НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ХОХЛАЧОВА Юлія Євгеніївна

УДК 004.056.53

МЕТОДИ ОЦІНЮВАННЯ УРАЗЛИВОСТЕЙ ТА ОПТИМІЗАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ В УМОВАХ ІНФОРМАЦІЙНИХ ВПЛИВІВ

Спеціальність 05.13.21 – «Системи захисту інформації»

Автореферат

дисертації на здобуття наукового ступеня

кандидата технічних наук

Київ – 2015

Дисертацією є рукопис.

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

Науковий керівник: доктор технічних наук, професор
Хорошко Володимир Олексійович,
Національний авіаційний університет,
професор кафедри безпеки інформаційних технологій.

Офіційні опоненти: доктор технічних наук, професор
Стасюк Олександр Іонович,
Державний економіко-технологічний університет транспорту;

кандидат технічних наук, доцент
Браіловський Микола Миколайович,
Державний університет телекомунікацій.

Захист відбудеться «28» травня 2015 р. о 16^{00} годині на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03680, Київ, пр. Космонавта Комарова, 1.

З дисертацією можна ознайомитись в науково-технічній бібліотеці Національного авіаційного університету.

Автореферат розісланий «28» квітня 2015 р.

Учений секретар
спеціалізованої вченої ради
к.т.н., доцент Гнатюк С.О.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. Розвиток сучасних інформаційних і комунікаційних технологій впливає на усі на сфери людської життєдіяльності, підвищуючи їх ефективність і, одночасно, породжуючи множину неконтрольованих загроз, у тому числі і в інформаційній сфері. З огляду на це, постійно підвищуються вимоги щодо захисту критично важливих інформаційних ресурсів. На сьогодні ключовими і визначальними міжнародними нормативно-правовими актами у галузі управління інформаційною безпекою (ІБ) і захисту інформації є серія стандартів ISO 27k. Згідно останньої основними процедурами для організації ефективної системи менеджменту ІБ є управління ресурсами, комунікаціями та операціями, ризиками, безперервністю роботи, інцидентами ІБ тощо. Менеджмент інцидентів, згідно міжнародного стандарту ISO/IEC 27035:2011, дозволяє своєчасно та ефективно виявляти, аналізувати й розслідувати інциденти ІБ для мінімізації негативних наслідків для інформаційних систем (ІС) і організацій взагалі. Крім зазначеного міжнародного стандарту, сьогодні є багато галузевих нормативних документів, а також практичних рекомендацій та керівництв, що базуються на кращих світових практиках щодо інцидент-менеджменту. Згідно цих документів виконання процедури управління інцидентами покладається на спеціалізовані групи швидкого реагування, які, відповідно до своїх організаційних і функціональних особливостей, надають своїм клієнтам певні сервіси. Серед базових сервісів варто виділити ідентифікацію та аналіз інцидентів, реагування на інциденти та їх розслідування, аналіз уразливостей ІС, а також випробування їх стійкості шляхом моделювання атак і впливів. З огляду на те, що успішність реалізації інформаційного впливу на систему залежить від її уразливостей і в гіршому випадку перетворюється на інцидент, дослідження поведінки системи (оптимізації її ключових параметрів та показників захищеності) під дією інформаційних впливів з точки зору захисту інформації є актуальним напрямком наукових досліджень.

Значний внесок у розвиток теорії і практики у цьому напрямку внесли такі вітчизняні і закордонні вчені як Баранов В.Л., Браіловський М.М., Гордон Л.А., Грищук Р.В., Дудикевич В.Б., Кобозєва А.А., Козловський В.В., Корченко О.Г., Лоеб М.П., Пархуць Л.Т., Самохвалов Ю.Я., Скурихін В.І., Стасюк О.І., Хорошко В.О., Юдін О.К. та ін.

Однак, у зазначеній галузі залишається низка завдань, вирішення яких має важливе наукове та практичне значення. З цих позицій, побудова і дослідження методів моделювання впливів на ІС, оцінювання уразливостей та оптимізація показників систем захисту в умовах впливів, є *актуальним науковим завданням.*

Зв'язок роботи з науковими програмами, планами, темами. Одержані результати дисертаційної роботи відображені у звітах держбюджетних науково-дослідних робіт Національного авіаційного університету («Організація систем захисту інформації від кібератак», № 0111U000171), Кіровоградського національного технічного університету («Розробка методів підвищення оперативності передачі та захисту інформації у телекомунікаційних системах», № 0113U003086) та Державного університету інформаційно-комунікаційних технологій («Безпека – 01П», що виконувалась відповідно до постанови КМУ №01086 від 25.12.2005).

Мета і задачі дослідження. Метою дисертаційної роботи є розробка методів оцінювання уразливостей та оптимізації інформаційних систем в умовах інформаційних впливів.

Для досягнення поставленої мети **необхідно розв’язати такі основні задачі:**

– проаналізувати існуючі методи і засоби оцінки уразливостей інформаційних систем для виявлення їх недоліків, а також провести аналіз сучасних методів моделювання впливів на інформаційні системи для їх подальшого використання в процесах оптимізації параметрів цих систем;

– розробити метод знаходження оптимальної конфігурації інформаційної системи на базі теорії графів;

– запропонувати систему правил щодо моделювання критеріїв оптимальності та обмеження загроз інформації для їх використання з метою оптимізації параметрів інформаційних систем в умовах інформаційних впливів;

– розробити метод оптимізації інформаційних систем на основі диференціальних ігор для визначення у реальному часі оптимальної стратегії поведінки сторони захисту в умовах інформаційних впливів;

– розробити метод оптимізації систем захисту інформації з метою визначення оптимальної поведінки у системі «вплив-безпека» і підвищення рівня захищеності інформації в інформаційній системі;

– розробити алгоритми та програмне забезпечення для реалізації розроблених методів і проведення експериментального дослідження з метою верифікації отриманих у роботі результатів.

Об'єктом дослідження є процеси оцінювання уразливостей та моделювання інформаційних впливів на інформаційні системи.

Предметом дослідження є моделі та методи моделювання впливів на інформаційні системи та оцінювання їх уразливостей.

Методи дослідження. Проведені у дисертаційній роботі дослідження базуються на методах теорії ймовірності (розробка та дослідження методики оцінювання уразливостей та розрахунки кількісних показників рівня ІБ), теорії диференціальних ігор (розробка методів оптимізації систем захисту інформації та параметрів ІС в умовах впливів), теорії графів (розробка методу знаходження оптимальної конфігурації ІС), моделювання інформаційних процесів та структур (дослідження антагоністичних відносин у системі «інформаційний вплив – система безпеки») та ін.

Наукова новизна одержаних результатів полягає в наступному:

– *вперше* запропоновано диференціально-ігровий метод оптимізації параметрів інформаційних систем, що, за рахунок врахування стратегії гравця впливу, критерію оптимізації ресурсів гравців у процесі оптимізації і енергетичної складової у заданий період часу, дозволяє визначати у реальному часі оптимальну стратегію безпеки інформації в інформаційних системах;

– *вперше* запропонована система правил щодо моделювання визначених критеріїв оптимальності для систем захисту інформації, яка, за рахунок синтезу морфологічним методом сепарабельних адитивних критеріїв та обмежень, дозволяє розв’язувати задачі аналізу, синтезу та оптимізації систем за обраними критеріями та виділеними обмеженнями, а також оцінювати рівень захищеності інформаційних систем з урахуванням дозволених границь гарантованого рівня захисту інформації;

– *отримав* подальший розвиток метод оптимізації систем захисту інформації, що, за рахунок врахування параметрів системи безпеки (кількість засобів безпеки, тип підсистеми безпеки, сумарний ресурс безпеки та цінність інформації), дозволяє визначати оптимальну поведінку в системі «вплив-безпека»;

– *удосконалено* метод знаходження оптимальної конфігурації інформаційної системи, який, за рахунок використання теоретико-графового моделювання

зворотного ходу побудови оптимального вихідного дерева, дозволяє визначати оптимальну архітектуру інформаційної системи в умовах інформаційних впливів.

Практичне значення одержаних результатів

Отримані в дисертаційній роботі результати можуть бути використані для розширення інструментарію груп швидкого реагування на інциденти ІБ, підрозділів ІБ організацій, оцінювання уразливостей ІС, а також для підвищення ефективності розробки методів і систем захисту інформації. Практична цінність роботи полягає у такому:

– використання запропонованих методів при розробці спеціального програмного забезпечення дозволило підвищити захищеність інформаційних ресурсів, що підтверджується актом впровадження у діяльність військової частини К-1410 (акт від 14.06.2012 р.) та ТОВ «Конзьюмер Експрес» (акт від 17.11.2014 р.);

– розроблена комп'ютерна програма, яка використовується для моделювання атакуючих дій і оцінки уразливостей в ІКС та у навчальному процесі підготовки фахівців у галузі ІБ. Практичне використання результатів дисертаційного дослідження підтверджується актами впровадження у навчальний процес Національного авіаційного університету (акт від 10.02.2015 р.), Державного університету інформаційно-комунікаційних технологій (акт від 26.06.2012 р.) та Кіровоградського національного технічного університету (акт від 17.09.2014 р.);

– запропоновано методику оцінки уразливостей та інформаційних впливів, які, за рахунок використання логіко-ймовірнісних пар зв'язок «параметри → уразливості», дозволяють ідентифікувати уразливості інформаційних систем в умовах впливів;

– розроблено методику проведення експерименту, що дозволила дослідити запропоновані у роботі методи.

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. У роботах, написаних у співавторстві, автору належать: [1] – дослідження існуючих методів теорії диференціальних ігор та визначення оптимальних стратегій; [2, 22, 23] – розробка моделі ІБ, на базі якої можна вибрати систему контрзаходів, що зменшують ризики з найбільшою ціновою ефективністю; [3, 20] – дослідження та аналіз функціональних особливостей систем управління інцидентами ІБ; [5, 13, 14, 16] – аналіз та дослідження існуючих методів і засобів оцінки уразливостей ІС та сучасних методів моделювання впливів на ІС; [6, 9, 21] – розробка методики оцінки захищеності ІС на основі застосування принципів системотехніки; [11] – розробка методики оцінки рівня захищеності системи зв'язку; [12] – аналіз та дослідження існуючих методик оцінювання рівня безпеки; [15] – розробка алгоритму визначення показників для оцінки надійності систем спеціального призначення; [17] – розробка та дослідження методик оцінки уразливостей та інформаційних впливів; [18, 19] – удосконалення методу знаходження оптимальної конфігурації інформаційної системи; [21, 30] – розробка методу оптимізації параметрів ІС.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідалися та обговорювалися на наукових конференціях та семінарах, серед яких: НПК «Захист інформації з обмеженим доступом та автоматизація її обробки» (Київ 2010 р.); X міжнародна НТК «АВІА-2011» (Київ 2011 р.); IX міжнародна НПК «ПОЛІТ-2011» (Київ 2011 р.); IV міжнародна НПК «Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2011)» (Київ 2011 р.); II НТК «Безпека інформаційних технологій («Information Technology Security», ITSEC-2012)» (Київ 2012 р.); НТК «Захист інформації і безпека інформаційних систем» (Львів 2013 р.,

2014 р.); XVI міжнародна НПК «Безопасность информации в информационно-телекоммуникационных системах» (Київ 2013 р.); НПК «Інформаційні управляючі системи та технології» (Одеса 2013 р., 2014 р.); VI міжнародна НПК «Проблеми і перспективи розвитку ІТ-індустрії» (Харків 2014 р.); XV міжнародна НПК «Современные информационные и электронные технологии (СИЭТ-2014)» (Одеса 2014 р.); IV міжнародна НПК «Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки» (Чернівці 2014 р.), НПК «Актуальні питання забезпечення кібернетичної безпеки та захисту інформації» (Київ 2015 р.).

Публікації. Основні положення дисертації опубліковано у 29 наукових працях, у тому числі 20 статей у наукових журналах та збірниках наукових праць, які входять до переліку фахових наукових видань МОН України (серед них 4 статті у виданнях, що входять до міжнародних наукометричних баз даних), а також 9 тез доповідей і матеріалів конференцій.

Структура роботи та її обсяг. Дисертація складається зі вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел і має 139 сторінок основного тексту, 37 рисунків, 6 таблиць, 33 сторінок додатків. Список літератури містить 105 найменувань і займає 10 сторінок. Загальний обсяг роботи 182 сторінок.

ОСНОВНА ЧАСТИНА

У **вступі** представлена загальна характеристика роботи, обґрунтована актуальність, сформульовані мета і задачі досліджень, відображені наукова новизна і практична цінність отриманих результатів, наведено дані про їх апробації та впровадження.

У **першому розділі** проведено детальний аналіз сучасних *засобів оцінювання уразливостей інформаційних систем* (зокрема, поширених систем Nessus, xSpider, Shadow Security Scanner, Microsoft Baseline Security, Windows Vulnerability Scanner, Nikto тощо). Аналіз проводився за такими базовими критеріями (рис. 1): *ОР* – оцінка ризиків; *ОЗ* – оцінка захищеності; *К* – кросплатформеність; *ЗК* – зручність у користуванні; *ВК* – відкритий код; *НВ* – низька вартість; *МС* – відповідність міжнародним стандартам у галузі ІБ. У результаті багатокритеріального аналізу встановлено, що усі ці засоби не є досконалими і мають певні обмеження щодо практичного застосування для розв'язання різного роду завдань ІБ.

Таблиця 1

Результати аналізу сучасних засобів оцінювання уразливостей ІС

№ з/п	Назва	Критерії						
		ОР	ОЗ	К	ЗК	ВК	НВ	МС
1.	Nessus 2.2.4	-	+	+	+	+	-	+
2.	AccessDiver 4.172	-	-	-	+	-	-	+
3.	xSpider 6.5.0.12	-	+	-	+	-	-	-
4.	LANguard Network Security Scanner 5.0	-	+	-	+	-	-	-
5.	Shadow Security Scanner 6.00	-	+	-	+	-	+	-
6.	Nikto 1.32	-	-	+	+	+	-	+
7.	14 Day Trial	-	-	+	+	-	+	-
8.	Windows Vulnerability Scanner	-	+	-	+	-	+	+
9.	Microsoft Baseline Security	-	+	-	+	-	+	+
10.	Cobra	+	+	-	+	-	-	+

11.	Cramm	+	+	-	+	-	-	+
12.	Calio Secura 17799	+	+	-	+	-	-	-
13.	Octave	+	+	-	+	-	-	+
14.	Proteus enterprise	+	-	-	+	-	-	+
15.	Ra2 the art of risk	+	+	-	-	-	-	+
16.	Risk watch	+	+	-	+	-	-	+
17.	VsRisk	+	+	-	-	+	-	+

Встановлено, що сучасна система оцінювання уразливостей має будуватися на базі міжнародних стандартів у галузі ІБ (наприклад, ISO 27k, ITIL, Cobit тощо), бути зручною у використанні пересічними користувачами, має володіти відкритою архітектурою (для можливості удосконалення шляхом розробки додаткових функціональних модулів), коректно працювати на різних програмних платформах (операційних системах), бути недорогою і виконувати ряд важливих функцій захисту інформації, а також оцінювання ризиків і захищеності ІС.

Крім того, визначено поняття *інформаційного впливу* як вхідних даних, що ініціюють в ІС алгоритми виведення її із штатного режиму функціонування. Очевидно, що інформаційний вплив використовує уразливості ІС для порушення їх захисних властивостей і виникнення інциденту. Для оцінювання захищеності ІС та виявлення їх уразливих ланок, як правило, використовують методи випробування стійкості, що штучно реалізують атаки зловмисників на ІС. З огляду на це, у роботі проведено аналіз *існуючих моделей і методів моделювання інформаційних впливів,* зокрема детально розглянуто модель Мухіна-Волокіти, модель Хартсона, модель на основі нейронних мереж та ланцюгів Маркова, модель на основі мереж Петрі-Маркова, графові моделі, диференціально-ігрові (одно- та багатокритеріальні) методи і моделі тощо. Встановлено, що *найбільш ефективним є підхід із використанням диференціально-ігрових перетворень*, так як він відображає динаміку інформаційного впливу у реальному часі (зокрема, враховує поведінку зловмисника), враховує більше параметрів і дозволяє оперативно здійснити перерозподіл ресурсів системи захисту.

У другому розділі розроблено метод знаходження оптимальної конфігурації ІС на базі теорії графів, а також методику оцінювання уразливостей ІС та інформаційних впливів, що базується на теорії ймовірностей.

Метод знаходження оптимальної конфігурації ІС (рис. 1) побудований на теоретико-графовому підході і реалізується у два етапи – прямого та зворотного ходу. Перший етап складається з блоків: обробки даних (БОД), знаходження суграфу (БЗС), перевірки умови 1 (БПУ1), знаходження сильно-зв'язкових компонентів (БСЗК); другий етап містить блоки: виділення множин (БМ), вибору мінімальної довжини дуги (БМД), знаходження величини дуги (БЗД), перевірки умови 2 (БПУ).

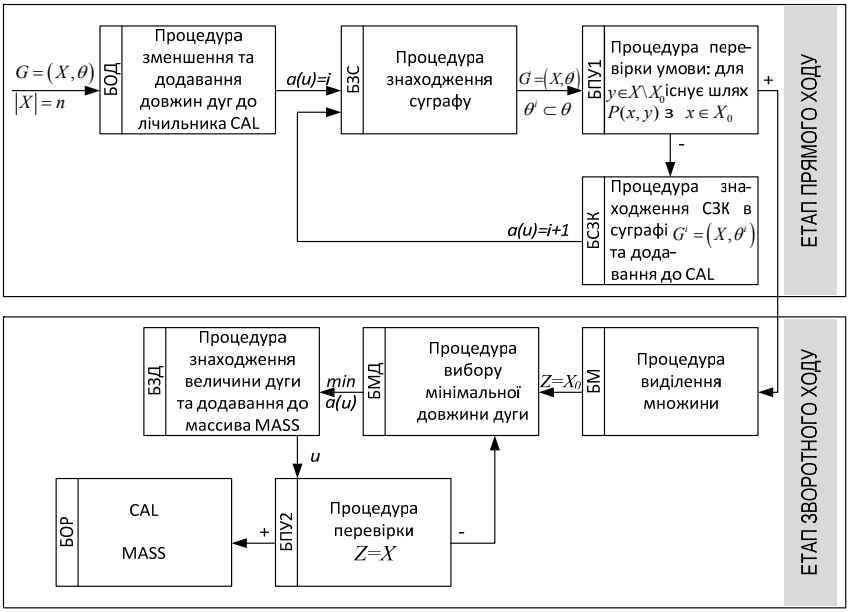

Рис. 1. Схематичне відображення методу знаходження оптимальної конфігурації ІС

Запропонований метод, на відміну від відомих (наприклад, методи Пріма-Краскала, Едмондо, Фалкерсона), охоплює нетривіальні деталі, що пов'язані із зворотнім ходом побудови оптимального вихідного дерева і дає можливість більш ефективно визначати оптимальну архітектуру інформаційної системи в умовах інформаційних впливів. У процесі розроблення зазначеного методу для довільного графа із заданою базою та визначеними довжинами дуг розв'язана задача побудови суграфу з аналогічними вершинами та мінімальною сумою довжин дуг, крім того, сформульовано і розв'язано дві суміжні задачі, доведено три леми і одну теорему.

Також, з урахуванням результатів багатокритеріального аналізу, розроблено *методику оцінювання уразливостей ІС та інформаційних впливів.* Ця методика базується на математичному апараті теорії ймовірностей і за рахунок використання логіко-ймовірнісних пар зв'язок «параметри → уразливості» дозволяють ідентифікувати уразливості інформаційних систем в умовах впливів.

Третій розділ роботи присвячено розробці системи правил моделювання критеріїв оптимальності та загроз інформації, а також розробці двох методів оптимізації параметрів ІС в умовах інформаційних впливів. Побудова *математичних моделей критеріїв ефективності (оптимальності) та обмежень* є ключовою проблемою в усіх задачах аналізу, синтезу та оптимізації ІС, що розробляються, тому побудова власне процедур формалізації критеріїв та обмежень є важливим та актуальним завданням. З огляду на це, у роботі розроблено відповідну систему правил, що базується на таких *принципах:* 1) критерії ефективності повинні дозволяти оптимальне керування, тобто готувати та приймати оптимальні рішення, у тому числі й при наявності обмежень; 2) з огляду на те, що у задачах оптимізації обмеження відіграють роль критеріїв, то математичні моделі обмежень конструюють також і моделі критеріїв; 3) будь-яка задача з обмеженнями може бути перетворена у

послідовність задач без обмежень, тому для вибору канонічних форм можна використовувати допоміжну функцію Лагранжа як узагальнений критерій оптимальності, який враховує обмеження. Зазначена система правил математичного моделювання критеріїв оптимальності та обмежень будується на необхідних та достовірних умовах існування екстремумів функцій та функціоналів. Система складається з 8 правил.

Правило оптимальності. Будь-яка безперервна двічі диференційована функція $OC(cv_1,...,cv_\varepsilon)$ від ε аргументів може бути критерієм оптимальності *OC* (Optimality Criterion) цільової функції, а самі аргументи є керованими змінними *cv* (Controlled Variables), якщо для області існування *OC* дотримуються необхідні та достатні умови існування екстремумів.

Правило обмеження. Будь-яка безперервна двічі диференційована функція $L(cv_1,...,cv_\varepsilon)$ від ε незалежних аргументів може бути обмеженням (Limitation), а самі аргументи є керованими змінними, якщо для області існування *L* дотримуються необхідні та достатні умови існування екстремумів та задані обмеження у вигляді:

$$L_1(cv_1,...,cv_\varepsilon) = L_1^*,...,L_\mu(cv_1,...,cv_\varepsilon) = L_\mu^*; \tag{1}$$

де μ – число обмежень.

Правило існування. Для того, щоб оптимальне рішення існувало та було єдиним, необхідно щоб число керованих змінних та число обмежень задовольняли умові:

$$\varepsilon > \mu. \tag{2}$$

Правило зведення. У випадках, коли обмеження (1) задані у вигляді нерівностей, оптимізація зводиться до відомих способів введення фіктивних допоміжних змінних. Якщо цільові функції та обмеження можуть мінятися місцями, то в задачах оптимізації повинна виконуватися необхідна умова (2).

Правило допоміжної функції. У задачах оптимізації з обмеженнями за критерій оптимізації використовується допоміжна функція Лагранжа виду:

$$\begin{aligned} &AL(cv_1,...,cv_\varepsilon) = OC(cv_1,...,cv_\varepsilon) + (\lambda_1\left[L_1(cv_1,...,cv_\varepsilon) - L_1^*\right] + ... \\ &+\lambda_\mu\left[L_\mu(cv_1,...,cv_\varepsilon) - L_\mu^*\right]), \end{aligned} \tag{3}$$

де λ_k – допоміжні невизначені множники Лагранжа, $k = \overline{1,\mu}$.

Правило канонічності. Система з $\varepsilon + \mu$ рівнянь оптимізації:

$$\begin{cases} \dfrac{\partial AL(cv_1,\lambda_1)}{\partial cv_1} = 0,..., \dfrac{\partial AL(cv_\varepsilon,\lambda_\varepsilon)}{\partial cv_\varepsilon} = 0 \\ \dfrac{\partial AL(cv_1,\lambda_1)}{\partial \lambda_1} = 0,..., \dfrac{\partial AL(cv_\mu,\lambda_\mu)}{\partial \lambda_\mu} = 0, \end{cases} \tag{4}$$

може бути подана у канонічній формі виду

$$\begin{cases} \dfrac{\partial AL_1(cv_1,\lambda_1)}{\partial cv_1} = \dfrac{\partial AL_2(cv_1,\lambda_1)}{\partial cv_1},..., \dfrac{\partial AL_1(cv_\varepsilon,\lambda_\varepsilon)}{\partial cv_\varepsilon} = \dfrac{\partial AL_2(cv_\varepsilon,\lambda_\varepsilon)}{\partial cv_\varepsilon} \\ L_1(cv_1,...,cv_\varepsilon) = L_1^*,...,L_\mu(cv_1,...,cv_\varepsilon) = L_\mu^*. \end{cases} \tag{5}$$

Таким чином систему (5) будемо називати *першою канонічною формою представлення системи рівнянь оптимізації.* Елементи обох частин рівнянь (5) будемо називати типовими елементами першої канонічної форми.

Правило критеріїв. Використання першої канонічної форми (5) системи рівнянь оптимізації дозволяє створювати критерії оптимізації у вигляді сепарабельних адитивних критеріїв:

$$OC(cv_1,...,cv_\varepsilon) = \sum_{i=1}^{\varepsilon}\left(\int \frac{\partial AL_1(cv_1,...,cv_\varepsilon;\lambda_1,...,\lambda_\mu)}{\partial cv_i} dcv_i - \right.$$

$$\left. -\int \frac{\partial AL_2(cv_1,...,cv_\varepsilon;\lambda_1,...,\lambda_\mu)}{\partial cv_i} dcv_i\right), \qquad (6)$$

Сепарабельність $OC(cv_1,...,cv_\varepsilon)$ означає, що всі недіагональні елементи матриці других часткових похідних цієї функції дорівнюють нулю.

Правило сепарабельного програмування. Сепарабельну форму та адитивність також зручно використовувати для обмежень виду (5):

$$OC_{1k}(cv_1) + ... + OC_{\varepsilon k}(cv_\varepsilon) = OC_k^*. \qquad (7)$$

Задачу оптимізації, у якій критерій оптимізації представлений у вигляді (6), а обмеження у вигляді (7), будемо називати *задачею сепарабельного програмування.* Якщо $OC(cv_1,...,cv_\varepsilon)$ є випуклою функцією, а $L_k(cv_1,...,cv_\varepsilon)$ – угнутою, існує рішення прямих задач сепарабельного програмування. Для зворотних задач функції $OC(cv_1,...,cv_\varepsilon)$ та $L_k(cv_1,...,cv_\varepsilon)$ повинні володіти протилежними властивостями. Властивості сепарабельності та адитивності дозволяють створювати ефективні обчислювальні алгоритми пошуку оптимальних рішень. Представлення критерію оптимізації у вигляді (6) називається *другою канонічною формою постановки задачі оптимізації.* У задачах оптимізації при побудові допоміжних функцій Лагранжа (3) критерій та одне з обмежень міняються місцями. При цьому змінюється і характер екстремуму, і вимоги випуклості та вгнутості цільових функцій та обмежень. Доданки суми (6) будемо називати типовими елементами другої канонічної форми.

$$F_2^T \frac{\partial \Phi_B^T}{\partial \phi},$$

$$J_B = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\left\{\phi(x,y) - G_2\left[(7;50;x),(0,5;0,6;y)\right]\right\}^2 dxdy +$$

$$+\int_{t_0}^{t}\int_{-\infty}^{\infty} U_B^2(x,y,t)dxdydt,$$

Відповідно до результатів аналізу, проведеного у першому розділі роботи, використання диференціально-ігрових моделей у системах безпеки інформації дозволяє: 1) описати задачу забезпечення безпеки у строгій математичній постановці; 2) знаходити область кількісних оцінок рівня безпеки інформації на відміну від інших якісних підходів; 3) знаходити оцінку поточного і прогнозованого рівнів безпеки; 4) знаходити аналітичні співвідношення оптимальних стратегій забезпечення безпеки; 5) досліджувати динаміку ходу конфлікту в ІС; 6) оптимізувати і керувати процесом забезпечення безпеки тощо. З огляду на це, розроблено *метод оптимізації ІС* (рис. 2).

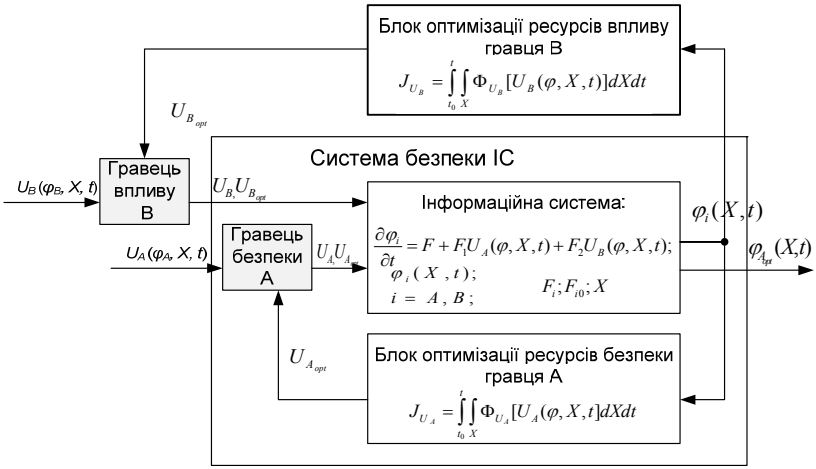

Рис. 2. Схема відображення методу оптимізації ІС на основі диференціальних ігор

Інформаційна система має систему безпеки по своєму периметру, гравець впливу ***B*** впливає на ІС з різною інтенсивністю (в тому числі, обираючи оптимальну стратегію впливу, що оптимізується у блоці оптимізації ресурсів впливу) U_B. Під впливом стратегії гравця ***B*** ІС змінює негативно стан безпеки. Потрібно оптимізувати ІС таким чином щоб забезпечити чи підвищити заданий рівень безпеки. Гравець безпеки ***A*** оптимізує свої ресурси безпеки так, щоб обрати серед стратегій захисту найоптимальнішу. Запропонований метод, на відміну від існуючих, враховує стратегію гравця впливу, критерій оптимізації ресурсів гравців у процесі оптимізації і енергетичну складову у заданий період часу.

Крім того, запропоновано *метод оптимізації поведінки системи безпеки інформації в умовах впливів* (рис. 3). Типовою задачею дослідження поведінки системи безпеки в умовах впливів на інформацію є оптимальний розподіл ресурсів гравця безпеки відносно ресурсів гравця впливу.

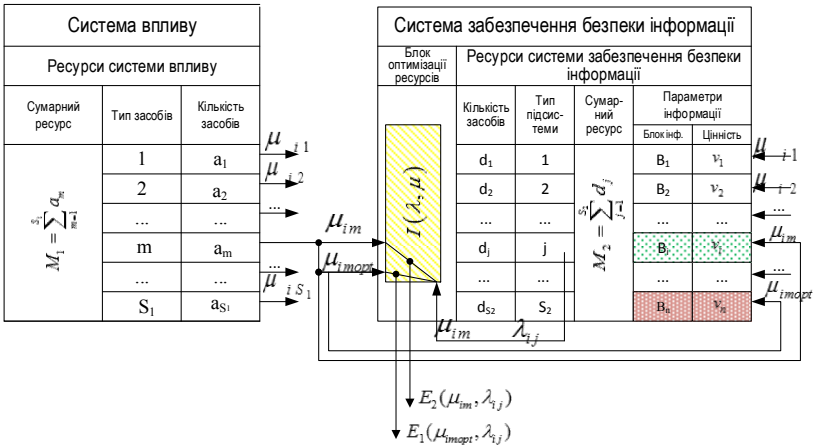

Рис. 3. Схема відображення методу оптимізації поведінки систем безпеки в умовах впливів

Нехай є дві системи – система впливу (СВ) – є гравцем, що впливає на інформацію іншої системи, системи забезпечення безпеки інформації (СЗБІ). Для цього СВ використовує певну кількість методів і засобів нападу. Засоби впливу СВ складаються з S_1 типів, причому в деяких умовних одиницях кількість засобів m-го типу дорівнює a_m. Сумарний ресурс (потенціал) впливу СВ M_1 становить величину, що дорівнює $M_1 = \sum_{m=1}^{S_1} a_m$. Аналогічно СЗБІ складається з S_2 типів підсистем безпеки, причому кількість засобів захисту j-го типу в умовних одиницях дорівнює d_j. Сумарний потенціал безпеки СЗБІ M_2 визначається як $M_2 = \sum_{j=1}^{S_2} d_j$. Інформація, яка підлягає захисту, має n інформаційних блоків $B_i, \ldots, B_n$, причому цінність B_i-го блоку оцінюється деякою умовною величиною v_i, де $i = \overline{1,n}$. Нехай також інформаційні блоки $B_i, \ldots, B_n$ упорядковані за їх цінністю, тобто $v_i \geq \ldots \geq v_n$.

Припустимо, що кожен незахищений інформаційний блок B_i під час впливу на інформацію та реалізації однієї атаки засобами m-го типу втрачає свої властивості – цілісність, доступність та конфіденційність. Величина втрат від впливу на інформацію в СЗБІ на B_i-й інформаційний блок оцінюється величиною $v_i \varepsilon_m$. Сумарні втрати цілісності, доступності та конфіденційності інформації $I(\lambda,\mu)$, які визначають її безпеку в СЗБІ за умови наявності впливів та протидії їм, можна оцінити величиною, пропорційною різниці їх сумарної кількості, якщо вона позитивно визначена, і рівною нулю у протилежному випадку, тобто

$$I(\lambda,\mu) = \sum_{i=1}^{n} v_i \max\left\{0, \sum_{m=1}^{S_1} \varepsilon_m \left(\mu_{im} - \sum_{j=1}^{S_2} \lambda_{mj} \lambda_{ij} \right)\right\}, \qquad (8)$$

де $\mu_{i\,m}$ – інтенсивність потоку інформаційних впливів, виділених СВ для атаки на B_i-й інформаційний блок засобами впливу m-го типу; $\lambda_{i\,j}$ – інтенсивність потоку захисних дій, виділених СЗБІ для захисту B_i-го інформаційного блоку засобами безпеки j-го типу; $\lambda_{m\,j}$ – інтенсивність потоку дій забезпечення безпеки, що виділяється СЗБІ для відбиття впливу від засобів m-го типу засобами безпеки j-го типу. Розподіл засобів безпеки j-го типу, що виділяються СЗБІ для відбиття впливу від засобів m-го типу за умови $\sum_{m=1}^{S_1}\lambda_{m\,j}=1$, $1\le j\le S_2$ та $1\le m\le S_1$ може бути поданий у матричному вигляді: $\Lambda=\left\|\lambda_{m\,j}\right\|$, за відповідних обмежень $0\le\lambda_{m\,j}\le\lambda_{m\,j_{\max}}$, де $\lambda_{m\,j_{\max}}$ – максимальна інтенсивність потоку дій безпеки, $\lambda_{m\,j_{\max}}=1$.

Нехай сумарна величина втрат інформації в СЗБІ $I(\lambda,\mu)$ (8) виступатиме основною характеристикою інформаційного конфлікту, джерелом якого є протиріччя інтересів СЗБІ та СВ. При цьому СЗБІ намагається підвищити рівень безпеки інформації шляхом зменшення величини сумарних втрат (8), що наносяться діями СВ. Мета СВ є протилежною, тому функція (8) може бути прийнята як плата системи безпеки СВ. У результаті задача синтезу оптимальної поведінки в системі безпека-вплив зводиться до антагоністичної гри двох гравців з опуклою по одній змінній λ функцією виграшу $I(\lambda,\mu)$ (8) при довільному фіксованому значенні іншої змінної μ.

Таким чином, зазначений метод оптимізації поведінки системи безпеки інформації, на відміну від відомих, враховує такі параметри СЗБІ, як кількість засобів безпеки, тип підсистеми, сумарний ресурс та цінність інформації, що дозволяє визначати оптимальну поведінку в системі «вплив-безпека».

Четвертий розділ присвячено практичним реалізаціям та експериментальним дослідженням розроблених рішень. Розроблено *методику проведення експериментального дослідження,* в якій визначено мету та задачі експерименту, вхідні та вихідні параметри, гіпотезу і критерії дослідження, а також послідовність необхідних дій. Для проведення експерименту, на основі методу оптимізації поведінки систем безпеки інформації в умовах впливів, було розроблено програмне забезпечення «Optima – 2014 v.1.0», фрагмент інтерфейсу якого подано на рис. 4.

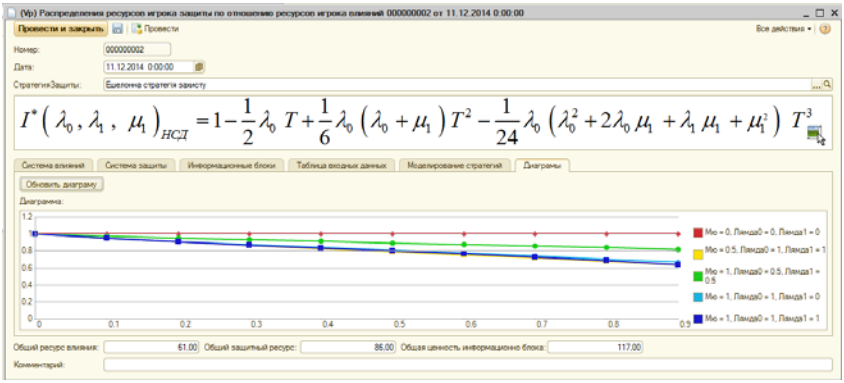

Рис. 4. Фрагмент інтерфейсу програмного забезпечення «Optima – 2014 v.1.0»

Задача синтезу оптимальної поведінки з використанням розробленого програмного забезпечення дозволяє оцінювати прогнозований $I\left(\lambda^{opt}, \mu^{opt}\right)$ та поточний $I(\lambda, \mu)$ рівні захищеності інформаційного ресурсу, залежно від стратегій λ та μ, які обираються гравцями – суб'єктами конфлікту на визначеному інтервалі $[t_0, T]$, де t_0 – момент часу початку інформаційного конфлікту, T – час його завершення. Процедура оцінювання зводиться до моделювання антагоністичної гри двох гравців.

Програмне забезпечення «Optima – 2014 v.1.0» реалізує оцінювання прогнозованого та поточного рівнів захищеності інформаційного ресурсу для таких стратегій побудови систем безпеки, як: ешелонована система захисту з n бар'єрів захисту; стратегія відведення гравця впливу на хибний інформаційний ресурс з подальшим втягуванням його в інформаційний конфлікт; стратегія оцінювання рівня захищеності за шаблоном нормальної поведінки системи.

Згідно опису методу оптимізації поведінки системи безпеки інформації в умовах впливів рівень захищеності, залежно від обраних стратегій побудови таких систем, у загальному вигляді визначається згідно з (8). При цьому для різних стратегій захисту систем безпеки, які обираються гравцем захисту, прогнозований $I\left(\lambda^{opt}, \mu^{opt}\right)$ та поточний $I(\lambda, \mu)$ рівні захищеності інформаційного ресурсу набувають значень, які варіюють у діапазоні $I \in [0,1)$.

Наприклад, для часткового випадку використання ешелонованої системи захисту з чотирьох бар'єрів захисту ($n = 4$) та довільних стратегій захисту і впливу типу Proba (сканування портів ІС), вираз (8) набуває вигляду

$$I^*(\lambda, \mu)_{НСД} = 1 - \frac{1}{2}\lambda T + \frac{1}{6}\lambda(\lambda + \mu)T^2 - \frac{1}{24}\lambda(\lambda + 2\lambda\mu + \mu)T^3 .$$

Для даного випадку у результаті проведення експерименту отримані наступні залежності рівня захищеності (табл. 2).

Таблиця 2

Рівень захищеності системи безпеки при різних значеннях λ і μ

	μ (інтенсивність впливів за одиницю часу, $T = 1$ с).				
	0	0,25	0,5	0,75	1

λ (інтенсивність захисних дій в одиницю часу, $T = 1$ с).	0	1,000	1,000	1,000	1,000	1,000
	0,25	0,885	0,893	0,900	0,906	0,911
	0,50	0,786	0,801	0,813	0,822	0,828
	0,75	0,701	0,719	0,732	0,742	0,748
	1,0	0,625	0,643	0,656	0,664	0,667

Як видно з табл. 2 при виборі гравцями оптимальних стратегій захисту та впливу відповідно (підсвічено кольором) прогнозований рівень захищеності інформаційного ресурсу при ешелонованій організації системи безпеки дорівнює 0,667, тобто $I\left(\lambda^{opt}, \mu^{opt}\right) = 0.667$. Для решти випадків, при відхиленні гравців від оптимальних стратегій, його величина варіює в діапазоні заданих обмежень. Гравець безпеки може спрогнозувати рівень захищеності та оптимізувати свої ресурси, в тому числі, для тих випадків коли гравець впливу використовує оптимальну стратегію.

З метою оцінювання уразливостей ІС реалізовано програмний засіб «Vulnerability Assessment – 2014 v.1.0» (рис. 5).

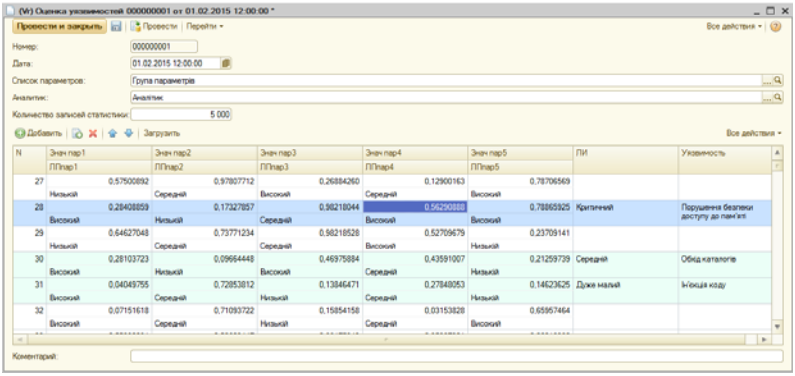

Рис. 5. Фрагмент інтерфейсу засобу «Vulnerability Assessment – 2014 v.1.0»

Цей засіб дозволяє ідентифікувати уразливості інформаційних систем в умовах впливів. Відповідно до зазначених у роботі мережевих та хостових параметрів проведено моделювання поточних станів ІС. На основі сформованих правил даний програмний засіб із заданими показниками точності проводив ідентифікацію шуканих уразливостей (отриманий результат відповідав умовам моделювання).

Таким чином, у результаті проведеного експериментального дослідження підтверджено достовірність розроблених у роботі методів, методик (їх реакції на модельовані дії) і висунутих теоретичних гіпотез.

У **додатках** вміщено акти впровадження результатів дисертаційної роботи та фрагменти кодів програм, що відображають практичну частину дисертаційного дослідження.

ВИСНОВКИ

Результатом виконаної роботи є розв'язання наукової задачі побудови і дослідження методів моделювання впливів на інформаційні системи, оцінювання уразливостей та оптимізації показників систем захисту, що можуть

використовуватися для підвищення ефективності сучасних систем захисту інформації. У процесі виконання дисертаційної роботи отримані такі вагомі результати:

1. Проведено аналіз існуючих методів і засобів оцінки уразливостей інформаційних систем, що дозволило виявити їх недоліки і формалізувати завдання щодо розробки більш ефективного засобу; аналіз сучасних методів моделювання впливів на інформаційні системи дав можливість визначити найбільш ефективний підхід і використати його з метою оптимізації параметрів систем захисту.

2. Запропоновано систему правил щодо моделювання критеріїв оптимальності, які, за рахунок синтезу морфологічним методом сепарабельних адитивних критеріїв та обмежень, дозволяють розв'язувати задачі аналізу, синтезу та оптимізації систем за обраними критеріями та виділеними обмеженнями, а також оцінювати рівень захищеності інформаційних систем з урахуванням дозволених границь гарантованого рівня захисту інформації.

3. Запропоновано диференціально-ігровий метод оптимізації параметрів інформаційних систем, що, за рахунок врахування стратегії гравця впливу, критерію оптимізації ресурсів гравців у процесі оптимізації і енергетичної складової у заданий період часу, дозволяє визначати у реальному часі оптимальну стратегію безпеки інформації в інформаційних системах.

4. Запропоновано метод оптимізації систем захисту інформації, що, за рахунок врахування параметрів системи безпеки (кількість засобів безпеки, тип підсистеми безпеки, сумарний ресурс безпеки та цінність інформації), дозволяє визначати оптимальну поведінку в системі «вплив-безпека»;

5. Удосконалено метод знаходження оптимальної конфігурації інформаційної системи, який, за рахунок використання теоретико-графового моделювання зворотного ходу побудови оптимального вихідного дерева, дозволяє визначати оптимальну архітектуру інформаційної системи в умовах інформаційних впливів.

6. Розроблено методику оцінки уразливостей і впливів на інформаційні системи, які, за рахунок використання логіко-ймовірнісних пар зв'язок «параметри $\rightarrow$ уразливості», дозволяють ідентифікувати уразливості інформаційних систем в умовах впливів.

7. Розроблено алгоритми та програмне забезпечення для реалізації розроблених методів, за допомогою якого проведено експериментальне дослідження, що підтвердило адекватність запропонованих методів з точки зору оптимізації параметрів інформаційних систем в умовах інформаційних впливів.

8. Зазначені результати роботи впроваджено у діяльність в/ч К-1410 (14.06.2012 р.), ТОВ «Конзьюмер Експрес» (17.11.2014 р.), Національного авіаційного університету (10.02.2015 р.), Державного університету інформаційно-комунікаційних технологій (26.06.2012 р.) та Кіровоградського національного технічного університету (17.09.2014 р.), що підтверджено відповідними актами впровадження, які містяться у додатках до дисертаційної роботи.

ПУБЛІКАЦІЇ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Грищук Р.В. Ігрові методи кібератак на інформаційну сферу / Р.В. Грищук, С.Ж. Піскун, В.О. Хорошко, Ю.Є. Хохлачова// Захист інформації. – 2012. – № 1(54). – С. 86-93.

2. Хорошко В.О. Особливості оцінки безпеки інформаційних систем / В.О. Хорошко, Ю.Є. Хохлачова // Захист інформації. – 2012. – № 2(55). – С. 9-15.

3. Гнатюк С.О. Теоретичні основи побудови та функціонування систем управління інцидентами інформаційної безпеки / С.О. Гнатюк, Ю.Є. Хохлачова,

А.О. Охріменко, А.К. Гребенькова // Захист інформації. – 2012. – № 1(54). – С. 121-126.

4. Хохлачова Ю.Є. Моделювання критеріїв оптимальності та обмежень для захисту інформаційних систем / Ю.Є. Хохлачова // Захист інформації. – 2012. – № 4 (57). – С. 106-109.

5. Хохлачова Ю.Є. Сучасні підходи до оцінювання уразливостей і моделювання впливів на інформаційні системи / Ю.Є. Хохлачова, С.С. Чумаченко, О.П. Дуксенко // Вісник Інженерної академії України. – 2014. – № 4. – С. 121-126.

6. Петров А.О. Синтез систем захисту інформації / А.О. Петров, В.Д. Степанов, В.О. Хорошко, Ю.Є. Хохлачова // Інформаційна безпека. – 2012. – № 1(7). – С. 48-54.

7. Хохлачова Ю.Є. Принципи побудови моделей загроз інформаційним системам / Ю.Є. Хохлачова // Сучасний захист інформації. – 2012. – №2. – С. 6-9.

8. Хохлачова Ю.Є. Уразливість інформаційних систем / Ю.Є. Хохлачова // Сучасний захист інформації. – 2012. – № 3. – С. 18-23.

9. Хорошко В.О. Оцінка захищеності інформаційних систем / В.О. Хорошко, Ю.Є. Хохлачова // Сучасний захист інформації. – 2012. – № 4. – С. 50-58.

10. Хохлачова Ю.Є. Політика інформаційної безпеки об'єкта / Ю.Є. Хохлачова // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012. – № 2(24). – С. 23-29.

11. Хорошко В.О. Оцінка захищеності систем зв'язку в інформаційно-комунікаційних системах / В.О. Хорошко, І.С. Іванченко, Ю.Є. Хохлачова // Системи обробки інформації. – 2013. – № 3(110). – С. 112-117.

12. Хорошко В.О. Методика оцінювання рівня безпеки юридичної особи / В.О. Хорошко, В.Д. Козюра, С.Ж. Піскун, Ю.Є. Хохлачова // Інформаційна безпека людини, суспільства, держави. – 2013. – № 1(11). – С 121-126.

13. Іванченко Є.В. Алгоритм прогнозування технічного стану комплексних систем захисту інформації / Є.В. Іванченко, В.О. Хорошко, Ю.Є. Хохлачова // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2013. – № 2(25). – С 9-16.

14. Хорошко В.А. Особенности защиты информации в сетях связи / В.А. Хорошко, Ю.Е. Хохлачева // Вісник східноукраїнського національного університету ім. В. Даля. – 2013. – № 15(204). – С. 219-221.

15. Сірченко Г.А. Алгоритм визначення показників для оцінки надійності систем спеціального призначення / Г.А. Сірченко, В.О. Хорошко, Ю.Є. Хохлачова // Інформаційна безпека. – 2013. – № 1(9). – С. 142-147.

16. Хорошко В.О. Оптимізація параметрів систем захисту в мережах передачі інформації / В.О. Хорошко, Ю.Є. Хохлачова // Інформатика та математичні методи в моделюванні. – 2013. – Т. 3. – № 1. – С. 69-75.

17. Піскун С.Ж. Оцінка безпеки інформаційної сфери / С.Ж. Піскун, В.О. Хорошко, Ю.Є. Хохлачова // Сучасна спеціальна техніка. – 2013. – № 1(32). – С. 93-100.

18. Хорошко В.А. Синтез систем защиты информации, имеющих допусковый разброс параметров / В.А. Хорошко, Ю.Е. Хохлачева, Е.П. Сластенко // Інформаційна безпека. – 2013. – №4 (12). – С. 130-134.

19. Хохлачова Ю.Є. Алгоритм знаходження оптимальної конфігурації мережі / Ю.Є. Хохлачова // Системи обробки інформації. – 2014. – № 2(118). – С. 101-106.

20. Иванченко Е.В. Обработка информационных потоков и составление для них расписаний в системах защиты информации / Е.В. Иванченко, В.А. Хорошко,

Ю.Е. Хохлачева // Інформатика та математичні методи в моделюванні. – 2014. – Т. 4. – № 3. – С. 256-260.

21. Хорошко В.О. Створення захищених інформаційних систем / В.О. Хорошко, Ю.Є. Хохлачова // Захист інформації і безпека інформаційних систем : II наук.-техн. конф. : Тези доп. – Львів, 2013. – С. 154-156.

22. Хорошко В.А. Противодействие несанкционированному получению информации в компьютерных сетях / В.А. Хорошко, Ю.Е. Хохлачева // Безпека інформації в інформаційно-телекомунікаційних системах : XVI наук.-практ. конф. : Тези доп. – Київ, 2013. – С. 87-88.

23. Пискун С.Ж. Проблемы внедрения и эксплуатации систем предотвращения утечки информации / С.Ж. Пискун, Ю.Е. Хохлачева // Інформаційні управляючі системи та технології (ІУСТ-2013) : міжнар. наук.-практ. конф. : Тези доп. – Одеса, 2013. – С. 240-242.

24. Хохлачева Ю.Е. Защита информации в информационных системах / Ю.Е. Хохлачева // Проблеми і перспективи розвитку ІТ-індустрії : VI наук.-практ. конф. : Тези доп. – Харків, 2014. – С. 261-262.

25. Хохлачева Ю.Е. Алгоритм нахождения оптимальной конфигурации сети / Ю.Е. Хохлачева // Современные информационные и электронные технологии : XV науч.-практ. конф. : Тезисы докл. – Одесса, 2014. – С. 167-168.

26. Орехов А.Н. Безопасность вычислительных сетей в управлении воздушным движением / А.Н. Орехов, В.А. Хорошко, Ю.Е. Хохлачева // Захист інформації і безпека інформаційних систем : III міжнар. наук.-практ. конф. : Тези доп. – Львів, 2014. – С. 120-121.

27. Хохлачова Ю.Є. Моделювання впливів на інформаційні системи / Ю.Є. Хохлачова // Актуальні питання забезпечення кібернетичної безпеки та захисту інформації : наук.-практ. конф. : Тези доп. – Київ, 2015. – С. 124-127.

28. Хохлачова Ю.Є. Нові підходи до інформаційної безпеки телекомунікаційних мереж / Ю.Є. Хохлачова // Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано-та мікроелектроніки : IV міжнар. наук.-практ. конф. : Тези доп. – Чернівці, 2014. – С. 136-137.

29. Хохлачова Ю.Є. Вимоги до побудови та критерії захищеності систем захситу до зовнішніх впливів / Ю.Є. Хохлачова // Інформаційна безпека в сучасному суспільстві : I міжнар. наук.-техн.конф. : Тези доп. – Львів, 2014. – С. 54-56.

АНОТАЦІЯ

Хохлачова Ю.Є. Методи оцінювання уразливостей та оптимізації інформаційних систем в умовах інформаційних впливів – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації». – Національний авіаційний університет, Київ, 2015.

Дисертаційна робота присвячена розв'язанню актуальної наукової задачі побудови і дослідження методів моделювання впливів на інформаційні системи, оцінювання уразливостей та оптимізації показників систем захисту.

У роботі запропоновано диференціально-ігровий метод оптимізації параметрів інформаційних систем, що, за рахунок врахування стратегії гравця впливу, критерію оптимізації ресурсів гравців у процесі оптимізації і енергетичної складової у заданий період часу, дозволяє визначати у реальному часі оптимальну стратегію безпеки інформації в інформаційних системах. Отримали подальший розвиток система правил

щодо моделювання критеріїв оптимальності, які, за рахунок синтезу морфологічним методом сепарабельних адитивних критеріїв та обмежень, дозволяють розв'язувати задачі аналізу, синтезу та оптимізації систем за обраними критеріями та виділеними обмеженнями, а також оцінювати рівень захищеності інформаційних систем з урахуванням дозволених границь гарантованого рівня захисту інформації. Крім того, отримав подальший розвиток метод оптимізації систем захисту інформації, що, за рахунок врахування параметрів системи безпеки (кількість засобів безпеки, тип підсистеми безпеки, сумарний ресурс безпеки та цінність інформації), дозволяє визначати оптимальну поведінку в системі «вплив-безпека». Також удосконалено метод знаходження оптимальної конфігурації інформаційної системи, який, за рахунок використання теоретико-графового моделювання зворотного ходу побудови оптимального вихідного дерева, дозволяє визначати оптимальну архітектуру інформаційної системи в умовах інформаційних впливів.

Ключові слова: захист інформації, інформаційна система, уразливість інформаційної системи, оптимізація інформаційної системи, інформаційний вплив, критерій оптимальності, система захисту інформації.

АННОТАЦИЯ

Хохлачева Ю.Е. Методы оценивания уязвимостей и оптимизации информационных систем в условиях информационных воздействий. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – «Системы защиты информации». – Национальный авиационный университет, Киев, 2015.

Диссертация посвящена решению актуальной научной задачи построения и исследования методов моделирования воздействий на информационные системы, оценки уязвимостей и оптимизации показателей систем защиты, которые могут использоваться для повышения эффективности современных систем защиты информации.

В работе предложено дифференциально-игровой метод оптимизации параметров информационных систем, за счет учета стратегии игрока воздействия, критерия оптимизации ресурсов игроков в процессе оптимизации и энергетической составляющей в заданный период времени, позволяет определять в реальном времени оптимальную стратегию безопасности информации в информационных системах. Получили дальнейшее развитие система правил моделирования критериев оптимальности, которые, за счет синтеза морфологическим методом сепарабельных аддитивных критериев и ограничений, позволяют решать задачи анализа, синтеза и оптимизации систем по выбранным критериям и выделенными ограничениями, а также оценивать уровень защищенности информационных систем с учетом разрешенных границ гарантированного уровня защиты информации. Кроме того, получил дальнейшее развитие метод оптимизации систем защиты информации, за счет учета параметров системы безопасности (количество средств безопасности, тип подсистемы безопасности, суммарный ресурс безопасности и ценность информации), позволяет определять оптимальное поведение в системе «влияние-безопасность». Также усовершенствован метод нахождения оптимальной конфигурации информационной системы, который за счет использования теоретико-графового моделирования обратного хода построения оптимального выходного дерева, позволяет определять оптимальную архитектуру информационной системы в условиях информационных воздействий.

Использование предложенных методов при разработке специального программного обеспечения позволило повысить защищенность информационных ресурсов. Разработана компьютерная программа, которая используется для моделирования атакующих действий и оценки уязвимостей в ИКС и в учебном процессе подготовки специалистов в области ИБ. Предложена методика оценки уязвимостей и информационных воздействий, которые, за счет использования логико-вероятностных пар связок «параметры → уязвимости», позволяют идентифицировать уязвимости информационных систем в условиях воздействий. Разработана методика проведения эксперимента, которая позволила исследовать предложенные в работе методы.

Проведение экспериментального исследования подтверждено достоверностью разработанных в работе методов, методик (их реакции на моделируемые действия) и выдвинутых теоретических гипотез.

Ключевые слова: защита информации, информационная система, уязвимость информационной системы, оптимизация информационной системы, инфор-мационное воздействие, критерий оптимальности, система защиты информации.

ABSTRACT

Khokhlachova Yu.Ye. Vulnerability assessment methods and methods of information systems optimization in the context of information impacts. – Manuscript

The dissertation is intended to proceed with PhD degree on specialty 05.13.21 – «Information security systems». – National Aviation University, Kyiv, 2014.

Dissertation work is devoted to actual scientific problem to develop and study methods of modeling influences on information systems, vulnerability assessment and security systems attributes optimization.

In work presented the differential-game method for information systems parameter optimization, by taking into account influence player strategies, resource optimization criteria players during optimization and energy component in a given period of time, allows to determine in real time the optimal strategy for information security in information systems. Was further developed system of rules for modeling criteria of the optimality, which, through morphological synthesis method, separable additive criteria and limits, can solve the problem of analysis, synthesis and optimization for systems by selected criteria and highlighted limits, and evaluate the level of information systems security based on permitted boundaries guaranteed data security level. In addition, further developed the optimization information security method, by taking into account security settings (security tools number, security subsystem type, overall resource security and information value) allows to determine the optimal behavior in "influence-security" system. Also improved method of finding the optimal configuration for information system, which, through the use of graph-theoretic modeling reverse construct the optimal source tree allows to define the optimum information systems architecture in the information influences conditions.

Index terms: information security, information system, information system vulnerability, information system optimization, information security system.