МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Прус Руслана Богданівна

УДК 004.056.5:519.8(043.3)

МЕТОДИ ТА МОДЕЛІ ДИНАМІЧНОГО УПРАВЛІННЯ РЕСУРСАМИ ЗАХИСТУ ІНФОРМАЦІЇ

21.05.01 – інформаційна безпека держави

Автореферат

дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2014

Дисертацією є рукопис.
Робота виконана в Національному авіаційному університеті Міністерства освіти і науки України.

Науковий керівник: кандидат технічних наук, доцент
Швець Валеріян Анатолійович
Національний авіаційни університет
доцент кафедри засобів захисту інформації

Офіційні опоненти: доктор технічних наук, професор
Архипов Олександр Євгенович
Національний технічний університет України
«Київський політехнічний інститут»
професор кафедри інформаційної безпеки

кандидат технічних наук
Дрейс Юрій Олександрович
Житомирський військовий інститут імені С.П. Корольова
Державного університету телекомунікацій
доцент кафедри безпеки інформаційних і
комунікаційних систем

Захист відбудеться «28» серпня 2014 р. о 14 ^{00} год. на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03680, м. Київ, просп. Космонавта Комарова, 1, НАУ, корп. 11, ауд. 111.

З дисертацією можна ознайомитися в науково-технічній бібіліотеці Національного авіаційного університету за адресою: 03680, м. Київ, просп. Космонавта Комарова, 1.

Автореферат розісланий «25» липня 2014 р.

Учений секретар
спеціалізованої вченої ради С.О. Гнатюк

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

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 частка втраченої 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 збитки від реалізації загроз. По-друге, оптимальним чином розподілити ресурси між об'єктами, які відрізняються природною захищеністю, динамічною уразливістю, імовірністю нападу з виділенням певної кількості ресурсів. Третій аспект полягає у визначенні оптимального моменту внесення ресурсів захисту – після з'ясування направленості та інтенсивності нападів та, відповідно, оцінки рівня збитків. Невизначеність умов протистояння, характерна для конкурентної боротьби, приводить до того, що першим етапом атаки стає розвідка, направлена на виявлення слабких місць в системі захисту. При цьому виникає питання оптимізації розподілу ресурсів між розвідкою та безпосередньою атакою. 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 отриманням доступу до 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 О.Є. Архипова, Б.Є. Журиленка, В.К. Задіраки, Г.Ф. Конаховича, О.Г. Корченка, Є.Г. Левченка, О.М. Новікова, В.О. Хорошка, О.К. Юдіна та закордонних науковців Р. Бьоме, В.А. Герасименка, Л. Гордона, М. Лоеба, В. Лью, К. Мацури, Т. Мура, К. Хуана. 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 «Методи і моделі управління ресурсами захисту інформації» (номер державної реєстрації 0113U006543), що виконувалась на кафедрі засобів захисту інформації Національного авіаційного університету, де автор була виконавцем.

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. У роботі використані аналітичні і графічні методи оптимізаційних задач дослідження операцій: методи дробово-лінійного і дробово-нелінійного програмування, метод динамічного програмування Белмана – для знаходження оптимального розподілу; 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 розмір завданої шкоди від реалізації загроз 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 величину очікуваної шкоди від реалізації загроз 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. Усі наукові результати, відображені в дисертаційній роботі, отримані автором самостійно. В опублікованих разом зі співавторами наукових працях за темою дисертації особисто здобувачем отримані аналітичні моделі та розрахункові вирази, проведено моделювання, на підставі якого отримані нові наукові та прикладні результати. Особистий внесок здобувача полягає у наступному: [1,9] – визначено умови існування сідлової точки цільової функції при протистоянні двох сторін в залежності від характеристик складних інформаційних структур; [2,10-12,16,18] – на основі теоретико-ігрових методів сформовано математичний апарат для пошуку оптимального розподілу ресурсів між об'єктами захисту за відсутності інформації про дії нападу; [3,5,6,14] – розроблено математичну модель, яка дозволяє підвищити ефективність захисту інформації в багаторубіжних системах за рахунок оптимального розподілу ресурсів захисту інформації; [4,15] – розроблено алгоритм для автоматизації процесу оптимізації розподілу ресурсів в складних інформаційних системах в динамічному режимі; [7] – проведено дослідження розробленої моделі із використанням методів безумовної і умовної оптимізації; [8] – розроблено методику розрахунку станів інформаційної безпеки в динамічному режимі з врахуванням зміни умов протистояння з часом та визначено оптимальний момент інвестування ресурсів; [13] – розраховано показники системи захисту інформації залежно від схеми розташування засобів захисту, розроблено методику побудування оптимальних схем; [17] – проведено аналіз функцій динамічної уразливості та імовірності нападу і їх вплив на продуктивності витрат.

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).

Структура дисертації. Дисертація складається із вступу, п'яти розділів, висновків, списку використаних джерел із 117 найменувань, 2 додатків, містить 13 таблиць, 47 рисунків. Загальний обсяг дисертації становить 134 сторінки.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обгрунтовано актуальність теми дисертації, зазначено зв'язок з науково-дослідними роботами, базовими для підготовки дисертаційної роботи та

роль автора у виконанні цих НДР, визначено мету, завдання, об'єкт та предмет дослідження, сформульовано наукову новизну та практичне значення отриманих результатів.

У **першому розділі** проаналізовано існуючі моделі інформаційної безпеки (табл.1), зокрема, модель Гроса, призначену для імітації тактичних військових операцій. Відповідно до цієї моделі, конфліктуючі сторони володіють ресурсами X та Y, а результат їхнього протистояння визначається цільовою функцією, котра лінійно залежить від різниці вкладених ресурсів.

Проаналізовано модель Гордона-Лоеба. Метою цієї моделі є визначення оптимальної кількості інвестицій в захист інформації. У моделі вперше приведено кількісну функцію уразливості. Недоліком моделі Гордона-Лоеба можна вважати відсутність аналізу протистояння в динамічному режимі.

Метою досліджень Б.Є. Журиленка є оцінка стійкості комплексу технічного захисту інформації в часі з використанням відомих розподілів ймовірностей. Модель Б.Є. Журиленка дає можливість при певних умовах розрахувати рівень збитків внаслідок реалізації загроз, що залежить від обсягу витрат на захист інформації.

Метою робіт В.В. Глушака та О.М. Новікова є оптимальне розміщення механізмів захисту між компонентами (об'єктами) системи, що забезпечить максимальний рівень захищеності.

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

Таблиця 1

Аналіз моделей управління ресурсами захисту інформації

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	+	+	-	+	+	+

За результатами аналізу відзначено особливості моделей та умови їх застосування, на основі чого сформульовано задачі дослідження, які вирішуються в наступних розділах дисертації.

Другий розділ присвячено розробці математичної моделі пошуку оптимального розподілу ресурсів між об'єктами захисту інформації. Розглянуто складні багаторубіжні системи захисту інформації, на основі яких проводиться моделювання. Визначено вхідні дані, необхідні для прийняття оптимальних рішень. Обгрунтовано використання параметрів та функціональних залежностей, що характеризують окремі елементи системи захисту інформації.

З метою оптимізації розподілу ресурсів між об'єктами захисту інформації розроблено математичну модель, в якій цільова функція визначає завдану шкоду від реалізації загроз при протистоянні двох сторін:

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

де $k=\overline{1,l}$ - номер об'єкта; x_k і y_k - ресурси нападу і, відповідно, захисту, $\sum_{k=1}^{l} x_k = X$, $\sum_{k=1}^{l} y_k = Y$; g_k - відносна цінність інформації на об'єкті, $\sum_{k=1}^{l} g_k = 1$; p_k - імовірність нападу на об'єкт; $f_k(x,y)$ - уразливість k-го об'єкта, яка залежить від співвідношення ресурсів нападу і захисту.

Приклад структури системи захисту інформації зображено на рис.1, де об'єкти g_1, g_2 захищає комплекс перешкод із різними уразливостями f.

Основні труднощі при розрахунку величини $i(x,y)$ за виразом (1) полягають у встановленні форми залежності $f(x,y)$. При формуванні цієї залежності 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. Тому змінні x, y входять у $f(x,y)$ у вигляді відношення x/y. Залежності $f(x,y)$ повинні задовольняти умовам: при $x/y \to 0$ $f(x,y)\to 0$, при $x/y \to \infty$ $f(x,y)\to 1$. До таких залежностей відносяться показникові функції виду $f(x,y)=1-e^{-m\left(x/y\right)^n}$ та дробово-степеневі:

$$f(x,y)=\frac{\left(x/y\right)^n}{\left(x/y\right)^n+c}, \qquad (2)$$

де параметри m n, c визначають форму і кривизну ліній. Надалі використано більш просту дробово-степеневу функцію. При $n=1$ вона виражає дробово-лінійну залежність, при $n>1$ – дробово-нелінійну. Вплив параметрів n і c на форму і положення кривих $f(x,y)$ показано на рис.2.

Дробово-лінійні ($n=1$) функції (2) 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 завданої шкоди. Дробово-нелінійні ($n>1$)

функції відображають властивості інформації, що циркулює у комп'ютерних системах, де для подолання захисту потрібно витратити значні ресурси. При зростанні нелінійності за рахунок збільшення показника n у (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 частка втраченої інформації зростає стрибкоподібно.

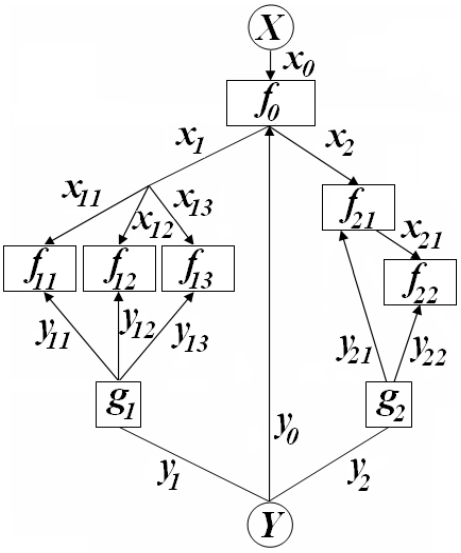


Рис. 1. Дворівнева багаторубіжна система захисту інформації, яка містить два об'єкти

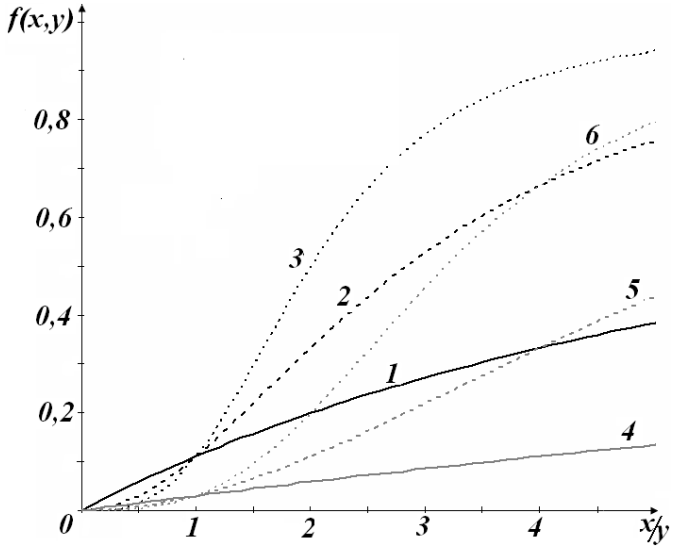
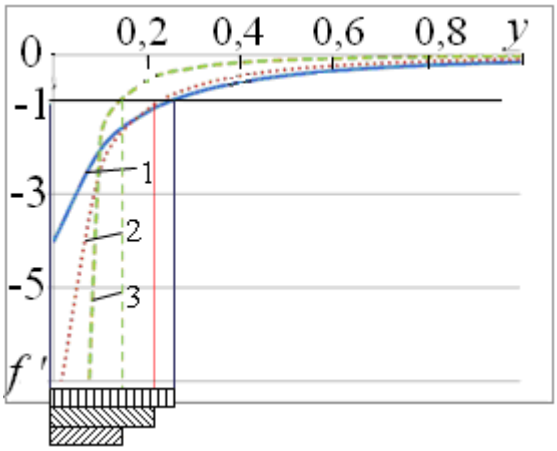


Рис.2. Залежності $f(x) = \dfrac{x^n}{x^n + c}$ $(y = const)$ при різних значеннях n і c: **1** – $n = 1$, $c = 8$; **2** – $n = 2$, $c = 8$; **3** – $n = 3$, $c = 8$; **4** – $n = 1$, $c = 32$; **5** - $n = 2$, $c = 32$; **6** – $n = 3$, $c = 32$

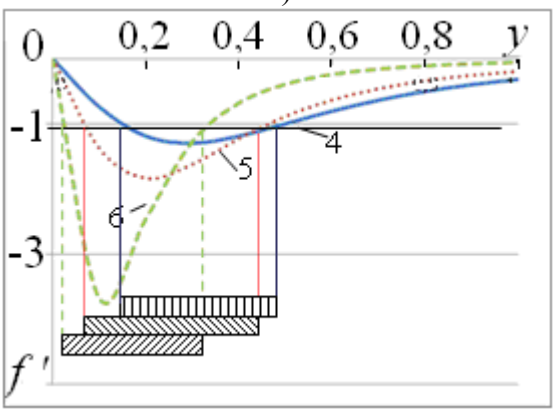
Для характеристики ефективності використання внесених коштів введено поняття економічної доцільності витрат, яке кількісно виражається таким показником як продуктивність зменшення уразливості (ПЗУ). Цей показник виражається параметрами n і c функції уразливості $f(x, y)$ (2). Залежність ПЗУ від розміру інвестицій y визначається крутизною кривої $f(y)$, тобто значеннями $f'(y)$ (рис.3,4).

При дробово-лінійних залежностях зона високої продуктивності (її межі встановлено на рівні $f'(y) = -1$) знаходиться в області низьких значень y (рис.3а). У даному типі систем необхідні початкові заходи, які не потребують великих витрат, проте можуть суттєво зменшити уразливість. При дробово-нелінійних залежностях $f(y)$ зона високої ПЗУ відповідає середнім значенням кількості ресурсів захисту інформації y (рис.4), що свідчить про те, що невеликі за розміром інвестиції в захист неефективні.

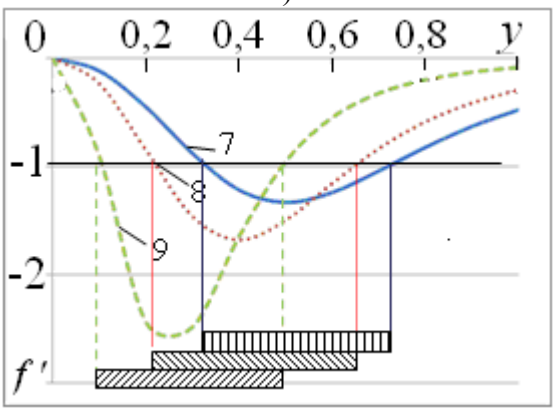
Пошук оптимального розподілу обмежених ресурсів між об'єктами захисту інформації ведеться із використанням математичного апарату теорії ігор. Конфліктне протистояння сторін нападу і захисту розглядається як несиметрична гра з нульовою сумою: виграти може тільки перший гравець (напад), причому його виграш, що оцінюється вартістю критичної інформації i, дорівнює програшу другого (захист).



а)

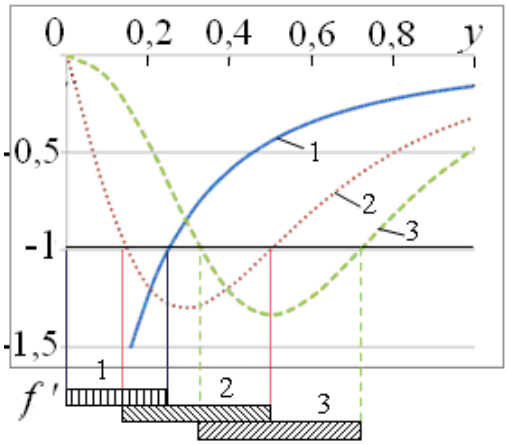


б)

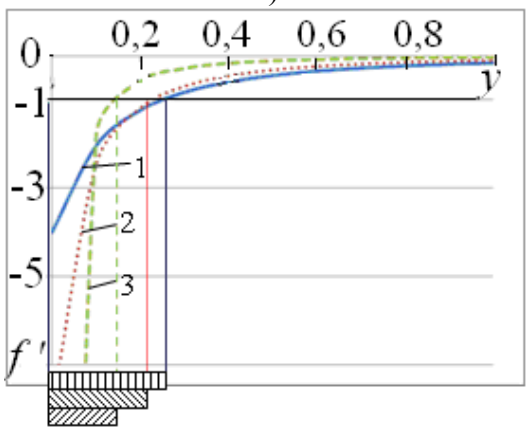


в)

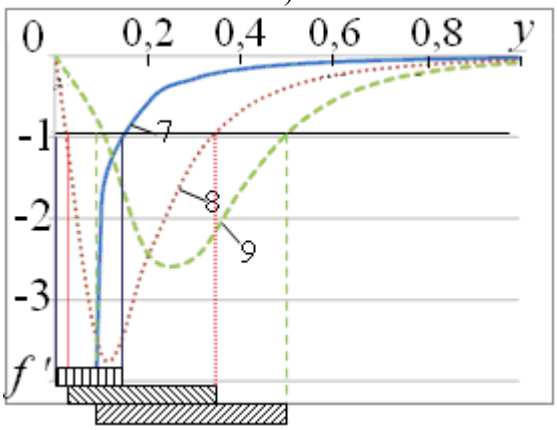
Рис. 3. Крутизна функцій $f'(y)$ в залежності від c при різних n: а) $n=1$; б) $n=2$; в) $n=3$; **1, 4, 7** — $c=4$; **2, 5, 8** — $c=8$; **3, 6, 9** — $c=32$



а)



б)



в)

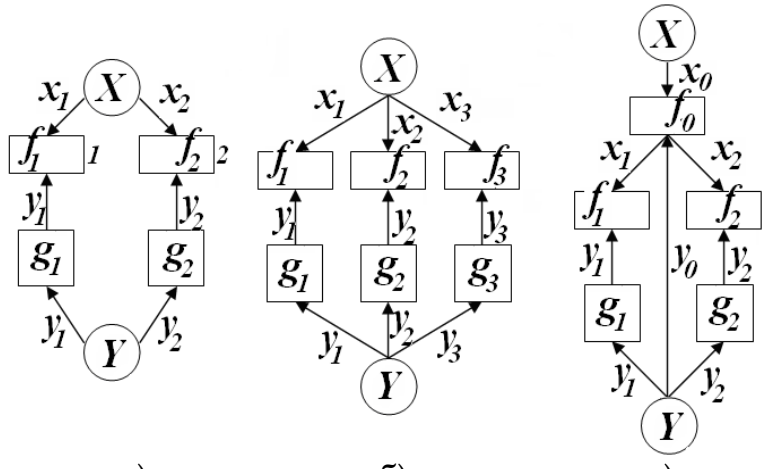
Рис. 4. Крутизна функцій $f'(y)$ в залежності від n при різних c: а) $c=4$; б) $c=8$; в) $c=32$; **1, 4, 7** — $n=4$; **2, 5, 8** — $n=8$; **3, 6, 9** — $n=32$

Метою захисту являється мінімізація величини завданої шкоди від реалізації загроз. Напад переслідує прямо протилежні цілі: розподіл своїх ресурсів, який створює максимальні можливості для успішної атаки. Виграш кожної із сторін залежить від стратегій (варіантів розподілу ресурсів) суперника і визначається цільовою функцією (1). Згідно з положеннями теорії ігор 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. Таким чином, згідно із поставленою задачею, пошук оптимального рішення (вибір варіанту розподілу обмежених ресурсів захисту, що забезпечує мінімальну завдану шкоду від реалізації загроз) проводиться у наступній послідовності: **1)** Проводиться оцінка об'єктів захисту g_k, визначаються функції уразливості (2) об'єктів (оцінка параметрів n і c); **2)** Проводиться аналіз дій сторін на основі положень теорії ігор. Для досягнення поставлених цілей у розпорядженні сторони нападу є X ресурсів та у сторони захисту Y ресурсів. Стратегія нападу полягає в розподілі своїх ресурсів між об'єктами у різних співвідношеннях: $\{x_{ik}\}=(x_1, x_2, ..., x_l)$, $\sum_{k=1}^{l} x_k = X, x_k \geq 0$. Захист використовує свою стратегію розподілу ресурсів: $\{y_{jk}\}=(y_1, y_2, ..., y_l)$, $\sum_{k=1}^{l} y_k = Y, y_k \geq 0$. Нападник намагається завдати максимальної шкоди i супернику, цільова функція (1) сторони нападу має вигляд: $i(x, y) \to \max$. Сторона захисту переслідує протилежні цілі – мінімізувати величину потенційної завданої шкоди: $i(x, y) \to \min$. **3)** Будується матриця виграшів для функції $i(x, y)$. **4)** Визначаються оптимальні рішення для нападу і захисту, що відповідають сідловій точці гри і забезпечують виконання умови $\max_x \min_y i(x, y) = \min_y \max_x i(x, y)$. Оптимальне рішення, що відповідає сідловій точці, забезпечує мінімальну шкоду від реалізації загроз при будь-яких діях зловмисника.

Третій розділ присвячений розробці методу пошуку оптимальних рішень в динамічному режимі. Динамічне протистояння розглянуто на прикладі системи (рис.5а), яка містить два об'єкти з різними уразливостями і різною цінністю інформації. Маючи на меті виявлення впливу основної характеристики системи – уразливостей $f(x, y)$ об'єктів, покладено $p_k = 1$. Цільову функцію прийнято у вигляді:

$$i(x, y) = \sum_{k=1}^{l} g_k f_k(x_k, y_k). \qquad (3)$$



а) б) в)

Рис. 5. Схеми однорівневих (а, б) та дворівневої (в) систем захисту

Умови протистояння визначено наступним чином. Напад і захист роблять почергові «ходи» (N) (рис. 6), знаючи розподіл ресурсів суперника після його попереднього ходу і на цій основі перерозподіляючи свої ресурси. Захист припиняє перерозподіл, коли черговий хід є для нього невигідним або він несе загрозу наступного ходу суперника, який приведе до значних збитків. В термінології теорії ігор це позиційна гра з відкритою інформацією.

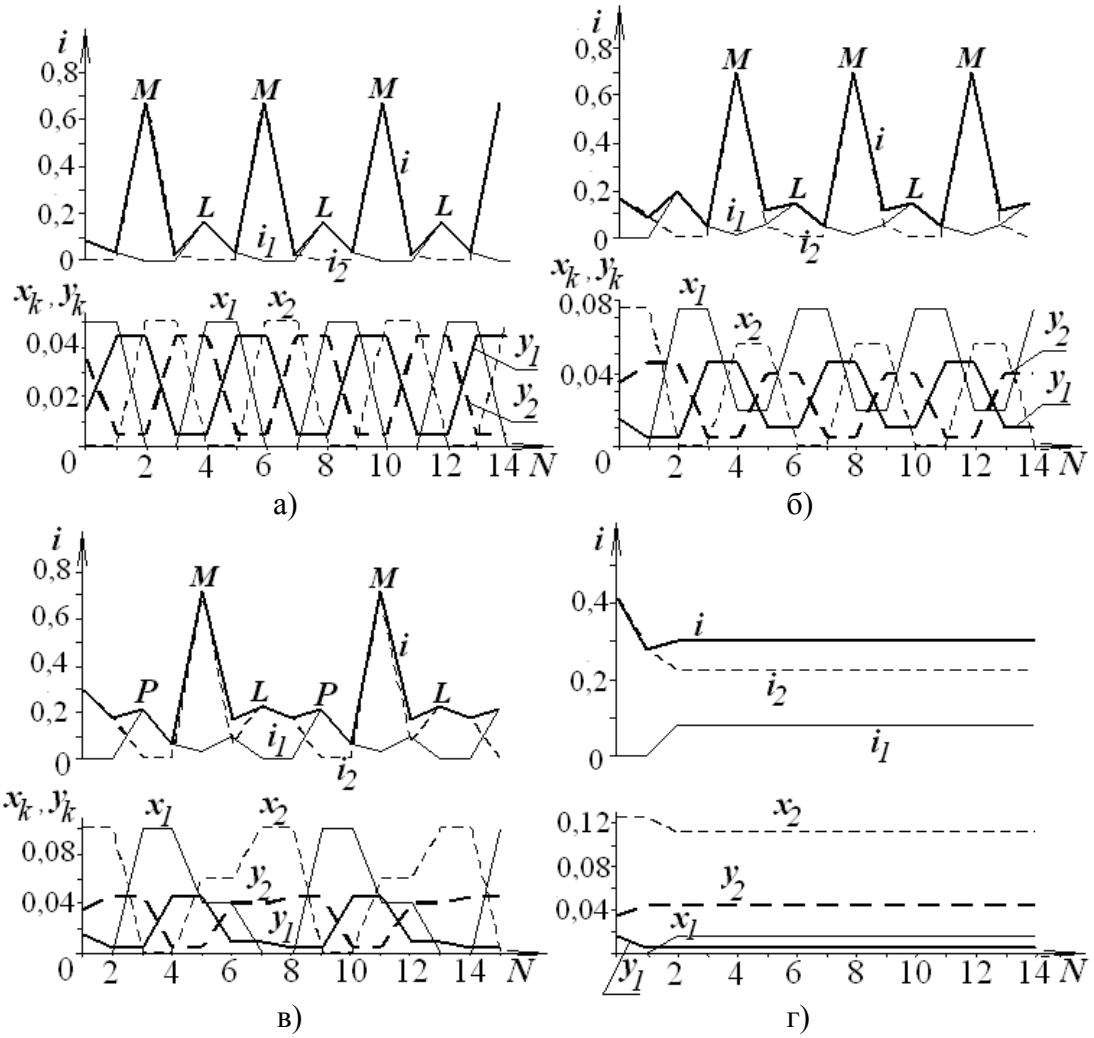


Рис. 6. Динамічний режим протистояння нападу і захисту в системі (рис.7а) при g_1=0,3; g_2=0,7;

$f_1(x,y)=\dfrac{x/y}{x/y+8}$; $f_2(x,y)=\dfrac{(x/y)^3}{(x/y)^3+32}$ і різних Z: а) $Z=1$; б) $Z=1{,}5$; в) $Z=2$; г) $Z=2{,}5$

Пошук оптимального розподілу $\{y_k^0\}$ ресурсів захисту, що забезпечує мінімальну шкоду від реалізації загроз при заданих ресурсах нападу $\sum_{k=1}^{l} x_k = X$ і захисту $\sum_{k=1}^{l} y_k = Y$ проводиться у наступній послідовності: **1.** Розподіл $\{y_k\}$ ресурсів захисту приймається пропорційним цінності інформації на об’єктах $\{g_k\}$. **2.** Задано функції динамічної уразливості об’єктів (2). Методом експертної оцінки визначено значення параметрів n та c. **3.** Переходячи до дискретного

програмування, розраховуються значення цільової функції (3) для низки варіантів розподілу ресурсів x_k нападу. **4.** Користуючись методом Белмана для прийнятого розподілу $\{y_k\}$ ресурсів захисту, знаходиться оптимальний для нападу розподіл $\{x_k\}$, послідовно максимізуючи величини завданої шкоди $i_k(x)$ за зворотною схемою. **5.** Враховуючи розподіл $\{x_k\}$ ресурсів нападу, знайдений на попередньому етапі, проводиться коригування розподілу $\{y_k\}$ ресурсів захисту. Пошук розподілу $\{y_k\}$ ресурсів захисту, що забезпечує мінімальну завдану шкоду $i(x,y)$ при заданому розподілі $\{x_k\}$ ресурсів нападу, проводиться за методом Белмана. **6.** Описана процедура (п.4,5) повторюється до моменту, коли величина $\max i_k(x)$ досягне найменшого значення (рис. 6г). Відповідний розподіл $\{y_k^0\}$ є оптимальним.

На рис.6 показано процес динамічного управління при різному співвідношенні ресурсів нападу і захисту, при $Z = X/Y = 1$ (рис.6а) відбувається повна почергова перекачка ресурсів з одного об'єкта на інший, що обумовлено обмеженістю коштів нападу ($Z = 1$), при концентрації ресурсів на одному з об'єктів напад отримує більше можливостей для успішної атаки до інформації, ніж при їх розподілі між об'єктами. Захист направляє свої ресурси на об'єкт, де зосереджені ресурси нападу. Зубчаста лінія $i(N)$ на рис.8а показує, що після кожного кроку нападу зростає величина завданої шкоди, а після наступного кроку захисту вона зменшується. При збільшенні Z (рис.6б) відбувається лише часткова перекачка ресурсів, оскільки їх вже достатньо для розподілу між обома об'єктами. При $Z = 2{,}5$ (рис.6г) досягається ситуація, в якій розподіли ресурсів стають стабільними.

В умовах невизначеності, коли можливості, наміри та дії суперника невідомі, доцільно обрати таку стратегію, яка забезпечує певний результат при будь-яких діях суперника. Така ситуація спостерігається в сідловій точці (рис.6г) цільової функції, де кожна з сторін досягає найкращого для себе результату і не зацікавлена в зміні своєї стратегії, яка полягає в певному розподілі своїх ресурсів між об'єктами.

На можливість існування сідлової точки впливають наступні фактори: форма протистояння – однонаправлена чи різнонаправлена; кількість l об'єктів; їх уразливості $f_k(x,y)$; цінність $\{g_k\}$ інформації на об'єктах. З врахуванням цих факторів сідлова точка може існувати при певних значеннях $Z = X/Y$. Інтервал ΔZ існування сідлової точки визначається зазначеними факторами.

У результаті розрахунків, проведених для систем (рис.5), встановлено такі закономірності: **1.** В найпростішій системі (рис.5а) при дробово-лінійних функціях уразливості $f_k(x,y)$ сідлова точка існує при всіх значеннях Z. **2.** Якщо хоч одна з функцій уразливості $f_k(x,y)$ має дробово-нелінійну форму ($n_k > 1$), то сідлова точка може існувати лише в певних інтервалах значень Z. При збільшенні уразливості $f_k(x,y)$ за рахунок зростання степеня n або зменшення значення c інтервал ΔZ існування сідлової точки звужується і зміщується в сторону менших

Z. **3.** Ступінь зростання завданої шкоди i зі збільшенням співвідношення ресурсів нападу і захисту Z визначається уразливостями $f_k(x,y)$ об'єктів. 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.7). **4.** Інтервал існування сідлової точки залежить також від цінності $\{g_k\}$ інформації на об'єктах (рис.7). Ступінь зменшення інтервалу ΔZ зростає із збільшенням нелінійності функцій $f_k(x,y)$. **5.** В системі з трьома засобами захисту (рис.5б-в) інтервал ΔZ стає обмеженим навіть при використанні дробово-лінійних функцій. В системі з дробово-нелінійними функціями введення третього об'єкта чи третього засобу захисту приводить до звуження інтервалу ΔZ і при деяких значеннях параметрів цей інтервал зникає – сідлова точка відсутня.

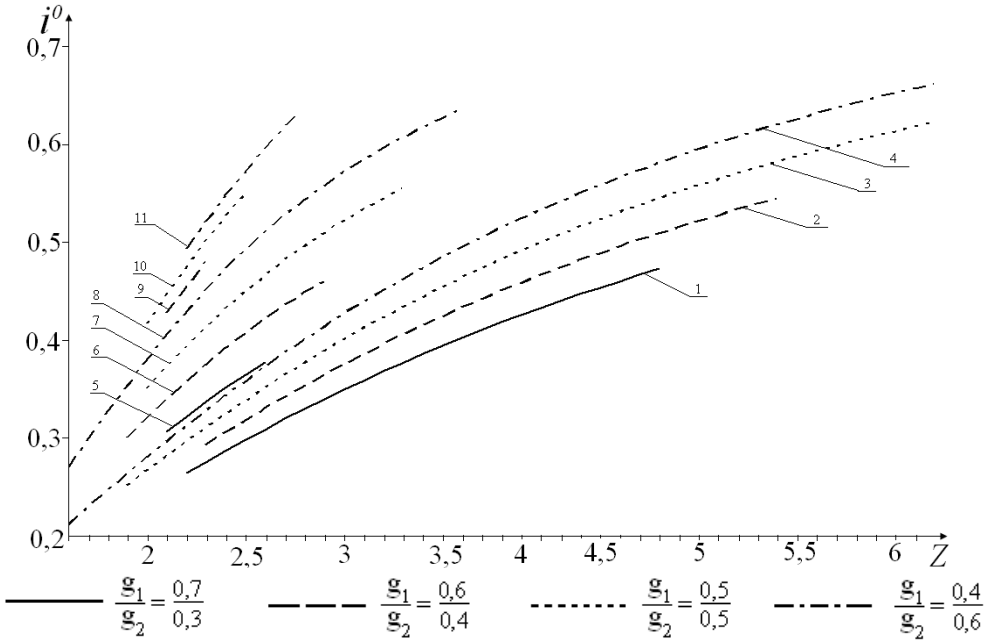


Рис. 7. Розмір завданої шкоди від реалізації загроз в інтервалах існування сідлової точки при $c=8$ і різних значеннях n і $g_1/g_2=G$: **1,2,3,4** – $n_1=1,\ n_2=2$; **5,6,7,8** – $n_1=1,\ n_2=3$; **9,10,11** – $n_1=2,\ n_2=3$

Четвертий розділ присвячено дослідженню різнонаправленого протистояння, за якого кожна з сторін прагне захистити свою інформацію і отримати доступ до інформації суперника. Цю ситуацію зображено на рис.8.

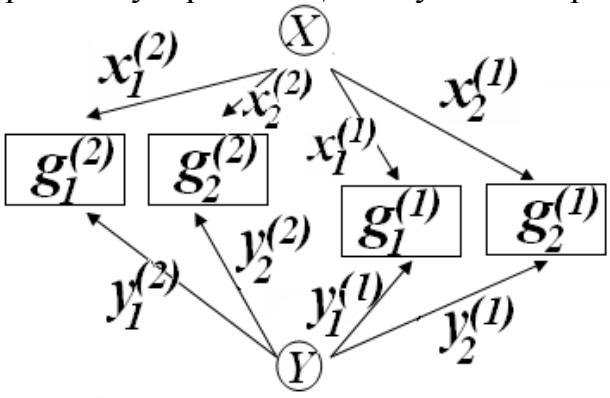


Рис. 8. Схема різнонаправленого протистояння двох сторін

Цільова функція $F(x, y)$ визначає сумарний інформаційний здобуток кожної з сторін, який включає зменшення збитків за рахунок внесення інвестицій в об'єкти захисту і вартість інформації, здобутої з об'єктів суперника:

$$F_1(x,y)=\sum_{k=1}^{2}\left[1-g_k^{(1)}f_k^{(1)}(x)+g_k^{(2)}f_k^{(2)}(y)\right],\ F_2(x,y)=\sum_{k=1}^{2}\left[1+g_k^{(1)}f_k^{(1)}(x)-g_k^{(2)}f_k^{(2)}(y)\right].$$

Оптимальні розподіли ресурсів нападу $\{x_k\}$ і захисту $\{y_k\}$ знаходяться шляхом динамічного програмування. Кожна з сторін почергово робить кроки, які полягають в конкретному розподілі ресурсів з врахуванням дій протилежної сторони, здійснених на попередньому кроці.

В умовах такого динамічного протистояння важливим показником є часова залежність стану інформаційної системи. На прикладі системи (рис.8) розглянуто динаміку зміни стану. Граф системи (рис.8) зображує переходи між станами, його показано на рис.9.

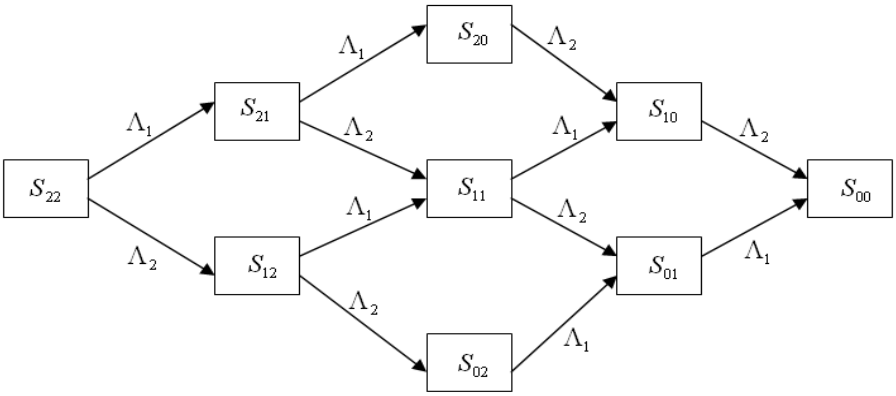


Рис. 9. Граф однорідної системи, в якій кожна з сторін містить два об'єкти

Спроби здійснення нападу утворюють пуассонівський потік подій, або неперервний марковський ланцюг. Для розрахунку станів введено позначення: λ_1 і λ_2 - кількість спроб, які здійснюють перша і друга сторони за одиницю часу (в подальшому першою стороною будемо вважати сторону з ресурсами Y, яка 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 кожної з сторін; $\Lambda = \Lambda_1 + \Lambda_2$ - сумарна частота успішних спроб; S_{ij} - стан системи, в якому неушкодженими залишаються i об'єктів першої сторони та j об'єктів другої сторони ($i=\overline{1,2}$, $j=\overline{1,2}$); p_{ij} - імовірність того, що система знаходиться в ij-му стані.

Система диференціальних рівнянь Колмогорова відповідно до цього графу має вигляд:

$$\frac{dp_{22}}{dt}=-\Lambda p_{22};\qquad \frac{dp_{20}}{dt}=\Lambda_1 p_{21}-\Lambda_2 p_{20};\qquad \frac{dp_{01}}{dt}=\Lambda_1 p_{02}+\Lambda_2 p_{11}-\Lambda_1 p_{01};$$

$$\frac{dp_{21}}{dt}=\Lambda_1 p_{22}-\Lambda p_{21};\qquad \frac{dp_{11}}{dt}=\Lambda_1 p_{12}+\Lambda_2 p_{21}-\Lambda p_{11};\qquad \frac{dp_{00}}{dt}=-\Lambda_1 p_{01}-\Lambda_2 p_{10}.$$

$$\frac{dp_{12}}{dt}=\Lambda_2 p_{22}-\Lambda p_{12};\qquad \frac{dp_{10}}{dt}=\Lambda_1 p_{11}+\Lambda_2 p_{20}-\Lambda_2 p_{10};$$

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

$$p_{22}(t) = e^{-\Lambda t};$$

$$p_{21}(t) = \Lambda_1 t \cdot e^{-\Lambda t};$$

$$p_{20}(t) = e^{-\Lambda_2 t} - (1+\Lambda_1 t)e^{-\Lambda t};$$

$$p_{11}(t) = \Lambda_1 \Lambda_2 t^2 \cdot e^{-\Lambda t};$$

$$p_{02}(t) = e^{-\Lambda_1 t} - (1+\Lambda_2 t)e^{-\Lambda t};$$

$$p_{12}(t) = \Lambda_2 t \cdot e^{-\Lambda t};$$

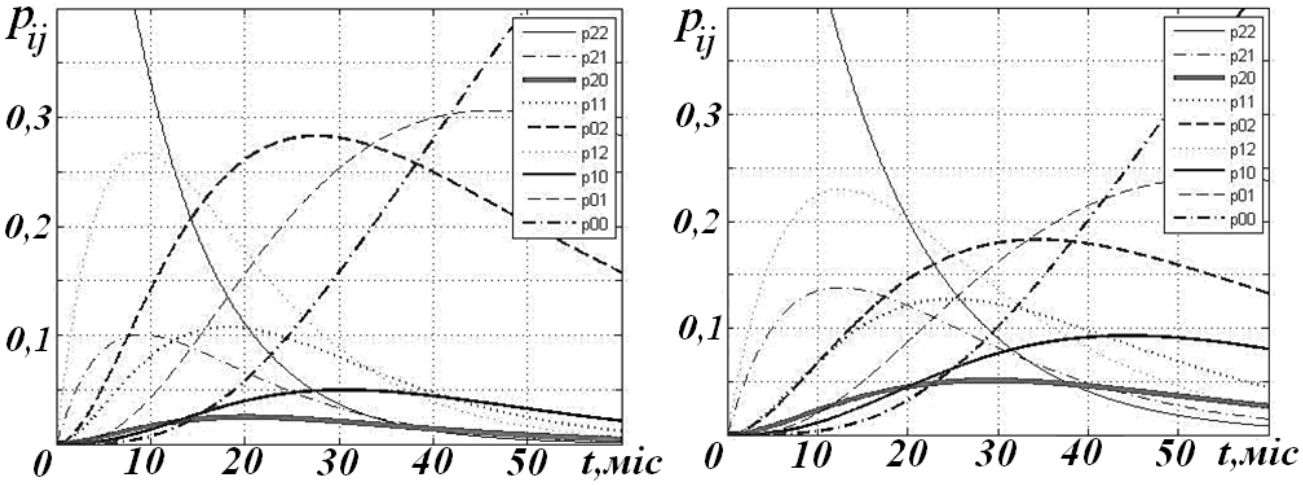
$$p_{10}(t) = \Lambda_2 t e^{-\Lambda_2 t} - (\Lambda_1 \Lambda_2 t^2 + \Lambda_2 t)e^{-\Lambda t}$$

;

$$p_{01}(t) = \Lambda_1 t e^{-\Lambda_1 t} - (\Lambda_1 t + \Lambda_1 \Lambda_2 t^2)e^{-\Lambda t}$$

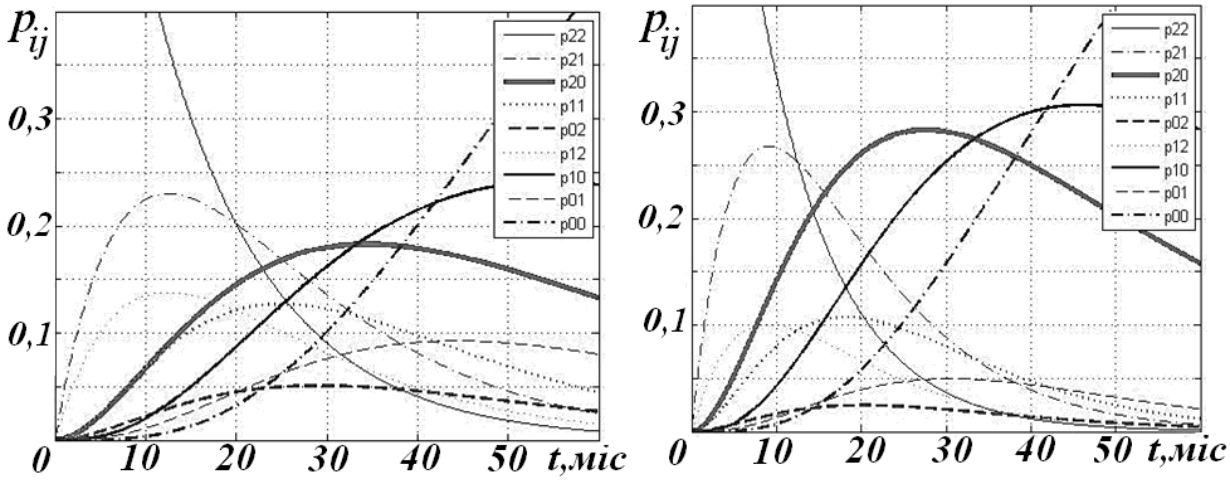
.

Залежності $p_{ij}(t)$ для різних значень Λ_1, Λ_2 наведені на рис. 10,11, вони визначаються імовірностями попередніх станів, з яких відбуваються переходи, та щільностями перехідних імовірностей, котрі виражаються величинами Λ_1, Λ_2.



а) $\Lambda_1 = 0{,}03$; $\Lambda_2 = 0{,}08$ б) $\Lambda_1 = 0{,}03$; $\Lambda_2 = 0{,}05$

Рис. 10. Залежності $p_{ij}(t)$ при $\Lambda_1 < \Lambda_2$



а) $\Lambda_1 = 0{,}05$; $\Lambda_2 = 0{,}03$ б) $\Lambda_1 = 0{,}08$; $\Lambda_2 = 0{,}03$

Рис. 11. Залежності $p_{ij}(t)$ при $\Lambda_1 > \Lambda_2$

Хід залежностей $p_{ij}(t)$ і 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 $p_{20} \geq 0$, $p_{21} > p_{20}$ і $\frac{dp_{20}}{dt} > 0$. З часом p_{21} зменшується, а p_{20} зростає і зрештою досягає максимуму в точці p_{20}^0, яка визначається рівністю:

$$\frac{p_{20}^0(t_{20}^0)}{p_{21}(t_{20}^0)} = \frac{\Lambda_1}{\Lambda_2}. \qquad (4)$$

Моменти t_{ij}^0, коли імовірності станів досягають своїх максимальних значень, визначаються з виразів для похідних $\frac{dp'_{ij}}{dt}$, які прирівнюються до нуля. Для початкових станів одержуються 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 знаходяться підставивши у вирази $p_{ij}(t)$ значення t_{ij}^0 або виразивши p_{ij}^0 через імовірності попередніх станів. Так, наприклад, з (4) одержано: $p_{20}^0 = \frac{\Lambda_1}{\Lambda_2} p_{21}(t_{20}^0)$.

У **п'ятому** розділі проведено експериментальну перевірку ефективності динамічного управління ресурсами. Для перевірки ефективності запропонованого методу проведено обчислювальний експеримент: розраховано оптимальні розподіли ресурсів між об'єктами захисту з різними характеристиками (рис. 12, 13). У якості вихідних даних використано параметри СЗІ функціонуючого підприємства.

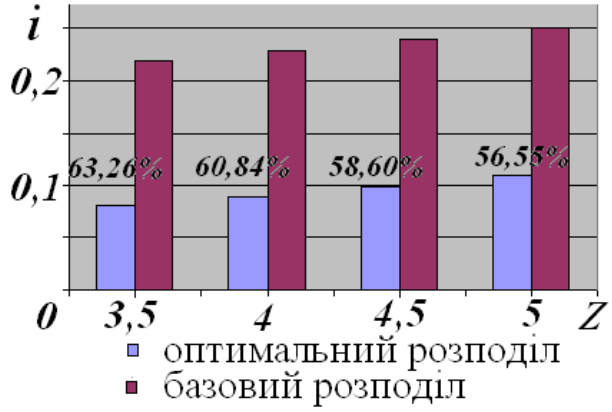


Рис. 12. Зниження рівня потенційної шкоди від реалізації загроз при переході від базового розподілу ресурсів захисту до оптимального

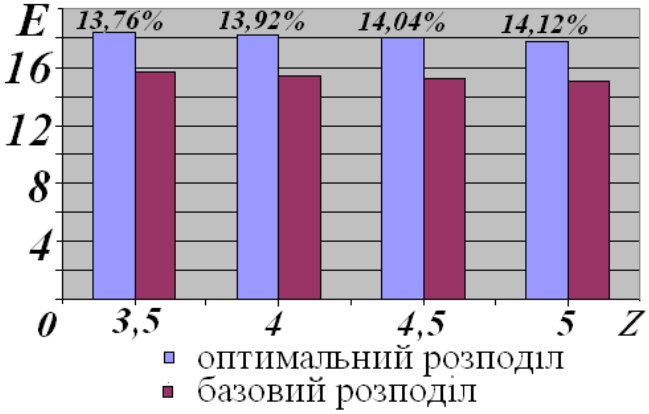


Рис. 13. Підвищення ефективності використання ресурсів захисту при переході до оптимального розподілу

На основі даних підприємства провендено аналіз динамічного протистояння сторін нападу і захисту. У процесі проведення моделювання: 1) проведено оцінку потенційних збитків від реалізації загроз на кожному об'єкті системи, кожному

об’єкту присвоєно ваговий коефіцієнт $g_1 = 0{,}05; g_2 = 0{,}45;\ g_3 = 0{,}5;$ 2) задано уразливості об’єктів; проведено аналіз та створено модель порушника та атак, що включає можливі загрози та варіанти їх реалізації; 3) у результаті моделювання процесу нападу і захисту обрано розподіл між об’єктами підприємства, який гарантує мінімальну потенційну шкоду від реалізації загроз інформації при найбільш несприятливих умовах. У порівнянні з запровадженим на підприємстві розподілом ресурсів це дозволить знизити рівень потенційних збитків від витоку інформації на 55-63% та підвищити ефективність використання ресурсів захисту на 14%

На основі порівняння встановлено, як різниця в розподілі ресурсів впливає на результат. Виявлено, що нова структура СЗІ ефективніша за існуючу. Запропонована модель із цільовою функцією, що включає основні показники системи, являється гнучкою, не потребує окремого аналізу параметрів системи та зручна при наданні рекомендацій, чим обґрунтовується ефективність та адекватність моделі.

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 метод її застосування дозволяють визначити не тільки загальну кількість ресурсів, які доцільно використати на захист інформації, а й оптимізувати їх розподіл між об’єктами в 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. На базі запропонованої цільової функції розроблено математичну модель динамічного управління ресурсами захисту інформації та сформовано інвестиційний метод, що за рахунок використання нових функціональних залежностей дає можливість обгрунтувати рішення щодо оптимального розподілу ресурсів і виявити вплив внесених інвестицій на величину завданої шкоди від реалізації загроз інформації і знизити рівень очікуваних збитків до 63%.

3. 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%.

4. 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 створити інструментарій оцінки рівня інформаційної безпеки та визначити стан інформаційної безпеки у конкретний момент часу.

5. На основі імітаційного моделювання наслідків почергового прийняття рішень сторонами нападу і захисту сформульовано рекомендації щодо оптимізації розподілу ресурсів та оцінки розміру 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 потенційних збитків на 42% у порівнянні із базовим розподілом, запровадженим на підприємстві.

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

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

8. 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 ОПУБЛІКОВАНИХ ПРАЦЬ АВТОРА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Прус Р.Б. Оптимізація розподілу ресурсів захисту інформації в динамічному режимі // Безпека інформації. – 2012. – №1. – С. 26-32.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

АНОТАЦІЯ

Прус Р.Б. Методи та моделі динамічного управління ресурсами захисту інформації. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – Інформаційна безпека держави. – Національний авіаційний університет, Київ, 2014.

Дисертація присвячена вирішенню питань теорії та практики створення ефективних систем захисту інформації. Метою роботи є підвищення рівня захищеності інформаційних систем за рахунок оптимального розподілу ресурсів захисту інформації між об'єктами захисту із врахуванням дій зловмисника.

На основі математичного апарату теорії ігор розроблено математичну модель складних інформаційних структур, що потребують захисту, яка дає можливість оптимізувати використання ресурсів захисту в системах, які відрізняються кількістю об’єктів, розташуванням перешкод, їх уразливістю, розподілом інформації по об’єктах при різних співвідношеннях ресурсів нападу і захисту. Розглянуто умови існування сідлової точки цільової функції, розраховані інтервали її існування по відносній кількості ресурсів в складних системах. На базі моделі розроблено метод удосконалення технології динамічного регулювання розподілу ресурсів захисту, що враховує зміну параметрів та характеристик системи захисту залежно від зміни націленості атак зловмисника. Запропоновано модель реалізації процесів різнонаправленого протистояння для визначення часової залежності інформаційного балансу конкуруючих сторін в умовах постійних спроб здобуття інформації.

Проведено дослідження систем захисту інформації, на основі яких сформульовано рекомендації щодо використання розроблених методів і моделей.

Ключові слова: інформаційна безпека, математична модель, уразливість об’єктів, розподіл ресурсів, оптимізація.

АННОТАЦИЯ

Прус Р.Б. Методы и модели динамического управления ресурсами защиты информации. – На правах рукописи.

Диссертация на соискание учёной степени кандидата технических наук по специальности 21.05.01 – Информационная безопасность государства. – Национальный авиационный университет, Киев, 2014.

Диссертация посвящена решению вопросов теории и практики создания эффективных систем защиты информации. Целью роботы является повышение уровня защищенности информационных систем за счет оптимального использования ограниченных ресурсов защиты с учетом действий злоумышленника. Эта задача имеет два аспекта. Во-первых, необходимо определить общее количество ресурсов, которые целесообразно выделить на защиту информации. Критерием целесообразности является минимум общих потерь. Эта задача рассматривалась разными авторами, и методика ее решения может считаться известной. Во-вторых, необходимо найти оптимальное распределение выделенных ресурсов между объектами. Показателями оптимальности могут быть доля утерянной информации, общие потери, прибыль от инвестиций в защиту, их рентабельность и т.п. Эта задача недостаточно разработана, и поиску ее решения посвящена данная работа.

Следуя поставленной цели, на основе математического аппарата теории игр разработана математическая модель сложных информационных структур, требующих защиты, которая дает возможность оптимизировать использование ресурсов в системах, которые отличаются количеством объектов, расположением препятствий, их уязвимостью, распределением информации по объектам при различных соотношениях ресурсов нападения и защиты. В результате исследований обоснован выбор целевой функции модели и функциональных зависимостей, которые входят в ее состав. Особое внимание уделено функции динамической уязвимости объектов, которая описывает уязвимости как

физических, так и электронных систем. Определение зон наибольшей продуктивности расходов в сложных системах защиты информации позволяет рассчитать объем ресурсов обеспечивающих достижение заданных значений продуктивностей и повышение эффективности использования выделенных средств.

На базе предложенной модели сформирован метод динамического управления ресурсами защиты информации, позволяющий обосновать решение о распределении ресурсов и показать влияние внесенных инвестиций на значение величины ожидаемых потерь информации и снизить ее уровень. Предложенный метод благодаря принятию во внимание действий злоумышленника позволяет оценить последствия принятых решений, прогнозировать уровень ожидаемых потерь и выбрать решение гарантирующее минимальные ожидаемые потери информации при наиболее неблагоприятных условиях.

Используя модель, разработан метод исследования в динамическом режиме комплексного противостояния, в случае одновременной защиты собственной информации и получении информации противника. Рассмотрены условия существования седловой точки целевой функции, рассчитаны интервалы ее существования по относительному количеству ресурсов в сложных условиях. На основе использования марковских цепей разработан метод определения временной зависимости информационного баланса конкурирующих сторон в условиях постоянных попыток получения информации.

Приведены расчеты систем, на основе которых сформулированы рекомендации насчет разработанного программного обеспечения.

Ключевые слова: информационная безопасность, математическая модель, уязвимость объектов, распределение ресурсов, оптимизация.

ABSTRACT

Prus R.B. The methods and models of dynamic resource control in information security. – Manuscript.

Thesis for scientific degree of candidate of technical science on a speciality 21.05.01– Information security of the state. – National Aviation University, Kyiv, 2014.

The thesis is dedicated to solving theoretical and practical problems of generation efficient information security systems. Research has as its object increasing information security indices by optimal use of resources.

Pursuing objective mathematical model of multilevel multibarrier information security systems is developed and studied; the model enables to optimize the use of resources in systems which differ in quantity of objects, placement of obstacles, vulnerability, and information distribution between the objects with different ratio of attack and defense resources. Conditions of saddle point existence of objective function are examined; saddle point existence intervals of values relative amount of resources in complicated systems, which differ in structure, number of objects, information distribution between the objects, their vulnerability, are calculated. Using mentioned model method of testing in dynamic mode of complex confrontation when each of the sides attempts both to defense his information and to get his opponent’s information. The method of determining time dependence of competitive sides’ information balance in permanent attempts to get information, which based on Markov chains, is devised.

System designs are provided, on base of which recommendations for software devising are made.

Keywords: information security, mathematical model, objects' vulnerability, resource allocation, optimization.