**СХІДНОЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ**

**ЕКОНОМІКИ І МЕНЕДЖМЕНТУ**

**КОПИТКО СЕРГІЙ БОГДАНОВИЧ**

УДК 330.47 : 004.056 : 519.86

**Економіко-математичне моделювання управління ефективністю систем захисту комп’ютерної інформації**

08.00.11 – математичні методи, моделі

та інформаційні технології в економіці

**АВТОРЕФЕРАТ**

дисертації на здобуття наукового ступеня

кандидата економічних наук

Черкаси – 2014

Дисертацією є рукопис.

Робота виконана у Львівському інституті банківської справи Університету банківської справи Національного банку України.

**Науковий керівник:** доктор технічних наук, професор

**Білий Леонід Адамович,**

Львівський інститут банківської справи Університету банківської справи Національного

банку України,

професор кафедри економічної кібернетики.

**Офіційні опоненти:** доктор економічних наук, професор

**Іванов Микола Миколайович,**

Класичний приватний університет (м. Запоріжжя),

завідувач кафедри менеджменту організацій та зовнішньоекономічної діяльності;

кандидат економічних наук, доцент

**Кирилишен Ярослав Вікторович,**

Донецький національний університет Міністерства освіти і науки України,

доцент кафедри інформаційних систем управління.

Захист дисертації відбудеться “29” травня 2014 р. о 14.00 годині на засіданні спеціалізованої вченої ради К 73.138.02 при Східноєвропейському університеті економіки і менеджменту за адресою: 18036, м. Черкаси, вул. Нечуя-Левицького, 16.

З дисертацією можна ознайомитись у бібліотеці Східноєвропейського університету економіки і менеджменту за адресою: 18036, м. Черкаси, вул. Нечуя-Левицького, 16.

Автореферат розісланий “\_\_\_\_” квітня 2014 р.

|  |  |  |
| --- | --- | --- |
| Вчений секретар  спеціалізованої вченої ради |  | С. О. Зульфугарова |

**ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ**

**Актуальність теми.** Розвиток та впровадження у різні сфери діяльності людини інформаційних технологій (ІТ) зумовлює зростання кількості їх засто­сувань із злочинною метою. Поширеним способом злочинного використання ІТ є несанкціонований доступ до інформації, що зберігається у пам’яті ком­п’ютерних систем, з метою її отримання, модифікації чи знищення. Згідно із сучасними прогнозами, активність хакерів характеризується експоненційним рос­том кількості атак у мережі Інтернет із значним різновидом сигнатур, необмеженістю числа вірусів. Тому захист інформаційних ресурсів має бути важливим завданням державної політики інформатизації.

Фундаментальні аспекти математичного моделювання інформаційної без­пеки (ІБ) в умовах ринкової економіки досліджували такі відомі зарубіжні вчені, як Андерсон Дж., Вернам Г., Віженер Б., Гаррісон М., Гордон Л., Діффі В., Кобліц Н., Кохен Ф., Лінде Р., Лоеб М., Мессі Д., Райвест Р., Терн Р., Хеллман М., Хоффман Л., Шамір А., Шеннон К., російські фахівці Анін Б., Деднєв М., Завгородній В., Зегжда Д., Касперський Є., Лукацький О., Петренко С., Сичов Ю., Табаков А., Щеглов Ю. та інші.

З набуттям Україною незалежності значна увага українських фахівців зо­середжувалась на забезпеченні захисту інформаційних ресурсів. Різні аспекти методології ІБ в умовах використання комп’ютерних систем (КС) досліджували такі українські вчені, як Алішов Н., Біленчук П., Вербіцький О., Вітлінський В., Гарбарчук В., Головань С., Грищук Р., Гундар К., Домарєв В., Дудикевич В., Ємець В., Задірака В., Іванов М., Кирилишен Я., Корченко О., Левченко Є., Палагін О., Петров  О., Хорошко В., Шорошев В. та інші. Ці дослідження охоп­люють широкий спектр проблем ІБ – від впровадження новітніх міжнародних стандартів до оцінювання ефективності засобів захисту та обґрунтування мето­дик проектування систем забезпечення ІБ організацій.

Незважаючи на значний обсяг напрацювань з проблематики ІБ, ряд аспек­тів методології побудови ефективної системи управління ІБ (СУІБ) організації на даний момент ще не мають задовільного вирішення. Причини криються як у складності самого об’єкту дослідження, так і у розвитку ІТ та падінням моралі у суспільстві, що продукує появу нових інформаційних загроз. Убезпечення інформаційних ресурсів організації від мінливого агресивного середовища вимагає відповідного розвитку СУІБ. Таке завдання покликаний вирішувати порівняно новий напрям у моделюванні ІБ, що отримав назву “менеджмент інформаційної безпеки”.

Отже, актуальність теми наукового дослідження визначається потребою розробки методології конструювання адекватних економіко-математичних мо­делей (ЕММ) оптимізації управління ефективністю систем захисту комп’ютер­ної інформації з урахуванням основних чинників невизначеності агресивного щодо захищених даних середовища.

**Зв’язок роботи з науковими програмами, планами, темами.** Досліджен­ня виконувалося у контексті науково-дослідних робіт Університету банківської справи НБУ за темою «Формування системи управлінської інформації в бан­ках» (номер державної реєстрації 0110U000030, довідка № 01-015/1025 від 26.11.2013). Особисто автором розроблений спосіб формалізації екстремальної проблеми управління ефективністю захисту комп’ютерної інформації у формі задачі динамічного програмування, комплекс ЕММ її реалізації та методичні положення щодо застосування запропонованого комплексу ЕММ на практиці.

**Мета та завдання дослідження**.Метою дисертаційної роботи є розробка теоретичних основ і науково-методичних засад та інструментарію моделювання процесу управління ефективністю систем захисту інформації (СЗІ).

Відповідно до сформульованої мети були поставлені такі **завдання:**

- проаналізувати вимоги до захисту інформації, що зберігається у комп’ю­терних системах, сучасні стандарти ІБ та ідентифікувати особливості СЗІ як об’єкта оптимізації;

- узагальнити існуючі підходи до математичного моделювання процесів побудови і функціонування систем захисту інформаційних ресурсів;

- розробити концепцію моделювання управління ефективністю СЗІ за умов мінливого середовища;

- удосконалити загальну динамічну модель оптимізації управління ефек­тивністю системи захисту комп’ютерної інформації у формі задачі динамічного програмування і дослідити умови існування її розв’язку;

- обґрунтувати вид функції корисності СЗІ для визначення її стаціонарних станів;

- запропонувати альтернативний підхід до класифікації інформаційних загроз комп’ютерній інформації;

- розвинути методи формування досьє типових інформаційних загроз як форми формалізованого подання моделі загроз СЗІ;

- розробити методичні положення щодо застосування на практиці запропо­нованого комплексу ЕММ оптимізації управління ефективністю СЗІ та здійсни­ти його апробацію на масиві описів реальних хакерських атак.

*Об’єкт дослідження* – процеси управління ефективністю систем захисту комп’ютерної інформації.

*Предмет дослідження* – комплекс моделей і методів управління ефективністю СЗІ за умов мінливого агресивного середовища.

*Методи дослідження.*Теоретичною і методологічною основою дисерта­ційної роботи стали фундаментальні положення зарубіжної та вітчизняної нау­ки у галузі економічної теорії, економіко-математичного моделювання, інфор­маційних технологій, інформатизації економіки України. У процесі досліджен­ня для досягнення визначеної мети застосовувався комплекс загальнонаукових методів: аналізу – для виявлення тенденцій і масштабу загроз інформації (п. 1.1); класифікації – у процесі систематизації описів інформаційних загроз акти­вам економічних агентів (п. 1.1);теоретичного узагальнення – при аналізі досві­ду і методів математичного моделювання ефективності СЗІ (п. 1.2); системного аналізу – з метою структуризації СЗІ (п. 1.3); теорії прийняття рішень – для роз­робки процедур пошуку розв’язків багатокритеріальних задач оптимізації уп­равління ефективністю СЗІ (п. 3.1, 3.3); динамічне програмування – для форма­лізації екстремальної проблеми управління ефективністю СЗІ та побудови опти­мальної стратегії її розвитку (п. 1.3, 2.1); теорія корисності – з метою обґрунтування способу оцінювання ефекту СЗІ (п. 1.3, 2.2); теорія аналогії – для обґрунтування вибору функції корисності СЗІ (п. 2.2); агентно-орієнтоване моделювання – з метою формалізації процесу захисту інформації в КС (п. 2.1); метод досьє – для подання моделі загроз комп’ютерній інформації (п. 2.3, 3.2); методи інтелектуального аналізу даних – з метою виділення типових інформаційних загроз (п. 2.3, 3.2) та для ідентифікації прихованих залежностей між обставинами здійснення хакерських атак (п. 3.2); методи теорії еластичності – з метою обґрунтування управлінських рішень щодо модифікації СЗІ організації (п. 1.3, 2.1, 3.3); сучасні ІТ – для автоматизації процедур обґрунтування оптималь­них рішень щодо інвестування розвитку СЗІ на підставі розробленого комплексу ЕММ (п. 3.2, 3.3).

**Наукова новизна одержаних результатів** полягає в такому:

*вперше:*

* розроблено концепцію моделювання управління ефективністю СЗІ на основі поєднання методу динамічного програмування і теорії корисності, яка реалізується комплексом ЕММ оптимізації інвестування розвитку СЗІ за крите­рієм мінімізації на проміжку управління вірогідних збитків від несанкціонова­ного доступу до інформаційних ресурсів організації, що уможливлює підви­щення ефективності діяльності служби ІБ за умов мінливого агресивного щодо інформаційних ресурсів середовища;

*удосконалено:*

* динамічну модель оптимізації управління ефективністю системи захисту комп’ютерної інформації у формі задачі динамічного програмування, яка, на відміну від відомих, включає рекурентні співвідношення Беллмана, орієнтовані на застосування в оптимізаційних моделях з двома критеріями, що дає змогу поетапної побудови оптимальної траєкторії розвитку СЗІ на заданому інтервалі управління;
* вид функції корисності системи захисту комп’ютерної інформації, яка, на відміну від базової моделі пріоритетного споживання, враховує контекст проблеми управління захистом інформації і тим самим уможливлює застосу­вання її для визначення стаціонарного стану СЗІ та обґрунтовує компоненти оп­тимального управлінського рішення щодо модифікації системи захисту даних;
* класифікацію інформаційних загроз комп’ютерній інформації, яка, на відміну від існуючих варіантів, використовує самоорганізуючі карти Кохонена, що дає змогу формувати класифікаційні схеми за більшої кількості ознак та підвищує їхню об’єктивність;

*одержали подальший розвиток:*

* методи формування досьє за рахунок використання правил “if…, then…” технології data mining, які, на відміну від існуючих, уможливлюють ідентифіка­цію та введення у модель загроз СЗІ прихованих залежностей між обставинами здійснення хакерських атак на КС з метою покращення якості моделі загроз.

**Практичне значення отриманих результатів**. Запропоновані в роботі моделі і методи доведені до рівня прикладних положень і рекомендацій та мо­жуть бути використані в організаціях для дослідження і аналізу стану захище­ності їх інформаційних ресурсів; формування стратегії розвитку СЗІ; оптиміза­ції планів інвестування розвитку СУІБ організацій; розширення функціональ­них можливостей інформаційної системи організації через впровадження модуля підтримки прийняття рішень щодо безпеки інформаційних ресурсів.

Основні результати дослідження були впроваджені в практичну діяльність ТзОВ “ЕДВАНТІС” (довідка № 45 від 18.10.2013). Теоретичні положення, ме­тоди та моделі, що визначають наукову новизну дисертації, використовуються в навчальному процесі при підготовці фахівців за економічними спеціальностя­ми у Львівському інституті банківської справи Університету банківської справи Національного банку України (довідка № 01015/1033 від 02.12.2013).

**Особистий внесок здобувача.** Дисертаційна робота є одноосібно викона­ною науковою працею, в якій викладено авторський підхід до моделювання уп­равління ефективністю СЗІ в організаціях. З публікацій, що написані у співав­торстві, використано лише ті результати, які отримані автором особисто.

**Апробація результатів дисертації.** Положення і результати дослідження доповідалися та обговорювалися на: ІІ Міжнародній науково-практичній кон­ференції ”Міжнародна банківська конкуренція: теорія і практика” (м. Суми, 2007 р.), ІІІ Всеукраїнській науково-практичній конференції аспірантів та моло­дих вчених “Розвиток фінансово-кредитної системи України: здобутки, пробле­ми, перспективи” (м. Львів, 2007 р.), Міжнародній науковій конференції “Дні науки” (м. Запоріжжя, 2007 р.), ІІІ Міжнародній науково-практичній конферен­ції аспірантів і студентів “Волинь очима молодих науковців: минуле, сучасне, майбутнє” (м. Луцьк, 2009 р.), VIII–Х та ХІІ Міжнародних наукових семінарах ,,Сучасні проблеми інформатики в управлінні, економіці, освіті та екології” (м. Київ – м. Шацьк, оз. Світязь, 2009–2011, 2013 рр.), V Міжнародній школі-семі­нарі ”Теорія прийняття рішень” (м. Ужгород, 2010 р,), Міжнародному науково-методичному форумі-конференції молодих економістів-кібернетиків ”Моде­лювання економіки: проблеми, тенденції, досвід” (м. Львів, 2010 р.), III Міжна­родній науково-практичній конференції ”Системний аналіз. Інформатика. Уп­равління” (м. Запоріжжя, 2012 р.), І Міжнародній науково-технічній конферен­ції ”Захист інформації і безпека інформаційних систем” (м. Львів, 2012 р.), Між­народному молодіжному форумі “Радіоелектроніка і молодь у ХХІ столітті”, 9-й тематичній конференції “Управління знаннями і конкурентна розвідка” (м. Харків, 2013 р.).

**Публікації.** Основні наукові положення, висновки і результати дослід­ження опубліковані у 17 наукових працях, із них 9 – статті у наукових фахових виданнях, 1 – колективна монографія, 7 – матеріали наукових конференцій, 1 – тези доповідей. Загальний обсяг публікацій становить 4,12 умовн. друк. арк.

**Структура** **та обсяг дисертації.** Дисертація складається зі вступу, трьох роз­ділів, висновків, списку використаних джерел, 14 додатків. Основний зміст роботи становить 181 сторінку. Дисертація містить 28 таблиць, 14 рисунків. Список використаних джерел містить 289 найменувань.

**ОСНОВНИЙ ЗМІСТ РОБОТИ**

У розділі 1 **“Методологічні засади управління ефективністю систем захисту комп’ютерної інформації”** на підставі аналізу праць з проблематики ІБ визначено особливості системи захисту комп’ютерної інформації як об’єкта оптимізації, простежено тенденції розвитку вимог ІБ у часі та їх стандартиза­цію, охарактеризовано економічні аспекти побудови систем захисту даних, відзначено недоліки сучасної методології управління ефективністю функціонуван­ня таких систем із застосуванням математичних моделей та здійснено концеп­туалізацію проблеми управління ефективністю СЗІ.

Враховуючи складність процесу управління ефективністю СЗІ в сучасних умовах, мінливість агресивного середовища, недосконалість інструментарію, спрямованого на поліпшення функціонування захисних компонентів комп’ю­терних систем (КС), у розділі обґрунтовано доцільність використання для вирішення завдань дослідження теорії динамічного програмування у поєднанні з методами теорії корисності.

Базуючись на рекомендаціях теорії систем і системного аналізу та методо­логії дослідження операцій в економіці, СЗІ **** розглядається на проміжку часу  як агентна і складна система, формалізований опис якої задається кортежем із семи компонентів:

 (1)

де для періоду :  – компонент, що характеризує множину загроз ком­п’ютерній інформації;  – інформація щодо втрат від несанкціонованого доступу до даних у комп’ютерній системі;  – параметри проектованої чи існуючої СЗІ;  – критерії ефективності СЗІ;  – підсистема управління ефективністю СЗІ;  – характеристики комп’ютерної інформації, яка підлягає захисту від несанкціонованого доступу;  – сукупність агентів, що взаємодіють з СЗІ;  – проміжок управління, протягом якого відстежується ефективність системи захисту даних.

У роботі пропонується оцінювати ефективність системи  виду (1) на підставі деякої функції корисності  Її значення характеризує якість систе­ми захисту у період , якщо  знаходиться в стані  Здійснено інтерпре­тацію аксіом функції корисності  у контексті ефективності СЗІ.

Принцип формування оптимальної стратегії розвитку СЗІ відображено на рис. 1. Тут ламана лінія зображує оптимальну стратегію, овали є множинами станів системи для відповідних періодів, точками позначено окремі стани, а криві – це гіперповерхні максимальної ефективності захисту інформації.

Розглядаємо ще простір  можливих управлінь ефективністю системи за­хисту  на часовому проміжку . Під *управлінням*  розуміємо дію чи сукупність дій адміністратора системи захисту , спрямованих на її модерні­зацію. Аналогічно, як і у випадку станів, припускаємо можливість застосувань управлінь (дій) за дискретною схемою у моменти (періоди) часу , а також скінченність множин  можливих управлінь у періоди часового проміжку . Очевидними вимогами до -го управління  є залежність його від стану системи захисту , що формально можна ідентифікувати як , та ототожнення його з вектором  значень керуючих параметрів , де через  позначено -вимірний евклідовий простір.



Рис. 1. Принцип формування оптимальної стратегії розвитку СЗІ

Застосовуючи управління  до системи , можна змінити її стан і тим самим покращити або погіршити ефективність захисту даних. Оскільки уп­равління можна застосувати у дискретні моменти часу , то нові стани систе­ми захисту будуть належати до наступного періоду. З метою оцінювання якості управлінь  пропонується така загальна постановка завдання щодо оп­тимізації управління ефективністю системи захисту комп’ютерної інформації: для заданої системи  захисту інформації зі структурою (1) знайти таке управління  , для якого

 (2)

за умов

; (3)

, (4)

де – початковий (у період ) стан системи захисту, який вважається відомим;  – вибраний критерій оцінювання якості управлінь; *extr* – тип оптимізації (мінімум чи максимум), який залежний від конкретного вибору 

Оптимізаційна модель (2) – (4) математично описує загальну постановку проблеми управління ефективністю системи захисту комп’ютерної інформації. З метою застосування метамоделі (2) – (4) для обґрунтування рішень щодо модернізації захисних елементів КС було здійснено конкретизацію формалізованого опису складових (1) та подано їх такими кортежами елементів:

 (5)

де для :  – відповідно множина загроз комп’ютерній інформа­ції, кількість типових загроз, виділених на множині , та досьє типових заг­роз;  – сумарні обсяги збитків у вартісному вимірі від несанкціонованого доступу до інформації ; компонент  вектора  позначає збитки від -ї типової інформаційної загрози;  – вектор часток роз­поділу збитків у розрізі типових загроз;  – евклідів простір;  – відпо­відно перелік та кількість компонентів, з яких складається система захисту ком­п’ютерної інформації;  – вартість системи захисту як сума вартостей  її компонентів; координата  вектора  є ціною реалізації захисту від -ї типової інформаційної загрози;  – індекс зростання обсягів фінансування системи захисту;  – критерій якості проектованої системи захисту комп’ютерної інформації;  – вектори часток розподілу збитків від несанкціонованого доступу до інформації на відповідно мінімальному і максимальному рівнях у розрізі типових загроз;  – деякий параметр, який задає ступінь наближення збитків до мінімального рівня;  – функція корисності, яка використовується для оцінювання ефективності системи захисту;  – вектор очікуваних змін цін реалізації захисту інформації типових загроз, причому  задає очікуваний приріст (у відносних одиницях) вартості протидії системи  атакам -ї типової загрози;  – квадратна матриця перехресних затратних еластичностей збитків від типових загроз;  позначають відповідно зловмисників, проектувальників та адміністраторів системи захисту інформації.

Розділ 2 **“Комплекс економіко-математичних моделей управління ефективністю системи захисту комп’ютерної інформації”** присвячено розробці математичних моделей для обґрунтування оптимальних управлінських рішень щодо розвитку СЗІ за умов мінливого агресивного середовища.

На підставі (5) уточнений варіант загальної постановки задачі оптимізації управління ефективністю захисту комп’ютерної інформації може бути описа­ний у такий спосіб: для заданої системи  захисту інформації вигляду (1), (5) і вибраного критерію оптимізації  знайти таке управління  для  з компонентами

, (6)

для якого

 (7)

за умов

; (8)

; (9)

; (10)

; (11)

* –* стаціонарний стан системи  у період ,(12)

де для :  – обсяг фінансування процесу модифікації системи ;  – множина компонентів  захисту інформації, які убезпечують від атак -ї типової інформаційної загрози;  – приріст вартості компоненти ;  – оптимальний за критерієм  вектор зміни цін реаліза­ції захисту даних від атак -ї типової інформаційної загрози;  – визначена на підставі  оптимальна матриця перехресних затратних еластичностей збитків від несанкціонованого доступу до комп’ютерної інформації, яка переводить систему  із стаціонарного стану ** у стан *.*

Розв’язок задачі динамічного програмування (7), (6), (8) – (12) може бути віднайдений за допомогою уточненого варіанту рекурентного рівняння Беллмана, а саме для **** маємо

**** (13)

У (13) додатково використано такі позначення:  – допоміжний критерій для визначення стаціонарного стану системи захисту ;  – оптимальна згідно з критерієм  матриця цінових перехресних еластичностей втрат від ти­пових загроз комп’ютерній інформації у період ;  – безпосередній ефект від управлінського рішення, досягнутий за період ;  – оптимальне значення ефекту, що досягається після  періодів;  – початкова умова, яка означає вимогу стабілізації ефективності системи  захисту комп’ютерної ін­формації на деякому достатньому рівні за межами прогнозного проміжку часу . Коефіцієнти  матриці  визначають оптимальну “поведінку” (реакцію) системи  у період  за умови зміни цін реалізації захисту від ти­пових інформаційних загроз із досьє  у цей період згідно  Ре­курентні співвідношення (13) дають змогу побудувати оптимальну стратегію розвитку системи  згідно з принципами, відображеними на рис. 1.

Необхідні умови застосування співвідношень (13) для пошуку розв’язку оптимізаційної моделі (7), (6), (8) – (12) формулюються як твердження 1.

**Твердження 1.** Для того, щоб управління  з ком­понентами вигляду (6), отриманими за допомогою багатокрокової двокритері­альної рекурентної процедури (13), визначало на проміжку  оптималь­ну згідно з вибраним критерієм  траєкторію розвитку системи  захисту інформації вигляду (1), (5) і було розв’язком задачі динамічного програмування (7) – (12), необхідно, щоб у контексті критерію  та вибраної функції корисності  існувала оптимальна матриця  цінових перехресних еластичностей втрат від типових атак на комп’ютерну інформацію для усіх періодів 

Подальша конкретизація специфікацій задачі динамічного програмування (7) – (12) пов’язана з урахуванням як мінливості зовнішнього агресивного сере­довища, так і компонентів самої системи захисту. Як наслідок було розглянуто такі три комбінації: 1) для усіх  кількість і множина типових загроз є однаковими; 2) для усіх  кількість типових загроз є однакова, проте параметри опису окремих з них у досьє можуть різнитися у різні періоди; 3) кількість типових загроз та їхній опис у досьє для різних періодів є різними.

Дослідження залежності специфікацій оптимізаційної моделі (7) – (12) від мінливості агресивного до комп’ютерної інформації зовнішнього середовища було здійснено на засадах агентно-орієнтованого моделювання.

Суттєвою вимогою обґрунтованого способу формалізації екстремальної проблеми управління ефективністю захисту інформації є застосування функцій корисності для оцінювання рівня захищеності даних. З цією метою потрібно вміти ідентифікувати стаціонарні стани системи  для періодів . З огляду на відсутність на сьогодні зразків функцій корисності СЗІ було обрано шлях їх конструювання через адаптацію існуючих функцій корисності подібних проце­сів. Вибір прототипу функції корисності  системи  здійснювався методом аналогії через встановлення подібності процесу ІБ з деяким іншим економічним процесом, для якого існують апробовані практикою зразки функцій корисності. З цією метою прийнято робоче припущення:

**Гіпотеза 1.** Процес кількісного оцінювання ефективності системи захисту комп’ютерної інформації аналогічний процесу оцінювання поведінки спожи­вача на ринку благ у середовищі ринкової економіки.

Справедливість такого припущення обґрунтовувалась за допомогою систе­ми Клінга. У результаті детального аналізу специфіки двох зазначених у гіпотезі 1 процесів було виділено по 11 ключових характеристик. Оскільки для 10 з 11 ключових ознак процесу споживання благ у ринковій економіці визначено їхні аналоги для моделі оцінювання ефективності СЗІ, то зроблено висновок щодо як структурної, так і змістовної подібності базових понять неокласичної моделі споживання з одного боку та моделі оцінювання ефективності СЗІ – з іншого. Цей факт, власне, і підтверджує справедливість сформульованої вище гіпотези 1. Тому вибір прототипу функції  для системи  здійснювався на підставі аналізу множини функцій корисності споживачів благ у ринковій економіці. З урахуванням додаткових вимог (6) щодо структури функції  СЗІ прийнято рішення про вибір відомої AIDS-функції корисності як прототипу для .

У результаті було обґрунтовано доцільність використання у якості моделі визначення стаціонарного стану системи  такої оптимізаційної задачі: для заданого вектора очікуваних змін цін реалізації захисту від типових інфор­маційних загроз із досьє  знайти вектор  та симетричну матрицю  цінових перехресних еластичностей втрат від інформаційних атак у період , щоб

, (14)  
за умови

 (15)

та обмежень

 (16)

Змістовно критерій (14) асоціюється із сумарним приростом збитків від не­санкціонованого доступу до комп’ютерної інформації при заданому векторі очікуваних змін цін реалізації захисту даних від типових загроз, які формують досьє . При цьому припускається, що кожна атака на комп’ютерну інфор­мацію, яка здійснена у період , може бути зарахована до однієї з  груп і опосередковано представлена відповідною типовою інформаційною загрозою із досьє . У (14)  є деякими так званими “прихованими” параметрами, які стабілізують зону існування розв’язку задачі (14) – (16).

У роботі розглянуто специфіку досьє  як неодмінної складової СЗІ та обґрунтовано модель його формування. Поширивши традиційне трактування цього поняття на проблематику ІБ, під досьє  розуміється сукупність формалізованих описів типових інформаційних загроз, виділених на вхідній множині  хакерських атак. Очевидно, процес побудови досьє  може суттєво залежати від певних концептуальних припущень щодо інформаційних описів його елементів. Було враховано такі припущення: 1) уточнення поняття “типова інформаційна загроза”; 2) опис хакерських атак і типових інформацій­них загроз різними множинами ознак.

Щодо першого аспекту, то доцільно вибрати представника групи (підмножини) подібних, тобто близьких за характеристиками, інформаційних загроз із вхідної множини  за типову інформаційну загрозу. Таке уточнення ототожнює з точки зору системи захисту групу подібних хакерських атак з одним представ­ником, а також уможливлює розпізнання достатньо різних загроз. Робоче при­пущення щодо другого аспекту може бути сформульоване як гіпотеза 2.

**Гіпотеза 2.** У кожен період часу  індивідуальна інформаційна загроза  із вхідної множини  загроз та типова інформаційна загроза  із досьє  формалізовано описуються однаковими множинами ознак.

З урахуванням зазначених припущень процес побудови досьє  систе­ми захисту може бути адекватно поданий як класифікація елементів мно­жини . З метою покращення якості результатів класифікації множини заг­роз запропоновано архітектуру нейромережі Кохонена.

Завершує процес конкретизації загальної задачі динамічного програму­вання (7) – (12) розробка ЕММ управління ефективністю СЗІ. Вибравши за ос­новний критерій  оптимізації очікувані сумарні обсяги збитків від хакерських атак на КС та конкретизувавши спосіб їхнього розрахунку, адекватне задачі (7) – (12) практичне завдання обґрунтування оптимальної стратегії розвитку СЗІ органі­зації таке: для заданої системи  захисту інформації виду (1), (4) знайти таке управління  на проміжку  з компонентами виду (6), для якого досягається мінімум функціоналу

 (17)  
за умов (12) та

 ; (18)

 ; (19)

 ; (20)

 , (21)

де – вірогідні сумарні обсяги втрат у вартісному виразі від несанкціо­нованого доступу до комп’ютерної інформації на проміжку управління  згідно з управлінським рішенням ;  – очікувані обсяги збитків від хакерських атак -ї типової інформаційної загрози із досьє  у період  за умови, що здійснена на початку цього періоду модифікація компонентів системи  відповідає заданому вектору ;  – очікувана кількість спроб несанкціонованого доступу до захищених даних у період , які за своїми характеристиками можуть бути віднесені до -ї типової загрози із .

Розв’язок задачі динамічного програмування (17) – (21) з обмеженнями (6), (11) можна отримати за допомогою рекурентних співвідношень (13), які (без урахування початкової умови) матимуть такий вигляд ()

 (22)

Саме рекурентні рівняння (22) забезпечують у контексті основного критерію  у формі (17) формування оптимального управлінського рішення з компонентами (6), які дають змогу поетапно побудувати оптимальну стратегію розвитку системи захисту  на проміжку управління  згідно з рис. 1.

У розділі 3 **“Реалізація комплексу економіко-математичних моделей управління ефективністю системи захисту комп’ютерної інформації”** розглянуто методологічні аспекти застосування задачі динамічного програ­мування (17) – (21) з обмеженнями (6), (11) та рівнянь Беллмана (22) для оптимі­зації ефективності СЗІ за умов мінливості агресивного середовища.

Обґрунтування методичних положень процесу управління ефективністю СЗІ за допомогою моделей розділу 2 роботи було предметом розгляду у першому параграфі даного розділу. Для цього окремі моделі були поєднані у цілісний комплекс ЕММ оптимізації управління ефективністю захисту комп’ютерної інформації (рис. 2), за допомогою якого розроблені положення для обґрунтування оптимальної стратегії розвитку СЗІ на проміжку  за критерієм мінімізації вірогідних обсягів збитків від несанкціонованого доступу до інфор­маційних ресурсів організації. Дані методичні положення задають алгоритм застосування окремих моделей комплексу залежно від вимог адміністратора системи  і характеристик мінливого агресивного середовища. У процесі розробки методичних положень здійснено подальшу конкретизацію рекурент­них співвідношень (22) з метою уточнення процедури побудови умовно-оптимального управління  як пошуку оптимального розподілу коштів на модернізацію захисних елементів СЗІ організації у період .

Моделі перших двох підсистем комплексу ЕММ апробовано на прикладі побудови досьє типових інформаційних загроз для деякої сукупності реальних атак на КC. Кожна спроба несанкціонованого доступу до інформації характеризувалась вектором ознак , який представлявся записом табличної БД MS Excel (табл. 1).

Для автоматизації процесу класифікації загроз із сформованої табличної БД використали додаток Kohonen Map 1.0 нейромережевого пакета програм Neural Package, задавши розмірність сітки Кохонена параметром . Тому програма ідентифікувала 4 кластери елементів множини  та розра­хувала значення ознак ядер кластерів у просторі . Значення характеристик цих ядер і формують початковий вміст досьє  типових інформаційних загроз (табл. 2).

­­

­





­

­

­

­­­



­











Рис. 2. Структура комплексу ЕММ для оптимізації управління ефективністю захисту комп’ютерної інформації

*Таблиця 1*

**Характеристика табличної БД інформаційних загроз модельного прикладу**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Назва характеристики | Всьо­го | З них описують | | | | |
| спрямова­ність загрози | систе­му за­хисту | обста­вини атаки | обставини виявлен­ня атаки | оцінку наслідків загрози |
| Кількість ознак опису атаки | 21 | 5 | 7 | 4 | 3 | 2 |
| Кількість якісних ознак | 14 | 5 | 7 | 1 | 1 | 0 |
| Кількість записів у БД | 15 | - | - | - | - | - |

Сформоване досьє типових загроз було уточнене з метою врахування прихованих і нетривіальних залежностей між обставинами здійснення хакерської атаки. На підставі частоти появи чинника ІБ у правилах можна судити про його важливість для врахування під час розробки СЗІ.

*Таблиця 2*

**Фрагмент досьє типових загроз інформації модельного прикладу**

|  |  |  |
| --- | --- | --- |
| Номер типової загрози | Номер кластера загроз | Опис характеристик типової інформаційної загрози |
| 1 | А1 | Спрямована проти невеликої компанії, об’єктом загрози є сервер (Web-сервер або сервер компанії), у більшості випадків мета атаки неясна, операційна система – або ОС Windows, або Macintosh, або Solaris. Сис­тема має компоненти захисту, проте програмне забезпечення Web-сер­вера відсутнє; у половині атакованих систем відсутній брандмауер та утиліти захисту, відсутній мережний компонент; дві з трьох атакованих систем мають 2-рівневу систему захисту. Атака у третині випадків про­водиться увечері і у третини випадків також вдень; час атаки близько 105 хвилин, час її виявлення – більше 9 год. Частота атак цього типу за період складає 0,881. Вірогідні втрати від такої загрози усереднено ся­гають $44,2 млн. Атака у двох випадках з трьох виконується за один етап. |

Апробації задачі динамічного програмування (17) – (21) виконувались на реальних даних за умови стабільності досьє типових загроз. З цією метою було сконструйовано віртуальну типову умовно-реальну систему, яка узагальнює структури захисних компонентів КС, що були атаковані загрозами із БД табл. 1. Базові показники, які використані для формування вхідних параметрів комплексу ЕММ, відображені у табл. 3.

*Таблиця 3*

**Використання захисних компонентів системи  для убезпечення від типових інформаційних загроз**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Компоненти захисту | Номер типової інформаційної загрози | | | |
|  |  |  |  |
| Операційна система, | + | + | + | + |
| Програмне забезпечення Web-сервера, | - | + | - | + |
| Брандмауер, | + | + | + | + |
| Утиліти захисту, | + | + | - | - |
| Мережевий компонент, | + | + | + | - |

“+” – використовується; “-” – не використовується

Використовуючи інформацію табл. 3 та оцінки характеристик типових заг­роз із сформованого досьє, для конкретизації моделі (14) – (16) та розрахунку її параметрів визначено вірогідний стаціонарний стан системи захисту  у нас­тупний період  за додаткового припущення щодо пропорційності зміни цін за­хисту від типових інформаційних загроз. У результаті отримано оптимальну матрицю  цінових перехресних еластичностей збитків від типових інфор­маційних загроз, за допомогою яких здійснено оцінку впливу одновідсоткової зміни ціни захисту від типової загрози на вірогідні зміни обсягів втрат від атак, що тяжіють до відповідної типової інформаційної загрози (рис. 3). На лівій вертикальній осі відкладено величину 1 %-ї зміни ціни реалізації захисту від типової загрози, а права вертикальна вісь відображає діапазон зміни .

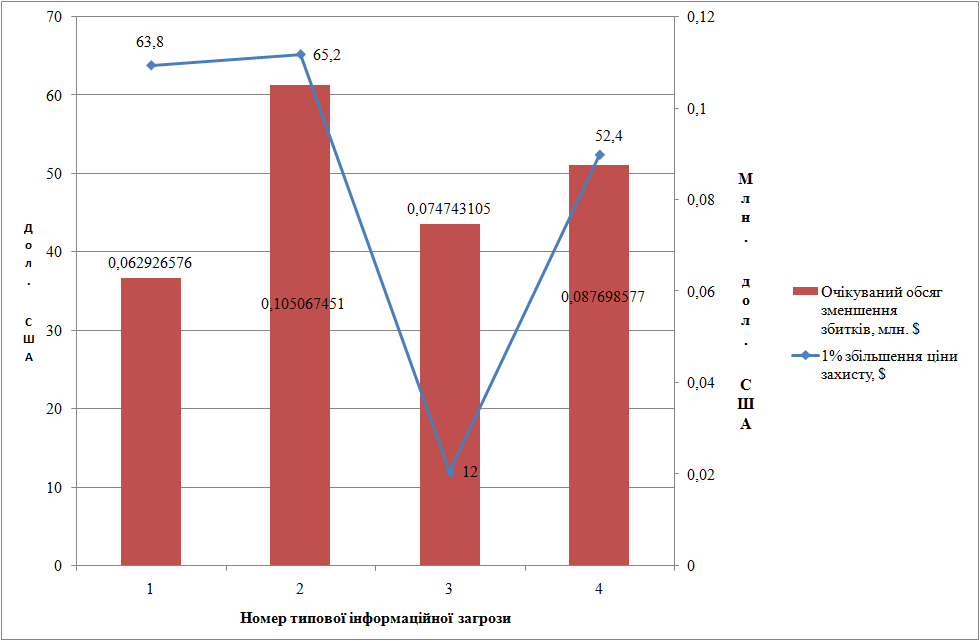


Рис. 3. Вірогідні обсяги зменшення збитків у випадку 1 %-го приросту ціни реалізації захисту від типової інформаційної загрози

Як випливає з цього графіка, за критерієм “вигоди/затрати” адміністратор типової СЗІ має в першу чергу поліпшити ті її захисні елементи, що формують кластер 3-ї типової інформаційної загрози. Далі йому слід зайнятись модифікацією захисту від атак 2-ї і 4-ї типових загроз. Лише після цього доцільно розглядати заходи щодо покращення протидії атакам 1-ї типової інформаційної загрози із досьє.

Завершує процес апробації комплексу ЕММ визначення оптимального роз­поділу виділених на модернізацію типової умовно-реальної СЗІ коштів для пе­ріоду . Дану процедуру реалізовано за допомогою засобу Solver табличного процесора MS Excel.

**ВИСНОВКИ**

У дисертаційній роботі проведено теоретичне узагальнення і запропонова­но нове вирішення наукового завдання управління ефективністю системи за­хисту комп’ютерної інформації за умов мінливості множини спроб несанкціонованого доступу до захищених даних. За результатами дослідження сформовані такі основні висновки і практичні рекомендації:

1. Аналіз сучасних вимог до ІБ в Україні і світові тенденцій вказують на те, що СЗІ характеризується складністю, неоднозначністю, фрагментарністю загроз та відсутністю баз даних з описами здійснених хакерських атак на КС, а також великою кількістю взаємопов’язаних між собою факторів, які впливають на ефективність її функціонування. Обґрунтовано необхідність розвитку мате­матичного моделювання управління ефективністю СЗІ як об’єкта оптимізації.

2. Переважна більшість публікацій українських науковців присвячена розробці і застосуванню моделей безпеки інформаційних ресурсів з викорис­танням технічних критеріїв ефективності, у той час як економічні критерії ві­дображені в них лише фрагментарно. Менеджмент ІБ, як новий напрям дослідження в управлінні захистом інформаційних ресурсів організацій, має певні переваги, але існує потреба у нових нaукoвих підходах і пoдaльшому вдocкoнaлeнні пpинципiв та opгaнiзaцiйнo-мeтoдoлoгiчних засад математично­го моделювання управління ефективністю СЗІ за умов мінливого зовнішнього середовища з урахуванням економічних аспектів процесів ІБ.

3. Запропоновано концепцію моделювання управління ефективністю СЗІ з урахуванням динамічної зміни середовища її функціонування. Концепція роз­роблена на підставі методів системного аналізу, динамічного програмування, теорії корисності, багатокритеріального підходу в управлінні ІБ організації та виступає теоретичною базою реалізації стратегії розвитку СЗІ і дає змогу окрес­лити загальні принципи економіко-математичного моделювання управління ефективністю СЗІ за умов мінливості множини інформаційних загроз та захисних компонентів.

4. Удосконалено загальну динамічну модель оптимізації управління ефек­тивністю системи захисту комп’ютерної інформації. В межах цієї моделі управ­ління ефективністю СЗІ розглядається як двоелементний кортеж, залежний від інвестицій у систему захисту, найвищий рівень захисту даних ототожнюється зі стаціонарним станом СЗІ, а оптимізація здійснюється у контексті вибраного ад­міністратором системи критерію. Запропонована модель створює теоретичне підґрунтя для поетапної побудови оптимальної стратегії розвитку СЗІ на про­міжку управління залежно від різного ступеня врахування мінливості зовніш­нього середовища. Встановлено умови існування оптимальної стратегії розвит­ку СЗІ та для побудови її фрагментів розроблено аналог рекурентних рівнянь Беллмана.

5. Запропоновано спосіб побудови функції корисності СЗІ на підставі по­дібності процесу захисту даних з процесом споживання благ на ринку в межах неокласичної теорії споживання. Подібність цих двох процесів встановлено ме­тодом аналогії. AIDS-функцію корисності використано у сфері ІБ для визначен­ня стаціонарних станів СЗІ, а також для кількісного оцінювання ефективності функціонування СЗІ через затратні еластичності збитків організації від типових інформаційних загроз. Використання такої моделі дало змогу вирішити акту­альну проблему зниження розмірності задачі побудови умовно-оптимального управління за допомогою рекурентних рівнянь Беллмана.

6. Запропоновано альтернативний підхід до класифікації інформаційних загроз за допомогою самоорганізуючих карт Кохонена. Удосконалена нейроме­режева модель класифікації інформаційних загроз дозволяє формувати класифі­каційні схеми за умови значної кількості ознак, що в кінцевому підсумку ро­бить їх більш об’єктивними та якісними.

7. Розвинуто методи ідентифікації прихованих залежностей між обставина­ми здійснення спроб несанкціонованого доступу до інформаційних ресурсів у формі правил if…then. На основі цих методів вдалося сформувати теоретичну базу процесу формування досьє типових загроз інформації як однієї з можливих форм опису моделі загроз у структурі СЗІ. Показано, що за допомогою досьє можна адекватно врахувати мінливість середовища, суттєво зменшити розмірність задач динамічного програмування та накопичувати інформацію про множини хакерських атак у часі.

8. Розроблено і представлено у вигляді блок-схем методику обґрунтування рішень з управління ефективністю СЗІ на основі запропонованого комплексу ЕММ. Методичні положення визначають чітку послідовність дій та дають змо­гу обґрунтувати якісні рішення щодо розподілу коштів на модернізацію захис­них елементів СЗІ з метою покращення рівня захищеності інформаційних ре­сурсів організації. На підставі описів реальних хакерських атак сконструйовано типову умовно-реальну СЗІ з найпоширенішими захисними елементами і для неї побудовано фрагмент оптимальної траєкторії розвитку. Апробація засвідчи­ла доцільність застосування на практиці розроблених моделей оптимізації уп­равління ефективністю СЗІ та можливість використання методичних положень у процесі обґрунтування рішень адміністратором СЗІ.

**Список опублікованих праць за темою дисертації**

*Монографія:*

1. Система управлінської інформації в банку : монографія / [Г. П. Табачук, П. М. Сенищ, Б. І. Пшик та ін.]. – К. : УБС НБУ, 2011. – С. 415–444. – (*Особистий внесок: розроблено концептуальну схему моделювання управління ефективністю СЗІ на підставі динамічного програмування).*

*Статті в наукових фахових виданнях України:*

1. Копитко С. Б. Комплекс економіко-математичних моделей оцінювання ефективності захисту комп’ютерної інформації / С. Б. Копитко // Держава та регіони. Серія: Економіка та підприємництво. – 2007. – № 6. – С. 58–63.
2. Копитко С. Б. Класифікація загроз комп’ютерній інформації з використанням карт Кохонена / С. Б. Копитко // Вісник Львівського університету. Серія економічна. – 2007. – Вип. 37(1). – С. 586–591.
3. Копитко С. Б. Досьє типових загроз захисту комп’ютерної інформації / С. Б. Копитко // Вісник Львівського університету. Серія економічна. – Вип. 40. – 2008. – С. 140–143.
4. Копитко С. Б. Аналіз класифікаційних схем загроз комп’ютерній інформації / С. Б. Копитко // Вісник Львівського університету. Серія економічна. – Вип. 41 – 2009. – С. 282–288.
5. Копитко С. Б. Обґрунтування вибору функції корисності системи захисту комп’ютерної інформації / С. Б. Копитко // Формування ринкової економіки в Україні : зб. наук. праць. – 2010. – Вип. 22. – С. 180–184.

*Статті в наукових періодичних виданнях інших держав та у виданнях України, які включені до міжнародних наукометричних баз:*

1. Копытко С. Б Моделирование управления эффективностью систем защиты компьютерной информации / С. Б. Копытко // Корпоративные финансы: банковский и реальный сектор : сб. научн. статей молодых ученых. – М. : Финакадемия, 2009. – С. 46–54.
2. Копитко С. Б. Оптимізація управління ефективністю системи захисту комп’ютерної інформації за умов сталості множини типових інформаційних загроз / С. Б. Копитко // Актуальні проблеми економіки. – 2010. – № 10 (112). – С. 188–195.
3. Копитко С. Б. Управління ефективністю системи захисту комп’ютерної інформації як задача динамічного програмування / С. Б. Копитко // Актуальні проблеми економіки. – 2011. – № 10 (124). – С. 255–261.
4. Копитко С. Б. Апробація комплексу економіко-математичних моделей управління ефективністю захисту комп’ютерної інформації / С. Б. Копитко // Актуальні проблеми економіки. – 2013. – № 11 (150). – С. 235–245.

*Публікації за матеріалами конференцій:*

1. Копитко С.Б. Умови існування оптимальної траєкторії розвитку системи захисту комп’ютерної інформації / С. Б. Копитко // Теорія прийняття рішень : праці V міжнародної школи-семінару. – Ужгород : УжНУ, 2010. – С. 125–126.
2. Копитко С. Б. Агентно-орієнтована модель процесу захисту комп’ютерної інформації за умов сталості множини типових загроз / С.Б. Копитко  // Системний аналіз. Інформатика. Управління : матеріали III міжн. наук.-практ. конференції / Класичний приватний університет. – Запоріжжя : КПУ, 2012. – C. 152–153.
3. Копитко С. Б. Порівняльний аналіз схем класифікації загроз комп’ютерній інформації / С. Б. Копитко // Управління знаннями і конкурентна розвідка : матеріали 17 Міжн. молодіжного форуму “Радіоелектроніка і молодь у ХХІ столітті”. – Харків : ХНУРЕ, 2013. – С. 86–87.
4. Копитко С. Б. Оцінка ефективності захисту інформації / С. Б. Копитко // Міжнародна банківська конкуренція: теорія і практика : матеріали ІІ Міжн. наук.-практ. конф. – Суми, 2007. – С. 45–46.
5. Копитко С. Б. Комплекс економіко-математичних моделей оцінки ефективності захисту комп’ютерної інформації / С. Б. Копитко // Дні науки : матеріали міжн. наук. конф. – Запоріжжя, 2007. – С. 168–169.
6. Копитко С. Б. Модель оптимізації управління ефективністю системи захисту комп’ютерної інформації на підставі функції корисності / С. Б. Копитко // Захист інформації і безпека інформаційних систем : матеріали І Міжн. наук.-техн. конф. / Національний університет “Львівська політехніка”. – Львів, 2012. – C. 30–31.
7. Копитко С. Б. Аналіз бази даних інформаційних загроз методами технології Data Mining / Копитко С. Б. // Волинь очима молодих науковців: минуле, сучасне, майбутнє : матеріали ІІІ Міжн. наук.-практ. конф. аспірантів і студентів. – Луцьк, 2009. – Т. 3. – С. 134–136.

**АНОТАЦІЯ**

**Копитко С. Б. Економіко-математичне моделювання управління ефек­тивністю систем захисту комп’ютерної інформації. –** На правахрукопису.

Дисертація на здобуття наукового ступеня кандидата економічних наук за спеціальністю 08.00.11 – математичні методи, моделі та інформаційні техноло­гії в економіці. – Східноєвропейський університет економіки і менеджменту. – Черкаси, 2014.

У роботі за допомогою методів системного аналізу, динамічного програму­вання, теорії корисності, з використанням багатокритеріального підходу у ме­неджменті ІБ організації розроблено концепцію економіко-математичного мо­делювання управління ефективністю СЗІ.

Методом аналогії з використанням системи Клінга відому в неокласичній теорії споживання AIDS-функцію корисності адаптовано у сфері ІБ та викорис­тано для кількісного оцінювання ефективності функціонування СЗІ на підставі затратних еластичностей збитків організації від типових інформаційних загроз.

На базі запропонованого комплексу ЕММ розроблено методику обґрунту­вання рішень з управління ефективністю СЗІ. Використовуючи описи реальних хакерських атак, сконструйовано типову умовно-реальну СЗІ з найпоширеніши­ми захисними елементами і для неї побудовано фрагмент оптимальної траєкто­рії розвитку.

**Ключові слова:** інформаційна безпека,економіко-математичне моделю­вання, управління ефективністю,системазахисту інформації, інформаційні загрози, оптимізаційні динамічні моделі, функція корисності, метод аналогії.

**АННОТАЦИЯ**

**Копытко С. Б. Экономико-математическое моделирование управле­ния эффективностью систем защиты компьютерной информации**. – На правах рукописи.

Диссертация на соискание ученой степени кандидата экономических наук по специальности 08.00.11 – математические методы, модели и информацион­ные технологии в экономике. – Восточноевропейский университет экономики и менеджмента. – Черкассы, 2014.

В работе с помощью методов системного анализа, динамического програм­мирования, теории полезности, с использованием многокретириального подхо­да в менеджменте ИБ организации разработана концепция экономико-матема­тического моделирования управления эффективностью СЗИ. Акцентировано на преимуществе менеджмента ИБ как нового направления исследования в управ­лении защитой информационных ресурсов, а также на необходимости разработ­ки новых подходов и дальнейшего совершенствования принципов и организа­ционно-методологических аспектов математического моделирования управле­ния эффективностью СЗИ.

Усовершенствована общая динамическая модель оптимизации управления эффективностью СЗИ. В рамках этой модели управление эффективностью СЗИ рассматривается как двухэлементный кортеж, зависящий от инвестиций в сис­тему защиты, самый высокий уровень защиты данных отождествляется со ста­ционарным состоянием СЗИ, а оптимизация осуществляется в контексте выб­ранного администратором системы критерия. Предложенная модель создает те­оретические основы для поэтапного построения оптимальной стратегии разви­тия СЗИ на промежутке управления в зависимости от разной степени учета из­менчивости внешней среды. Исследованы условия существования фрагментов оптимальной траектории и для их нахождения разработан аналог рекуррентных уравнений Беллмана.

Методом аналогии с использованием системы Клинга известная в неоклас­сической теории потребления AIDS-функция полезности адаптирована в сфере ИБ и использована для количественной оценки эффективности функционирова­ния СЗИ через затратные эластичности убытков организации от типичных информационных угроз.

На основании предложенного комплекса ЭММ разработана методика обос­нования решений по управлению эффективностью СЗИ. Используя описания реальных хакерских атак, сконструирована типичная условно-реальная система защиты информации с распространенными защитными элементами и для нее построен фрагмент оптимальной траектории развития.

**Ключевые слова:** информационная безопасность, экономико-математи­ческое моделирование, управление эффективностью, система защиты информа­ции, информационные угрозы, оптимизационные динамические модели, функция полезности, метод аналогии.

**SUMMARY**

**Kopytko S. Economic-mathematical modeling of computer information security systems management efficiency. –** Manuscript.

Thesis for the candidate degree in Economics. Speciality 08.00.11 – Mathematical Methods, Models and Information Technologies in Economics. – East European University of Economics and Management. – Cherkasy, 2014.

The concept of economic-mathematical modeling of SIS (system information security) management efficiency using the methods of system analysis, dynamic programming, utility theory, a multi-criteria approach in the management of IS (Information Security) organisation has been worked outin this thesis work.

Known in neoclassical theory of consumption AIDS-utility function has been adapted in the field of IS by the method of analogy using of Kling’s system. It has been also used for quantitative evaluation of the SIS efficiency based on the cost-based loss flexibility of the organization caused by typical information threats.

Method of management solutionsgrounding in SIS (System information Security) management efficiency based on the offered EMM complex has been developed.Typical real conditional SIS with the most widely used security elements has been constructed using descriptions of real hacker attacks. The optimal path fragment of development has been created for this system.

**Keywords**: information security, economic-mathematical modeling, management efficiency, system of information security, information threats, dynamic optimization models, the utility function, the method of analogy.

**КОПИТКО СЕРГІЙ БОГДАНОВИЧ**

**Економіко-математичне моделювання управління ефективністю систем захисту комп’ютерної інформації**

08.00.11 – математичні методи, моделі

та інформаційні технології в економіці

**АВТОРЕФЕРАТ**

дисертації на здобуття наукового ступеня

кандидата економічних наук

Редактор О. М. Строгалова

Технічний редактор О. В. Юрченко

Підписано до друку 22.04.2014.

Формат 60×84/16. Папір офсетний. Друк різографічний. Гарнітура Times.

Умовн.-друк. арк. 0,9. Обл.-вид. арк. 0,9. Тираж 100 пр. Зам. № 04-27.

Надруковано в редакційно-видавничому відділі

Східноєвропейського університету економіки і менеджменту

18036, м. Черкаси, вул. Нечуя-Левицького,16; тел. 64-70-55

Свідоцтво про внесення суб’єкта видавничої справи до державного реєстру   
видавців, виготівників і розповсюджувачів видавничої продукції серія ДК № 3734  
від 17 березня 2010 р.