують одночасно уразливості об'єктів. Цільова функція для системи (рис. 3.5,а) має вигляд:

$$i(x,y) = g_1 f_1(x_1, y_1) + g_2 f_2(x_2, y_2). \qquad (3.5)$$

На рис. 3.5,в показана дворівнева система, котра містить спільну для обох об'єктів перешкоду f_0 та дві індивідуальні перешкоди – f_1 і f_2. Для цієї системи цільова функція описується виразом

$$i(x,y) = f_0(x_0, y_0) \cdot \left[g_1 f_1(x_1, y_1) + g_2 f_2(x_2, y_2) \right]. \qquad (3.6)$$

Тут і надалі через k позначається номер перешкоди, а $f_k(x_k, y_k)$ виражає уразливість перешкоди, тобто безумовну імовірність її подолання. Форма і значення цільової функції (3.6) в значній мірі визначаються залежностями $f_k(x_k, y_k)$. Вибір залежностей $f_k(x_k, y_k)$ обгрунтовано у п.1.1, ними являються дробово-степеневі функції виду

$$f(x,y) = \frac{\left(x/y\right)^n}{\left(x/y\right)^n + c} = \frac{1}{1 + c\left(y/x\right)^n}, \qquad (3.7)$$

де параметри n і c визначають форму і кривизну ліній.

Прикладом захищуваної системи (рис. 3.5,в) може бути система, в котрій спільна перешкода f_0 являє собою захищений периметр території, об'єкти g_1, g_2 - приміщення, а перешкоди f_1, f_2 - засоби, які захищають ці приміщення (замки на дверях, ґрати на вікнах, генератори шуму, камери відеоспостереження тощо). Іншим варіантом системи (рис. 3.5,в) є, приміром, комп'ютери g_1, g_2, захищені спільною (firewall) та індивідуальними перешкодами (антивірусне програмне забезпечення, шифрування даних, антиспамфільтри).

Більш складні системи, котрі містять декілька спільних та індивідуальних перешкод, можуть, зрештою, бути зведені до системи (рис. 3.5,в).

Розглядаючи системи рис. 3.5, порівнюються однорівневі системи (рис. 3.5,а,б) з дворівневою системою (рис. 3.5,в). Об'єкти відрізняються уразливістю і відносною вартістю інформації – вони задаються в розрахунок. Незалежною змінною є $Z = \frac{X}{Y}$ – відносна кількість ресурсів нападу і захисту. Показники, по яким ведеться порівняння систем:

- область існування сідлової точки;

- величина заданої шкоди від реалізації загроз інформації в цій області.

Зазначені показники в значній мірі залежать від уразливостей об'єктів. Ці залежності в формі (3.7) зображені на рис. 3.5 для різних значень n і c. Параметр n впливає, в основному, на нелінійність кривих, параметр c - на їх положення.

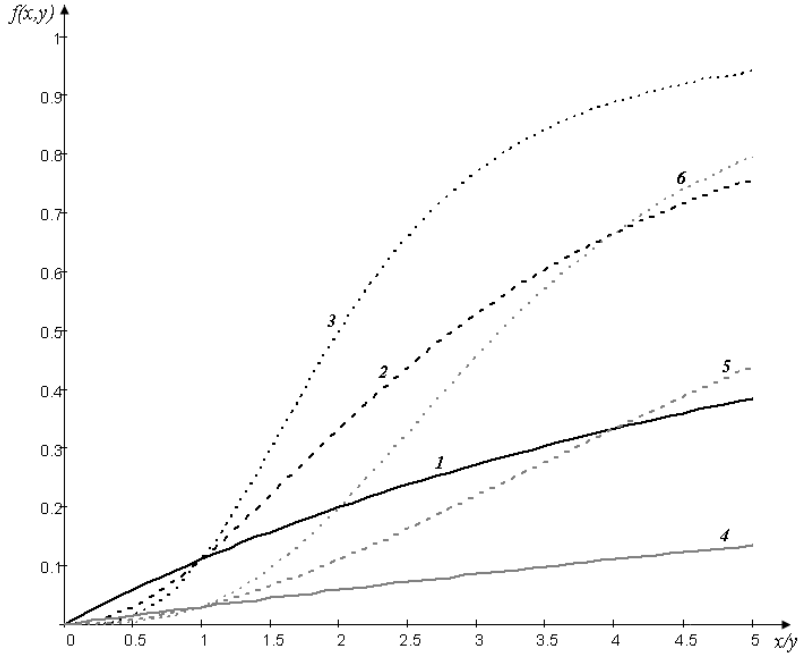


Рис. 3.6. Залежності $f(x)=\dfrac{x^n}{x^n+c}$ при різних значеннях n і c: криві **1-3** – $c=8$; **4-6** – $c=32$; **1, 4** – $n=1$; **2, 5** – $n=2$; **3, 6** – $n=3$

Пошук сідлової точки ведеться з допомогою програмного комплексу MatLab шляхом почергової оптимізації ресурсів нападу і захисту [60,64,112]. Розподіл ресурсів протилежної сторони, досягнутий на попередньому кроці, вважається відомим. На першому кроці покладено розподіл $\{y_k\}$ ресурсів захисту на об'єктах пропорційним розподілу інформації $\{g_k\}$ і знаходиться розподіл $\{x_k\}$ ресурсів нападу, котрий забезпечує досягнення $\max\limits_x i(x,y)$ в межах заданої кількості ресурсів $\sum\limits_{k=1}^{l} x_k = X$. На другому кроці, виходячи з одержаного розподілу $\{x_k\}$, знаходиться оптимальний для захисту розподіл $\{y_k\}$, котрий

забезпечує досягнення $\min_y i(x,y)$ в межах заданого значення $\sum_{k=1}^{l} y_k = Y$. Якщо сідлова точка для функції $i(x,y)$ існує, то цей процес є збіжним і продовжується до досягнення рівності $\max_x i(x,y) = \min_y i(x,y)$. Ця точка і визначає оптимальні розподіли $\{x_k^0\}$, $\{y_k^0\}$. Якщо сідлова точка відсутня, то після певної кількості кроків процес буде циклічно повторюватись необмежене число разів, показуючи, що стаціонарного стану не існує.

Проведені розрахунки виявили такі закономірності.

1. В найпростішій системі (рис.3.5,а) при дробово-лінійних залежностях $f_k(x,y)$ сідлова точка існує при всіх значеннях Z.

2. Якщо хоч одна з залежностей $f_k(x,y)$ має дробово-нелінійну форму, то сідлова точка може існувати лише в певних інтервалах значень Z. При збільшенні уразливості за рахунок зростання значення n або зменшення значення c інтервал ΔZ існування сідлової точки звужується і зміщується в сторону менших Z (рис.3.7).

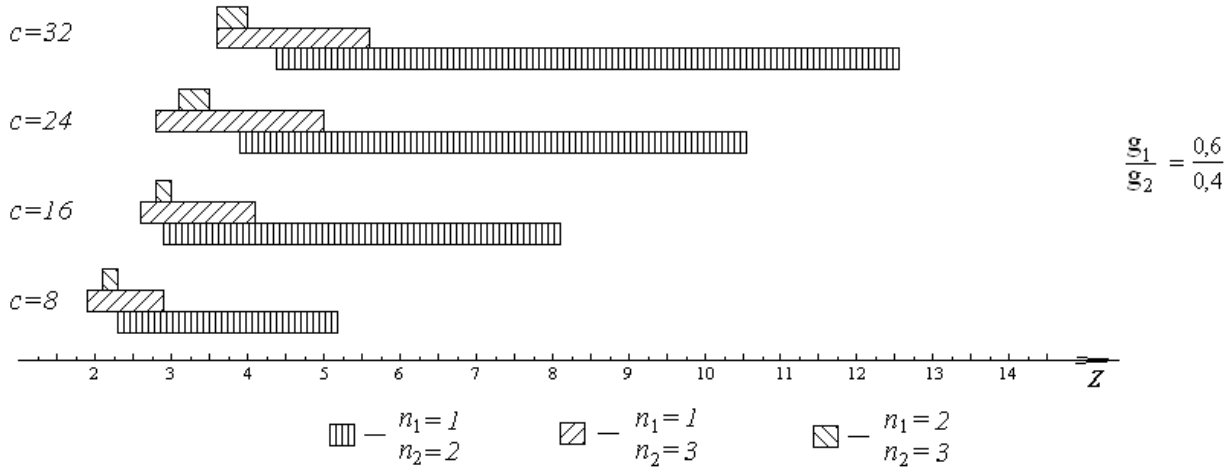


Рис. 3.7. Вплив форми функцій $f(x,y)$ на інтервал існування сідлової точки в системі (рис. 3.5,а)

Збільшення n в робочому діапазоні значень x/y, тобто при $x/y>1$, відповідно до (3.7), приводить до збільшення уразливості, а при $x/y<1$ – до її зменшення (рис. 3.7). Відносна вартість інформації на об'єктах в наших системах визначаєтсья уразливостями об'єктів: інформація з більшою вартістю міститься на об'єктах з меншою уразливістю.

3. Ступінь зростання $i(Z)$ визначається уразливостями об'єктів і близьке по формі до залежностей $f_k(x,y)$ (функція $i(Z)$ фактично усереднює залежності $f_k(x,y)$ з ваговими коефіцієнтами g_k (3.6), (3.7)). При зміні форм $f_k(x,y)$ і переході до залежностей з більшим n, що відображає більшу уразливість об'єктів, криві $i(Z)$ зміщуються в бік більших значень i (рис. 3.8).

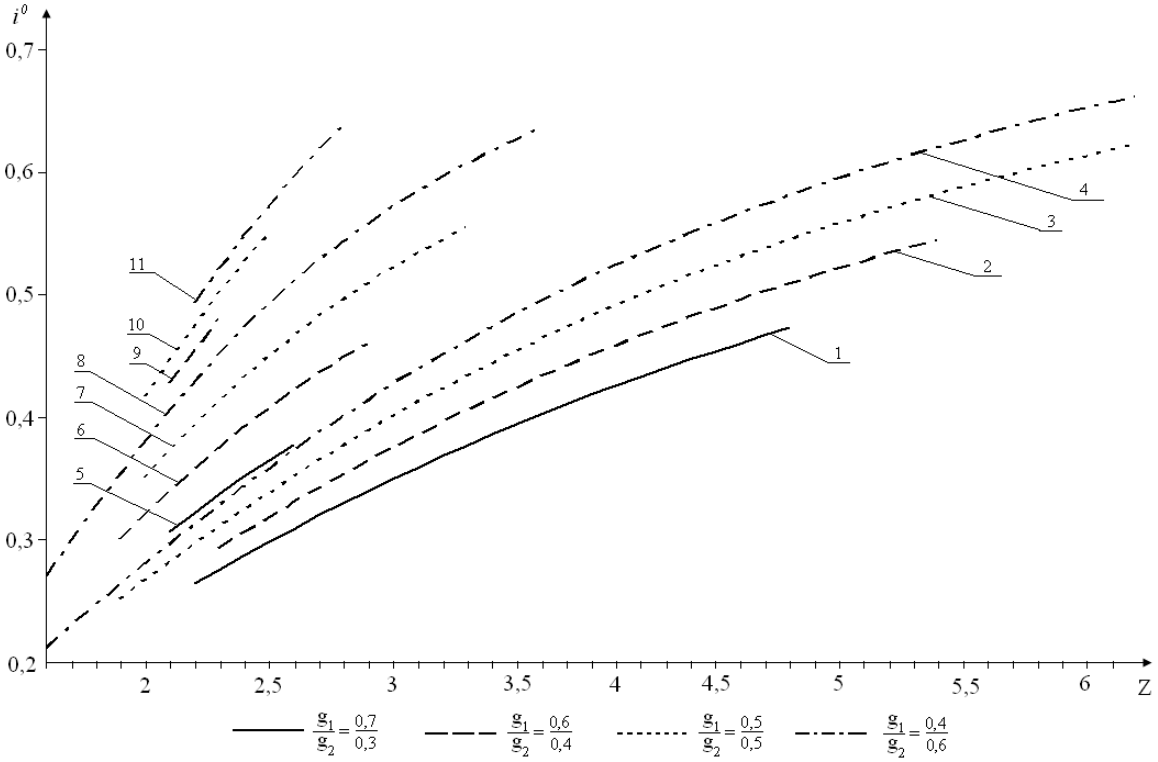


Рис. 3.8. Величина завданої шкоди від реалізації загроз інформації в інтервалах існування сідлової точки в системі (рис. 3.5,а) при $c=8$ і різних значеннях g_1/g_2 і n: **1-4** – $n_1=1$, $n_2=2$; **5-8** – $n_1=1$, $n_2=3$; **9-11** – $n_1=2$, $n_2=3$

4. Інтервал існування сідлової точки залежить також від відносної цінності $\{g_k\}$ інформації на об'єктах (в системі (рис. 3.5,а) – від співвідношення g_1/g_2 – рис.3.8). В приведених розрахунках інтервалів існування сідлової точки в перших варіантах інформація з більшою цінністю розміщувалась на об'єктах з меншою уразливістю. Слід зазначити, однак, що співвідношення x/y на різних об'єктах обирається таким чином, що забезпечує досягнення оптимального значення $i(x, y)$. При зміні Z ці значення також змінюються. В результаті співвідношення між динамічними уразливостями різних об'єктів за наявності нелінійності деяких з них може змінитись на протилежне (на рис. 3.6 при $x>1$ виконується нерівність $f_3(x) > f_1(x)$, а при $x<1$ – $f_3(x) < f_1(x)$).

Вплив відносної вартості g_1/g_2 інформації також показано на рис. 3.8. Видно, що при «неправильному» розміщенні інформації на об'єктах (варіант 4), величини $i(Z)$ досягають більших значень порівняно з іншими варіантами, проте зростає й інтервал ΔZ. При переході до розподілу ресурсів, обернено пропорційного уразливостям об'єктів, значення $i(Z)$ зменшуються, але й зменшується інтервал ΔZ (варіант 1). Ступінь зменшення інтервалу ΔZ зростає із збільшенням нелінійності функцій $f_k(x, y)$ і при $g_1/g_2 = 0{,}7/0{,}3$, $n_1 = 2$, $n_2 = 3$ інтервал ΔZ зникає.

5. В системі з трьома перешкодами (однорівневій або дворівневій) ситуація змінюється. Інтервал ΔZ стає обмеженим навіть при використанні дробово-лінійних функцій (рис. 3.9,а; 3.10), хоча він займає досить широку смугу. Вплив параметрів n і c залишається незмінним: при зростанні n і зменшенні c інтервал ΔZ зменшується і зміщується в сторону менших Z (рис. 3.9,в).

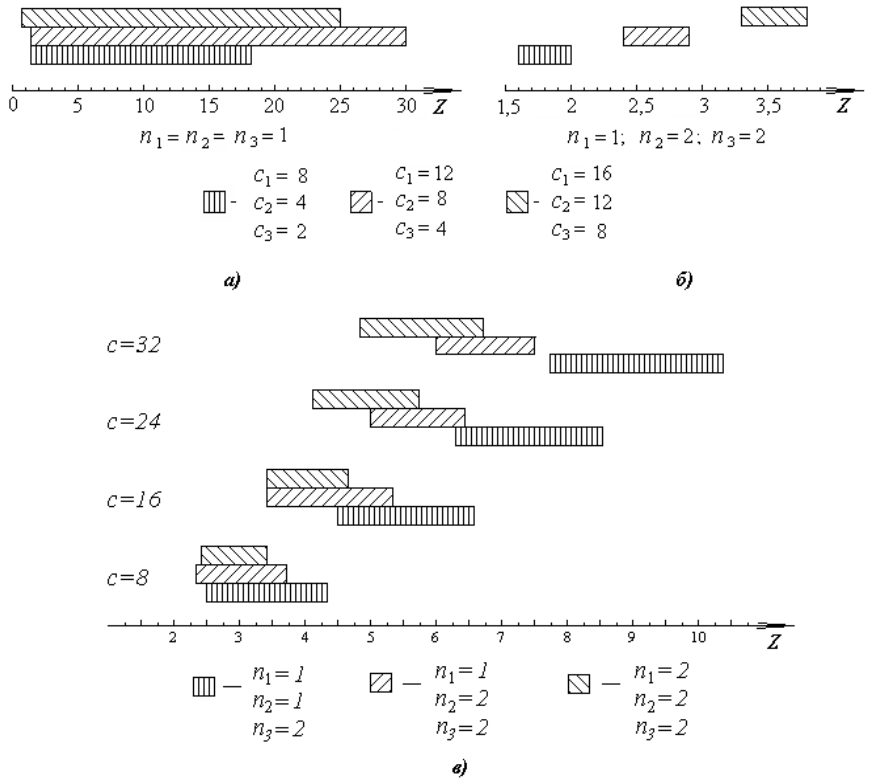


Рис. 3.9. Інтервали існування сідлової точки в однорівневій системі з трьох об'єктів (рис. 3.5,б) при $g_1 = 0{,}4$, $g_2 = 0{,}3$, $g_3 = 0{,}3$ і різних функціях уразливості: а) дробово-лінійні функції, різні значення c_k; б) дробово-нелінійні функції, різні значення c_k; в) дробово-нелінійні функції, однакові c_k

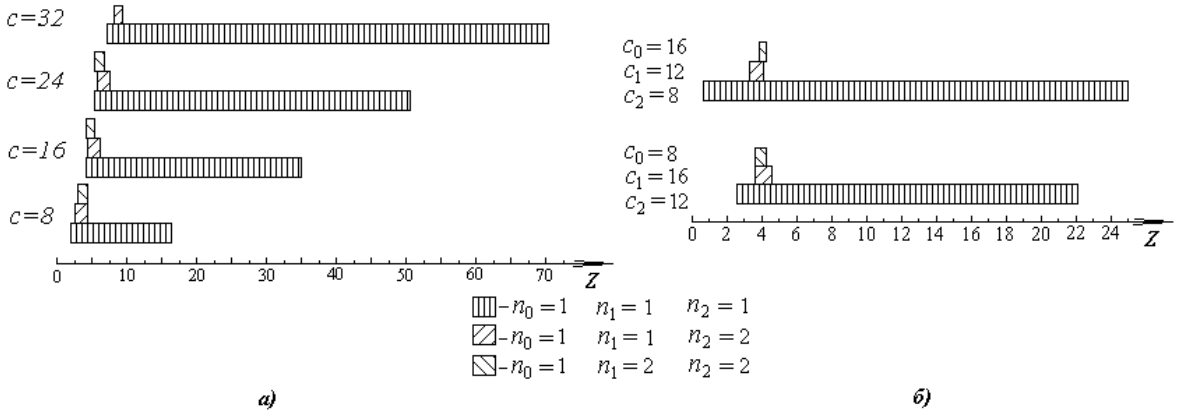


Рис. 3.10. Інтервали існування сідлової точки в дворівневій системі (рис.3.5,в) при $g_1 = 0{,}6$, $g_2 = 0{,}4$

В системі з дробово-нелінійними функціями введення третього об'єкта (рис. 3.5,б) чи третьої перешкоди (рис. 3.5,в) приводить до звуження інтервалу ΔZ і при деяких значеннях параметрів цей інтервал зникає – сідлова точка відсутня. Збільшення будь-якого із значень n_k порівняно з рис. 3.9, 3.10

приводить саме до такої ситуації – $\Delta Z = 0$. Зміна показника уразливостей c_k на $c_0 = 8$, $c_0 = 8$, $c_0 = 8$ не має суттєвого впливу на інтервали ΔZ.

Наведені результати показують, що ускладнення системи приводить до звуження інтервалу існування сідлової точки. Це пояснюється тим, що введення нових перешкод чи нових об'єктів збільшує число ступенів свободи в розподілі ресурсів, і забезпечити умови, котрі задовольняють обидві сторони, стає складніше. Пояснення потребує вплив уразливості об'єктів на умови існування сідлової точки. При дробово-лінійних залежностях $f(x)$ зростання $i(x)$ відбувається монотонно, майже лінійно в широкому інтервалі значень x. Деякі з цих значень відповідають умовам існування сідлової точки. При переході до дробово-нелінійних функцій зростання $i(x)$ відбувається більш стрімко, у вужчому інтервалі значень x. При збільшенні нелінійності ми наближаємось до ступінчастої функції $i(x)$, в котрій зростання $i(x)$ відбуваєтсья стрибком в одній точці, і значення $i(x)$ в цій точці стає невизначеним. Задовольнити умовам стаціонарності в цій точці неможливо.

Звертаючись до реальних систем, зазначено, що дробово-лінійні залежності можуть відображати властивості фізичних систем, в яких збільшення ресурсів приводить до приблизно пропорційного зменшення уразливості. Прикладом різко нелінійної залежності $f(x, y)$ є шифрування даних. В цьому випадку вкладання коштів не дає результату до того моменту, коли вдається зламати шифр, що приводить до стрибкоподібного зростання значення $i(x, y)$.

Підтвердженням коректності застосування наведеної методики є її порівняння з моделлю Гордона-Лоеба [89], котра знайшла своє емпіричне підтвердження [85,88]. Показано, що обидві методики дають схожі, а при певному виборі параметрів – співпадаючі результати [52].

Висновки до 3 розділу

1. У процесі досліджень розроблено метод визначення оптимального розподілу ресурсів між об’єктами захисту в динамічному режимі. Метод дозволяє визначити умови досягнення стаціонарних режимів і знайти відповідну величину втрат. При динамічному управлінні розподіл ресурсів проводиться з затримкою – після того, як визначено націленість атак, що забезпечує досягнення оптимальних показників в ситуаціях, які постійно змінюються.

2. Установлено, що оптимальне рішення, що відповідає сідловій точці, забезпечує зменшення величини очікуваної шкоди від реалізації загроз інформації при будь-яких діях суперника. У сідловій точці цільової функції кожна з сторін досягає найкращого для себе результату і не зацікавлена в тому, щоб змінювати свою стратегію.

3. При виконанні аналітичного моделювання процесу захисту та здобуття інформації, виявлено та формалізувано взаємозв’язок між умовами існування сідлової точки цільової функції при протистоянні двох сторін та характеристиками складних інформаційних структур. Існування сідлової точки залежить від наступних показників: відносної вартості інформації на об’єктах g_k, динамічної уразливості об’єктів $f_k(x, y)$, співвідношення ресурсів нападу і захисту $Z = X/Y$. На підставі проведених досліджень встановлено, що ускладнення системи приводить до звуження інтервалу існування сідлової точки: введення нових перешкод чи нових об’єктів збільшує число ступенів свободи в розподілі ресурсів, і забезпечити умови, що задовольняють обидві сторони, стає складніше.

4. Запропонований метод динамічного управління ресурсами захисту інформації за рахунок врахування дій суперника дає змогу оцінити наслідки прийнятих рішень, прогнозувати рівень очікуваних втрат і у разі відсутності сідлової точки у чистих стратегіях обрати таке рішення, що гарантує найменшу очікувану шкоду від реалізації загроз при найбільш несприятливих умовах.

РОЗДІЛ 4
УПРАВЛІННЯ РЕСУРСАМИ ЗАХИСТУ ІНФОРМАЦІЇ В УМОВАХ КОМПЛЕКСНОГО ПРОТИСТОЯННЯ

4.1. Модель динамічного протистояння в умовах конкурентної боротьби

Розвиток економічних відносин та інформаційної сфери приводить до збільшення обсягів інформації, кількості інформаційних об’єктів і зрештою — до посилення конкурентної боротьби і збільшення частоти нападів. При цьому умови протистояння постійно змінюються, і процес протистояння необхідно розглядати в динамічному режимі [105,110,112]. Причинами змін є напади суперників, а також «старіння» інформації, введення нової інформації і додаткових ресурсів, перерозподіл їх між об’єктами [23,67,72].

Аналіз протистояння в інформаційній сфері має зазвичай однонаправлений характер і спрямований на розробку заходів по захисту власної інформації. Разом з тим в умовах конкурентної боротьби протистояння відбувається в обох напрямках: кожна сторона прагне захистити свою інформацію і здобути інформацію суперника. Перехід до двонаправленого протистояння суттєво розширює коло проблем, котрі виникають при проектуванні систем інформаційної безпеки. Кожна з сторін розв’язує низку задач, направлених на оптимізацію важливих показників, пов’язаних з виділенням і розподілом ресурсів [64,68,69]. До таких показників відносяться:

1) загальна кількість ресурсів, виділених на захист власної інформації і здобуття інформації суперника;

2) співвідношення між кількістю ресурсів, виділених на захист і на здобуття інформації;

3) розподіл ресурсів між окремими об’єктами.

Розв’язок цих задач залежить від вартості інформації, якою володіє кожна з сторін, її розміщення на об’єктах, їх уразливості, імовірності виділення певної кількості ресурсів протилежною стороною і їх розподілу між об’єктами.

Критерієм оптимальності є досягнення максимальної ефективності інвестиції в інформаційну безпеку, тобто максимальної сумарної вартості захищеної і здобутої інформації [68].

Розглянуто однорідну систему з двох конкуруючих сторін, кожна з яких містить два однакових об’єкти (рис. 4.1).

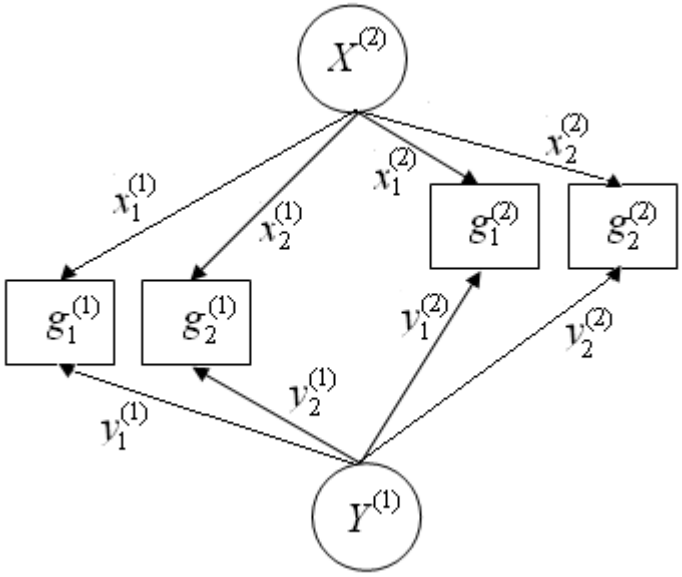


Рис. 4.1. Схема комплексного протистояння двох сторін

Через X і Y позначені ресурси суперників, g_k^m - вартість інформації на об’єкті. Верхній індекс – номер інформаційної системи, нижній – номер об’єкта. В силу однорідності системи $g_1^{(1)} = g_2^{(1)} = g^{(1)}$, $g_1^{(2)} = g_2^{(2)} = g^{(2)}$. Верхній індекс характеризує відношення до відповідної інформаційної системи, нижній – номер об’єкта.

Цільова функція $F(x, y)$ визначає сумарний інформаційний здобуток, що включає зменшення величини завданої шкоди від реалізації загроз інформації $j(x, y)$ за рахунок внесення інвестицій в об’єкти захисту і вартість інформації $i(x, y)$, здобутої з об’єктів суперника (ці величини відносні). Цільові функції для першої сторони $F_1(x, y)$ і для другої $F_2(x, y)$ мають вигляд [114]:

$$F_1(x,y)=\sum_{k=1}^{2}\left[j_k^{(1)}(x,y)+i_k^{(2)}(x,y)\right],$$

$$F_2(x,y)=\sum_{k=1}^{2}\left[i_k^{(1)}(x,y)+j_k^{(2)}(x,y)\right].$$

Використовуючи цільову функцію (1.4), величину завданої шкоди від реалізації загроз інформації на k-му об'єкті, представлено у вигляді:

$$i_k(x,y)=g_k\cdot p_k\cdot f_k(x_k,y_k) \qquad (4.1)$$

де x та y – ресурси двох сторін, виділені на об'єкт;

g_k – відносна вартість інформації на об'єкті;

p_k – імовірність нападу на об'єкт;

$f_k(x_k,y_k)$ – уразливість об'єкта.

Більшість величин, які входять в (4.1) – відносні: x, y, та $f_k(x,y)$ віднесені до вартості інформації на об'єкті; g_k та $i_k(x,y)$ віднесено до вартості інформації усієї системи. Відповідно до розробленої моделі, вважається, що змінні x та y входять в наведені вирази у вигляді відношення, тобто величина завданої шкоди від реалізації загроз інформації залежить від співвідношення ресурсів нападу і захисту: для першої інформаційної системи це x/y, для другої — y/x. Крім того, прийнято, що при відсутності інвестицій у захист напад отримує доступ до усієї інформації об'єкта, вартість якої рівна одиниці. Імовірнісні показники встановлено на рівні $p_k=1$ (напад відбувся). Розподіл ресурсів по об'єктах протилежною стороною також вважається рівномірним [14,28], кількість ресурсів на кожному об'єкті рівна одиниці: таким чином відбувається перехід від x/y до x, а від y/x – до y.

При використанні зазначених умов цільові функції приймають вигляд:

$$F_1(x,y)=\sum_{k=1}^{2}\left[1-g_k^{(1)}f_k^{(1)}(x)+g_k^{(2)}f_k^{(2)}(y)\right] \qquad (4.2)$$

$$F_2(x,y)=\sum_{k=1}^{2}\left[1+g_k^{(1)}f_k^{(1)}(x)-g_k^{(2)}f_k^{(2)}(y)\right] \qquad (4.3)$$

Для спрощення запису в функціональних залежностях $f(x)$, $f(y)$ індекси при незалежній змінній не зазначаються, проте під x, y необхідно розуміти відносні ресурси на об'єктах відповідних систем.

Основний вплив на результати розрахунків має форма залежностей $f(x)$, $f(y)$. Вони задані у вигляді дробово-степеневих функцій [55]:

$$f(x)=\frac{x^n}{x^n+c}; \qquad f(y)=\frac{1}{1+cy^n},$$

де параметри n і c виражають продуктивність витрат, тобто зменшення динамічної уразливості $f(y)$ або відповідне збільшення $f(x)$. В наступних розрахунках використовуються такі форми функцій (виражаємо їх через ресурси нападу, оскільки ресурси захисту розподілені рівномірно):

1) перша система (рис. 4.2,а)

$$f_1^{(1)}(x)=\frac{x}{x+8}; \qquad f_2^{(1)}(x)=\frac{x}{x+16}; \qquad (4.4)$$

2) друга система (рис. 4.2,б)

$$f_1^{(2)}(y)=\frac{1}{1+16y^2}; \qquad f_2^{(2)}(y)=\frac{1}{1+32y^3}. \qquad (4.5)$$

У виразах (4.2), (4.3) використовуються незалежні змінні відповідних функцій: у функціях $f_k^{(1)}(x)$ — x_k^1, у функціях $f_k^{(2)}(x)$ — y_k^2. Параметри n і c у (4.4), (4.5) вибрано довільно – з метою максимально виразного представлення

результатів [40,49]. Розподіл інформації по об'єктах в кожній системі приймаємо рівномірним: $g_1^{(1)} = g_2^{(1)} = 0{,}5$, $g_1^{(2)} = g_2^{(2)} = 0{,}5$, $\sum_{k=1}^{2} g_k^{(s)} = 1$, $s = 1{,}2$.

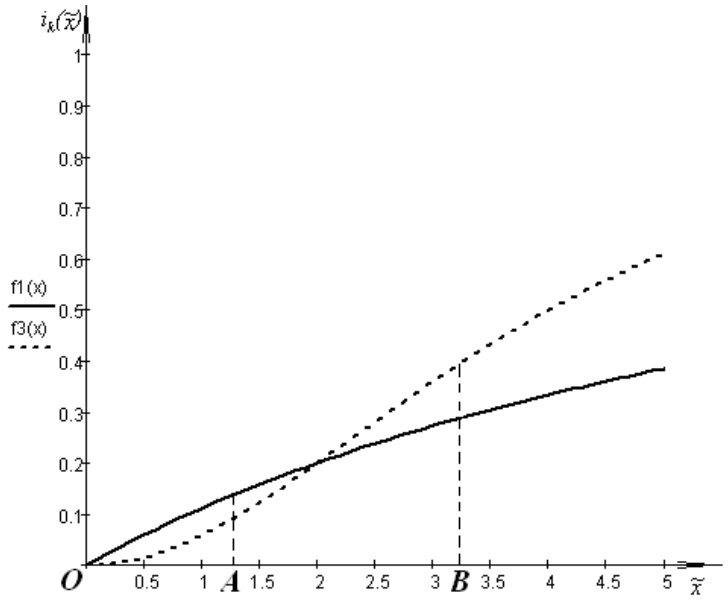


Рис. 4.2. Залежності $f(x)$ для дробово-лінійних та дробово-нелінійних функцій

Доцільність витрат визначається їх ефективністю для кожного з об'єктів. Цей показник чисельно виражається продуктивністю витрат [113], а графічно – крутизною відповідної характеристики: $f^{(1)}(x)$ для здобуття інформації та $f^{(2)}(y)$ для захисту [30]. Оскільки ці характеристики мають подібні форми, то зони доцільності розташовані ідентично: при дробово-лінійних залежностях $f(x, y)$ - це інтервали ОА в початкових областях значень x і, відповідно, y (рис. 4.2), при дробово-нелінійних інтервали – ВС в області середніх значень x і y. Збільшення x і y за межами цих інтервалів не дає суттєвого зростання значень $f^{(1)}(x)$ та $f^{(2)}(y)$.

4.2. Аналіз впливу форми протистояння на оптимізацію процесу управління ресурсами захисту інформації

Інформаційне протистояння відбувається частіше всього в умовах невизначеності, коли дії суперника невідомі і можуть бути передбачені лише з певною імовірністю. Це утруднює оптимізацію розподілу ресурсів між об’єктами захисту і управління ресурсами в динамічному режимі (об’єкти можуть мати як фізичну, так і електронну форми). Проте можлива ситуація, коли змінювати розподіл ресурсів невигідно ні одній з сторін. В термінології теорії ігор така ситуація відображає сідлову точку матричної гри [39,80,87]. Визначення умов існування сідлової точки є важливою задачею економічного менеджменту інформаційної безпеки. Пошук розв’язку ускладнюється його залежністю від значної кількості параметрів і характеристик інформаційної системи. Існування сідлової точки можливе лише в певному інтервалі значень зазначених параметрів.

В [112,114] розглянуто деякі аспекти сформульованої проблеми для найпростішої форми протистояння, коли дії однієї з сторін направлені на здобуття інформації, а другої – на її захист. Подібна задача розглядалась в [21], де пошук оптимального набору механізмів захисту, який забезпечує мінімум ризику втрат інформації, проводиться на прикладі системи районних відділень банку. Обсяг інформації в кожному відділенні пропорційний потенційній кількості клієнтів, тобто чисельності жителів району. Імовірність реалізації окремих загроз, а також вартість і ефективність кожного з механізмів захисту визначається методом експертної оцінки. При цьому припускається, що імовірність реалізації загрози проти кожного об’єкта однакова і залежить тільки від виду загрози. Розглядаючи різні комбінації елементів захисту для кожного з відділень, розраховується сумарний збиток для всієї системи (який і характеризує ступінь ризику) і оптимальний набір елементів захисту для кожного відділення за умови введення обмеження на загальну вартість системи захисту. При розрахунку повного ризику залишається відкритим питання про

величину перехресних членів, котрі виражають величину завданої шкоди від реалізації загроз інформації (ці події є сумісними).

В умовах конкурентної боротьби кожна з сторін прагне захистити свою інформацію і здобути інформацію суперника. В цьому випадку розглядається різнонаправлене, або комплексне протистояння.

На можливість існування сідлової точки впливають наступні фактори [115]:

- форма протистояння – однонаправлена чи різнонаправлена [116];
- кількість l об'єктів;
- ступінь уразливості об'єктів, тобто форма функцій $f_k(x,y)$;
- відносна вартість $\{g_k\}$ інформації на об'єктах.

З врахуванням цих факторів сідлова точка може існувати при певних значеннях $Z = X/Y$, де $X = \sum_{k=1}^{l} x_k$, $Y = \sum_{k=1}^{l} y_k$ – загальна кількість ресурсів кожної з сторін. Інтервал ΔZ існування сідлової точки визначається зазначеними факторами. Використовуючи математичну модель (1.4), відповідно до якої цільова функція $i(x,y)$ визначає величину завданої шкоди від реалізації загроз інформації $i(x,y) = \sum_{k=1}^{l} i_k(x,y) = \sum_{k=1}^{l} g_k p_k q_k (x.y) f_k(x,y)$, основну увагу приділено впливу величин $\{g_k\}$ і залежностей $f_k(x,y)$ на інтервал ΔZ. З цією метою покладено в (1.4) $p_k = 1$ і отримано $i(x,y) = \sum_{k=1}^{l} g_k f_k(x,y)$.

Відповідно до моделі (1.4) залежності $f_k(x,y)$ оберано у формі дробово-степеневих функцій

$$f_k(x,y) = \frac{\left(x/y\right)^n}{\left(x/y\right)^n + c}, \qquad (4.6)$$

де параметр n визначає кривизну залежностей, а c - висоту підйому над віссю абсцис. За фізичною суттю величини n і c виражають продуктивність витрат.

В попередніх розділах встановлено вплив окремих факторів на ΔZ при однонаправленому протистоянні. На даному етапі досліджень необхідно встановити як виявлені закономірності змінюються при переході до різнонаправленого протистояння. Обидві форми протистояння ілюструє рис.4.3. На рис.4.3,а зображено однонаправлене протистояння в системі з двох об'єктів, котрі містять інформації з відносною цінністю g_1 і g_2. Сторона X прагне здобути інформацію, сторона Y її захищає. На рис.4.3,б кожна з сторін має один об'єкт захисту - $g^{(1)}$ для сторони Y, $g^{(2)}$ - для сторони X і прагне здобути інформацію з об'єкта суперника. В позначеннях нижній індекс – номер об'єкта в системі, верхній – номер системи.

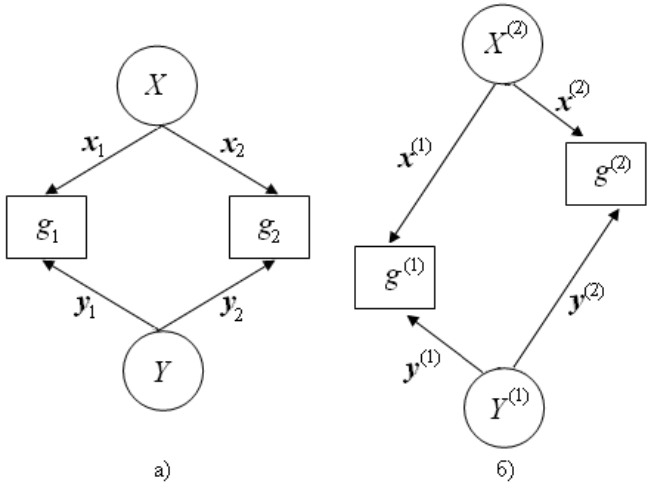


Рис. 4.3. Схеми протистояння: а) однонаправлене;
б) різнонаправлене

При однонаправленому протистоянні і дробово-лінійній формі функцій уразливості (4.6) (тобто при $n_1 = n_2 = n = 1$) сідлова точка в системі, що містить два об'єкти (рис.4.3,а), існує при всіх значеннях Z. При зростанні кількості l об'єктів інтервал ΔZ стає обмеженим, і його ширина зменшується зі збільшенням l. Якщо в системі (рис.4.3,а) хоч одна з залежностей $f_k(x, y)$ стає дробово-нелінійною, то інтервал ΔZ також стає обмеженим. При збільшенні уразливості за рахунок зростання показника n або зменшення параметра c цей інтервал звужується і зміщується в сторону менших Z.

При переході до різнонаправленого протистояння навіть в системі з двох об’єктів (рис.4.3,б) з дробово-лінійними функціями уразливості інтервал ΔZ стає обмеженим. Залежність $\Delta Z(n)$ якісно зберігає свій характер: при зростанні n величина ΔZ зменшується. Ці залежності для обох форм протистояння зображено на рис.4.4, формування інтервалу $\Delta Z(n)$ - на рис.4.5.

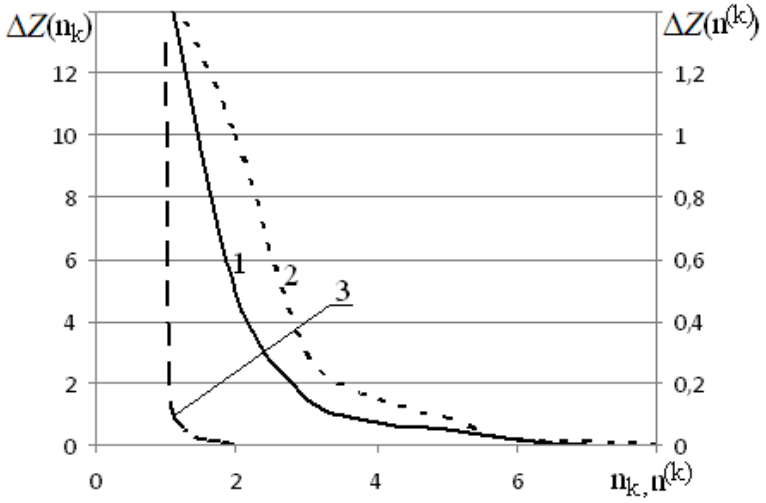


Рис. 4.4. Залежності ширини інтервалу ΔZ від n для двох систем: **1** - $\Delta Z(n_1)$, **2** - $\Delta Z(n_2)$ для системи (рис.4.3,а); **3** - $\Delta Z(n)$ для системи (рис.4.3,б)

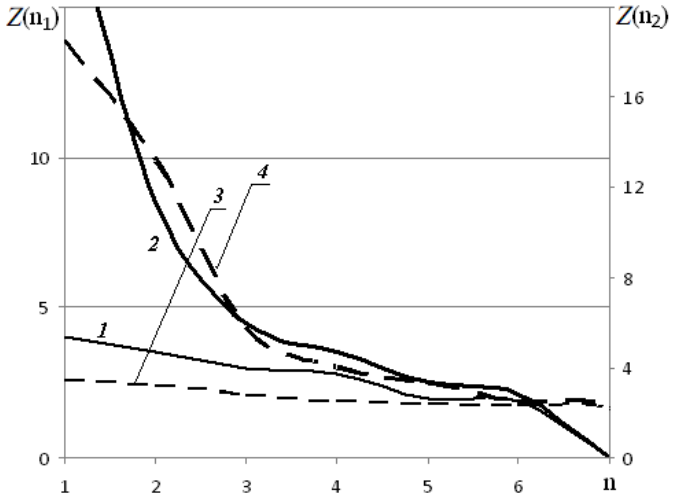


Рис. 4.5. Межі інтервалу ΔZ в залежності від n для системи (рис.4.3,а): **1** - $Z_{\min}(n_1)$, **2** - $Z_{\max}(n_1)$, **3** - $Z_{\min}(n_2)$, **4** - $Z_{\max}(n_2)$

Результати (рис.4.4,4.5) отримані при однаковій вартості інформації на об'єктах: $g_1/g_2 = g^{(1)}/g^{(2)} = 0{,}5/0{,}5$. Інші розрахункові параметри мали такі значення: $c_1 = c^{(1)} = 8$, $c_2 = c^{(2)} = 32$. Залежності $\Delta Z(n_1)$ і $Z(n_1)$ розраховані при $n_2 = 1$, $\Delta Z(n_2)$ і $Z(n_2)$ - при $n_1 = 1$, залежності $\Delta Z(n)$ - при $n^{(1)} = n^{(2)} = n = 1$. Криві 1,2 на рис.2, а також аналогічні залежності на рис.3 відображають вплив параметрів c_k.

Результати (рис.4.5) отримані для однонаправленого протистояння (рис.4.3,а) і дозволяють знайти ширину інтервалу $\Delta Z = Z_{\max} - Z_{\min}$, показану на рис.4.4. Для системи (рис. 4.3,б) аналогічні залежності не приводяться, оскільки $Z_{\min}(n^{(1)}) = Z_{\min}(n^{(2)}) = 0$, і верхня межа $Z_{\max}$ визначає ширину інтервалу (крива 3, рис.4.4).

На рис.4.6 зображені залежності $\Delta Z(c)$. Криві 1,2 одержані при $n_1 = n_2 = 2$, оскільки в системі (рис.1,а) при $n_1 = n_2 = 1$ $\Delta Z \to \infty$, криві 3,4 – при $n_1 = n_2 = 1$, через те, що в системі (рис.1,б) при $n_1 = n_2 > 1$ $\Delta Z \to 0$.

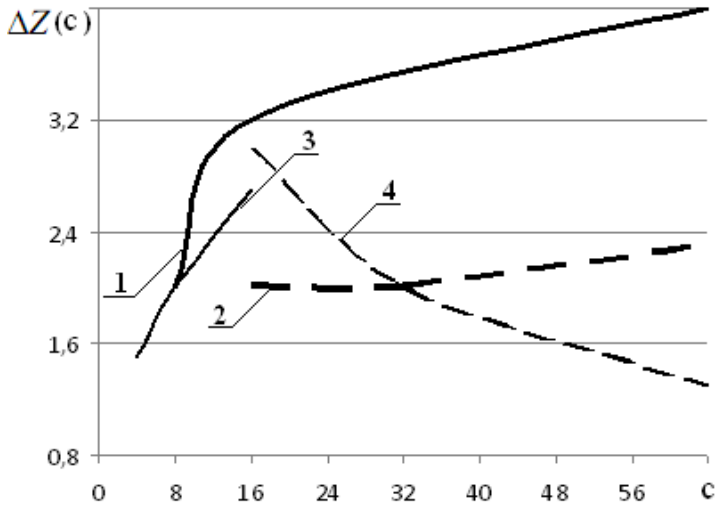


Рис. 4.6. Залежності ΔZ від c для двох систем: **1** - $\Delta Z(c_1)$, **2** - $\Delta Z(c_2)$ для системи (рис.4.3,а); **3** - $\Delta Z(c^{(1)})$, **4** - $\Delta Z(c^{(2)})$ для системи (рис.4.3,б)

В функціях $\Delta Z(c)$ суттєво проявляються відмінності двох форм протистояння. Залежності $\Delta Z(c^{(1)})$ і $\Delta Z(c^{(2)})$ (рис.4.6) мають якісно протилежний

характер: величина $\Delta Z(c^{(1)})$ зростає (крива 3), так само, як $\Delta Z(c)$ для системи (рис.4.3,а) (криві 1 і 2), в той час, як $\Delta Z(c^{(2)})$ спадає (крива 4). Це можна пояснити тим, що внесення ресурсів у захист і напад має різний ефект: система захисту повинна бути більш ефективна, ніж система нападу, тобто для зламу системи необхідно вкласти більше ресурсів, ніж вкладено в захист. Формально це обумовлено тим, що у вирази уразливості (3) x входить в чисельники дробів, а y - в знаменники, і зміна цих величин на Δx та, відповідно, Δy приводить до різної зміни Δf уразливості.

Нижня межа інтервалу $\Delta Z(c)$ для системи (рис.4.3,б) так, як і в залежності $\Delta Z(n)$, співпадає з віссю абсцис (рис.4.7,б). Таким чином, верхня межа залежності $Z(c)$ визначає одночасно ширину інтервалу $\Delta Z(c)$.

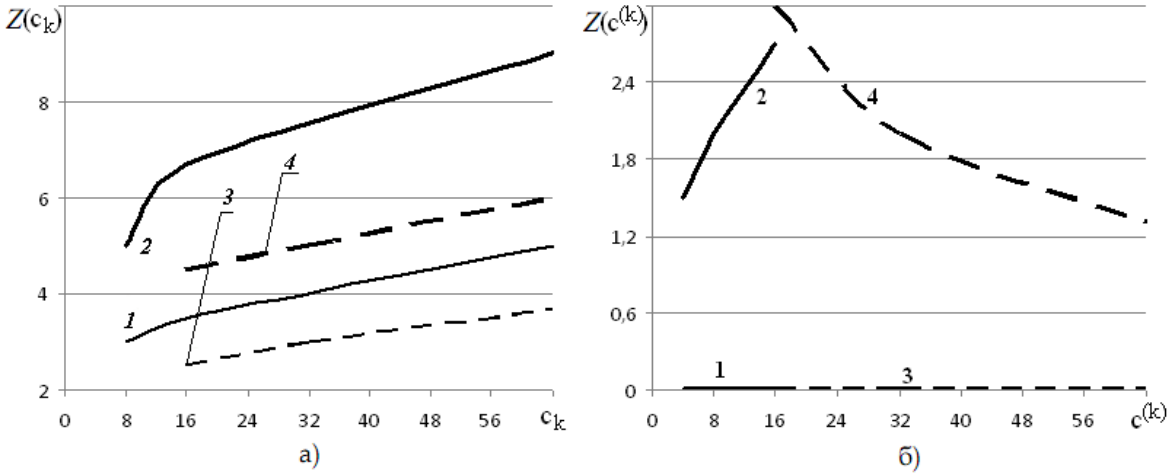


Рис.4.7. Межі інтервалу ΔZ в залежності від c: а) **1** – $Z_{\min}(c_1)$, **2** - $Z_{\max}(c_1)$, **3** - $Z_{\min}(c_2)$, **4** - $Z_{\max}(c_2)$ для системи (рис.4.3,а);
б) **1** - $Z_{\min}(c^{(1)})$, **2** - $Z_{\max}(c^{(1)})$, **3** - $Z_{\min}(c^{(2)})$, **4** - $Z_{\max}(c^{(2)})$ для системи (рис.4.3,б)

Крім ширини інтервалу ΔZ важливим показником є значення $i(Z)$ в межах цього інтервалу (рис.4.8). При збільшенні c, що відображає зменшення уразливості об’єктів, криві $i(Z)$ зміщуються в бік менших значень i (перехід від кривої 1 до кривих 2,3). При збільшенні n, тобто зростанні уразливості, значення i в системі (рис.4.3,а) збільшуються (ці залежності приведені в [115]). В системі (рис. 4.3,б) залежність $i(Z)$ при $n>1$ не існує, оскільки $\Delta Z = 0$.

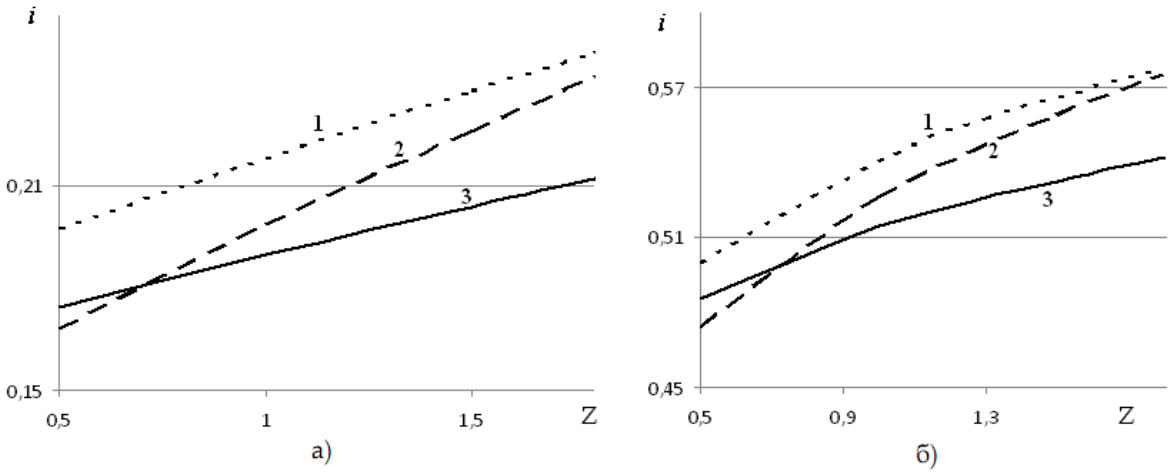


Рис.4.8. Величина завданої шкоди від реалізації загроз інформації в інтервалах існування сідлової точки в залежності від c для двох форм протистояння при $g_1 = g_2 = 0{,}5$ та $n_1 = 1$, $n_2 = 1$: а) для системи (рис.4.3,а); б) для системи (рис.4.3,б)

1 - $c_1 = c^{(1)} = 8$, $c_2 = c^{(2)} = 16$; **2** - $c_1 = c^{(1)} = 8$, $c_2 = c^{(2)} = 32$; **3** - $c_1 = c^{(1)} = 16$, $c_2 = c^{(2)} = 32$

Залежність ширини інтервалу ΔZ від відносної вартості інформації на об'єктах видно з рис.4.9. Зі збільшенням відношення g_1/g_2 величина ΔZ в системі (рис.4.3,а) зростає, а в системі (рис.4.3,б) звужується.

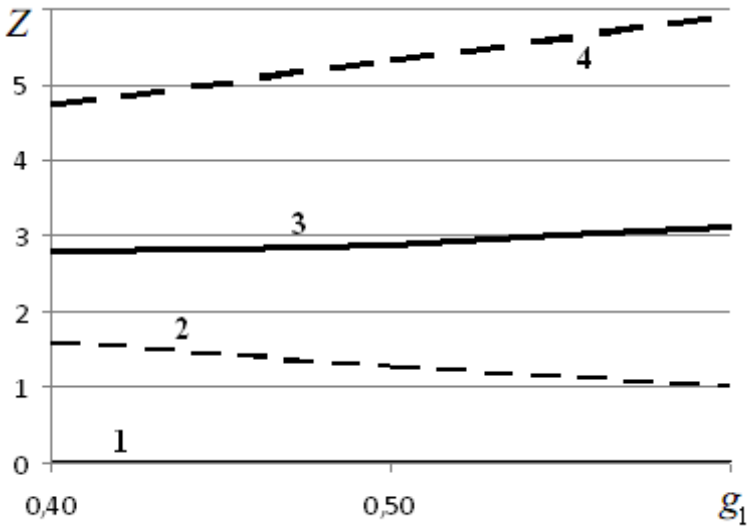


Рис.4.9. Межі інтервалу ΔZ в залежності від g_1/g_2 при $c_1 = c^{(1)} = 8$, $c_2 = c^{(2)} = 32$, $n_1 = n^{(1)} = n_2 = n^{(2)} = 1$ для двох систем:

1 - $z_{\min}$, **2** - $z_{\max}$ для системи (рис.4.3,б);

3 - $z_{\min}$, **4** - $z_{\max}$ для системи (рис.4.3,а)

Для обох форм протистояння зміна параметрів системи (n, c, g_1/g_2) приводить до зміни основних показників - i та ΔZ, причому ці зміни мають протилежний характер: найкращі показники по $i(Z)$ досягаються при найгірших показниках ΔZ. Для системи (рис.4.3,а) найменша величина завданої шкоди від реалізації загроз інформації, але при найвужчій ширині інтервалу існування сідлової точки відповідає розміщенню інформації, обернено пропорційному уразливостям об'єктів: для кривої 1 $g_1/g_2 = 0{,}7/0{,}3$ при $n_1 = 1$, $n_2 = 2$. Найширша смуга ΔZ (при найбільших значеннях i) має місце при «неправильному» розміщенні інформації, коли більша частина інформації розміщена на більш уразливих об'єктах: для кривої 4 $g_1/g_2 = 0{,}6/0{,}4$ при $n_1 = 1$, $n_2 = 2$.

При однонаправленому протистоянні ускладнення інформаційної структури за рахунок збільшення кількості об'єктів та зростання ступеня нелінійності залежностей, що описують динамічну уразливість об'єктів, приводить до звуження інтервалу ΔZ існування сідлової точки. Розміщення інформації по об'єктах обернено пропорційно їх уразливостям дозволяє зменшити збитки, проте при одночасному зменшенні ΔZ.

Перехід від однонаправленого до різнонаправленого протистояння підтверджує зазначені тенденції, однак, виявляє деякі нові закономірності. Відмінності двох форм протистояння суттєво проявляються при дослідженні залежностей інтервалів ΔZ існування сідлової точки від параметра c, що входить до функції уразливості як продуктивність витрат.

Проведені розрахунки дозволяють встановити вплив окремих факторів на оптимальне рішення і розробити рекомендації по досягненню режиму сідлової точки в умовах конкурентної боротьби.

4.3. Метод оцінки рівня інформаційної безпеки з використанням часових залежностей інформаційного балансу конкуруючих сторін

В умовах динамічного протистояння важливим показником є часова залежність стану інформаційної системи [34,56,67]. Динаміку зміни стану розглянуто на прикладі системи (рис. 4.1).

Спроби здобуття інформації суперника утворюють пуассонівський потік подій, або неперервний марковський ланцюг [13,16,76]. Введено наступні позначення [114]:

λ_1 і λ_2 - кількість спроб несанкціонованого доступу, які здійснюють суперники за одиницю часу (в подальшому першою стороною будемо вважати сторону з ресурсами Y, котра захищає два об'єкти першої інформаційної системи);

p_1 і p_2 - імовірності того, що відповідні спроби будуть успішними.

$\Lambda_1 = p_1\lambda_1$ і $\Lambda_2 = p_2\lambda_2$ - частоти успішних спроб суперників;

$\Lambda = \Lambda_1 + \Lambda_2$ - сумарна частота успішних спроб;

S_{ij} - стан системи, в якому неушкодженими залишаються i об'єктів першого з суперників та j об'єктів другого суперника ($i = \overline{1,2}$, $j = \overline{1,2}$);

p_{ij} - імовірність того, що система знаходиться в ij-му стані.

Граф системи, який зображує переходи між станами, показано на рис.4.10.

Система диференціальних рівнянь Колмогорова [13] відповідно до графу системи (рис.4.10) має вигляд:

$$\frac{dp_{22}}{dt} = -\Lambda p_{22};$$

$$\frac{dp_{21}}{dt} = \Lambda_1 p_{22} - \Lambda p_{21};$$

$$\frac{dp_{12}}{dt} = \Lambda_2 p_{22} - \Lambda p_{12};$$

$$\frac{dp_{20}}{dt} = \Lambda_1 p_{21} - \Lambda_2 p_{20};$$

$$\frac{dp_{11}}{dt} = \Lambda_1 p_{12} + \Lambda_2 p_{21} - \Lambda p_{11};$$

$$\frac{dp_{10}}{dt} = \Lambda_1 p_{11} + \Lambda_2 p_{20} - \Lambda_2 p_{10};$$

$$\frac{dp_{01}}{dt} = \Lambda_1 p_{02} + \Lambda_2 p_{11} - \Lambda_1 p_{01};$$

$$\frac{dp_{00}}{dt} = -\Lambda_1 p_{01} - \Lambda_2 p_{10}$$

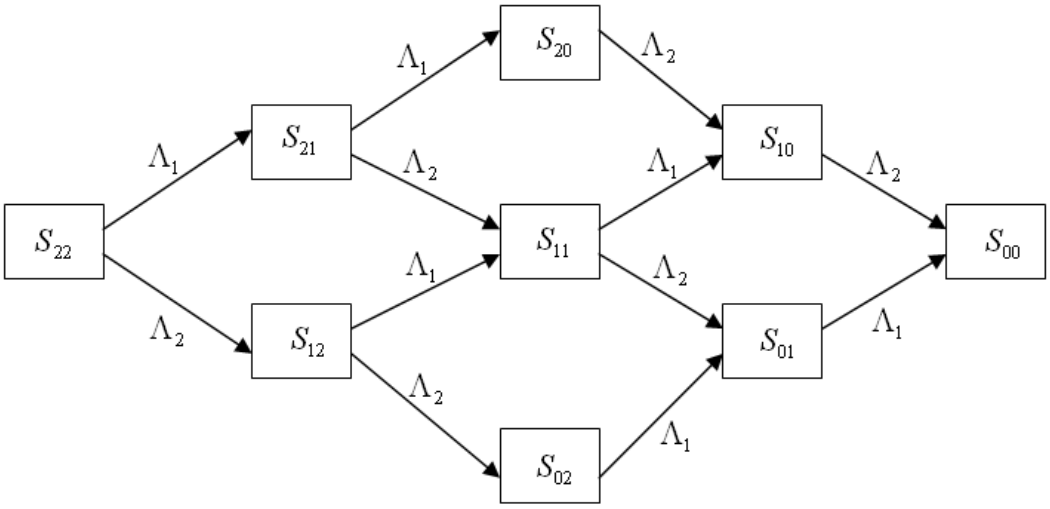


Рис. 4.10. Граф однорідної системи, в якій кожна з сторін містить два об’єкти

Послідовно інтегруючи диференціальні рівняння, одержано вирази для $p_{ij}(t)$:

$$p_{22}(t) = e^{-\Lambda t}$$
$$p_{21}(t) = \Lambda_1 t \cdot e^{-\Lambda t}$$
$$p_{20}(t) = e^{-\Lambda_2 t} - (1+\Lambda_1 t)e^{-\Lambda t}$$
$$p_{11}(t) = \Lambda_1 \Lambda_2 t^2 \cdot e^{-\Lambda t}$$
$$p_{02}(t) = e^{-\Lambda_1 t} - (1+\Lambda_2 t)e^{-\Lambda t}$$

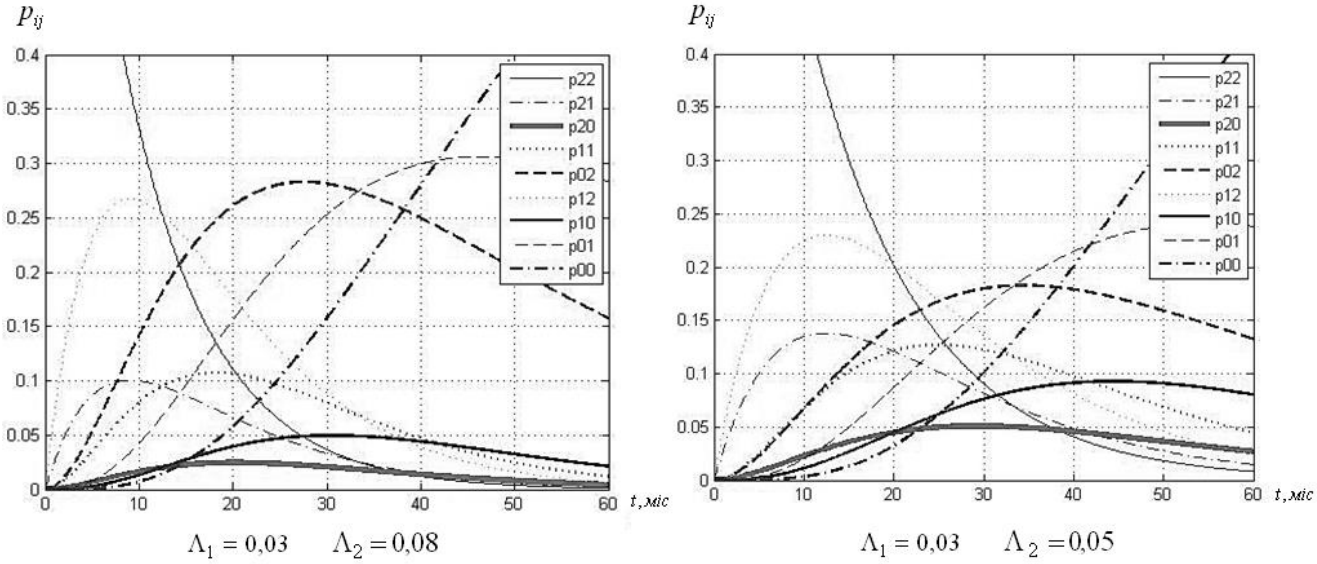
$$p_{12}(t) = \Lambda_2 t \cdot e^{-\Lambda t}$$
$$p_{10}(t) = \Lambda_2 t e^{-\Lambda_2 t} - (\Lambda_1 \Lambda_2 t^2 + \Lambda_2 t)e^{-\Lambda t}$$
$$p_{01}(t) = \Lambda_1 t e^{-\Lambda_1 t} - (\Lambda_1 t + \Lambda_1 \Lambda_2 t^2)e^{-\Lambda t}$$
$$p_{01}(t) = \Lambda_1 t e^{-\Lambda_1 t} - \left[\Lambda_1 t + \Lambda_1 \Lambda_2 t^2\right] e^{-\Lambda t}$$

Ці залежності для різних значень Λ_1, Λ_2 наведені на рис. 4.11, 4.12. Величини $p_{ij}(t)$ визначаються імовірностями попередніх станів, з яких відбуваються переходи, та щільностями перехідних імовірностей, які визначаються величинами Λ_1, Λ_2 [60,66]. Хід залежностей $p_{ij}(t)$, зокрема, положення максимумів показано на прикладі стану S_{20}. Швидкість зміни $p_{20}(t)$ виражається рівнянням:

$$\frac{dp_{20}}{dt} = \Lambda_1 p_{21} - \Lambda_2 p_{20}.$$

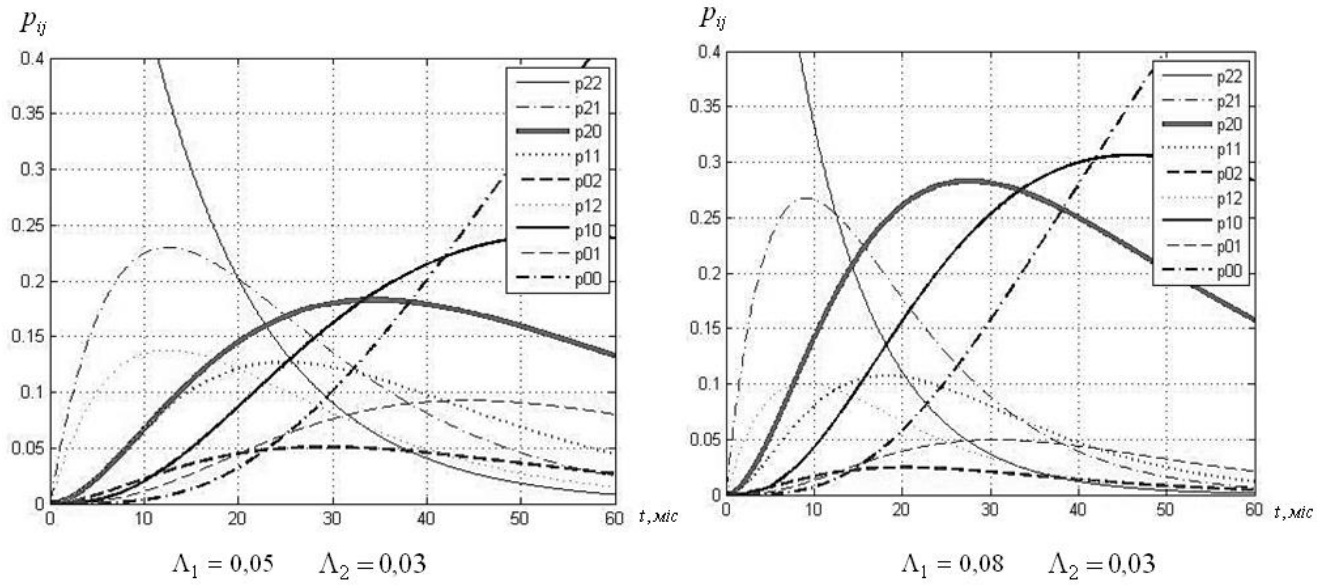
На початковій стадії $p_{20} \geq 0$ або $p_{20} \approx 0$, $p_{21} > p_{20}$ і $\frac{dp_{20}}{dt} > 0$. З часом в результаті потоку спроб p_{21} зменшується, а p_{20} зростає [79] і зрештою досягає максимума в точці, котра визначається рівністю:

$$\frac{p_{20}^0(t_{20}^0)}{p_{21}(t_{20}^0)} = \frac{\Lambda_1}{\Lambda_2}. \qquad (4.6)$$



а) б)

Рис.4.11. Залежності $p_{ij}(t)$ при $\Lambda_1 < \Lambda_2$



а) б)

Рис.4.12. Залежності $p_{ij}(t)$ при $\Lambda_1 > \Lambda_2$

Визначити моменти t_{ij}^0, в які імовірності станів досягають своїх максимальних значень, можна з виразів для похідних $\frac{dp'_{ij}}{dt}$. Прирівнявши похідні до нуля, знаходяться значення t_{ij}^0 []. Для початкових станів отримано аналітичні вирази:

$$t_{22}^0 = 0;\ t_{21}^0 = t_{12}^0 = \frac{1}{\Lambda}.$$

Для знаходження t_{20}^0 необхідно розв'язати трансцендентне рівняння:

$$t_{20}^0 = \frac{1}{\Lambda}\left(1 + \frac{\Lambda_2}{\Lambda_1} e^{\Lambda_1 t_{20}^0}\right).$$

Максимальні значення p_{ij}^0 можна знайти, підставляючи у вирази $p_{ij}(t)$ значення t_{ij}^0. Інший шлях – виразити p_{ij}^0 через імовірності попередніх станів, наприклад, з (4.6):

$$p_{20}^0 = \frac{\Lambda_1}{\Lambda_2} p_{21}(t_{20}^0).$$

Значення t_{ij}^0 та p_{ij}^0 залежать від обох величин - Λ_1 і Λ_2, так як кожний з станів, за виключенням кінцевих, знаходиться в динамічному двонаправленому процесі: в стан S_{21} можливо перейти з попереднього стану S_{22} з імовірністю, пропорційною значенню Λ_1, а також перейти з цього стану в наступні – в стан S_{20} з імовірністю Λ_1 і в стан S_{11} з імовірністю Λ_2 [57,79].

Оскільки $\Lambda = p\lambda$, то задача зводиться до визначення величин p, λ. Ці величини для різних інформаційних систем можна оцінити на основі статистичних даних. Імовірності успішних спроб нападу p можна визначити також теоретично, використовуючи певну математичну модель. Динамічна уразливість виражається степеневими функціями:

$$f(x,y)=\frac{\left(x/y\right)^n}{\left(x/y\right)^n+c}, \qquad (4.7)$$

де n і c - параметри, котрі виражають міру продуктивності витрат. Величину $f(x,y)$ можна розглядати як імовірність успішного нападу суперника [20,81]. Специфіка її використання в якості параметра p_k для кожного з об'єктів пов'язана з тим, що вона не є сталою величиною, а залежить від співвідношення ресурсів x_k, y_k. Ступінь зростання величини p зі збільшенням x/y залежить від ступеня нелінійності функції $f(x,y)$ [113], тобто від параметрів n і c (рис. 4.13).

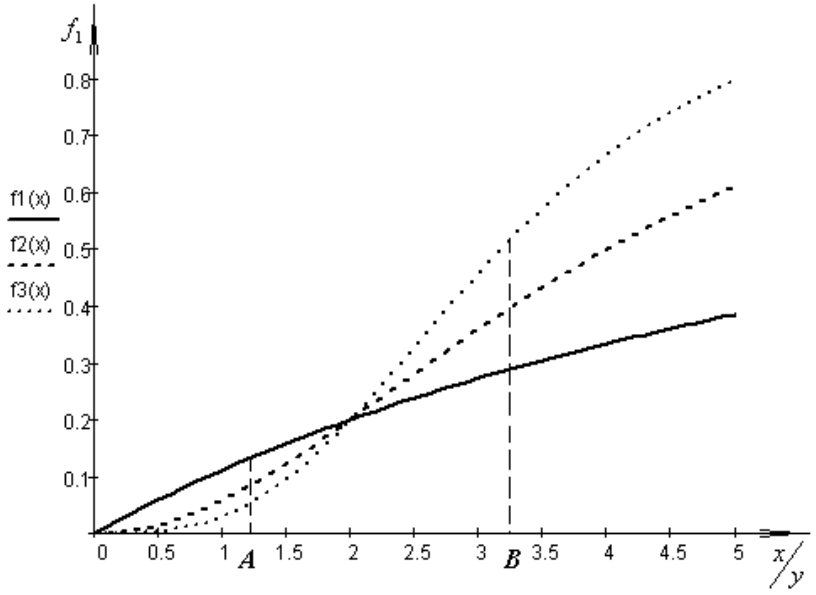


Рис. 4.13. Динамічні уразливості при різних формах залежності $f(x,y)$:

$$1-\ f_1(x,y)=\frac{x/y}{x/y+8};\ 2-\ f_2(x,y)=\frac{\left(x/y\right)^2}{\left(x/y\right)^2+16};\ 3-\ f_3(x,y)=\frac{\left(x/y\right)^3}{\left(x/y\right)^3+32}$$

При зміні x_k/y_k співвідношення між уразливостями об'єктів і, відповідно, між значеннями p_k може змінитись якісно. Так в точці A (рис. 4.13) найбільше

значення $p(x,y)$ має перший об'єкт (з дробово-лінійною залежністю $f_1(x,y)$), а в точці B через дробово-нелінійний характер залежності $f_3(x,y)$ - третій об'єкт.

Для першого з суперників найбільш бажаним є стан S_{20}, в який можливо потрапити зі стану S_{21}. При цьому пріоритетним завданням є досягнення найбільшого значення p_{20}^0 при найменшому t_{20}^0 (рис. 4.10, 4.11). При збільшенні відношення Λ_1 / Λ_2 величина p_{20}^0 зростає. Вплив Λ_1, Λ_2 на t_{20}^0 має більш складний характер (значення t_{20}^0 показані на рис. 4.11, 4.12 штриховими лініями, опущеними з точок p_{20}^0 на вісь t). Збільшити відношення Λ_1 / Λ_2 можна за рахунок збільшення ресурсів першого з суперників – при цьому Λ_1 збільшується, а Λ_2 зменшується. Якщо для другого суперника імовірність успішних спроб задається виразом (4.7), то для першого – виразом

$$f^{(1)}(x,y) = \frac{\left(y/x\right)^n}{\left(y/x\right)^n + c}$$

Вплив відношення Λ_1 / Λ_2 на p_{ij}^0 та t_{ij}^0 показано на рис. 4.14.

Розглянутій інформаційній системі можна співставити гідравлічну структуру, котра містить набір резервуарів, до кожного з яких підходить дві системи труб: одна з них наповнює резервуар, друга одночасно його вивільняє (рис. 4.15).

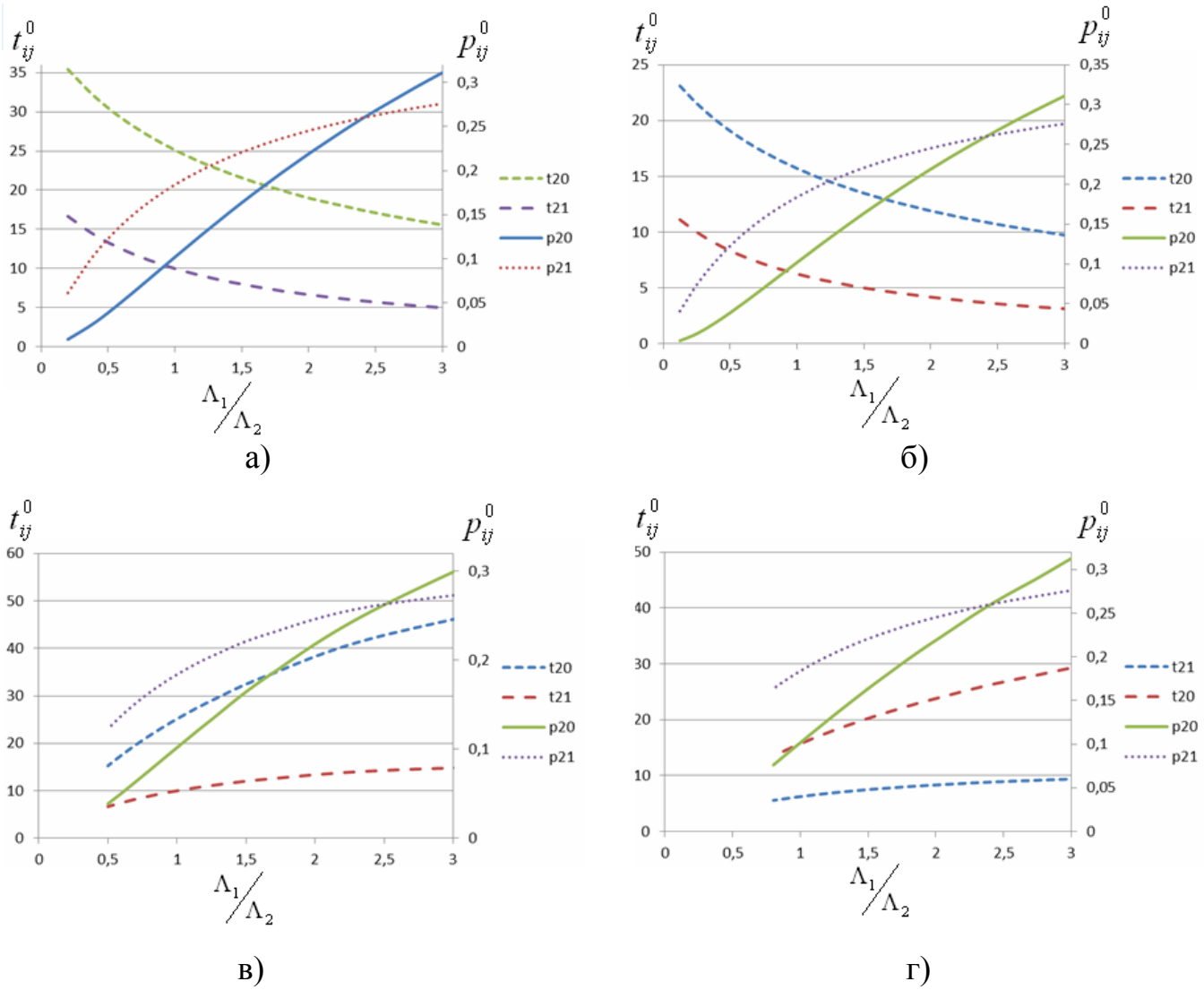


Рис. 4.14. Вплив відношення Λ_1/Λ_2 на оптимальні значення p_{ij}^0, t_{ij}^0:

а) $\Lambda_2 = 0,05$; $\Lambda_1 - \text{var}$; б) $\Lambda_2 = 0,08$; $\Lambda_1 - \text{var}$;

в) $\Lambda_1 = 0,05$; $\Lambda_2 - \text{var}$; г) $\Lambda_1 = 0,08$; $\Lambda_2 - \text{var}$;

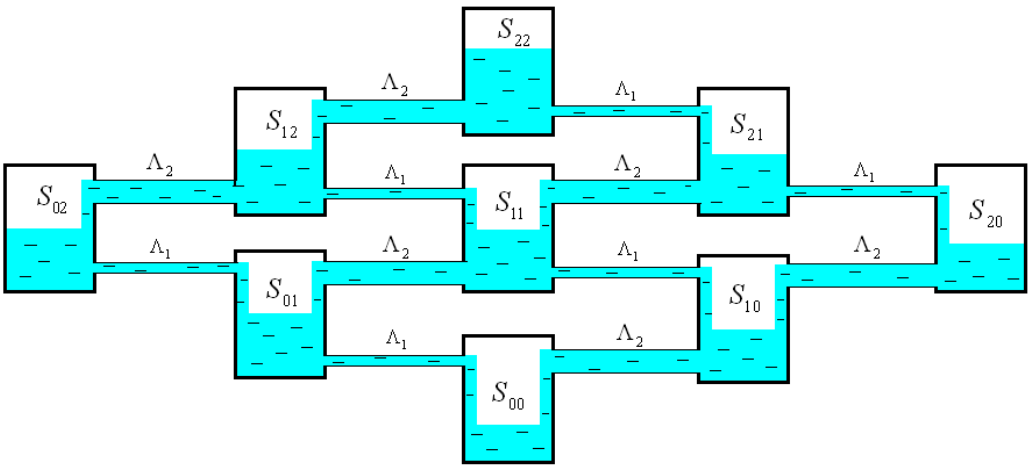


Рис. 4.15. Еквівалентна гідравлічна система

Величина p_{ij} має значення швидкості течії з ij-го резервуара, котра визначається тиском води в ньому, Λ_1 і Λ_2 - площі поперечних перерізів труб. Витік з резервуара S_{ij} в $S_{i,j-1}$ здійснюється через трубу з поперечним перерізом Λ_1, а з S_{ij} в $S_{i-1,j}$ - з поперечним перерізом Λ_2. Швидкість наповнення, а потім вивільнення резервуара при заданих Λ_1, Λ_2 визначається часовою залежністю значень $p_{ij}(t)$. Для резервуара S_{20} це $p_{21}(t)$ і $p_{20}(t)$. Обидві функції спочатку зростають, досягаючи своїх максимумів в певні моменти часу, а потім спадають. Час, за який досягається максимальне значення p_{20}^0, залежить як від функцій $p_{21}(t)$, $p_{20}(t)$, так і від значень Λ_1, Λ_2. Для резервуару S_{20} різниця $\Lambda_1 p_{21} - \Lambda_2 p_{20}$ визначає об'єм води, котрий прибуває (чи вибуває) за одиницю часу. Таким чином, диференціальні рівняння Колмогорова описують водяний баланс відповідних резервуарів.

Використання еквівалентної структури спрощує розуміння одержаних закономірностей [64,73]. Для прикладу, на рис. 4.14,в,г при $\Lambda_1/\Lambda_2 < 2{,}5$ отримано $p_{20}^0 < p_{21}^0$, а при $\Lambda_1/\Lambda_2 > 2{,}5$ — $p_{20}^0 > p_{21}^0$. Це можна пояснити тим, що на рис.4.14,в,г малі значення Λ_1/Λ_2 досягаються за рахунок значних величин Λ_2 при фіксованому Λ_1 (саме варіант $\Lambda_2 > \Lambda_1$ показано на рис. 4.15). При цьому резервуар S_{20} не встигає наповнитись, і p_{20}^0 не досягає великих значень. При великих значеннях Λ_1/Λ_2 спостерігається протилежна ситуація і $p_{20}^0 > p_{21}^0$.

Далі розглянуто варіанти ускладнення схеми протистояння. Збільшення кількості об'єктів в однорідній системі, де всі об'єкти кожної з сторін однакові, не викликає принципових змін, лише стає більш громіздкою схема протистояння, оскільки зростає кількість можливих станів, і, відповідно, процедура розрахунків. Перехід до неоднорідної схеми може вестись в декількох напрямках, які визначаються параметрами, котрими відрізняються окремі об'єкти. До цих параметрів відносяться:

g_k - відносна вартість інформації на об'єкті;

p_k - імовірність успішного нападу на об'єкт, яка залежить від уразливості об'єкта;

λ_k - частота нападів на об'єкт, яка залежить від кон'юнктури ринку.

Оскільки величини p_k і λ_k входять в розрахунок у вигляді добутку $p_k\lambda_k = \Lambda_k$, то задача зводиться до виявлення впливу двох розрахункових параметрів - g_k і Λ_k. Граф системи, в якій кожна з двох сторін містить два об'єкти з різними Λ_k, зображено на рис. 4.16.

Верхні індекси в позначенні станів виражають номери неушкоджених об'єктів, а в позначенні частоти успішних нападів – номер об'єкта, на який направлена спроба. Так, $S_{21}^{(2)}$ позначає стан, в якому неушкодженими залишились два об'єкти першої сторони і один об'єкт другої сторони, причому неушкодженим об'єктом другої сторони є другий об'єкт. Величина $\Lambda_1^{(1)}$ визначає частоту успішних спроб першої сторони, направлених на перший об'єкт другої сторони.

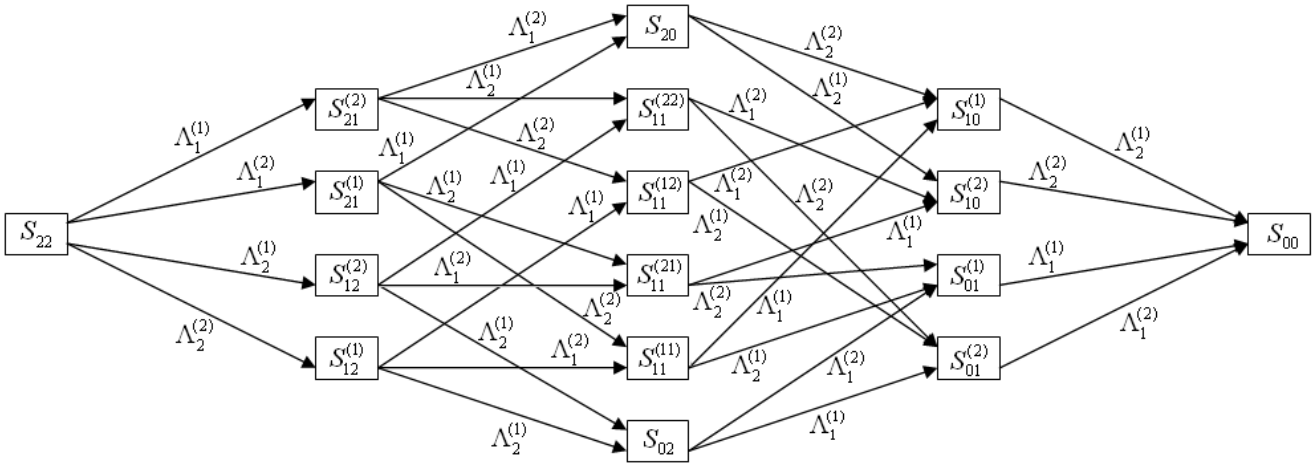


Рис. 4.16. Граф неоднорідної системи

При нерівномірному розподілі інформації по об'єктах, коли об'єкти відрізняються не тільки уразливістю (тобто параметрами p_k), а й відносною вартістю інформації g_k, граф системи залишається незмінним, проте стани

тепер будуть відрізнятись не тільки номерами неушкоджених об’єктів, а й часткою захищеної і здобутої інформації.

Наведену методику можна розповсюдити на більшу кількість об’єктів, які відрізняються відносною вартістю інформації, частотою нападів та імовірністю досягнення успіху. Розрахункові вирази стають при цьому громіздкими, проте задача піддається розв’язанню з допомогою програмних засобів. Проведений аналіз можна розглядати як крок до створення методу динамічного адаптивного управління ресурсами в умовах багатостороннього протистояння.

Для прикладу розглянуто випадок, коли співвідношення $\frac{\Lambda_1}{\Lambda_2} = 2$. При цьому $\Lambda_1 = 0{,}1$, а $\Lambda_2 = 0{,}05$. Якщо $\lambda_1 = \lambda_2$, то $p_1 = 2p_2$. Виконавши деякі розрахунки, знайдено $\frac{y}{x}$ на першому і другому об’єктах: $\left(\frac{y}{x}\right)_1 = 0{,}125$, $\left(\frac{y}{x}\right)_2 = 0{,}255$. Тоді $Y = y_1 + y_2 = \frac{x_2}{0{,}255} + 0{,}125x_1$, якщо $x_1 = x_2$, то можна підрахувати відношення загальних ресурсів першої сторони до другої: $\frac{Y}{X} = 0{,}129$.

Висновки до 4 розділу

1. В умовах конкурентної боротьби в інформаційному протистоянні зростає роль проведення розвідки при розробці заходів щодо захисту інформації. Врахування різнонаправленого характеру протистояння, коли кожна сторона прагне захистити власну інформацію і отримати несанкціонований доступ до інформації суперника, в окремих випадках дає змогу раціонально використати ресурси та отримати максимальний економічний ефект.

2. Перехід до двонаправленого протистояння суттєво розширює коло проблем, котрі виникають при проектуванні систем інформаційної безпеки. Важливими показниками при пошуку оптимального розподілу ресурсів є відносна вартість інформації, якою володіє кожна з сторін, її розміщення на об'єктах, уразливості об'єктів, розподіл ресурсів між об'єктами. Критерієм оптимальності є досягнення максимальної ефективності інвестиції в інформаційну безпеку, тобто максимальної сумарної вартості захищеної і здобутої інформації.

3. Математична модель різнонаправленого інформаційного протистояння включає цільову функцію $F(x, y)$, що визначає сумарний прибуток в результаті зменшення величини завданої шкоди від реалізації загроз інформації $j(x, y)$ за рахунок внесення інвестицій в об'єкти захисту та здобуття інформації $i(x, y)$ суперника.

4. Ключовим завданням при моделюванні різнонаправленого протистояння є визначення часової залежності інформаційного балансу конкуруючих сторін в умовах постійних спроб здобуття інформації, що дозволяє визначити момент часу, коли імовірність загрози найвища та необхідне внесення інвестицій у захист інформації.

РОЗДІЛ 5
ЕФЕКТИВНІСТЬ ЗАПРОПОНОВАНОГО МЕТОДУ ТА МОДЕЛЕЙ ДИНАМІЧНОГО УПРАВЛІННЯ РЕСУРСАМИ

5.1. Методика проведення експерименту

Для перевірки ефективності запропонованого підходу проведено обчислювальний експеримент, який полягає у наступному. У відповідності до запропонованого методу обчислено оптимальні розподіли ресурсів між об’єктами захисту з різними характеристиками. У якості вихідних даних використано параметри СЗІ функціонуючого підприємства.

Метою експерименту являється оцінка адекватності та ефективності розробленого методу за результатами порівняння функціонуючої СЗІ і системи з оптимальним розподілом ресурсів захисту розрахованим з допомогою розробленої методики.

Проведення експерименту включає наступні етапи:

1) побудова математичної моделі СЗІ на основі наданої інформації про вартість інформації на об’єктах, їх уразливість, імовірність нападу на об’єкти, імовірність виділення певної кількості ресурсів нападу на кожен з об’єктів;

2) визначення оптимального розподілу ресурсів захисту між об’єктами захисту;

3) представлення результатів розрахунків у найбільш доступній та інформативній формі (таблиці та графіки);

4) представлення висновків та надання рекомендацій.

Рішення про оптимальний розподіл ресурсів захисту приймаємо згідно з критерієм $i^0 = \min\limits_{\{y_k\}} \max\limits_{\{x_k\}} i = \max\limits_{\{x_k\}} \min\limits_{\{y_k\}} i$, що відповідає сідловій точці цільової функції і гарантує мінімум збитків за найгірших умов.

Відхилення від рішення, що відповідає сідловій точці, приводить до погіршення результату, тому відхилення нападу від оптимального розподілу

своїх ресурсів $\{x_k^0\}$ при незмінному розподілі ресурсів захисту $\{y_k^0\}$ зменшує величину завданої шкоди від реалізації загроз інформації. Збільшення збитків спостерігаємо при відхиленні від оптимального розподілу ресурсів захисту $\{y_k^0\}$ при сталому розподілі ресурсів нападу $\{x_k^0\}$.

Ефективність використання ресурсів захисту розраховуємо за формулою:

$$E = \frac{1 - \sum_{k=1}^{l} i_k}{Y}, \qquad (5.1)$$

де за 1 приймаємо інформацію, що потребує захисту, $\sum_{k=1}^{l} i_k$ - відносна величина завданої шкоди від реалізації загроз на об'єктах. Оскільки у знаменнику $Y = const = 0{,}05$ (вважаємо доцільним використання на захист ресурсів, що еквівалентні 5% вартості інформації), максимальна можлива ефективність $E = 20$.

5.2. Ефективність використання розробленої моделі

Застосування розробленої моделі показано на прикладі приватного підприємства «Волиньхолдінг». Підприємство займається виробництвом харчових продуктів та являється лідером серед українських виробників соусів. ПрАТ «Волиньхолдінг» (якому належить торгова марка «Торчин») входить до складу компанії Nestle в Україні та співпрацює з іноземними партнерами. Технологія виробництва продукції постійно вдосконалюється та є об'єктом інтелектуальної власності підприємства. Захист активів підприємства є важливом елементом успішної діяльності підприємства. Захисту підлягають:

- персональні дані працівників підприємства;
- територія фабрики, будівлі та приміщення;
- технологія виробництва (інформація в електронному вигляді, структура технологічних ліній);
- фінансова діяльність підприємства.

Для підтримання належного рівня захищеності критичної інформації підприємство виділяє 5% від величини очікуваного прибутку від використання цієї інформації. Розподіл цих коштів між елементами захисту на даний час проводиться методом експертних оцінок (рис. 5.1).

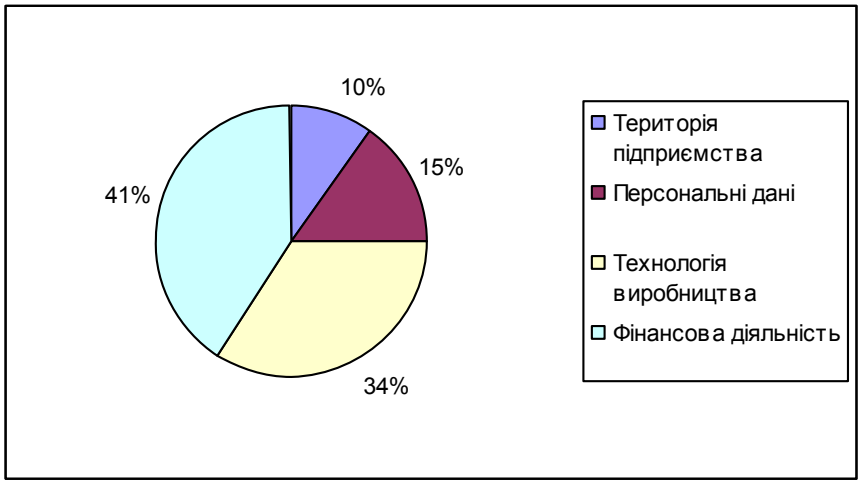


Рис. 5.1 Розподіл ресурсів захисту підприємства між об'єктами захисту

Згідно з даними підприємства відносна вартість інформації, що підлягає захисту, на кожному об'єкті становить: $g_1 = 0{,}05$, $g_2 = 0{,}15$, $g_3 = 0{,}45$, $g_4 = 0{,}35$. Для кожного об'єкту встановлено форму функцій уразливості $f_k = \dfrac{(x_k / y_k)^n}{(x_k / y_k)^n + c}$. Таким чином, вхідні дані для розрахунку оптимального розроділу ресурсів захисту за допомогою розробленої моделі (2.1) приведені у табл. 5.1.

У ході дослідження розраховано мінімальна величина завданої шкоди від реалізації загроз інформації при існуючій системі захисту (базовий розподіл ресурсів захисту: $y_1 = 0{,}10$, $y_2 = 0{,}15$, $y_3 = 0{,}34$, $y_4 = 0{,}41$). Оптимальни варіант розподілу ресурсів знайдено згідно з методом динамічного управління ресурсами та при цьому розраховані відповідна очікувана сумарна шкода від реалізації загроз інформації. Результати приведені у таблиці 5.2 для різних значень співвідношення $Z = X/Y$ ресурсів нападу і захисту, при яких існує сідлова точка. Значення E ефективності розподілу ресурсів відповідають

сідловій точці, через $E_б$ позначено ефективність базового розподілу прийнятого на підприємстві.

Таблиця 5.1

Опис об'єктів захисту підприємства ПрАТ «Волиньхолдінг»

Номер об'єкта, k	Об'єкти захисту	Відносна вартість інформації, що підлягає захисту, на k -му об'єкті, g_k	Відносна кількість коштів, виділена підприємством для захисту k -го об'єкта, y_k	Функція уразливості k -го об'єкта, $f_k(x,y)$
1	Територія фабрики, будівлі та приміщення	0,05	0,10	$f_k = \frac{(x_k/y_k)^1}{(x_k/y_k)^1 + 16}$
2	Персональні дані працівників	0,15	0,15	$f_k = \frac{(x_k/y_k)^2}{(x_k/y_k)^2 + 16}$
3	Технологія виробництва	0,45	0,34	$f_k = \frac{(x_k/y_k)^2}{(x_k/y_k)^2 + 120}$
4	Фінансова діяльність підприємства	0,35	0,41	$f_k = \frac{(x_k/y_k)^2}{(x_k/y_k)^2 + 64}$

Таблиця 5.2

Ефективність оптимального розподілу ресурсів захисту на ПрАТ «Волиньхолдінг» при $Y = 0{,}05$, $g_1 = 0{,}05$, $g_2 = 0{,}15$, $g_3 = 0{,}45$, $g_4 = 0{,}35$

Параметри функцій уразливості $f_k = \frac{(x_k/y_k)^n}{(x_k/y_k)^n + c}$		$Z = X/Y$	Розподіл ресурсів захисту, що відповідає сідловій точці		Існуючий (базовий) розподіл ресурсів захисту інформації	
			Максимальна очікувана шкода від реалізації загорз інформації, i^0	$E^0 = \frac{1-i^0}{Y}$	$\max\limits_{\{x_k\}} i_б$	$E_б = \frac{1-i_б}{Y}$
$n_1 = 1$	$c_1 = 16$	3,5	0,0799	18,4023	0,2175	15,65
$n_2 = 2$	$c_2 = 16$	4	0,0896	18,2073	0,2288	15,424
$n_3 = 2$	$c_3 = 120$	4,5	0,0992	18,0164	0,2396	15,208
$n_4 = 2$	$c_4 = 64$	5	0,1085	17,8294	0,2497	15,006

На рис. 5.2 та 5.3 для порівняння існуючого та оптимального розподілів ресурсів приведені значення очікуваної шкоди від реалізації загроз інформації та, відповідно, ефективності використання ресурсів.

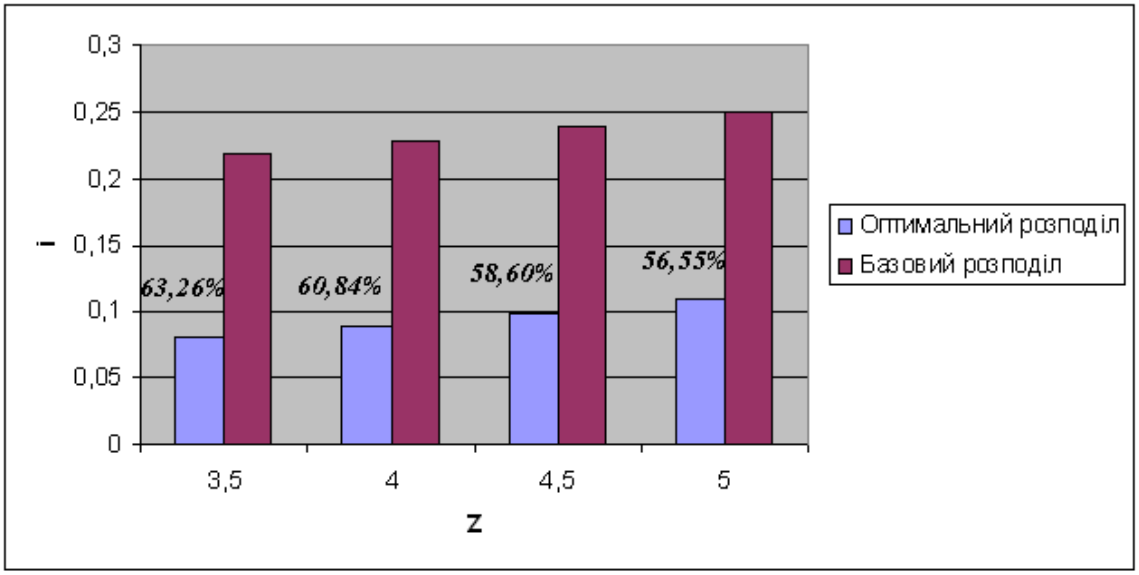


Рис. 5.2. Зниження величини очікуваної шкоди від реалізації загроз інформації при переході від базового розподілу ресурсів захисту до оптимального

За результатами розрахунків зроблено висновок, що при застосуванні оптимального розподілу ресурсів, розрахованого із використанням розробленої моделі, величина очікуваної шкоди від реалізації загроз інформації порівняно із базовим розподілом знижується більш, ніж вдвічі.

На рис. 5.3 приведено для порівняння ефективності розглянутих варіантів розподілу ресурсів.

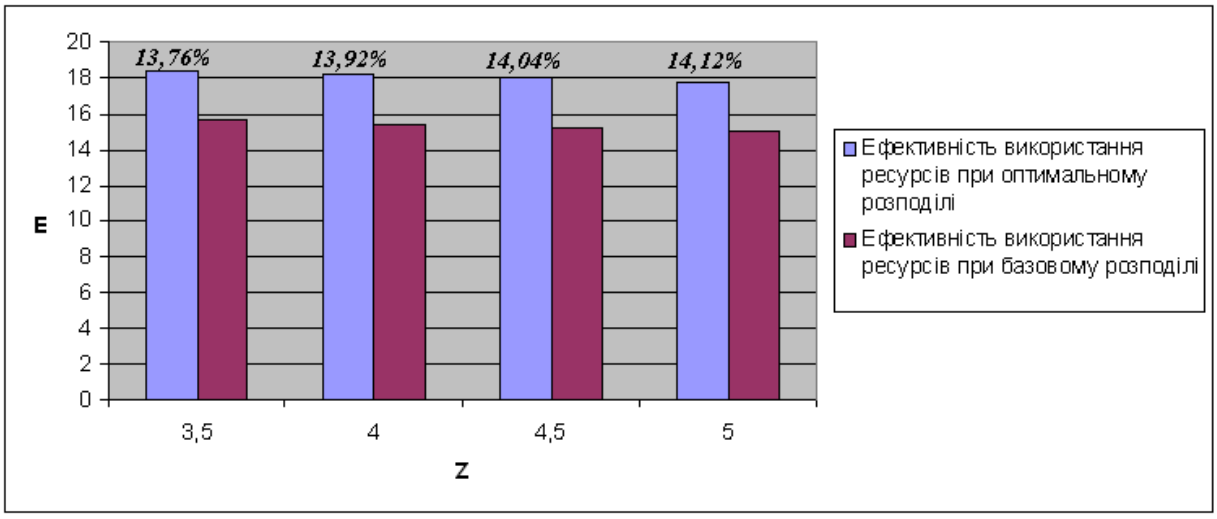


Рис. 5.3 Підвищення ефективності використання ресурсів захисту при переході до оптимального розподілу

За результатами проведених експериментів робимо висновок, що ефективність оптимального розподілу ресурсів, визначеного із використанням запропонованого у дослідженні методу, вища порівняно із базовим варіантом розподілу ресурсів (рис. 5.3).

Запропонований підхід визначає оптимальний розподіл ресурсів, що гарантує мінімальні збитки за найбільш несприятливих умов у будь-яких системах, тоді як, зазвичай, при виборі варіанту розподілу ресурсів акцентується увага на одному із показників (відносна вартість інформації g_k на об'єкті, уразливість f_k об'єкта, мінімальна очікувана шкода від реалізації загроз інформації). Таким чином, запропонована модель із цільовою функцією, що включає усі згадані показники, являється гнучкою, не потребує окремого аналізу параметрів системи та зручна при наданні рекомендацій, чим обґрунтовується ефективність та адекватність моделі.

5.3. Ефективність методів визначення оптимального розподілу ресурсів у динамічному режимі

За результатами проведених досліджень виявлено, що у системах з кількістю об'єктів більше 2 ($l > 2$) сідлова точка у чистих стратегіях може існувати при певних значеннях співвідношення $Z = X/Y$ ресурсів нападу X і захисту Y. Наприклад, у розрахунках приведених у п. 5.2 при $Z = 3$ (табл. 5.2) сідлової точки не існує. У таких випадках рішення приймаємо на основі аналізу динамічного протистояння, коли напад і захист почергово здійснюють кроки. Кожен крок сторони нападу відповідає розподілу ресурсів x_k, що забезпечує максимальну очікувану шкоду від реалізації загроз інформації, крок захисту відповідає розподілу y_k, за якого, враховуючи попередній крок нападу, величина завданої шкоди буде мінімальною.

У зв'язку із розміщенням інформації про персональні дані працівників та фінансову діяльність підприємства на одному сервері та використанням

спільних механізмів захисту цієї інформації об'єкти 2 і 4 можуть бути об'єднані в один. Вивільнені при цьому кошти розподілено між двома іншими об'єктами (табл. 5.3)

Таблиця 5.3

Опис об'єктів захисту підприємства ПрАТ «Волиньхолдінг»

Об'єкти захисту	Відносна вартість інформації, що підлягає захисту, на k-му об'єкті, g_k	Відносна кількість коштів, виділена підприємством для захисту k-го об'єкта, y_k	Функція уразливості k-го об'єкта, $f_k(x, y)$
Територія фабрики, будівлі та приміщення	0,05	0,15	$f_k = \frac{(x_k / y_k)^1}{(x_k / y_k)^1 + 16}$
Технологія виробництва	0,45	0,40	$f_k = \frac{(x_k / y_k)^2}{(x_k / y_k)^2 + 120}$
Фінансова діяльність підприємства та персональні дані працівників	0,50	0,45	$f_k = \frac{(x_k / y_k)^2}{(x_k / y_k)^2 + 64}$

На основі даних підприємства (табл. 5.3) проведно аналіз динамічного управління ресурсів $i(n)$, де n - номер кроку, приведеного на рис. 5.4. У результаті обрано розподіл між об'єктами підприємства із ваговими коефіцієнтами $g_1 = 0{,}05$; $g_2 = 0{,}45$; $g_3 = 0{,}5$, який гарантує мінімальну очікувану шкоду від реалізації загроз інформації при найбільш несприятливих умовах.

В ситуації, зображеній на рис. 5.4. захист припиняє гру у точці С, коли його власний черговий крок (точка А) для нього є невигідним, оскільки він несе загрозу наступного кроку суперника, котрий приведе до значних збитків (точка В).

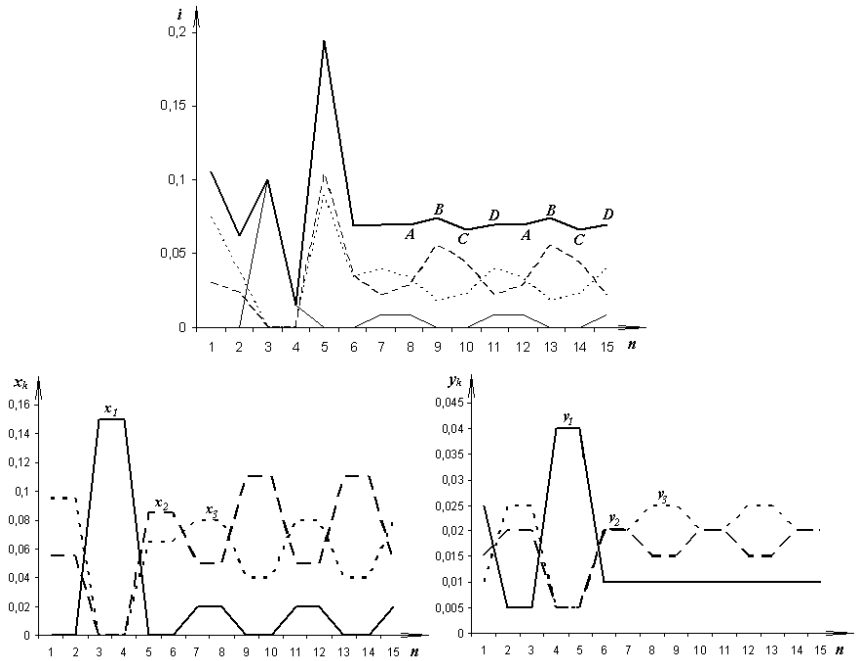


Рис. 5.4 Динамічне управління ресурсами для захисту об’єктів підприємства (табл. 5.3) і співвідношенні ресурсів нападу і захисту Z=3

Аналіз ефективності описаного методу приведено у таблиці 5.4 та на рис.5.5.

Таблиця 5.4

Ефективність методу визначення оптимального розподілу ресурсів у динамічному режимі

	$\{y_k\}$	$\{x_k\}$	$\max\limits_{\{x_k\}} i$ (точка D)	$E = \frac{1-i}{Y}$	Величина завданої шкоди від реалізації загроз інформації на наступному кроці $\max\limits_{\{x_k\}} i$ (точка B)	$E = \frac{1-i}{Y}$
Оптимальний розподіл ресурсів захисту	0,005; 0,02; 0,025	0,15; 0; 0	0,0699	18,602	0,0741	18,518
Базовий розподіл ресурсів захисту	0,025; 0,015; 0,01	0; 0,055; 0,095	0,1053	17,894	0,1000	18

За результатами розрахунків зроблено висновок, що ефективність обраного розподілу $E = 18{,}602$ вища за ефективність на наступному кроці – $E = 18{,}518$. Базовий розподіл ресурсів захисту є менш ефективним, і наступний крок лише покращить результат.

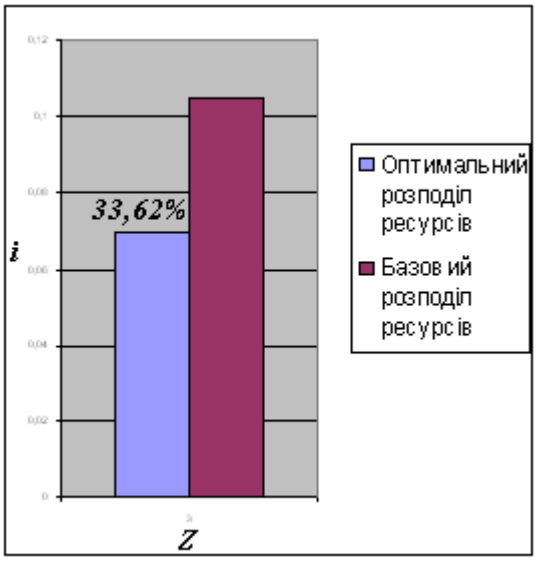


Рис. 5.5. Зниження рівня очікуваної шкоди від реалізації загроз інформації при переході від базового розподілу до оптимального

З рис. 5.5. видно при розрахованому оптимальному розподілі ресурсів максимальна очікувана шкода від реалізації загроз інформації не перевищать значення 0,07, що на 33,62% менше, аніж при базовому розподілі коштів на даний час. Дані числа значно менші, ніж у випадку існування сідлової точки (рис. 5.2, 5.3), однак, в умовах невизначеності (за відсутності інформації про дії суперника), коли сідлової точки у чистих стратегіях не існує, розроблений метод дозволяє визначити оптимальний розподіл ресурсів в динамічному режимі при найбільш несприятливих умовах і при цьому гарантує найменші очікувані збитки від реалізації загроз.

5.4. Результати впровадження методів оптимізації розподілу ресурсів захисту інформації на ПрАТ «Волиньхолдінг»

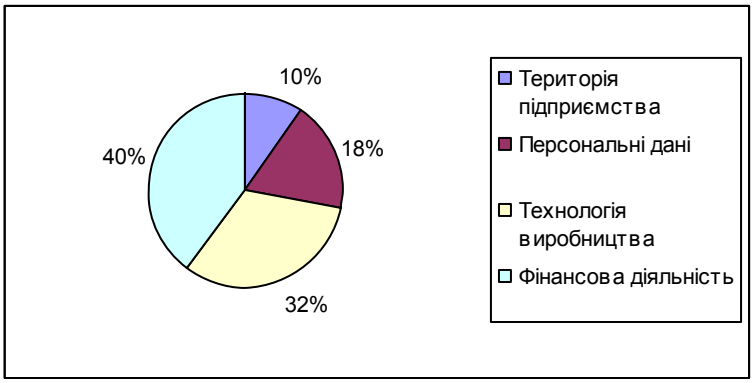
У результаті проведеного моделювання функціонуючої системи захисту інформації на ПрАТ «Волиньхолдінг» з метою оптимізації розподілу коштів, виділених на захист інформації, запропоновано наступні рішення.

1. Інформацію про персональні дані працівників та фінансову діяльність підприємства розмістити на одному файловому сервері. Для

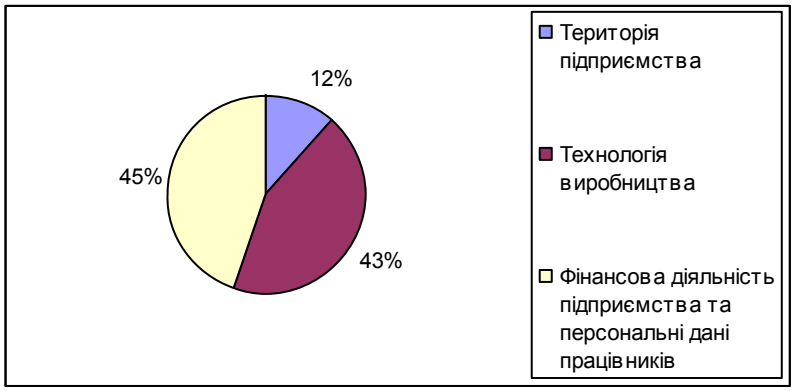
контролю санкціонованого використання об'єктів інформаційної системи застосувати засоби розмежування доступу.

Вивільнені кошти внаслідок об’єднання двох об’єктів розподілити між об’єктами, що залишились.

Оптимальний розподіл коштів знайдено із використанням розробленого методу динамічного управління ресурсами (рис. 5.6). Вхідні дані для розрахунку приведені у табл. 5.1.



а)



б)

Рис. 5.6 Розподіл ресурсів захисту підприємства між об’єктами захисту а) базовий; б) оптимальний

За результатами проведеного моделювання інформаційної системи, що складається із трьох об’єктів захисту інформації, виявлено, що оптимальним варіантом є розподіл вивільнених 18% коштів наступним чином (табл. 5.5):

- 2% коштів направити на захист території фабрики, будівель та приміщень;
- 11% – на захист технологій виробництва продукції;

- 5% – на захист інформації про фінансову діяльність підприємства та персональні дані працівників.

Таблиця 5.5

Опис об'єктів захисту підприємства ПрАТ «Волиньхолдінг» внаслідок реалізації управлінського рішення

Об'єкти захисту	Відносна вартість інформації, що підлягає захисту, на k-му об'єкті, g_k	Відносна кількість коштів, виділена підприємством для захисту k-го об'єкта, y_k	Функція уразливості k-го об'єкта, $f_k(x, y)$
Територія фабрики, будівлі та приміщення	0,05	0,12	$f_k = \frac{(x_k / y_k)^1}{(x_k / y_k)^1 + 16}$
Технологія виробництва продукції	0,45	0,43	$f_k = \frac{(x_k / y_k)^2}{(x_k / y_k)^2 + 120}$
Фінансова діяльність підприємства та персональні дані працівників	0,50	0,45	$f_k = \frac{(x_k / y_k)^2}{(x_k / y_k)^2 + 64}$

Вибір засобів захисту проводиться на основі аналізу моделі загроз та моделі порушника (рис.5.7.).

Обґрунтування вибору додаткових засобів захисту проводиться із використанням розробленої моделі на основі формалізованої схеми функціонування системи захисту інформації. Для прикладу приведено результати розрахунків для вибору оптимального набору засобів захисту інформації про технологію виробництва. Схема розташування елементів інформаційної системи зображена на рис. 5.8., 5.9.

Модель загроз		
Розкриття	Порушення цілісності	Відмова в обслуговуванні
витік крадіжка	модифікація видалення підміна	блокування ресурсів інформаційної системи блокування системи ідентифікації

Модель порушника	
Внутрішні порушники	Зовнішні порушники: Конкуренти Недобросовісні партнери Хакери
Мотиви порушення:	
- ненавмисні порушення; - реакція на догану; - злий намір; - продаж інформації; - промисловий шпіонаж	
Шляхи отримання несанкціонованого доступу	
- підкуп - фото- і відеозйомка - перехват ЕМВ - крадіжка носіїв інформації - копіювання інформації - отримання реквізитів розмежування доступу, паролів	

Рис. 5.7. Побудова моделі загроз та моделі порушника

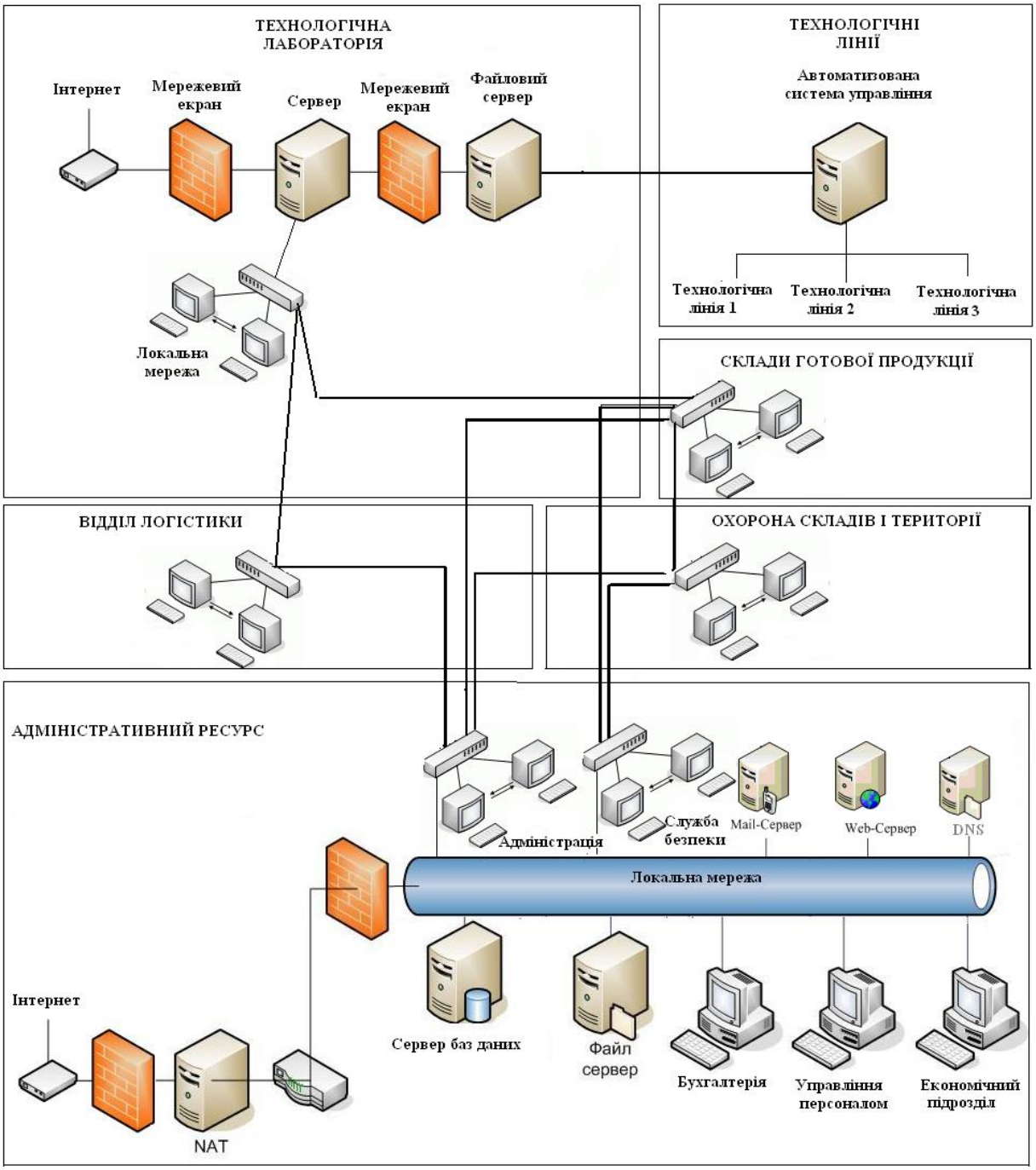


Рис. 5.8. Базова схема інформаціїйної системи технологічного цеху підприємства ПрАТ «Волиньхолдінг»

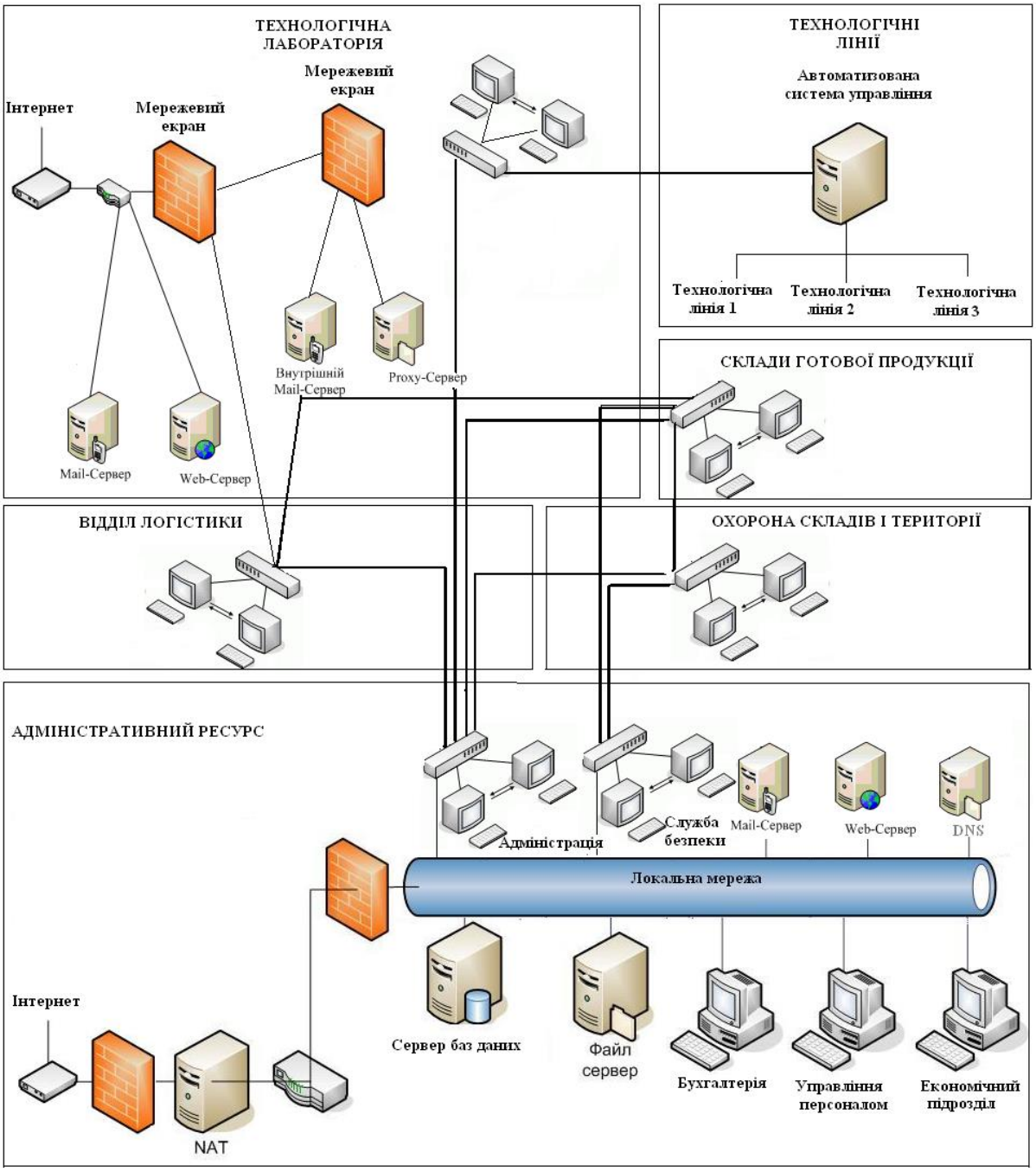


Рис. 5.9. Оптимальна схема інформаціїйної системи технологічного цеху підприємства ПрАТ «Волиньхолдінг»

Методом експертної оцінки визначено ефективність кожного додаткового засобу захисту проти наявних загроз (табл. 5.6)

Таблиця 5.6

Імовірності нейтралізації загроз засобами захисту, $f(y)$

Засоби захисту, r	Перелік загроз, s				$\max_s f_{rs}$
	Модифікація даних	Відмова в обслуговуванні	Підбір паролів	Витік інформації	
Системи ідентифікації та аутентифікації	0,1	0,3	0,7	0,1	0,3
Антивірусне програмне забезпечення	0,1	0,1	0,1	0,2	0,2
Шифрування даних	0,6	0,1	0,4	0,8	0,8
Резервне копіювання	0,9	0,2	0,1	0,1	0,9
$\min_r f_{rs}$	0,1	0,1	0,1	0,1	

Таблиця 5.7

Оптимальний розподіл виділених коштів між обраними засобами захисту

Засоби захисту	Відносна кількість ресурсів на засоби захисту, y_k	Зменшення очікуваної завданої шкоди
Системи ідентифікації та аутентифікації	0,18	7%
Антивірусне програмне забезпечення	0,09	11%
Шифрування даних	0,43	15%
Резервне копіювання	0,30	9%

Згідно з проведеними розрахунками, розмір ***очікуваної завданої шкоди при використанні нових засобів захисту знизиться з*** $i = 0{,}1199$ ***до*** $i^0 = 0{,}0699$ ***(на 42%).*** Вплив окремих засобів захисту на зменшення втрат приведено на рис.5.10.

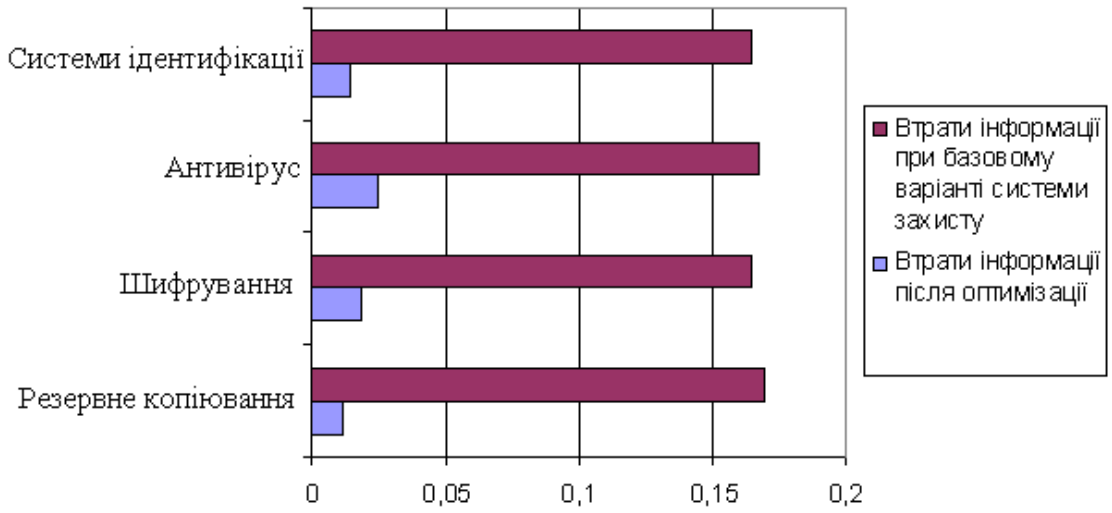


Рис. 5.10. Зменшення очікуваної шкоди від реалізації загроз інформації при використанні нових засобів захисту

2. В результаті проведених досліджень запропоновано:

- встановлення антивірусного програмного забезпечення;

- впровадження нової системи ідентифікації та аутентифікації на технологічних лініях;

- застосування методів шифрування інформації про технологічні розробки, що зберігається на файловому сервері;

- виділення додаткового інформаційного простору для резервного копіювання інформації.

Висновки до 5 розділу

1. Теоретичні положення, моделі та методи, представлені у даній роботі дозволяють забезпечити необхідний рівень захищеності інформаційних систем за рахунок оптимального розподілу ресурсів захисту інформації між елементами систем із врахуванням часової зміни умов протистояння.

2. У ході обчислювального експерименту показано підвищення ефективності захисту в результаті застосування оптимального розподілу ресурсів, визначеного з використанням розроблених моделі та методу порівняно із базовим варіантом захисту. Запропонований метод визначає оптимальний розподіл ресурсів, що гарантує мінімальну величину завданої шкоди від реалізації загроз інформації за найбільш несприятливих умов у будь-яких системах, тоді як, зазвичай, при виборі варіанту розподілу ресурсів акцентується увага на одному із показників (відносна вартість інформації g_k на об'єкті, уразливість f_k об'єкта, мінімальна очікувана шкода).

3. За результатами порівняння функціонуючої системи захисту інформації і системи з оптимальним розподілом ресурсів захисту, розрахованим з допомогою розробленого методу на прикладах чисельно показанно ефективність розробленого методу. Реалізація оптимального розподілу ресурсів захисту забезпечить зниження величини очікуваної завданої шкоди від реалізації загроз інформації на 33,62% у порівнянні із базовим розподілом, запровадженим на підприємстві.

4. У результаті проведеного моделювання функціонуючої системи захисту інформації на ПрАТ «Волиньхолдінг» з метою оптимізації розподілу коштів, виділених на захист інформації, запропоновано наступні рішення:

- інформацію про персональні дані працівників та фінансову діяльність підприємства розмістити на одному файловому сервері;

- обрано механізми захисту, що зменшить розмір очікуваної шкоди на 42%.

ЗАГАЛЬНІ ВИСНОВКИ

Проведені дослідження направлені на підвищення рівня захищеності інформації при динамічному протистоянні конкуруючих сторін за рахунок оптимізації розподілу ресурсів захисту між елементами систем із врахуванням часової зміни умов протистояння. Розроблена модель і методи її застосування дозволяють визначити не тільки загальну кількість ресурсів, які доцільно використати на захист інформації, а й оптимізувати їх розподіл між об’єктами в багаторівневих багаторубіжних системах, які відрізняються кількістю об’єктів, їх уразливістю, розподілом інформації між об’єктами.

В ході розв’язання поставлених задач отримано такі наукові результати:

1. Проведено аналіз теоретико-ігрових методів прийняття рішень та математичних моделей управління ресурсами захисту інформації, відмічено, що лишається відкритим питання оптимального розподілу інвестицій між об’єктами захисту, відсутні моделі управління ресурсами в динамічному режимі, чим обґрунтовано напрямки досліджень та задачі дисертаційної роботи.

2. Розроблено і досліджено математичну модель багаторубіжної системи захисту інформації, яка дає можливість оптимізувати використання ресурсів захисту в системах, які відрізняються кількістю об’єктів, розташуванням перешкод, їх уразливістю, відносною вартістю інформації на об’єктах при різних співвідношеннях ресурсів нападу і захисту. В результаті досліджень обгрунтовано вибір цільової функції моделі та функціональних залежностей, що входять до складу цільової функції. Особливу увагу приділено функції динамічної уразливості об’єктів, що описує різні типи інформаційних систем. Визначення зон найбільшої економічної доцільності витрат в складних системах захисту інформації дозволяє розрахувати об’єм ресурсів, що забезпечують досягнення заданих значень продуктивностей та підвищення ефективності використання внесених коштів.

3. На базі запропонованої математичної моделі сформовано метод динамічного управління ресурсами захисту інформації, що дає можливість обгрунтувати рішення щодо розподілу ресурсів та виявити вплив внесених інвестицій на значення величини завданої шкоди від реалізації загроз інформації і знизити рівень збитків інформації на 55-63%. Метод дозволяє визначити умови досягнення стаціонарних режимів і знайти відповідну величину очікуваної завданої шкоди. При динамічному управлінні розподіл ресурсів проводиться з затримкою – після того, як визначено націленість атак, що забезпечує досягнення оптимальних показників в ситуаціях, які постійно змінюються. На основі імітаційного моделювання наслідків почергового прийняття рішень сторонами нападу і захисту визначено показники інформаційного протистоянння в динамічному режимі, які враховують оптимальний розподіл ресурсів і відповідну частку втрат.

4. Запропоновано метод удосконалення технології динамічного регулювання розподілу ресурсів захисту на базі теоретико-ігрових методів та розробленої моделі реалізації процесу пошуку оптимальних рішень, яка враховує зміну параметрів та характеристик системи захисту залежно від дій зловмисника та підвищити ефективність використання ресурсів захисту на 14%. Запропонований метод завдяки врахуванню дій суперника дає змогу оцінити наслідки прийнятих рішень, прогнозувати розмір завданої шкоди від реалізації загроз інформації і у разі відсутності сідлової точки у чистих стратегіях обрати таке рішення, що гарантує найменшу величину завданої шкоди від реалізації загроз інформації при найбільш несприятливих умовах.

5. Розроблено модель реалізації процесів різнонаправленого протистояння конкуруючих сторін в умовах постійних спроб здобуття інформації, які розглядаються як неперервний випадковий процес; модель враховує часові зміни умов протистояння, завдяки чому з’явилась можливість визначити стан інформаційної безпеки у конкретний момент часу. Цільова функція $F(x, y)$ моделі визначає сумарний інформаційний здобуток в результаті зменшення

величини завданої шкоди від реалізації загроз інформації $j(x, y)$ за рахунок внесення інвестицій в об’єкти захисту та здобуття інформації $i(x, y)$ суперника.

6. На основі імітаційного моделювання наслідків почергового прийняття рішень сторонами нападу і захисту сформульовано рекомендації щодо оптимізації розподілу ресурсів та оцінки величини очікуваної завданої шкоди від реалізації загроз інформації, які були використані при розробці нової системи захисту на ПрАТ «Волиньхолдінг». Реалізація оптимального розподілу ресурсів захисту забезпечить зниження рівня очікуваної шкоди на 42% у порівнянні із базовим розподілом, запровадженим на підприємстві.

7. На основі імітаційного моделювання різнонаправленого протистояння конкуруючих сторін завдяки розрахунку моменту часу, коли імовірність успішної атаки найвища, сформульовано практичні рекомендації щодо нейтралізації загроз.

8. Сформульовано рекомендації щодо проведення аналізу ефективності використання розробленого інвестиційного методу при оптимальному розподілі ресурсів захисту, що дозволяє оцінити гарантованість інформаційної безпеки.

9. Розроблено програмний апарат комплексної реалізації процесу динамічного управління ресурсами в складних інформаційних системах, який дозволяє автоматизувати процес оптимального розподілу ресурсів захисту в багаторубіжних системах захисту інформації, що містять довільну кількість об’єктів з різною уразливістю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андронов А.А. Теория колебаний. / А.А. Андронов, А.А. Витт, С.Э.Хайкин. – М.: ГИФМЛ. – 1959. – 915 с.

2. Андрощук Г.А. Экономическая безопасность предприятия: защита коммерческой тайны. / Г.А. Андрощук, П.П. Крайнев. – К.: Изд. Дом «Ин Юре», 2000. – 400 с.

3. Анохин А.М. Методы определения коэффициентов важности критериев. / А.М. Анохин, В.А. Глотов, В.В. Павельев, А.М. Черкашин // Автоматика и телемеханика. – 1997. – №8. – С.3-35.

4. Архипов А.Е. Применение экономико-мотивационных соотношений для оценивания вероятностных параметров информационных рисков // Захист інформації. – 2011. – №2(51). – С.69-76.

5. Архипов О.Є. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації / А.Є. Архипов, А.В. Скиба // Захист інформації. – 2013. – №4. – С.366-375.

6. Белов А.И. Составление электрических схем, эквивалентных механическим колебательным системам // ЖТФ. – 1935. – т.5, вып. 9. – С. 1545-1551.

7. Беллман Р. Динамическое программирование. – М.: Изд-во Иностранная литература. – 1960. – 400 с.

8. Боровик О.Л. Дослідження операцій в економіці. / О.Л. Боровик, Л.В.Боровик. – К.: Центр учбової літератури. – 2007. – 424 с.

9. Бочарников В.П. Fuzzy-технология: Математические основы. Практика моделирования в экономике. – С.-Пб.: «Наука». – 2001. – 328с.

10. Бочарников В.П. Свешников С.В. Fuzzy Technology: Основы моделирования и решения экспертно-аналитических задач. / В.П. Бочарников С.В. Свешников – К.: Эльга, Ника-Центр. – 2003. – 296 с.

11. Булгаков Б.В. Колебания. – М.: ГИТТЛ. – 1954. – 891 с.

12. Васин А.А. Теория игр и модели математической экономики. /

А.А.Васин, В.В.Морозов. – М.: МАКС Пресс. – 2005. – 272 с.

13. Вентцель Е.С. Исследование операций. – М.: Сов. Радио. – 1972. – 552с.

14. Вентцель Е.С. Теория вероятностей. / Е.С. Вентцель, Л.А. Овчаров. – М.: Наука. – 1973. – 366 с.

15. Вентцель Е.С. Прикладные задачи теории вероятностей. / Е.С.Вентцель, Л.А. Овчаров. – М.: Радио и связь. – 1983. – 416 с.

16. Вентцель Е.С. Теория случайных процессов и ее инженерные приложения. / Е.С. Вентцель, Л.А. Овчаров. – М.: Наука. – 1991. – 295 с.

17. Вербовська Г.В. Динамічне управління ресурсами захисту інформації / Г.В. Вербовська, Є.Г. Левченко // Захист інформації. – 2011. – №1(50). – С.74-80.

18. Герасименко В.А. Защита информации в автоматизованных системах обработки данных. Кн. 1. / В.А. Герасименко. – М.: Энергоатомиздат, 1994. – 400 с.

19. Гермейер Ю.Б. Введение в теорию исследования операций. – М.: Наука. – 1971. – 383 с.

20. Гихман И.И. Теория вероятностей и математическая статистика / И.И.Гихман, А.В. Скороход, М.И. Ядренко. – К.: Вища школа. – 1988. – 438 с.

21. Глушак В.В. Синтез структури системи захисту інформації з використанням позиційної гри захисника та зловмисника / В.В. Глушак, О.М.Новіков // Системні дослідження та інформаційні технології. – 2013. – №2. – С. 89-100.

22. Гончар М.С. Математичні основи інформаційної економіки. – К.: Ін-т теор. фізики. – 2007. – 464 с.

23. Гриців Л.І. Вплив особливостей об'єктів на оптимальний розподіл ресурсів захисту / Л.І. Гриців, А.О. Рабчун // Защита информации: сб. науч. трудов НАУ. – К.: НАУ. – 2010. – вып. 17. – С.204-207.

24. Грищук Р.В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальний ігор та диференціальних перетворень: Монографія / Р.В. Грищук. – Житомир: Рута, 2010. – 280 с.

25. Грищук Р.В. Ігрові методи аналізу кібератак на інформаційну сферу / Р.В. Грищук, С.Ж. Піскун, В.О. Хорошко, Ю.Є. Хохлачова // Захист інформації. – 2012. – №1.

26. Глухов В.В. Математические методы и модели менеджмента / В.В.Глухов, М.Д. Медников, С.Б. Коробко. – С-Пб.: Лань. – 2005. – 528 с.

27. Глушик М.М. Дослідження операцій / М.М. Глушик, Н.М.Телесницька. – Львів: «Новий світ - 2000». – 2009. – 368 с.

28. Гурский Е.И. Сборник задач по теории вероятностей и математической статистике. – Минск: Высшая школа. – 1984. – 223 с.

29. Давыдов Э.Г. Методы и модели теории антагонистических игр. – М.: Изд. Моск. Ун-та. – 1978. – 208 с.

30. Демчишин М.В. Геометрична інтерпретація оптимізації розподілу ресурсів між об'єктами захисту інформації // Захист інформації. – 2011. – №2(51). – С.21-28.

31. Демчишин М.В. Ефективність розвідки при протистоянні двох сторін в інформаційній сфері / М.В. Демчишин, Є.Г.Левченко // Сучасний захист інформації. – 2011. – №2. – С.5-15.

32. Домарев В.В. Безопасность информационных технологий. – М.: Diasoft. – 2004. – 992 с.

33. Дрешер М. Стратегические игры. – М.: Сов. Радио. – 1964. – 352 с.

34. Журиленко Б.Е., Николаева Н.К., Пелих Н.С. Оценка стойкости технической защиты информации во времени / Б.Е. Журиленко, Н.К. Николаева, Н.С. Пелих // Захист інформації. – 2012. – №1. – С.104-108.

35. Журиленко Б.Е. Математическая модель вероятностной надежности комплекса технической защиты информации // Безпека інформації. – 2012. – №2(18). – С.61-65.

36. Журиленко Б.Е. Определение вероятностной надежности единичной технической защиты информации из реальных попыток взлома // Безопасность информации. – 2013. – №1(19). – С.34-39.

37. Задірака В.К. Фінансування витрат на захист інформації в економічній

діяльності / В.К.Задірака, О.С. Олексюк, Р.П. Смоленюк, П.І. Штабалюк // Університетські наукові записки. – 2006. – №3-4 (19-20). – С.479-490.

38. Зайченко Ю.П. Исследование операций. – К.: «Слово». – 2003 – 688 с.

39. Замков О.О. Математические методы в экономике / О.О. Замков, А.В. Толстопятенко, Ю.Н. Черемных. – М.: Изд. «Дело и Сервис». – 2004. – 368 с.

40. Івченко І.Ю. Математичне програмування. – К.: Центр учбової літератури. – 2007. – 232 с.

41. Івченко І.Ю. Моделювання економічних ризиків і ризикових ситуацій. – К.: Центр учбової літератури. – 2007. – 343 с.

42. Исследование операций. Сб. статей под. ред. Ю.Б. Гермейера. – М.: Наука. – 1972. – №2.

43. Исследование операций в экономике / Под ред. Н.Ш. Кремера. – М.: ЮНИТИ. – 2006. – 407 с.

44. Катренко А.В. Дослідження операцій. – Львів: «Магнолія». – 2009. – 352с.

45. Корченко А.Г. Анализ и оценивание рисков информационной безопасности / А.Г. Корченко, А.Е. Архипов, С.В. Казмирчук. К.: ООО «Лазурит-Полиграф». – 2013. – 275 с.

46. Корченко О.Г. Методологія синтезу та програмна реалізація системи оцінювання шкоди нацональній безпеці у сфері охорони державної таємниці / О.Г.Корченко, М.Г. Луцький, М.В. Захарова, Ю.О. Дрейс // Захист інформації. – 2013. – том 15. – №1. – С. 14-20.

47. Крушевский А.В. Теория игр. – К.: Вища школа. – 1977. – 216 с.

48. Кулініч Р.В. Продуктивність інвестицій в інформаційну безпеку / Р.В.Кулініч, Є.Г. Левченко // Захист інформації. – 2011. – №1(50). – С.80-84.

49. Лабскер Л.Г. Вероятностное моделирование в финансово-экономической области. – М.: Альпина Паблишер. – 2002. – 224 с.

50. Лабскер Л.Г. Игровые методы в управлении экономикой и бизнесом / Л.Г. Лабскер, Л.О. Бабешко. – М.: Дело. – 2001. – 460 с.

51. Левченко Є.Г. Оптимізація розподілу ресурсів між об'єктами захисту

інформації // Захист інформації. – 2007. – №1. – С.33-38.

52. Левченко Є.Г. Математичні моделі економічного менеджменту інформаційної безпеки / Є.Г. Левченко, М.В.Демчишин, А.О. Рабчун // Системні дослідження та інформаційні технології. – 2011. – №4. – С.88-96.

53. Левченко Є.Г. Експертні оцінки в економічних задачах інформаційної безпеки / Є.Г. Левченко, А.О. Рабчун // Захист інформації. – 2009. – №3. – С.81-85.

54. Левченко Є.Г. Модель Гросса в протистоянні двох сторін у сфері захисту інформації / Є.Г. Левченко, А.О. Рабчун // Сучасна спеціальна техніка. – 2009. – №3(18). – С.75-81.

55. Левченко Є.Г. Оптимізаційні задачі менеджменту інформаційної безпеки / Є.Г. Левченко, А.О. Рабчун // Сучасний захист інформації. – 2010. – №1. – С.16-23.

56. Левченко Є.Г. Неперервні марковські ланцюги у визначенні станів інформаційної безпеки / Є.Г. Левченко, А.О. Рабчун // Сучасний захист інформації. – 2011. – №3. – С.66-69.

57. Левченко Є.Г. Неоднорідні напівмарковські ланцюги у визначенні рівня інформаційної безпеки / Є.Г. Левченко, А.О. Рабчун // Безпека інформації. – 2012. – №2. – С.22-27.

58. Лук'янова В.В. Економічний ризик / В.В. Лук'янова, Т.В. Головач. – К.: Академвидав. – 2007 – 462 с.

59. Мигулин В.В. Основы теории колебаний / В.В. Мигулин, В.И.Медведев, Е.Р. Мустель, В.Н. Парыгин. – М.: Наука. – 1978. – 392 с.

60. Михалевич В.С. Методы последовательной оптимизации в дискретных сетевых задачах оптимального распределения ресурсов / В.С.Михалевич, А.И.Кукса. – М.: «Наука». – 1983. – 208 с.

61. Молодцов Д.В. Модель Гросса // ЖВММФ. – 1972. – т.2. – №12. – С.309-320.

62. Нейман Дж. Теория игр и экономическое поведение / Дж. Нейман, О.Моргенштерн. – М.: Наука. – 1970. – 983 с.

63. Подиновский В.В. Аксиоматическое решение проблемы оценки важности критериев в многокритериальных задачах // Современное состояние теории исследования операций. –М.: Наука. – 1979. – С.117-149.

64. Понтрягин Л.С. Математическая теория оптимальных процессов / Л.С.Понтрягин, В.Г. Болтянський, Р.В. Гамкрелидзе, Е.Ф. Мищенко. – М.: Физматгиз. – 1961. – 391 с.

65. Применение теории игр в военном деле / под ред. В.О. Ашкеназы. – М.: Сов. Радио. – 1964. – 360 с.

66. Пугачев В.С. Теория вероятностей и математическая статистика. – М.: Наука. – 1979. – 495 с.

67. Рабчун А.О. Аналіз статистики нападів в сфері інформаційної безпеки // Вісник Інженерної академії України. – 2010. – №2. – С. 18-27.

68. Рабчун А.О. Оптимізація сумарних втрат в сфері захисту інформації // Безпека інформації. – 2012. – №1. – С.32-36.

69. Рабчун А.О. Методи та моделі оптимізації показників систем захисту інформації в умовах інформаційного протиборства. Дисертація на здобуття наукового ступеня. – К.: НАУ. – 2014. – 120 с.

70. Ржевский С.В. Дослідження операцій / С.В. Ржевский, В.М.Александрова – К.: Академвидав. – 2006. – 560 с.

71. Саати Т.Л. Математические модели конфликтных ситуаций. – М.: Сов. Радио. – 1977. – 302 с.

72. Сборник задач по теории вероятностей, математической статистике и теории случайных функций / Под ред. А.А. Свешникова. – М.: Наука. – 1965. – 656 с.

73. Современная математика для инженеров / Под ред. Э. Беккенбаха. – М.: Изд. иностр. Литератур. – 1959. – 500 с.

74. Смирнов Н.В. Дунин-Барковский И.В. Краткий курс математической статистики для технических приложений / Н.В. Смирнов, И.В. Дунин-Барковский. – М.: Физматгиз. – 1959. – 436 с.

75. Таха Х. Введение в исследование операций. – М.: Вильяме. – 2001. –

912 с.

76. Тихонов В.И. Марковские процессы / В.И. Тихонов, М.А. Миронов – М.: Сов. Радио. – 1977. – 488 с.

77. Федоренко І.К. Дослідження операцій в економіці / І.К. Федоренко, О.І. Черняк, О.О. Карагодова, Г.О. Чорноус, О.В. Горбунов. – К.: Знання. – 2007. – 558 с.

78. Хаяси Т. Нелинейные колебания в физических системах. – М.: Мир. – 1968. – 293 с.

79. Ховард Р. Динамическое програмирование и марковские процессы. – М.: Сов. Радио. – 1964. – 280 с.

80. Челкован В.І. Матричний підхід до оцінки інформаційних ризиків / В.І.Челкован, А.О. Рабчун // Защита информации: сб. науч. трудов НАУ. – К.: НАУ. – 2010. – вып. 17. – С.109-112.

81. Чемерис А. Методи оптимізації в економіці / А. Чемерис, Р. Юринець, О. Мищишин. – К.: Центр учбової літератури. – 2006. – 152 с.

82. Шапкин А.С. Экономические и финансовые риски. – М.: Изд.-торг. корпорація «Дашков и К°». – 2006. – 544 с.

83. Шикин Е.В.Исследование операций / Е.В. Шикин, Г.Е. Шикина.– М.: Проспект. – 2006. – 280 с.

84. Штонер Р. Многокритериальная оптимизация. – М.: Радио и связь. – 1992. – 504с.

85. Bellman R. Decision-making in a fuzzy environment / R. Bellman, L.Zadeh // Management science. – 1970. – V.I7. – №4. – pp.141-164.

86. Böhme R. The Iterated Weakest Link: A Model of Adaptive Security Investment / R. Böhme, T. Moor. – WEIS, London June 24, 2009.

87. Dulois D. Fuzzy Real Algebra: Some Results / D. Dulois, H. Prade // Fuzzy Sets and Systems. – vol.2. – 979 p.

88. Gordon L. Return on Information Security Investments: Myths vs. Reality / L. Gordon, M. Loeb // Strategic Finance. – Nov. 2002. – pp. 26-31.

89. Gordon L. The Economics of Information Security Investment / L. Gordon,

M. Loeb // ACM Transactions on Information and System Security. – Nov. 2002. – Vol. 5. – №4. – pp.438-457.

90. Huang C.D. Economics of Information Security investment in the Case of Simultaneous Attacks / C.D. Huang, Q. Hu, R.S. Behara.// Proceedings of the Fifth Workshop on the Economics of Information Security, June 26-28, 2006, Cambridge, England.

91. Lui W. Empirical Analysis Methodology for Information Security Investment and its Application to a Reliable Survey of Japanese Firms / W. Lui, H.Tanaka, K. Matsuura // Information Proceeding of Japan Digital Courier. – Vol.3. – Sept. 2007. – pp. 585-599.

92. Marcovitz H.M. Portfolio Selection: Efficient Diversification of Investment – New York.: John Wiley, 1959.

93. Matsuura K. Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model, The Seventh Workshop on the Economics of Information Security. June 25-28, Hanover, USA – 2008.

94. Moitra S., Konda S. A Simulation Model for Managing Survivability of Networked Information Systems // Technical Report CMU / SEI – 2000 – TR – 020, Dec.2000.

95. Paulauskas N. Survivability Modelling of Lithuanian Government Information System / N. Paulauskas, E. Garsva, L. Gulbinovic, A. Stankevicius, D.Poviliauskas // Electronics and Electrical Engineering. – Kaunas: Technologija, 2012. – No. 4(120). – P. 95-98.

96. Richardson. R. 2007 CSI/FBI Computer Crime and Security Survey.

97. Richardson. R. 2008 CSI/FBI Computer Crime and Security Survey.

98. Richardson. R. 2010/2011 CSI Computer Crime and Security Survey.

99. Tatsumi Ken-ichi. Optimal Timing of Information Security Investment: A Real Options Approach / Ken-ichi Tatsumi, Makoto Goto – WEIS, July 21, 2009.

100. Левченко Є.Г. Визначення об’єктів захисту інформації в умовах обмеженості коштів / Є.Г. Левченко, Р.Б. Прус // Защита информации: сб. науч. тр. НАУ. – 2008. – №15. – С. 35-38.

101. Прус Р.Б. Застосування теоретико-ігрових методів при побудові системи захисту інформації // Інтегровані інтелектуальні робототехнічні комплекси 2008. Збірник тез за матеріалами міжнародної науково-практичної конференції, 19-23 травня 2008 р. – К.: НАУ. – 2008. – С. 155-156.

102. Левченко Є.Г. Антагоністичні ігри у сфері інформаційної безпеки / Є.Г.Левченко, Р.Б. Прус, В.А. Швець // Інформаційна безпека. Зб. тез за мат. наук.-практ. конф. 26-27 бер. 2009 р. – К.: ДУІКТ. – 2009. – С.161-165.

103. Прус Р.Б. Вибір цільової функції та її вплив на розподіл ресурсів захисту інформації // Защита информации: сб. науч. тр. НАУ. – К.: НАУ. – 2009. – №16. – С. 172-175.

104. Прус Р.Б. Модель визначення об'єктів та засобів захисту підприємства від загроз / Р.Б. Прус, А.С. Сільченко // Защита информации: сб. науч. тр. НАУ. – К.: НАУ. – 2009. – №16. – С. 192-195.

105. Прус Р.Б. Моделювання конфліктних ситуацій в економічних задачах інформаційної безпеки // Захист інформації в інформаційно-комунікаційних системах. Збірник тез за матеріалами науково-практичної конференції, 25-27 травня 2009 р. – К.:НАУ. – 2009. – С.15.

106. Левченко Є.Г. Показники багатоступінчастих систем захисту інформації / Є.Г. Левченко, Р.Б. Прус, А.О. Рабчун // Вісник Інженерної академії України. – 2009. – №1. – С.61-65.

107. Левченко Є.Г. Багаторівневий розподіл ресурсів між елементами систем захисту інформації / Є.Г. Левченко, Р.Б. Прус, В.А. Швець // Вісник Інженерної академії України. – 2009. – №2. – С.90-94.

108. Prus R.B. Formation of the objective function in the tasks of information security management / R.B. Prus, V.A. Shvets // The Fourth World Congress "Aviation in the XXI-st Century" Safety in Aviation and Space Technologies. September 21-23, 2010. – pp. 17.14 – 17.17.

109. Левченко Є.Г. Оптимізаційні економічні задачі в системах захисту інформації / Є.Г. Левченко, Р.Б. Прус // Системні дослідження та інформаційні

технології. – 2011. – №2. – С. 98-103.

110. Левченко Є.Г. Розподіл ресурсів інформаційної безпеки в динамічному режимі / Є.Г. Левченко, Р.Б. Прус, В.А. Швець // Захист інформації. – 2011. – №4. – С. 31-35.

111. Прус Р.Б. Динамічна модель процесу захисту інформації в задачах розподілу ресурсів // Комплексне забезпечення якості технологічних процесів та систем. Збірник тез за матеріалами II міжнародної науково-практичної конференції, 23-25 травня 2012 р. – С. 122-123.

112. Прус Р.Б. Оптимізація розподілу ресурсів захисту інформації в динамічному режимі // Безпека інформації. – 2012. – №1. – С. 26-32.

113. Левченко Є.Г. Показники продуктивності витрат на захист інформації / Є.Г. Левченко, Р.Б. Прус, Д.І. Рабчун // Безпека інформації. – 2012. – №2. – С.6-11.

114. Левченко Є.Г. Динамічне протистояння в умовах конкурентної боротьби / Є.Г.Левченко, Р.Б. Прус, Д.І. Рабчун // Сучасна спеціальна техніка. – 2012. – №4. – С.150-158.

115. Левченко Є.Г. Умови існування сідлової точки в багаторубіжних системах захисту інформації / Є.Г. Левченко, Р.Б. Прус, Д.І. Рабчун // Безпека інформації. – 2013. – №1. – С. 70-76.

116. Левченко Є.Г. Вплив форми протистояння на оптимізацію процесу управління ресурсами захисту інформації / Є.Г. Левченко, Р.Б. Прус, Д.І. Рабчун // Безпека інформації. – 2013. – №3. – С. 218-223.

117. Левченко Є.Г. Рішення зворотної задачі економічного менеджменту інформаційної безпеки / Є.Г. Левченко, Р.Б. Прус // Захист інформації. – 2014. – Том 16, №2. – С.167-171.

ДОДАТОК А

Програмний код методу пошуку оптимальних рішень в умовах динамічного протистояння

```
clear
G=1; % Сукупна вартість інформації
q=0.5; % Розподіл інформації між обєктами
g1=q*G;
g2=(1-q)*G;
X=0.5; % Виділені ресерси нападу
Y=0.1; % Виділені ресурси захисту
ratio=X/Y;
x1_x2_lim=ratio; % Обмеження ресурсів нападу X=x1+x2
x_ob=X;
y_ob=Y;

% Залежності f(x,y) (Параметри)
delta_x_y=100;
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
x=X/delta_x_y:X/delta_x_y:X;
x_y=ratio/delta_x_y:ratio/delta_x_y:ratio; % Відносна шкала x/y
x_vis=x_y; %Встановлення осі x-ів
y=y_ob;
a1=sym('1');
a2=sym('1');
a_1=char(a1);
a_2=char(a2);
a1=double(a1);
a2=double(a2);
b1=sym('1');
b2=sym('1');
b_1=char(b1);
b_2=char(b2);
b1=double(b1);
b2=double(b2);
n1=sym('1');
n2=sym('2');
n_1=char(n1);
n_2=char(n2);
n1=double(n1);
n2=double(n2);
c1=sym('4');
c2=sym('32');
c_1=char(c1);
c_2=char(c2);
```

```
c1=double(c1);
c2=double(c2);
% y1=g1*(a1*(x./y).^n1./((x./y).^n1+c1));
% y2=g2*(a2*(x./y).^n2./((x./y).^n2+c2));
% y1_=10*diff(y1,1);
% y2_=10*diff(y2,1);
% y1_diff=[y1_(1) y1_];
% y2_diff=[y2_(2) y2_];

y1=g1*(a1*(x_y).^n1./((x_y).^n1+c1));
y2=g2*(a2*(x_y).^n2./((x_y).^n2+c2));
y1_=10*diff(y1,1);
y2_=10*diff(y2,1);
y1_diff=[y1_(1) y1_];
y2_diff=[y2_(2) y2_];

figure ('Position',[100 100 600 400])
hold on
w1=plot (x_vis,y1,'-k','LineWidth',2);
w2=plot (x_vis,y2,'--k','LineWidth',2);
w3=plot (x_vis,y1_diff,'-k','LineWidth',1);
w4=plot (x_vis,y2_diff,'--k','LineWidth',1);
plot_handles=[w1(1) w2(1) w3(1) w4(1)];
string1=['1) i_1(x,y)=' num2str(g1) '*' a_1  '(x/y)^{' num2str(n_1) '}/((x/y)^{' num2str(n_1) '}+'
num2str(c_1) ')'];
string2=['2) i_2(x,y)=' num2str(g2) '*' a_2  '(x/y)^{' num2str(n_2) '}/((x/y)^{' num2str(n_2) '}+'
num2str(c_2) ')'];
font1=10;
string3=['{\fontsize{' num2str(font1) '}3) d(i_1)/dx}' ];
string4=['{\fontsize{' num2str(font1) '}4) d(i_2)/dx}' ];
legend(plot_handles, string1, string2, string3, string4, 3);
xlim([0,max(x_vis)])
ylim_max1=1.2*max([y1 y2]);
ylim_max2=ceil(100*ylim_max1);
ylim([0,ylim_max2/100])
%xlabel(['x, (y=' num2str(y) ')'])
xlabel(['x/y'])
ylabel('i(x)')
pos1=ceil(1/3*delta_x_y);
pos2=ceil(2/3*delta_x_y);
pos3=delta_x_y;
%makedatatip(w1(1), pos1);
%makedatatip(w1(1), pos2);
makedatatip(w1(1), pos3);
%makedatatip(w2(1), pos1);
%makedatatip(w2(1), pos2);
makedatatip(w2(1), pos3);
hold off

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

```
Resources_min=0.01;
Resources_max=0.3;
step=0.01;
Resources=Resources_min:step:Resources_max;
Graph=0; % True=1, False=0;
precision=6; % Точність, кількість знаків після коми
y_open_door_percent=50; % "Відкриті двері" сторни захисту (мінімальне значення y1,y2 у відсотках до Y)
Y_min_lim=Y*y_open_door_percent/100;

for i=1:1:length(Resources) % Виділені ресерси нападу

clear Y_optimization
clear X_optimization
X=Resources(i);
count=1;
I_opt_X=0;
I_opt_Y=1;

while (I_opt_X(count)~=I_opt_Y(count))&&(count<=20)
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

% 1) Формування поверхні функції f(x1,x2)
if (count==1)
Y1=Y/2;
Y2=Y/2;
else
Y1=Y1_opt;
Y2=Y2_opt;
end

kroku(i)=count;
count=count+1;

A=[1 1]; % Коефіцієнти обмежувальних нерівностей (x1+x2<=X)
b=[X];
Aeq=[]; % Коефіцієнти обмежувальних рівняня
beq=[];
x0=[X; X];
lx=[0; 0]; % Нижня межа x1 та x2
ux=[X; X]; % Верхня межа x1 та x2
nonlcon=[];
%options=[];
options = optimset('Algorithm','interior-point');

% if (Y1==0)
%    X1_opt=0;
%    X2_opt=X;
%    I1_opt=g1*a1;
%    I2_opt=g2*a2*(X2_opt/Y2).^n2./((X2_opt/Y2).^n2+c2);
```

```
%     Z_max=I1_opt+I2_opt;
%     I1_opt_x(i)=round(Z_max*10^p)/10^p;
% end
% if (Y2==0)
%     X1_opt=X;
%     X2_opt=0;
%     I1_opt=g1*a1*(X1_opt/Y1).^n2./((X1_opt/Y1).^n2+c2);
%     I2_opt=g2*a2;
%     Z_max=I1_opt+I2_opt;
%     I1_opt_x(i)=round(Z_max*10^p)/10^p;
% end
% if (Y1~=0)&&(Y2~=0)
    myfun_opt=@(x)(-
1*(g1*(a1*(x(1)./Y1).^n1./((x(1)./Y1).^n1+c1))+g2*(a2*(x(2)./Y2).^n2./((x(2)./Y2).^n2+c2))));
    [x_opt_fmincon, I_opt_x_fmincon]= fmincon(@(x)myfun_opt(x), x0, A, b, [], [], lx, ux,
nonlcon, options);
    X1_opt=x_opt_fmincon(1);
    X2_opt=x_opt_fmincon(2);
    Ratio_X_1=X1_opt/Y1;
    Ratio_X_2=X2_opt/Y2;
    %disp ([I_opt_x  X1_opt X2_opt])
%     if (round(X1_opt*10^p)/10^p==0)
%         X1_opt=0;
%         X2_opt=X;
%     end
%     if (round(X2_opt*10^p)/10^p==0)
%         X1_opt=X;
%         X2_opt=0;
%     end

   % Визначення оптимальних значень I1(x1) та I2(x2)
   I1_opt=g1*a1*(X1_opt/Y1).^n1./((X1_opt/Y1).^n1+c1);
   I2_opt=g2*a2*(X2_opt/Y2).^n2./((X2_opt/Y2).^n2+c2);
   Z_max=I1_opt+I2_opt;
   I_opt_X(count)=round(-1*I_opt_x_fmincon*(10^precision))/10^precision;

   %disp ([Z_max  X1_opt X2_opt I1_opt_x(count)])
%end

X_optimization(count,:)=[(count-1) X X1_opt X2_opt I_opt_X(count) I1_opt I2_opt Ratio_X_1
Ratio_X_2];
%display ([num2str(i-2) ')   Xmax      x1_0      x2_0  I(x1_0,x2_0) I1_x1_0   I2_x2_0']);
%disp ([X X1_opt X2_opt Z_max I1_opt I2_opt]);

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%

% 2) Формування поверхні функції f(y1,y2)
X1=X1_opt;
X2=X2_opt;
```

```
A=[1 1]; % Коефіцієнти обмежувальних нерівностей (y1+y2<=X)
b=[Y];
Aeq=[]; % Коефіцієнти обмежувальних рівняня
beq=[];
y0=[0; 0];
ly=[0; 0]; % Нижня межа x1 та x2
uy=[Y; Y]; % Верхня межа x1 та x2
nonlcon=[];
%options=[];
options = optimset('Algorithm','interior-point');


myfun_opt=@(y)(g1*(a1*(X1/y(1))^n1/((X1/y(1))^n1+c1))+g2*(a2*(X2/y(2))^n2/((X2/y(2))^n2+c
2)));
   [y_opt_fmincon, I_opt_y_fmincon]= fmincon(@(y)myfun_opt(y), y0, A, b, [], [], ly, uy, nonlcon,
options);
   Y1_opt=y_opt_fmincon(1);
   Y2_opt=y_opt_fmincon(2);

   % Визначення оптимальних значень I1(x1) та I2(x2) (Двері)
if (Y1_opt<Y_min_lim)
%if (round(Y1_opt*(10^precision))/10^precision==0)
   Y1_opt=Y_min_lim;
   Y2_opt=Y-Y1_opt;
elseif (Y2_opt<Y_min_lim)
%elseif (round(Y2_opt*(10^precision))/10^precision==0)
   Y2_opt=Y*y_open_door_percent/100;
   Y1_opt=Y-Y2_opt;
end

   Ratio_Y_1=X1/Y1_opt;
   Ratio_Y_2=X2/Y2_opt;

   I1_opt=g1*a1*(X1/Y1_opt).^n1./((X1/Y1_opt).^n1+c1);
   I2_opt=g2*a2*(X2/Y2_opt).^n2./((X2/Y2_opt).^n2+c2);
   Z_max=I1_opt+I2_opt;
   I_opt_Y(count)=round(I_opt_y_fmincon*(10^precision))/10^precision;

Y_optimization(count,:)=[(count-1) Y Y1_opt Y2_opt I_opt_Y(count) I1_opt I2_opt Ratio_Y_1
Ratio_Y_2];
%display ([num2str(i-2) ')   Ymax      y1_0      y2_0  I(y1_0,y2_0) I1_y1_0   I2_y2_0']);
%disp ([Y Y1_opt Y2_opt Z_max I1_opt I2_opt]);

end

X_optimization=X_optimization(2:end,:);
Y_optimization=Y_optimization(2:end,:);

for j=1:1:length(X_optimization(:,1))
disp ([num2str(j) ')    X       x1       x2       I       I_x1      I_x2       R_x1      R_x2']);
disp(X_optimization(j,2:end))
```

```
disp ([num2str(j) ')    Y       y1        y2       I       I_y1     I_y2       R_y1      R_y2']);
disp(Y_optimization(j,2:end))
end

display(['Кількість кроків: ' num2str(kroku(end)) '. Точність: ' num2str(precision) ' знаки(-ів) 
після коми.'])
display(['Оптимум I: ' num2str(X_optimization(end,5))  ' при  x1=' 
num2str(X_optimization(end,3)) ', x2='  num2str(X_optimization(end,4)) ', (X=' 
num2str(X_optimization(end,3)+X_optimization(end,4)) ')'])
display ([])

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%

optumym_I_X(i)=X_optimization(end,5);
optumym_I1_x1(i)=X_optimization(end,6);
optumym_I2_x2(i)=X_optimization(end,7);

optumym_R1(i)=X_optimization(end,8);
optumym_R2(i)=X_optimization(end,9);
optumym_R1_x1(i)=X_optimization(end,3);
optumym_R1_y1(i)=Y_optimization(end,3);
optumym_R2_x2(i)=X_optimization(end,4);
optumym_R2_y2(i)=Y_optimization(end,4);

%optumym_R1_y(i)=Y_optimization(end,8);
%optumym_R2_y(i)=Y_optimization(end,9);

if Graph==1
summa1=summa1(3:end,:);
summa2=summa2(3:end,:);
g_count=summa1(:,1);
g_x1=summa1(:,3);
g_x2=summa1(:,4);
g_I_x=summa1(:,5);
g_y1=summa2(:,3);
g_y2=summa2(:,4);
g_I_y=summa2(:,5);
figure ('Position',[100 100 600 400])
hold on
w1=plot(g_count, g_I_x, '-k','LineWidth',2);
w2=plot(g_count, g_x1, '-k','LineWidth',1);
w3=plot(g_count, g_x2, '--k','LineWidth',1);
w4=plot(g_count, g_I_y, '--k','LineWidth',2);
w5=plot(g_count, g_y1, '-.k','LineWidth',1);
w6=plot(g_count, g_y2, ':k','LineWidth',1);
plot_handles=[w1(1) w2(1) w3(1) w4(1) w5(1) w6(1)];
string1=['I(x1,x2), x1+x2=' num2str(Res)];
string2=['x1'];
string3=['x2'];
```

```
string4=['I(y1,y2), y1+y2=' num2str(Y)];
string5=['y1'];
string6=['y2'];
legend(plot_handles, string1, string2, string3, string4, string5, string6, 2);
xlabel(['Кроки (точність ' num2str(p) ' знаків після коми)'])
ylabel('I(x1,x2), x1, x2, I(y1,y2), y1, y2')
xlim([min(g_count) max(g_count)])
ylim([0 1.4*max(g_I_x)])
hold off
end

end

figure1 = figure('Position',[100 100 600 800]);
% Create subplot 1
subplot1 = subplot(3,1,1,'Parent',figure1);
view([0 90]);
grid('off');
hold('all');
hold on
w1=plot (Resources,optumym_I_X,'-k','LineWidth',3,'Parent',subplot1);
w2=plot (Resources,optumym_I1_x1,'-k','LineWidth',2,'Parent',subplot1);
w3=plot (Resources,optumym_I2_x2,'--k','LineWidth',2,'Parent',subplot1);
plot_handles=[w1(1) w2(1) w3(1)];
string1=['Iопт(x1,x2)'];
string2=['Iопт(x1)'];
string3=['Iопт(x2)'];
legend(plot_handles, string1, string2, string3, 2);
xlabel('X')
xlim([min(Resources) max(Resources)])
hold off


% Create subplot 2
subplot2 = subplot(3,1,2,'Parent',figure1);
view([0 90]);
grid('off');
hold('all');
hold on
w1=plot (Resources,optumym_R1,'-k','LineWidth',2,'Parent',subplot2);
w2=plot (Resources,optumym_R2,'--k','LineWidth',2,'Parent',subplot2);
w3=plot (Resources,kroku/2,':k','LineWidth',2,'Parent',subplot2);
%w4=plot (Resources,optumym_R1_y,':k','LineWidth',1,'Parent',subplot2);
%w5=plot (Resources,optumym_R2_y,'-k','LineWidth',1,'Parent',subplot2);
plot_handles=[w1(1) w2(1) w3(1)];
string1=['x1/y1 при I1опт(x1)'];
string2=['x2/y2 при I2опт(x2)'];
string3=['Кроки'];
legend(plot_handles, string1, string2, string3, 2);
xlabel('X')
xlim([min(Resources) max(Resources)])
hold off
```

```
% Create subplot 3
subplot3 = subplot(3,1,3,'Parent',figure1);
view([0 90]);
grid('off');
hold('all');
hold on
w1=plot (Resources,optumym_R1_x1,'-k','LineWidth',1,'Parent',subplot3);
w2=plot (Resources,optumym_R1_y1,'--k','LineWidth',1,'Parent',subplot3);
w3=plot (Resources,optumym_R2_x2,'-.k','LineWidth',1,'Parent',subplot3);
w4=plot (Resources,optumym_R2_y2,':k','LineWidth',1,'Parent',subplot3);
plot_handles=[w1(1) w2(1) w3(1) w4(1)];
string1=['x1 при I1опт'];
string2=['y1 при I1опт'];
string3=['x2 при I2опт'];
string4=['y2 при I2опт'];
legend(plot_handles, string1, string2, string3, string4, 2);
xlabel({'X', ['Y=' num2str(Y) ', min(y1)=min(y2)=' num2str(y_open_door_percent/100) 'Y,
max(I)=' num2str(a1*g1+a2*g2,2)]})
xlim([min(Resources) max(Resources)])
hold off
```

ДОДАТОК В

Акти впровадження результатів дисертаційної роботи

ЗАТВЕРДЖУЮ

Проректор з навчальної роботи НАУ

_____ А. В. Полухін

«26» 05 2014р.

АКТ

впровадження в навчальний процес Національного авіаційного університету результатів дисертаційної роботи Р.Б. Прус «Методи та моделі динамічного управління ресурсами захисту інформації», представленої на здобуття наукового ступеня кандидата технічних наук.

Комісія у складі:

голова – Павленко П.М., д.т.н., проф., заступник директора ІІДС;

члени комісії:

Гумен М.Б., к.т.н., доц., заступник директора ІІДС;

Квасніков В.П., д.т.н., проф., зав. кафедри комп'ютеризованих електротехнічних систем та технологій;

Куц Ю.В., д.т.н., проф., зав. кафедри інформаційно-вимірювальних систем,

яка діє на підставі розпорядження директора Інституту інформаційно-діагностичних систем Національного авіаційного університету Філоненка С.Ф. №38 від 11 листопада 2013 року, засвідчує, що результати дисертаційної роботи Прус Р.Б. впроваджені у навчальний процес і використовуються на кафедрі засобів захисту інформації при викладанні дисципліни «Економіка інформаційної безпеки».

№ п/п	Результати, що впроваджуються	Форма впровадження	Ефективність впровадження
1.	Показники багаторубіжних систем захисту інформації	лекція	Засвоєння студентами методів розрахунку показників складних систем захисту інформації
2.	Моделювання протистояння двох сторін у сфері захисту інформації на основі теоретико-ігрових методів	лабораторне заняття	Засвоєння студентами теоретико-ігрових методів оптимізації розподілу ресурсів захисту між об'єктами інформаційної безпеки.
3.	Динамічне управління ресурсами захисту інформації	лабораторне заняття	Набуття студентами практичних навичок управління ресурсами захисту інформації
4.	Оптимальний розподіл ресурсів в комплексних задачах конкурентної боротьби в інформаційній сфері	лабораторне заняття	Засвоєння студентами методів визначення оптимального розподілу ресурсів для захисту та здобуття інформації для об'єктів підприємства з заданими кількістю інформації і вразливістю.

Результати зазначеної дисертації відображені також у лабораторному практикумі «Економіка інформаційної безпеки», та у розділах навчального посібника «Економіка інформаційної безпеки» з грифом МОН. Видання підготовлено згідно Плану підготовки рукописів навчальної літератури ІІДС на 2011/2012 рр.

Голова комісії П.М. Павленко

Члени комісії М.Б. Гумен

— В.П. Квасніков

Ю.В. Куц

Nestlé.

« 22 » липня 2014 р.

Щодо: впровадження результатів дослідження дисертаційної роботи Прус Руслани Богданівни «Методи та моделі динамічного управління ресурсами захисту інформації» в діяльність ПрАТ «Волиньхолдінг»

Цим листом підтверджуємо, що Прус Р.Б. провела імітаційне моделювання функціонування системи захисту інформації підприємства групи Nestle в Україні - ПрАТ «Волиньхолдінг» - на основі характеристик об'єктів інформаційної діяльності. Запропонувала використати математичну модель на базі теорії ігор для розрахунку оптимального варіанту розподілу ресурсів між об'єктами захисту, що зменшує величину очікуваної шкоди від витоку інформації.

Розроблений нею метод динамічного управління ресурсами захисту апробовано на підприємстві і він показав свою працездатність та результативність при оцінці ефективності функціонування системи інформаційної безпеки.

Підтверджуємо, що отримані результати досліджень Прус Р.Б., зокрема: математична модель та інвестиційний метод використовуються для оцінки ефективності використання ресурсів захисту інформації і дає можливість виявити вплив внесених інвестицій на зменшення величини очікуваної завданої шкоди від реалізації загроз інформації.

Директор з корпоративних зв'язків – керівник служби безпеки Nestle в Україні **Г.Ю.Радченко**

Україна * Товариство з обмеженою відповідальністю * м.Київ
«НЕСТЛЕ УКРАЇНА»
Ідентифікаційний код 32531437

ТОВ "НЕСТЛЕ УКРАЇНА",
КОД ЄДРПОУ 32531437
ВУЛ. ВЕРХНІЙ ВАЛ, 72 В ЛІТЕРІ "А'"
04655 М. КИЇВ, УКРАЇНА

ТЕЛ./TEL.: +380 44 490 8000
ФАКС/FAX: +380 44 490 8021

NESTLE UKRAINE LLC
CODE 32531437
VUL. VERKHNII VAL, 72 V LITERI "A'"
04655 KYIV, UKRAINE

ЗАТВЕРДЖУЮ
Директор
Л.С. Стефанович
підпис
« 22 » липня 2019 р.

АКТ

впровадження результатів дослідження дисертаційної роботи
Прус Руслани Богданівни «Методи та моделі динамічного управління ресурсами захисту інформації» в діяльність ТзОВ «ЖИТЛОБУД-2»

Цей акт складено комісією ТзОВ «ЖИТЛОБУД-2» у складі голови комісії – директора Стефановича Л. С. та членів комісії: головного інженера будівельної лабораторії Капризової Г. О. , начальника відділу охорони праці Набитовича Я. І. , яка констатує, що Прус Р.Б. провела імітаційне моделювання наслідків прийняття інвестиційних рішень у динамічному режимі, сформулювала рекомендації щодо оптимізації розподілу ресурсів та оцінки величини очікуваної шкоди від реалізації загроз інформації. Запропонувала використати метод дослідження динаміки зміни стану інформаційної безпеки для розрахунку моменту часу, коли імовірність успішної атаки найвища.

В результаті використання зазначених розробок сформулювано практичні рекомендації щодо оптимального розподілу коштів для захисту об'єктів інформаційної діяльності та підвищено ефективність використання коштів, виділених на захист інформації.

Комісія підтверджує, що отримані результати досліджень Прус Р.Б., зокрема: метод удосконалення технології динамічного регулювання розподілу ресурсів захисту, що базується на математичному апараті теорії ігор та розробленій математичній моделі реалізації процесу пошуку оптимальних рішень, використано для підвищення ефективності використання ресурсів захисту інформації та врахувати вплив зміни націленості атак зловмисника на значення параметрів та характеристик систем.

Голова комісії:
директор Стефанович Л. С.

Члени комісії:
Головний інженер
будівельної лабораторії
Капризова Г. О.

начальник відділу
охорони праці
Набитович Я. І.

ЗАТВЕРДЖУЮ
Керівник
_____ І.І. Рогаля
підпис

«21» липня 2014 р.

АКТ

впровадження результатів дослідження дисертаційної роботи
Прус Руслани Богданівни «Методи та моделі динамічного управління ресурсами захисту інформації» в діяльність ТзОВ «Західелектромонтаж»

Комісія у складі голови комісії – провідного інженера відділу інформаційних систем Ксьондзика С.П. та членів комісії: начальника технічного відділу Кревської Л.І., головного інженера Костюка С.М. констатує, що Прус Р.Б. провела аналіз ефективності функціонування ситеми захисту інформації використовуючи розроблений нею інвестиційний метод.

При виконанні даної роботи автором встановлено і формалізовано взаємозв'язок між внесеними інвестиціями у захист інформації на зменшенням потенційних збитків від реалізації загроз інформації. Це дозволило сформулювати рекомендації щодо оптимізації розподілу ресурсів між об'єктами захисту та оцінити величину очікуваної шкоди від реалізації загроз інформації.

Комісія підтверджує, що наукові положення та висновки по дисертаційній роботі Прус Р.Б., зокрема: метод удосконалення технології динамічного регулювання розподілу ресурсів захисту, який базується на математичному апараті теорії ігор та математичній моделі реалізації процесу пошуку оптимальних рішень використано при виконанні заходів з удосконалення системи захисту інформації.

Комісія відмічає теоретичний внесок Прус Р.Б. у вирішення задач оцінки рівня інформаційної безпеки.

Голова комісії:
Провідний інженер відділу
інформаційних систем _____ С.П.Ксьондзик

Члени комісії:
начальник технічного
відділу _____ Л.І.Кревська

головного інженера _____ С.М.Костюк

ЗАТВЕРДЖУЮ
Директор-розпорядник
_____ В.О. Бондар
підпис
«22» липня 2014 р.

АКТ

впровадження результатів дослідження дисертаційної роботи
Прус Руслани Богданівни «Методи та моделі динамічного управління ресурсами захисту інформації» в діяльність СП «3Д Україна»

Цей акт складено комісією СП «3Д Україна» у складі:
голова комісії:
- начальник служби безпеки,
члени комісії:
- начальник управління інформаційних систем;
- головний інженер.

яка констатує, що Прус Р.Б. провела імітаційне моделювання функціонування системи захисту інформації на основі характеристик об'єктів інформаційної діяльності. Запропонувала використати математичну модель на базі теорії ігор для розрахунку оптимального варіанту розподілу ресурсів між об'єктами захисту, що зменшує величину очікуваної шкоди від витоку інформації.

Розроблений нею метод динамічного управління ресурсами захисту апробовано на підприємстві, і він показав свою працездатність та результативність при оцінці ефективності функціонування системи інформаційної безпеки.

Комісія підтверджує, що отримані результати досліджень Прус Р.Б., зокрема: математична модель та інвестиційний метод використовуються для оцінки ефективності використання ресурсів захисту інформації і дає можливість виявити вплив внесених інвестицій на зменшення величини очікуваної завданої шкоди від реалізації загроз інформації.

Голова комісії:
начальник служби
безпеки _____ Л. Аксьонов

Члени комісії:
начальник управління
інформаційних систем _____ Ю. Ярмолюк

головний інженер _____ А. Поліщук