КопиткоСергійБогдановичЕкономікоматематичнемоделюванняуправлінняефективністюсистемзахистукомпютерноїінформаціїДискандеконнаукСхідноєвропунтекономікиіменеджментуЧеркасис

**ЛЬВІВСЬКИЙ ІНСТИТУТ БАНКІВСЬКОЇ СПРАВИ УНІВЕРСИТЕТУ БАНКІВСЬКОЇ СПРАВИ НАЦІОНАЛЬНОГО БАНКУ УКРАЇНИ**

**На правах рукопису**

**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

Дисертація на здобуття наукового ступеня

кандидата економічних наук

**Науковий керівник:**

Білий Леонід Адамович

**Доктор технічних наук, професор**

**ЛЬВІВ – 2014**

|  |  |
| --- | --- |
| **ЗМІСТ** | |
|  | |
| **ВСТУП** | 4 |
| **Розділ І.** **Методологічні засади управління ефектив­ністю систем захисту комп’ютерної інформації** | 10 |
| 1.1. Інформація як об’єкт захисту в комп’ютерних системах | 10 |
| 1.2. Економічні аспекти побудови систем захисту комп’ютерної інформації | 27 |
| 1.3. Концептуалізація проблеми управління ефективністю системи захисту комп’ютерної інформації | 47 |
| Висновки до розділу І | 67 |
| **Розділ 2.** **Комплекс економіко-математичних моде­лей управління ефективністю системи захисту комп’ютерної інформації** | 69 |
| 2.1. Аналіз умов існування оптимальної стратегії розвитку системи захисту комп’ютерної інформації | 69 |
| 2.2. Модель визначення стаціонарного стану системи захисту комп’ютерної інформації | 84 |
| 2.3. Модель формування досьє типових загроз комп’ютерній інформації | 102 |
| 2.4. Моделі оптимізації управління ефективністю системи захисту комп’ютерної інформації | 113 |
| Висновки до розділу ІІ | 120 |
| **Розділ 3.** **Реалізація комплексУ економіко-матема­тичних моделей управління ефективніСтю системи захисту комп’ютерної інформації** | 124 |
| 3.1. Методичні положення щодо застосування комплексу ЕММ оптимізації управління ефективністю системи захисту комп’ютерної інформації | 124 |
| 3.2. Формування досьє типових загроз комп’ютерної інформації | 140 |
| 3.3. Оптимізація ефективності системи захисту комп’ютерної інформації | 159 |
| Висновки до розділу ІІІ | 177 |
| **ВИСНОВКИ** | 179 |
| **СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ** | 182 |
| **ДОДАТКИ** | 211 |

**ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ**

|  |  |
| --- | --- |
| АС | *‒* автоматизована система; |
| ДСТУ | *‒* державні стандарти України; |
| ЕММ | *‒* економіко-математичні моделі; |
| ЗІ | *‒* захист інформації; |
| ІБ | *‒* інформаційна безпека; |
| ІС | *‒* інформаційна система; |
| ІТ | *‒* інформаційні технології; |
| КС | *‒* комп’ютерна система; |
| НД | *‒* нормативний документ; |
| НД ТЗІ | *‒* нормативні документи в галузі технічного захисту інформації; |
| ПРД | *‒* правило розмежування доступу; |
| СЗІ | *‒* система захисту інформації; |
| СУІБ | *‒* система управління інформаційною безпекою; |
| ТЗІ | *‒* технічний захист інформації; |
| ISO | *‒* міжнародна організація зі стандартизації; |
| ISO/IEC | *‒* міжнародний стандарт інформаційної безпеки. |

**ВСТУП**

**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 розроблено 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 і 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 авторській 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, з 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, 3-х роз­ділів, висновків, списку використаних джерел, 14 додатків. Основний зміст роботи становить 181 сторінок. Дисертація містить 28 таблиць, 14 рисунків. Список використаних джерел містить 289 найменувань.

**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 ВИКОРИСТАНИХ ДЖЕРЕЛ

1. [Про державну таємницю: закон України вiд 21 січня 1994 року № 3855-XII](http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3855-12) // Відомості Верховної Ради України. – 1994. – № 16. – С. 422.
2. Про електронний цифровий підпис: закон України вiд 22 травня 2003 року № 852-IV // Офіційний вісник України. – 2003. – № 25. – С. 111.
3. Про електронні документи та електронний документообіг: закон України вiд 22 травня 2003 року № 851-IV // Офіційний вісник України. – 2003. – № 25. – С. 106.
4. [Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави: постанова Кабінету Міністрів України від 27.11.1998 р. № 1893](http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1893-98-%EF) // Офіційний вісник України. – 1998. – № 48. – С. 31.
5. [Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: постанова Кабінету Міністрів України від 29.03.2006 р. № 373](http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=373-2006-%EF) // Офіційний вісник України. – 2006. – № 13. – С. 164.
6. [Про захист інформації в інформаційно-телекомунікаційних системах: закон України вiд 5 липня 1994 року № 80/94-ВР](http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=80%2F94-%E2%F0) [Електронний ресурс]. – Режим доступу : <http://zakon3.rada.gov.ua>.
7. [Про захист персональних даних: закон України вiд 1 червня 2010 року № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – С. 1188.](http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2297-17)
8. Про інформацію: закон України вiд 2 жовтня 1992 року № 2657-XII [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua>.
9. Нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування систем захисту інформації (СЗІ). [Електронний ресурс]. – Режим доступу : <http://www.rusnauka.com/11_NPE_2012/Informatica/4_108307.doc.htm>.
10. Об участии в международном информационном обмене : федеральный закон РФ от 04. 07. 1996 г. № 85-ФЗ [Электронный ресурс]. – Режим доступа : <http://zakonbase.ru/content/base/18181>.
11. Акулич И.Л. Математическое программирование в примерах и задачах : учебн. пособ. для студ. экон. спец. вузов / И. Л. Акулич. – М. : Высшая школа, 1986. – 319 с.
12. Алишов Н.И. Архитектура распределенной проактивной системы безопасности информации / Н.И. Алишов, М.И. Огурцов, Ю.Н. Ханенко // Комп’ютерні засоби, мережі та системи. – 2005. – № 4. – С. 94-103.
13. Аналитико-статистический обзор о деятельности 155 страховых компаний России по итогам 2002 г. – М. : Центр экономического анализа агентства ”Интерфакс”, 2003. – С. 16-19.
14. Андрощук Г. Какие сведения могут составлять коммерческую тайну / Г. Андрощук, Л. Вороненко // Бизнес Информ. – 1999. – № 9-10. – С. 12-18.
15. Андрухів А.І. Порівняння методів оцінки захищеності корпоративних інформаційних систем / А.І. Андрухів, Д.О. Тарасов // Вісник національного університету “Львівська політехніка”. Серія : Комп’ютерні системи та мережі. – 2006. – № 573. – С. 9-14.
16. Арикава С. Теория аналогий : [пер. с япон.] / С. Арикава, М. Харагути // Приобретение знаний ; под ред. С. Осуги, Ю. Саэки. – М. : Мир, 1990. – С. 262-296.
17. Арлінський О.Ю. Методи захисту мережевого середовища від атак, які використовують клієнтське програмне забезпечення / О.Ю. Арлінський, Т.В. Командіна // Інформаційна безпека. – 2009. – №2(2). – С. 33-38.
18. Артемов В.Ю. Законодавче забезпечення охорони державної таємниці в умовах становлення національної державності / В.Ю. Артемов, А.С. Пашков // Інформаційна безпека. – 2010. – № 1(3). – С. 45-50.
19. Астахов А. Анализ защищенности корпоративних автоматизированных систем / А. Астахов // Jet Info. – 2002. – № 7. – C. 3-28.
20. Атаманов Г.А. “О персональных данных” – закон, построенный на понятиях / Г.А. Атаманов // Защита информации. Inside. – 2010. – № 2. – С. 28-45.
21. Ахрамович В.М. Захист інформації в комп’ютері під час застосування операційної системи Windows 7 / В.М. Ахрамович // Науковий вісник Національної академії статистики, обліку та аудиту. – 2012. – № 2(35). – С. 97-116.
22. Бабак В.П. Теоретичні основи захисту інформації : підручн. / В.П. Бабак. – К. : НАУ, 2008. – 752 с.
23. Бабич І.В. Огляд стеганографічних методів перетворення інформації в зображеннях / [І.В. Бабич, С.А. Паламарчук, Н.А. Паламарчук та ін.] // Захист інформації. – 2012. – Т. 14. – № 1. – С. 55-59.
24. Бабій А.С. Аналіз тенденцій розвитку злочинності / А.C. Бабій, М.М. Зацеркляний // Системи обробки інформації. – 2007. – Вип. 4(62). – С. 153-155.
25. Балаян Г.Г. Информационное моделирование научно-технических программ / Г.Г. Балаян. – М. : Наука, 1990. – 248 с.
26. Баронін А.С. Аналіз і прогноз у політиці та бізнесі : курс лекцій / А.С. Баронін. – К. : Вид-во Паливода А.В., 2005. – 128 с.
27. Белозеров Е.В. Особенности проектирования и построения защищенных Web-систем / Е.В. Белозеров, Д.А. Ладик, Ю.Э. Ладик // Вісник Східноукраїнського національного університету ім. В. Даля. – 2007. – №5. – Ч. 1. – С. 85-89.
28. Бєгун А.В. Безпека інтелектуальних інформаційних систем / А.В. Бєгун  // Моделювання та інформаційні системи в економіці. – 2008. – Вип. 78.1. – С. 182-190.
29. Биркгоф Г. Современная прикладная алгебра : [пер. с англ.] / Г. Биркгоф, Т. Барти. – М. : Мир, 1976. – 400 с.
30. Біленчук П.Д. Комп’ютерна злочинність : навч. посібник / [П.Д. Біленчук , Б.В. Романюк , В.С. Цимбалюк  та ін.]. – К. : Атіка, 2002. – 240 с.
31. Богуш В.М. Інформаційна безпека держави : навч. посібник / В.М. Богуш, О.К. Юдін. – К. : МК-Прес, 2005. – 432 с.
32. Боровик О.В. Дослідження операцій в економіці : навч. посібник / О.В. Боровик, Л.В. Боровик. – К. : Центр учбової літератури, 2007. – 424 с.
33. Брожик Л.Л. Проблема информационной безопасности как фактор безопасности национальной / Л.Л. Брожик // Економічна кібернетика. – 2008. – № 35-36 (53-54). – С. 78-80.
34. Брюхович Е.И. К вопросу об истинности утверждений в дедуктивных теориях / Е.И. Брюхович // Комп’ютерні засоби, мережі та системи. – 2006. – № 5. – С. 3-11.
35. Бурдин О.А. Комплексная экспертная система управления информационной безопасностью “АванГард” / О.А. Бурдин, А.А. Кононов // Информационное общество. – 2002. – № 1. – С. 38-44.
36. Буч Г. Язык UML. Руководство пользователя : [пер. с англ.] / Г. Буч, Дж. Рамбо, А. Джекобсон. – М. : ДМК Пресс, 2001. – 432 с.
37. Вагнер Г. Основы исследования операцій : [пер. с англ.] ; в 3 т. / Г. Вагнер. – Т. 2. – М. : Мир, 1973. – 486 с.
38. Василиу Е.В. Анализ стойкости к некогерентной атаке четырех квантовых протоколов распределения ключей с кутритами. // Захист інформації. – 2010. – №2. – С. 20-26.
39. Величко В.Ю. Методологія вирішення задачі прогнозування властивостей об’єктів методами виведення за аналогією на основі структурно-атрибутивної моделі знань / В.Ю.Величко, Н.М. Москалькова // Комп’ютерні засоби, мережі та системи. – 2005. – № 4. – С. 70-77.
40. Вербіцький О.В. Вступ до криптології / О.В. Вербіцький. – Львів : ВНТЛ, 1998. – 247 с.
41. Вербовська Г.В. Динамічне управління ресурсами захисту інформації / Г.В. Вербовська, Є.Г. Левченко // Захист інформації. – 2011. – Т. 13 – № 1(50). – С. 12-17.
42. Вітлінський В.В. Моделювання загроз ефективного функціонування інформаційної системи на підґрунті інструментарію нечіткої логіки / В.В. Вітлінський, Г.В. Мельник // Моделювання та інформаційні системи в економіці : зб. наук. праць. – 2009. – Вип. 79. – С. 22-29.
43. Волошин О.Ф. Теорія прийняття рішень : навч. посібник / О.Ф. Волошин, С.О. Мащенко. – К. : ВПЦ “Київський університет”, 2006. – 304 с.
44. Волянська В. Моделі еталонів лінгвістичних змінних для систем виявлення та ідентифікації порушника інформаційної безпеки / В. Волянська, А. Гізун, В. Гнатюк // Безпека інформації. – 2013. – Т. 19. – №1. – С. 13-20.
45. Воробьев А.А. Оценивание защищенности автоматизированных систем на основе методов теории игр / А.А. Воробьев, Г.В. Куликов, А.В. Непомнящих // Информационные технологии. – 2007. – № 1. – С. 1-24.
46. Герасін О.П. Використання інформаційних технологій організованою злочинністю / О.П. Герасін // Інформаційна безпека. – 2010. – № 2(4). – С. 127-131.
47. Гладунський В.Н. Логіка / В.Н. Гладунський, Г.А. Гладунська. – Львів : Каменяр, 1996. – Ч.2. – 188 с.
48. Глушак В.В. Синтез структури системи захисту інформації з використан­ням позиційної гри захисника та зловмисника / В.В. Глушак, О.М. Новіков // Системні дослідження та інформаційні технології. – 2013. – №2. – С. 89-100.
49. Головань В.Г. Синтез моделей угроз для распределенных вычислительных систем / В.Г. Головань, Ю.В. Щербина. // Інформаційна безпека. – 2010. – №2(4). – С. 66-70.
50. Головань С.М. Вимоги до побудови моделі загроз інформаційних систем / С. М. Головань // Інформаційна безпека. – 2009. – № 1(1). – С. 107-116.
51. Головань С.М. Вимоги до побудови моделі загроз інформаційних систем / С.М. Головань // Інформаційна безпека. – 2009. – №2(2). – С. 77-84.
52. Головань С.М. Класифікація інформації на основі законодавчих актів України / С.М. Головань // Сучасний захист інформації. – 2010. – № 1. – С. 4-7.
53. Голубенко А.П. Формирование политики информационной безопасности в жизни современного общества / [А.П. Голубенко, А.С. Петров, А.А. Петров  та ін.] // Вісник Східноукраїнського національного університету ім. В. Даля. – 2009. – №6(136). – Ч. 1. – С. 8-11.
54. Голубенко О.Л. Соціальні мережі як загроза безпеки / О.Л. Голубенко , А.С. Петров, А.О. Петров // Вісник Східноукраїнського національного університету ім. В. Даля. – 2011. – №7(161). – Ч. 1. – С. 7-10.
55. Горбулін В.П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В.П. Горбулін, О.Г. Додонов, Д. В. Ланде. – К. : Інтертехнологія, 2009. – 164 с.
56. Гранберг А.Г. Моделирование социалистической экономики : учебн. для студ. экон. вузов / А.Г. Гранберг. – М. : Экономика, 1988. – 487 с.
57. Грездов Г.Г. Модифицированный способ решения задачи формирования эффективной комплексной системы защиты информации автоматизированных систем / Г.Г. Грездов // Інформаційна безпека. – 2009. – №2(2). – С. 88-95.
58. Грездов Г.Г. Улучшенный способ решения задачи формирования эффек­тивной комплексной системы защиты информации автоматизированной системы / Г.Г. Грездов // Наукові записки УНДІЗ. –2010. – № 1(13). – С. 63-69.
59. Грибунин В.Г. Цифровая стеганография / В.Г.Грибунин, И.Н. Оков, И.В. Туринцев. – М. : Солон-Пресс, 2002. – 261 с.
60. Грищук Р.В. Диференціально-ігрова модель системи захисту інформації при нестаціонарній природі потоків захисних дій та інформаційних атак / Р.В. Грищук // Інформаційна безпека. – 2010. – №2(4). – С. 23-29.
61. Грищук Р.В. Диференціально-ігрові моделі векторної оптимізації процесів нападу на інформацію та її захист / Р.В. Грищук // Інформаційна безпека. – 2010. – №1(3). – С. 79-86.
62. Грищук Р.В. Теоретичні основи моделювання процесів нападу на інформацію методами теорії диференціальних ігор та диференціальних перетворень : монографія / Р.В. Грищук. – Житомир : Рута, 2010. – 280 с.
63. Грищук Р.В. Ігрові методи аналізу кібератак на інформаційну сферу / [Р.В. Грищук, С.Ж. Піскун, В.О. Хорошко та ін.] // Захист інформації. – 2012. – Т. 14. – № 1(54). – С. 19-24.
64. Грищук Р.В. Метод диференціально-ігрового Р-моделювання процесів нападу на інформацію / Р.В. Грищук // Інформаційна безпека. – 2009. – № 2(2). – С. 128-132.
65. Гулак Г.М. Забезпечення безпеки програмних засобів криптографічного захисту інформації та оцінка її рівня / Г.М. Гулак // Сучасний захист інформації. – 2010. – № 2. – С. 42-48.
66. Гундарь К.Ю. Защита информации в компьютерных системах / К.Ю. Гун­дарь, А. Ю. Гундарь, Д. А. Янишевский. – К. : Корнейчук, 2000. – 152 с.
67. Гуркин Ю.Н. Модельный прогноз для числа сетевых вторжений на ближайшие годы [Электронный ресурс] / Ю.Н. Гуркин, Ю.А. Семенов // Исследовано в России. – 2006. – С. 260-263. – Режим доступа : <http://zhurnal.fpe.relarn.ru/articles/2006/026.pdf>.
68. Даниліна Г.В. Статистичний підхід до аналізу комп’ютерних погроз / Г.В. Даниліна, Я.В. Милокум // Проблеми інформатизації та управління. – 2009. – № 3(27). –С. 52-56.
69. Деднев М.А. Защита информации в банковском и электронном бизнесе / М.А. Деднев, Д.В. Дыльнов, М.А. Иванов. – М. : Кудиц-образ, 2004. – 512 с.
70. Демчишин М.В. Вплив вразливості об’єктів на розв’язок прямої та зворотної задач менеджменту інформаційної безпеки / М.В. Демчишин, Є.Г. Левченко // Системні дослідження та інформаційні технології. – 2012. – №3. – С. 43-57.
71. Демчишин М.В. Співставлення чіткого та нечіткого підходів до розв’язку задач інформаційної безпеки / М.В. Демчишин, Є.Г. Левченко // Системні дослідження та інформаційні технології. – 2013. – №2. – С. 101-113.
72. Джексон П. Введение в экстренные системы : [пер. с англ.] / П. Джексон. – М. : Издательский дом “Вильямс”, 2001. – 624 с.
73. Диго С.М. Проектирование баз даннях : учебник / С.М. Диго. – М. : Финансы и статистика, 1988. – 216 с.
74. Дмитренко О.П. Побудова структурної моделі інформаційної системи для синтезу комплексної системи захисту інформації / О.П. Дмитренко, В.О. Хорошко // Сучасний захист інформації. – 2010. – №1. – С. 64-69.
75. Доктрина інформаційної безпеки України : затверджена Указом Президента України від 8 липня 2009 р. №514/2009 [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/9570.html.
76. Домарев В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев. – К. : ООО ТИД “ДС”, 2004. – 992 с.
77. Домарев В.В. Защита информации и безопасность компьютерных систем / В.В. Домарев. – К. : Диасофт, 1999. – 480 с.
78. Домарев Д.В. Математическое описание процессов атак на компьютерные сети / Д.В. Домарев // Проблеми інформатизації та управління. – 2010. – №1(29). – С. 50-54.
79. Домарєв В.В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k) / В.В. Домарєв, В.Д. Домарєв. – Донецьк : Велстар, 2012. – 146 с.
80. Домарєв Д. Методика управління інформаційною безпекою в банківських установах за допомогою СУІБ “Матриця” / Д. Домарєв, В. Домарєв. // Безпека інформації. – 2013. – Т. 19. – №1. – С. 60-70.
81. Дубов Д.В. Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців : аналітична доповідь / Д.В. Дубов, М.А. Ожеван. – К. : НІСД, 2012. – 32 с.
82. Дубовіков А.Ю. Методика формування тесту на проникнення. / А.Ю. Дубовіков, Е.Ю. Дубовіков // Інформаційна безпека. – 2010. – №1(3). – С. 119-123.
83. Дудикевич В.Б. Дослідження механізмів комплексного забезпечення безпеки і достовірності передачі даних в комп'ютерних системах і мережах / В.Б. Дудикевич, Б.П. Томашевський // Захист інформації. – 2010. – №3. – С.22-27.
84. Дудикевич В.Б. Синтез математичної моделі прогнозування для систем захисту інформації / В.Б. Дудикевич, В.М. Стеренчук, Л.М. Ракобовчук // Сучасний захист інформації. – 2010. – №1. – С. 70-72.
85. Дудикевич В.Б. Інформаційна безпека в банківських установах при роботі по платежах в системі SWIFT / В.Б.Дудикевич, Ю.В .Лах, С.М. Буджерак // Вісник Східноукраїнського національного університету ім. В. Даля. – 2011. – №7(161). – Ч. 1. – С. 51-57.
86. Дудикевич В.Б. Крипто-кодовий захист інформації з недвійковим рівноваговим кодуванням / В.Б. Дудикевич, О.О. Кузнєцов, Б.П. Томашевський // Сучасний захист інформації. – 2010. – № 2. – С. 14-23.
87. Дюк В. Data mining : учебный курс (+ CD) / В. Дюк, А. Самойленко. – С.-Петербург : Питер, 2001. – 368 с.
88. Електронна комерція і право : навч.-метод. посібник / [укл. А.А. Маєвська]. – Харків, 2010. – 256 с.
89. Ємельянов С.Л. Методика та результати оцінки якості законодавчого забезпечення правового інституту таємниць в Україні / С.Л. Ємельянов // Вісник Східноукраїнського національного університету ім. В. Даля. – 2011. – № 7(161). – Ч. 1. – С. 57-62.
90. Ємець В. Сучасна криптографія. Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів : БаК, 2003. – 144 с.
91. Живко З.Б. Інформаційні загрози : суть та проблеми / З.Б. Живко, М.О. Живко // Системи обробки інформації : збірник наукових праць. – 2009. –7(81). – С. 116–118.
92. Живко М.О. Захист інформації: правовий аспект і проблематика / М.О. Живко // Інформаційна безпека. – 2010. – № 1(3). – С. 72-78.
93. Забок М.І. Безпека банківської діяльності : навч. посібник / М.І. Забок. – К. : КНЕУ, 2002 – 190 с.
94. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99. – К. : ДСТСЗІ СБ України, 1999. – 15 с.
95. Задірака В.К. Фінансування витрат на захист інформації в економічній діяльності / [В.К. Задірака, О.С. Олеснюк, Р.П. Смоленюк, І.П. Штаблюк] // Університетські наукові записки. – 2006. – №33-4 (19-20). – С. 479-490.
96. Заенцев И.В. Нейронные сети: основные модели : учебн. пособие / И.В. Заенцев. – Воронеж : изд-во Воронежского гос. университета, 1999. – 76 с.
97. Зайченко Ю.П. Основи проектування інтелектуальних систем : навч. посібник. / Ю.П. Зайченко. – К. : Видавничий дім “Слово”, 2004. – 352 с.
98. Замков О.О. Математические методы в экономике : учебник / О.О. Замков, А.В. Толстопятенко, Ю.Н. Черемных. – М. : МГУ им. М.В. Ломоносова, изд-во “Дело и сервис”, 1999. – 368 с.
99. Захаров А.И. Информационные системы: оценка рисков / А.И. Захаров // Information Security/Информационная безопасность. – 2005. – №6. – С. 18-19.
100. Захист інформації. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. – [Чинний від 1996–01–01]. – К. : Держстандарт України, 1996. – 5 с.
101. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD): ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. – К. : Національний банк України, 2010. – 163 с.
102. Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. – М. : Горячая линия-Телеком, 2000. – 98 с.
103. Земляна Н.О. Оцінка ефективності функціонування систем захисту інформації [Електронний ресурс] / Н.О. Земляна, М.В. Торбєєва. – Режим доступу:
104. Зиатдинов А.Ю. Метод обнаружения аномалий в специализированных корпоративных сетях / А.Ю. Зиатдинов // Проблеми інформатизації та управління. – 2010. – №1(29). – С. 70-75.
105. Иванов Н.Н. Информационно-аналитические системы в управлении экономическими объектами / Н.Н. Иванов // Науковий журнал «Бізнес інформ». Харків: ВД«ІНЖЕК»,№10(429). 2013.–С.141-145.
106. Индеева В.В. К вопросу об определении понятия “риск” [Электронный ресурс] / В.В. Индеева // РГМУ им. акад. И.П. Павлова. – Рязань, 2007. – Режим доступа: <http://www.rae.ru/zk/ari/2007/02/Indeeva.pdf>.
107. Интриллигатор М. Математические методы оптимизации и экономическая теория / М. Интриллигатор. – М. : Прогресс, 1975. – 606 с.
108. Искусственный интеллект : справочник : [в 3-х кн.] ; [ред. Д. А. Поспелов]. – Модели и методы : Кн. 2. – М. : Радио и связь, 1990. – 304 с.
109. Исмайлов Б.Г. Сравнительный анализ результатов различных подходов к моделированию системы защиты и информации в распределенных сетях обслуживания / Б.Г. Исмайлов // Інформаційні технології та комп’ютерна інженерія. – 2010. – №2(18). – С. 44-50.
110. Ігнатьєва О.В. Інформаційна безпека й основні загрози захисту комп’ютерів / О.В. Ігнатьєва // Інформаційна безпека. – 2010. – № 2(4). – С. 48-53.
111. Інформатика. Комп’ютерна техніка. Комп’ютерні технології : посібник / [за ред. О. І. Пушкаря]. – К. : Видавничий центр “Академія”, 2001. – 542 с.
112. Іщенко Ю.М. Додаткові властивості безпеки електронних транзакцій у системах, що використовують сервіси комбінованої ІВК / Ю.М. Іщенко, А.В. Лєншин // Вісник Харківського національного університету. – 2010. – № 890. – С. 109-114.
113. Каллан Р. Основные концепции нейронных сетей : [пер. с англ.] / Р. Каллан. – М. : Издательский дом “Вильямс”, 2001. – 287 с.
114. Кальянов Г.Н. CASE – структурный системный анализ (автоматизация и применение) / Г. Н. Кальянов. – М. : ЛОРН, 1996. – 242 с.
115. Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться / Е.В. Касперский. – М. : СК Пресс, 1998. – 288 с.
116. Кирилишен Я.В. Концепция информационного сервиса модели менеджмента информационной системы управления / Я.В. Кирилишен // Модели управления в рыночной экономике : сб. научных трудов / Под общ. ред. Ю. Г. Лысенко. – Донецк : ДонНУ, 2008. – С. 186-193.
117. Кігель В.Р. Методи і моделі підтримки прийняття рішень у ринковій економіці : монографія / В.Р. Кігель. – К. : ЦУЛ, 2003. – 202 с.
118. Клювак О.В. Роль та особливості організації сертифікаційних центрів в електронній комерції / О.В. Клювак // Вісник Східноукраїнського національного університету ім. В. Даля. – 2010. – № 9(151). – Ч. 1. – С. 136-142.
119. Коваль В.Н. Системы вывода по аналогии для получения новых математических знаний / [В.Н.Коваль , Ю.В.Кук , Е.И. Лаврикова  та ін.] // Коп’ютерні засоби, мережі та системи. – 2004. – № 3. – С. 9-18.
120. Козлова К.В. Кількісна оцінка захисту радіоелектронних об’єктів / К.В. Козлова, В.О. Хорошко // Захист інформації. – 2007. – №  1. – С. 30-32.
121. Комашинский Д.В. Концептуальные основы использования методов Data Mining для обнаружения вредоносного програмного обеспечения / Д.В. Комашинский, И.В. Котенко // Защита информации. INSIDE. – 2010. – №2. – С. 74-82.
122. Конев И.Р. Информационная безопасность предприятия / И.Р. Конев, А.В. Беляев. – С.-Петербург : БХВ-Санкт-Петербург, 2003. – 752 с.
123. Кононович В.Г. Страхування ризиків інформаційної безпеки як метод захисту інформації / В.Г. Кононович, Ю.В. Копитін // Інформаційна безпека. – 2010. – №2(4). – С. 33-39.
124. 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 р. – C. 152-153.
125. Копитко С.Б. Аналіз бази даних інформаційних загроз методами технології Data Mining / С.Б. Копитко // Волинь очима молодих науковців: минуле, сучасне, майбутнє : матеріали ІІІ міжн. наук.-практ. конф. аспірантів і студентів. – Луцьк, 2009. – Т. 3. – С. 134–136.
126. Копитко С.Б. Аналіз класифікаційних схем загроз комп’ютерній інформації / С.Б. Копитко // Вісник Львівського університету. Серія економічна. – Вип. 41 – 2009. – С. 282-288.
127. Копитко С.Б. Апробація комплексу економіко-математичних моделей управління ефективністю системи захисту комп’ютерної інформації / С.Б. Копитко // Актуальні проблеми економіки. – 2013. – № 12(150). – С. 235-245.
128. Копитко С.Б. Досьє типових загроз захисту комп’ютерної інформації / С.Б. Копитко // Вісник Львівського університету. Серія економічна. – Вип. 40 – 2008. – С. 140-143.
129. Копитко С.Б. Економіко-математична модель мінімізації втрат від несанкціонованого доступу до інформації / С.Б. Копитко // Розвиток фінансово-кредитної системи України: здобутки, проблеми, перспективи : матеріали ІІІ Всеукраїнської наук.-практ. конф. аспірантів та молодих вчених. – Львів, 2007. – С. 223-225.
130. 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.
131. 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.
132. 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.
133. Копитко С.Б. Обґрунтування вибору функції корисності системи захисту комп’ютерної інформації / С.Б. Копитко // Формування ринкової економіки в Україні. – 2010. – Вип. 22. – С. 180-185.
134. 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. 188-194.
135. 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.
136. Копитко С.Б. Порівняльний аналіз схем класифікації загроз комп’ютерній інформації / С.Б. Копитко // Управління знаннями і конкурентна розвідка : матеріали 17 Міжнародного молодіжного форуму “Радіоелектроніка і молодь у ХХІ столітті”. – Харків : ХНУРЕ, 2013. – С. 86-87.
137. Копитко С.Б. Система управлінської інформації в банку : монографія / [Г.П. Табачук, П.М. Сенищ, Б.І. Пшик та ін.]. – К. : УБС НБУ, 2011. – С. 415-444.
138. 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.
139. 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.
140. Копытко С.Б. Моделирование управления эффективностью систем защиты компьютерной информации / С.Б. Копытко // Корпоративные финансы: банковский и реальный сектор: сборник научных статей молодых ученых. – М. : Финакадемия, 2009. – С. 46-54.
141. Коробко В.В. Методы построения комбинированных систем обнаружения атак на цифровые сети / В.В. Коробко, А.А. Скоропаденко // Захист інформації. – 2010. – Т. 12. – № 1(46). – С. 23-30.
142. Корольов О. Л. Критерії оцінювання ефективності впровадження і використання інформаційних систем та інформаційних технологій / О. Л. Корольов, А. В. Сігал // Моделювання та інформаційні системи в економіці : міжвід. наук. зб. Заснов. у 1965 р. / відп. ред. В. К. Галіцин. – К. : КНЕУ, 2005. – Вип. 72. – С. 40–48.
143. Коростіль Ю.М. Можливості сучасних технологій при розв’язку задач захисту доступу / Ю.Ю. М. Коростіль, С.О. Нікулін // Моделювання та інформаційні технології. – 2009. – Вип. 51. – С. 124-132.
144. Корченко А.Г. Анализ и определение понятия риска для его интерпретации в области информационной безопасности / А.Г. Корченко, Е.В. Иванченко, С.В. Казмирчук // Захист інформації. – 2010. – №3. – С. 31-36.
145. Корченко А.Г. Анализ и оценивание рисков информационной безопасности. / А.Г. Корченко, А.Е. Архипов, С.В. Казмирчук. – К. : ООО “Лазурит-Полиграф”, 2013. – 275 с.
146. Корченко А.О. Моделі аномального стану для систем виявлення кібератак в комп’ютерних мережах : автореф. дис… к.т.н. : 05.13.05 / А.О. Корченко – К., 2013. – 20 с.
147. Корченко О.Г. Системи захисту інформації на основі теорії нечіткості : автореф. дис…. д.т.н. : 05.13.21 / О.Г. Корченко. – К., 2004. – 32 с.
148. Корченко А.Г. Методы анализа и оценки рисков потерь государственных информационных ресурсов / А.Г. Корченко, В.П. Щербина, С.В. Казмирчук // Захист інформації. – 2012. – Т. 14. – № 1(54). – С. 28-32.
149. Корченко О.Г. Квантово-криптографічна система з безумовною стійкістю / [О.Г. Корченко, С.О. Гнатюк, О.В. Васько та ін.] // Захист інформації. – 2010. – Т. 12. – № 2(47). – С. 43-49.
150. Корченко О.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / О.Г. Корченко. – К. : МК-Пресс, 2006. – 320 с.
151. Корченко О.Г. Сучасні квантові технології захисту інформації / О.Г. Корченко, Є.В. Васіліу, С.О. Гнатюк // Захист інформації. – 2010. – Т. 12. –№ 1(46) – С. 77-89.
152. Коцьо О.Я. Моделювання споживання домогосподарств за умов невизначеності інформації : автореф. дис… к.е.н. : 08.00.11 / Коцьо О.Я. – Львів, 2009. – 21 с.
153. Критерии оценки безопасности компьютерных систем МО США («Оранжевая книга») TCSTC (Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, 1983).
154. Кулініч Р.В. Продуктивність інвестицій в інформаційну безпеку / Р.В. Кулініч, Є.Г. Левченко // Захист інформації. – 2011. – №1. – С. 22-27.
155. Курицкий Б.Я. Поиск оптимальных решений средствами Excel 7.0 / Б.Я. Курицкий. – С.-Петербург : BHV, 1997. – 384 с.
156. Лавренюк С.П. Математичні основи мікроекономіки. Теорія споживання : текст лекцій / С.П. Лавренюк. – Львів : Видавничий центр ЛНУ ім. Івана Франка, 1999. – 80 с.
157. Ланкастер К. Математическая экономика : [пер. с англ.] / К. Ланкастер. – М. : Советское радио, 1972. – 464 с.
158. Лахно В.А. Експериментальні дослідження зміни продуктивності корпоративних інформаційних систем підприємств в умовах реалізації комп’ютерних атак. / В.А. Лахно, О.С. Петров // Інформаційна безпека. – 2011. – №1(5). – С. 182-190.
159. Лахно В.А. Использование пакетов MATLAB 2009 и SIMULINK для моделирования уязвимостей автоматизированніх систем обработки єкономической информации. / В.А. Лахно, Т.П. Романенко, Н.Т. Миронюк // Бизнес Информ. – 2010. – №4(2). – С. 170-174.
160. Лахно В.А. Исследование конфликтных потоков заявок в системах защиты информации / В.А. Лахно, А.С. Петров, Н.Т. Чертунина // Вісник Східноукраїнського національного університету імені В. Даля. – 2009. – № 6(136). – Ч. 1. – С. 200-209.
161. Лахно В.А. Моделирование компьютерных атак на адаптивные системы защиты информации предприятий / В.А. Лахно, А.С. Петров // Інформаційна безпека. – 2011. – №2(6). – С. 60-69.
162. Лебедев В.В. Математическое моделирование социально-экономических процессов / В.В. Лебедев. – М. : Изограф, 1997. – 224 с.
163. Левченко Є. Умови існування сідловок точки в багато рубіжних системах захисту інформації / Є. Левченко, Р. Прус, Д. Рабчун // Безпека інформації. – 2013. – Т. 19. – 31. – С. 13-20.
164. Левченко Є.Г. Оптимізаційні задачі менеджменту інформаційної безпеки / Є.Г. Левченко, А.О. Рабчун // Сучасний захист інформації. – 2010. – №1. – С. 16-23.
165. Левшаков С. Перспективи розвитку послуг із надання цифрових електронних підписів у банківській системі України / С. Левшаков // Вісник Національного банку України. – 2012. – №4. – С. 50-53.
166. Ленков С.В. Методы и средства защиты информации : [в 2-х т.] / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко – К. : Арий, 2008. – Т. 1 – 464 с.; Т. 2 – 344 с.
167. Лєнков С.В. Методи протидії шкідливому програмному забезпеченню / [С.В. Лєнков, Г.Б. Жиров, В.Б. Бахвалов, Н.М. Берназ] // Інформаційна безпека. – 2010. – №1(3). – С. 23-30.
168. Лєнков С.В. Захист національних інформаційних ресурсів в аспекті інформаційної безпеки України / Лєнков С.В., Балабін В.В. // Вісник Східноукраїнського національного університету ім. В. Даля. – 2007. – №5. – Ч. 1. – С. 21-23.
169. Лук’янова В.В. Економічний ризик : навч. посібник / В.В. Лук’янова, Т.В. Головач. – К. : Академ-видав, 2007. – 464 с.
170. Лукацкий А. Обнаружение атак / А. Лукацкий. – С.-Петербург : БХВ – Санкт-Петербург, 2003. – 608 с.
171. Луценко В.М. Автоматизація проектування комплексних систем захисту інформації з використанням засобів підтримки прийняття рішень / В.М. Луценко // Захист інформації. – 2012. – Т. 14. – № 1(54). – С. 10-14.
172. Луценко В.М. Відповідність етапів побудови систем захисту інформації стадіям створення автоматизованих систем / В.М. Луценко // Захист інформації. – 2011. – Т. 13. – № 3(52). – С. 23-27.
173. Луцкий М.Г. Исследование программных средств анализа и оценки риска информационной безопасности / [М.Г. Луцкий, А.Г. Корченко, Е.В. Иванченко и др.] // Захист інформації. – 2011. – Т. 13. –№ 3(52). – С. 44-49.
174. Лысенко Ю.Г. Нейронные сети и генетические алгоритмы : учебн. пособие / Ю.Г. Лысенко, Н.Н. Иванов, А.Ю. Минц. – Донецк : ООО “Юго – Восток, ЛТД”, 2003. – 230 с.
175. Макконел К.Р. Аналітична економія: принципи, проблеми і політика. Мікроекономіка / К.Р. Макконел, С.Л. Брю. – Львів : Просвіта, 1999. – 650 с.
176. Мартино Дж. Технологическое прогнозирование : [пер. с англ.] / Дж. Мартино. – М. : Прогресс, 1977. – 591 с.
177. Марченко В.А. Формализованная технология проектирования системы защиты информации / В.А. Марченко  // Комп'ютерні засоби, мережі та системи. – 2007. – № 6. – C. 126-132.
178. Маслова Н.А. Построение модели защиты информации c заданными характеристиками качества / Н.А. Маслова // Штучний інтелект. – 2007. – № 1. – С. 51-57.
179. Матвійчук Ю. Зміцнення безпеки банків як відповідь на нові виклики і загрози / Ю. Матвійчук // Вісник Національного банку України. – 2012. – №8. – С. 48-50.
180. Медведовский И. Особенности систем анализа информационных рисков на примере алгоритма ГРИФ [Электронный ресурс] / И. Медведовский. – Режим доступа : <http://www.bre.ru/security/22122.html>.
181. Медведский И.А. Атака на Интернет. / И.А. Медведский, П.В. Семьянов, Д.Г. Леонов. – М. : ДМК, 1999. – 128 с.
182. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі: НД ТЗІ 3.7-001-99. – К. : ДСТСЗІ СБ України, 1999. – 10 с.
183. Мороз А.О. Біометричні технології. Методи дактилоскопії / А.О. Мороз // Математичні машини і системи. – 2011. – № 3. – С. 58-65.
184. Мухин В.Е. Инструментарий минимизации риска защищенности в распределенных компьютерных системах (РКС) / В.Е. Мухин // Системні дослідження та інформаційні технології. – 2010. – № 4. – С. 58-68.
185. Мясіщев О.А. Математичний апарат опису моделей функціонування системи захисту інформаційних ресурсів / О.А. Мясіщев, А.В. Джулій, Є.В. Стьопін // Інформаційна безпека. – 2011. – №2(6). – С. 106-111.
186. НейрOK Excel Neural Package (Kohonen Map 1.0) [Электронный ресурс]. – Режим доступа : [www.soft.neurok.ru](http://www.soft.neurok.ru).
187. Никитенко Л.Л. Исследование критерия стойкости при пассивных атаках / Л.Л. Никитенко // Компьютерная математика. – 2009. – № 1. – С. 96-104.
188. Орлов С. А. Технологии разработки программного обеспечения: учебник / С.А. Орлов. – С.-Петербург : Питер, 2002. – 464 с.
189. Остроухов В.В. Основні загрози особистісній безпеці від деструктивних інформаційних впливів (інформаційно-психологічна безпека особи) / В.В. Остроухов // Захист інформації. – 2010. – Т. 12. –№ 1(46). – 2010. – С. 5-9.
190. Павлов І.М. Неформальний опис життєвого циклу комплексної системи захисту інформації / І.М. Павлов, В.О. Бірюков // Інформаційна безпека. – 2011. – №1(5). – С. 117-125.
191. Паклин Н.Б. Бизнес-аналитика: от данных к знаниям (+ CD) : учеб. пособие / Н.Б. Паклин, В.И. Орешков. – 2-е изд., перераб. и доп. – С.-Петербург: Питер, 2010. – 704 с.
192. Палагин А.В. Парадигма построения информационной защиты компьютерных систем в зависимости от степени важности информации / А.В. Палагин, Ю.С. Яковлев, Б.М. Тихонов // Комп’ютерні засоби, мережі та системи. – 2003. – № 2. – С. 3-14.
193. Палагин А.В. Технология защиты больших баз данных от несанкционированного копирования / [А.В. Палагин, Н.И. Алишов, В.А. Марченко  та ін.] // Комп’ютерні засоби, мережі та системи. – 2006. – № 5. – С. 73-79.
194. Панчишин С.М. Макроекономіка : навч. посібник / С.М. Панчишин. – К. : Либідь, 2002. – 616 с.
195. Пархуць Ю.Л. Криптографічні механізми захисту інформації в мобільному зв’язку / Ю.Л. Пархуць // Захист інформації. – 2011. – Т. 13. –№ 1(50). – С. 5-10.
196. Пасічник В.В. Організація баз даних та знань / В.В. Пасічник, В.А. Резніченко. – К. : Видавнича група BHV, 2006. – 384 с.
197. Пасічник В.В. Сховища даних : навч. посібник / В.В. Пасічник, Н.Б. Шаховська. – Львів : “Магнолія 2006”, 2008. – 469 с.
198. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М. : АйТи Пресс, 2004. – 384 с.
199. Петров А.С. Анализ уязвимостей web-систем / А.С. Петров, О.А. Талыкин // Інформаційна безпека. – 2009. – № 1(1). – С. 107-116.
200. Печень С.А. Современные антикризисные меры информационной безопасности: блокировка утечек информации, критичных для бизнес-процессов предприятия / С.А. Печень // Сучасний захист інформації. – 2010. – № 2. – С. 9–13.
201. Положення про порядок здійснення криптографічного захисту інформації в Україні : затверджено Указом Президента України від 22 травня 1998 року № 505/98 // Офіційний вісник України. – 1998. – № 21. – С. 4.
202. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі: НД ТЗІ 3.7-003-05. –   
     К.: ДСТСЗІ СБ України, 2005. – 30 с.
203. Приймак В.І. Математичні методи економічного аналізу: навч. посібник / В.І. Приймак. – К. : Центр учбової літератури, 2009. – 296 с.
204. Присяжнюк М.М. Інформаційний захист людини, суспільства, держави – складові національної безпеки країни / М.М. Присяжнюк // Сучасні інформаційні технології у сфері безпеки та оборони. – 2009. – № 1(4). – С. 86-89.
205. Притула М.М. Динамічні моделі та методи прийняття рішень у ринковій економіці : навч. посібник / М.М. Притула. – Львів : Видавничий центр ЛНУ ім. І. Франка, 2007. – 256 с.
206. Проект “Розробка та впровадження типових рішень щодо комплексної системи захисту інформації в АІС НАНУ”. Безпека GRID-технологій. Огляд технічних рішень. – К. : Інститут програмних систем НАН України, 2009. –   
     78 с.
207. Проскурин В.Г. Программно-аппаратные средства обеспечения информа­ционной безопасности. Защита в операционных системах / В.Г. Проскурин , С.В. Крутов, И.В. Мацкевич. – М. : Радио и связь, 2000. – 166 с.
208. Рассел Б. Человеческое познание: его сфера и границы : [пер. с англ.] / Б. Рассел. – К. : Нико-Центр, 1997. – 560 с.
209. Ромец Н.Е. Модели принятия решений взаимодействующими агентами / Н.Е. Ромец // Комп’ютерні засоби, мережі та системи. – 2004. – № 3. – С. 149-155.
210. Ряба Е.И. Программно-аппаратные компоненты комплексной системы защиты информации / Е.И. Ряба, Л.Г.Черниш, А.Я. Бабич // Захист інформації – 2012. – Т. 14. – № 1(54). – С. 8-12.
211. Ряба О.І. Створення комплексного захисту web-сервісів SOAP на базі специфікації WS-SECURITY / О.І. Ряба, Л.Г. Черниш, Г.Ю. Гончар // Захист інформації. – 2012. – Т. 14. – №1(54). – С. 50-54.
212. Сабадаш В.П. Шахрайство в електронній комерції: реалії сьогодення / В.П. Сабадаш // Вісник Запорізького національного університету. – 2011. – №1. – С. 216-220.
213. Самарченко Є.О. Безпека електронних платіжних систем / Є.О. Самарченко , О.С. Петров // Інформаційна безпека. – 2009. – № 1(1). – C. 135-138.
214. Сафонов А.С. Применение организационно-технических методов для развития системы информационной безопасности организации / А.С. Сафонов, О.Е. Плачинда, Ю.П. Венедиктов. // Праці Одеського політехнічного університету. – 2011. – Вип. 1(35). – С. 262-266.
215. Светлов В.А. Практическая логика : учебн. пособие / В.А. Светлов. – С.-Петербург : ПИД “МиМ”, 1997. – 576 с.
216. Семенов М.И. Автоматизированные информационные технологии в экономике / [М.И. Семенов, И.Т. Трубилин, В.И. Лойко и др.]. – М. : Финансы и статистика, 2002. – 416 c.
217. Семеренко В.П. Интегрированная защита информации: криптография плюс помехоустойчивое кодирование / В.П. Семеренко // Захист інформації. – 2011. – Т. 13. – № 3(52). – С. 1-9.
218. Сергеева Л.Н. Нелинейная экономика: модели и методы / Л.Н. Сергеева. – Запорожье : Полиграф, 2003. – 218 с.
219. Сердюк В. Аудит информационной безопасности – основа эффективной защиты предприятия / В. Сердюк // BYTE/Россия. – 2006. – №4(92). – С. 32-35.
220. Симонов С.В. Технологии и инструментарий для управления рисками / С.В. Симонов // Информационный бюлетень JetInfo. – 2003. – № (117). – С. 9-13.
221. Сирченко Г.А. Имитационное моделирование для исследования информационных потоков в системах защиты / Г.А. Сирченко, В.А. Хорошко // Сучасний захист інформації. – 2010. – №1. – С. 73-77.
222. Сирченко Г.А. Принципы построения моделей угроз информационным ресурсам систем и сетей святи / Г.А. Сирченко // Вісник Східноукраїнського національного університету ім. В. Даля. – 2010. – №9(151). – Ч. 1. – С. 18-19.
223. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD): ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. – К. : Національний банк України, 2010. – 49 с.
224. Ситник Н.В. Проектування баз і сховищ даних : навч. посібник / Н.В. Ситник. – К. : КНЕУ, 2004. – 348 с.
225. Словарь по кибернетике / [под ред. В.С. Михалевича]. ; 2-е изд. – К. : гл. ред УСЭ им. М.П. Бажана, 1989. – 751 с.
226. Словник іншомовних слів / [ред. О. С. Мельничук] ; 2-е вид., виправл. і доповн. – К. : Головна редакція УРЕ, 1985. – 966 с.
227. Слухай С.В. Довідник базових термінів та понять з мікроекономіки / С. В. Слухай. – К. : Лібра, 1998. – 256 с.
228. Слуцкий Е.Е. К теории сбалансированного бюджета потребителя / Е.Е. Слуцкий // Экономико-математические методы. – М., 1963. – Вып. 1. – С. 241-271.
229. Соколов В.Ю. Кількісні показники оцінювання захищеності і ризиків від порушень безпеки у розподілених системах рухомого зв’язку / В.Ю. Соколов // Захист інформації. – 2010. – №3. – С. 42-47.
230. Соколов А.В. Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. – М. : ДМК Пресс, 2002. – 656 с.
231. Стандарт ISO:17799-00 (Стандарт Великобритании BS 7799-95 “Практические правила управления информационной безопасностью”).
232. Стасюк А.И. Использование теории нечетких множеств для выбора криптографических алгоритмов шифрования / А.И. Стасюк, А.А. Корченко, А.В. Малофеев // Захист інформації. – 2010. – Т. 12. –№ 2(47). – С. 12-20.
233. Стасюк О.І. Сучасні стеганографічні методи захисту інформації / [О.І. Стасюк, С.О. Гнатюк, Н.І. Довгич та ін.] // Захист інформації. – 2011. – Т. 13. – № 1 – С. 1-7.
234. Сычев Ю.Н. Оценивание средств защиты компьютерных систем при наличии рисков искажения экономической информации : дисс. к.э.н. : 08.00.13 / Ю.Н. Сычев. – М., 2004. – 163 с.
235. Табаков А.Б. Структурирование системы информационной безопасности: методы, модели, инструментальные средства: дисс. к.э.н. : 08.00.13 / А.Б. Табаков. – М., 2005. – 129 с.
236. Твердохліб І. Адаптація ринкових моделей споживання в умовах перехідної економіки України / І. Твердохліб // Соціально-економічні дослідження в перехідний період. Застосування статистичних методів (регіональний аспект) : щорічник наукових праць. – 1999. – Вип. Х. – С. 138-143.
237. Твердохліб І. Методика оцінки еластичності попиту на продукти в регіоні з використанням моделей споживання / І. Твердохліб // Соціально-економічні дослідження в перехідний період. Застосування статистичних методів (регіональний аспект) : щорічник наукових праць. – 1999. – Вип. ХІ. – С. 130-138.
238. Твердохліб І. Оцінка еластичності попиту на продукти в регіоні в умовах перехідної економіки за теорією збалансованості бюджету споживача Є. Слуцького / І. Твердохліб // Вісник Львівського університету. Серія економічна. – 1999. – Вип. 29. – С. 153-163.
239. Твердохліб І. Спосіб формалізації проблеми оцінювання споживання домогосподарств у регіоні за умов невизначеності інформації / І. Твердохліб, О. Коцьо // Формування ринкової економіки в Україні : наук. збірник. – 2008. – Вип. 18. – С. 185-194.
240. Твердохліб І.П. Моделювання споживання в регіоні в умовах перехідної економіки : автореф. дис… к.е.н. : 08.00.13 / І.П. Твердохліб. – Львів, 1999. –   
     20 с.
241. Твердохліб І.П. Моделювання споживання в регіоні в умовах перехідної економіки : дис... к.е.н. : 08.00.13 / І.П. Твердохліб. – Львів, 1999. – 208 с.
242. Твердохліб І.П. Оцінка ефективності функціонування регіональної системи управління з використанням моделей пріоритетного споживання / І.П. Твердохліб // Автоматика-98 : праці 5 Української конф. з автоматичного управління. – К. : НТУУ “Київський політехнічний інститут”, 1998. – Ч.2. – С. 231-235.
243. Твердохліб І.П. Удосконалення методології економіко-математичного прогнозування на підставі методів Data Mining / І.П. Твердохліб // Теорія прийняття рішень : праці ІІІ міжн. школи-семінару. – Ужгород : УжНУ, 2006. – С. 84-85.
244. Теория потребительского поведения и спроса. Серия “Вехи экономической мысли” ; под ред. В. М. Гальперина. – С.-Петербург : Экономическая школа, 1993. – Вып. 1.– 1380 с.
245. Терейковський І. Нейромережева методологія розпізнавання Інтернет-орієнтованого шкідливого програмного забезпечення. / І. Терейковський // Безпека інформації. – 2013. – Т. 19. – №1. – С. 24-28.
246. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1-003-99. – К. : ДСТСЗІ СБ України, 1999. – 30 с.
247. Тигров В. Пять способов взломать (и защитить) сети “by Microsoft” / В. Тигров // Защита информации. Inside. – 2010. – № 2. – С. 62-66.
248. Тихонов В.А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты : учеб. пособие / В.А. Тихонов, В.В. Райх. – М. : Гелиос АРВ, 2006. – 528 с.
249. Топилин Я.Н. Положение о порядке организации и проведении работ по обеспечению безопасности персональных данных при их обработке в организации / Я.Н. Топилин, А.М. Хабаров // Защита информации. Inside. – 2010. – № 2. – С. 20-27.
250. Украинский А.П. Функции и задачи систем идентификации утечки информации в информационных системах / А.П. Украинский , А.С. Петров // Інформаційна безпека. – 2010. – № 1(3). – С. 124-127.
251. Учебник по защите от хакеров // CD “Эксперт: криптографическая защита данных”. – Новые технологи, 2004. – 2,12 Мб.
252. Хоффман Л. Современные методы защиты информации : [пер. с англ.] / Л. Хоффман ; под ред. В.А. Герасименко. – М .: Сов. радио, 1980. – 264 с.
253. Цимбалюк В.С. Основи інформаційного права України : навч. посібник / [B.C. Цимбалюк, В.Д. Гавловський, В.В. Гриценко та ін.]; за ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. – К. : Знання, 2004. – 274 с.
254. Чаки Ф. Современная теория управления: нелинейные, оптимальные и адаптивные системы : [пер. с англ.] / Ф. Чаки. – М. : Мир, 1975. – 424 с.
255. Чекурін В.Ф. Взаємодія об’єктів і аналіз загроз інформаційній безпеці систем електронного навчання / В.Ф. Чекурін, О.О. Будік // Вісник Східноукраїнського національного університету ім. В. Даля. – 2011. – №7(161). – Ч. 1. – С. 112-119.
256. Черваньов Д.М. Методичний посібник з курсу “Мікроекономічне моделювання” на тему “Теорія особистого споживання” / [Д.М. Черваньов, О.О. Карагодова, А.М. Романенко  та ін.]. – К. : РВВ КІЕМБСС, 1998. – 28 с.
257. Черноморец В.А. Анализ угроз техногенным обьектам / В.А. Черноморец, С.К. Горбунов, Н.С. Сташкова // Комп’ютерні засоби, мережі та системи. – 2002. – №1. – С. 119-126.
258. Черняєв Ю.Б. Злочинність і правоохоронна діяльність як об'єкти економічного аналізу / Ю.Б. Черняєв, В.П. Мазуренко // Актуальні проблеми економіки. – 2012. – №3. – С. 297-304.
259. Чертов О.Р. Виявлення спроб шахрайства в системах контекстної реклами / О.Р. Чертов, Д.Г. Павлов, В.В. Мальчиков // Вісник Східноукраїнського національного університету ім. В. Даля. – 2010. – №9(151). – Ч. 1. – С. 101-105.
260. Чертов О.Р. Методи захисту конфіденційної інформації в мікрофайлах / О.Р. Чертов // Вісник Східноукраїнського національного університету імені В. Даля. – 2009. – № 6(136). – Ч. 1. – С. 16-19.
261. Чипига А.Ф. Оценка эффективности защищенности автоматизированных систем от несанкционированного доступа / А.Ф. Чипига, В.С. Пелешенко // Вестник Северо-Кавказкого государственного технического университета. – 2000. – № 1(8). – С. 180-182.
262. Чорноус Г.О. Рівняння Слуцького в сучасній мікроекономічній теорії / Г.О. Чорноус, А.В. Ставицький ; за ред. В.Д. Базилевича. – К. : Знання, 2007. – С. 121-141.
263. Шелестов А.Ю. Обеспечение безопасности GRID-систем на основе модели поведения пользователей. / А.Ю. Шелестов, С.И. Лавренюк // Кибернетика и вычислительная техника. – 2009. – Вып. 156. – С. 87-96.
264. Шляхтина С. Рынок ПО для обеспечения безопасности [Электронный ресурс] / С. Шляхтина // Компьютер Пресс. – 2007. – Режим доступа : <http://www.compress.ru/article.aspx?id=17360&iid=805>.
265. Шорошев В.В. Нова архітектура системи захисту інформації в комп’ютерних системах від несанкціонованого доступу / В.В. Шорошев // Інформаційна безпека. – 2009. – № 2(2). – С. 45-58.
266. Щеглов А.Ю. Защита компьютерной информации от несанкционировоного доступа / А.Ю. Щеглов. – С.-Петербург : Наука и техника, 2004. – 384 с.
267. Юдін О.К. Методи виявлення атак до інформаційних ресурсів автоматизованих систем / О.К. Юдін, Е.О. Коновалов, І.Є. Рогоза // Захист інформації. – 2010. – Т. 12. – № 2(47). – С. 5-12.
268. Якушев В. Антихакер / В. Якушев // Львівська газета. – 18 квітня 2013 року. – №16(717). – С. 19.
269. Ясинчук Л. На наші гроші полюють шахраї! / Л. Ясинчук // Газета “Експрес”. – 18.10.2013 – 20.10.2013. – № 115(7211). – С. 1, 8.
270. Ястремський О.І. Основи теорії економічного ризику : навч. посібник / О.І. Ястремський. – К. : Артек, 1997. – 248 с.
271. Aggarwal C. C. Privacy-Preserving Data Mining: Models and Algorithms / C. C. Aggarwal, P. Ыю Yu. – New York: Springer. – 2008. – 535 p.
272. Bohme R. The iterated weakest link / R. Bohme, // IEEE Security & Privacy. – 2010. – Vol. 8, № 1. – P. 53-55.
273. Böhme Moor. The iterated weakest link: A model of adaptive security investment / Moor Böhme //WEIS, London, 24 June. – 2009. – P.
274. Cohen F. Computer Viruses: theory and experiments / F. Cohen // DOD/NBS 7th Conference on Computer Security, 1984. – Computers and Security, 1987. – Vol. 6, iss. 1. – P. 22–35.
275. Deaton A.S. An Almost Ideal Demand System / Deaton A.S., Muellbauer I. // American Economic Review. – 1980. – Vol. 70. – P. 312-326.
276. Garbarczuk W. Projectowanie systemow ochrony informacji / Garbarczuk W., Swic A., Wojcik W. – Lublin: Wyd.Politechniki Lubelskiej, 2006. – 218 s.
277. Gordon L. A. The economics of information security investment / L. A. Gordon, M. P. Loeb // ACM Transactions on Information and System Security. – 2002. – Vol. 5, № 4. – P. 438-457.
278. How CRAMM works [Electronic resource]. – Available from:http://www.cramm.com/.
279. Huang C.D. Economics of information security investment in the case of simultaneous attacks / D.C. Huang, Q. Hu, R.S. Behara //Proceeding of the 5-th workshop on the economics of information security, Cambridge, England< June 26-28. – 2006. – P. 1-33.
280. Huffman S. K. Re-evaluation of Welfare Changes during the Transition in Poland [Electronic resource] / Sonya Kostova Huffman, Stanley R.Johnson // Center for Argiculture and Pural Development Jowa State University. – November 2000 [OO-WP 255]. – 34 p. – Available from: <http://www.card.iastate.edu/publications>.
281. ISO/IECTR 13335–1: 1996 (E) «Information technology–Guidelines for the management of it Security». – ISO/IEC, 1996. – Part 1. – 132 p.
282. Kotenko I. V. Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle / I. V. Kotenko, M. V. Stepashkin // Lecture Notes in Computer Science. – 2005. – Vol. 3685. – P. 311-324.
283. Lewbel A. Demand System With Nonstationary Prices / Arthur Lewbel, Serena Ng // The Review of Economics and Statistics. – 2005. – Vol. 87, iss. 3. – P. 479-494.
284. Lye K. Game Strategies in Network Security / K. Lye, J. Wing // International Journal of Information Security. – 2005. – Vol. 4, iss. 1-2. – P. 71-86.
285. Matsuura K. Productivity space of information security in an extension of the Gordon-Loeb’s investment model / K. Matsuura // The 7th workshop on the economics of information security, Hanover, USA, June 25-28-2008 [Electronic resource] – Available from: <http://weis2008.econinfosec.org/papers/Matsuura.pdf>.
286. OECD. Guidelines for the Security of Information Systems and Networks towards a Culture of Security [Electronic resource]. – Paris: OECD, July 2002. – Available from : [www.oecd.org](http://www.oecd.org).
287. Official RiskWatch site [Electronic resource]. – Available from: http://www.riskwatch.com/.
288. Trusted System Evaluation Criteria: CSC-STD-001-83. – National Computer Security Center, 1983. – 112 p.
289. Willenborg L. Elements of Statistical Disclosure Control: Series: Lecture Notes in Statistics. V. 155 / L. Willenborg, T. de Waal. – New York: Springer-Verlag. – 2001. – 261 p.