

В.Л. БУРЯЧОК

**ОСНОВИ ФОРМУВАННЯ
ДЕРЖАВНОЇ СИСТЕМИ КІБЕРНЕТИЧНОЇ
БЕЗПЕКИ**

Видавництво "Магнолія 2006"

Львів

УДК 351.86:004.056

Б 91

*Рекомендовано до друку на засіданні вченої ради
Національного авіаційного університету*

Автор: канд. техн. наук, ст. наук. співроб. Бурячок В.Л.

Рецензенти: докт. техн. наук, проф. Козловський В.В.

докт. техн. наук, проф. Рибальський О.В.

докт. техн. наук, проф. Хорошко В.О.

Б 91 Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – Львів: «Магнолія 2006» – 432 с.

ISBN 978-617-574-129-0

У монографії надаються основні аспекти формування системи кібернетичної безпеки України, що ґрунтуються на методах оцінювання рівня захищеності власних ІТ систем від впливу внутрішніх і зовнішніх кібернетичних втручань та загроз, а також злому систем захисту протиборчих, методах отримання суспільно значущої інформації з відкритих, відносно відкритих і закритих електронних джерел та автоматизації усіх, супутніх цьому процесів (пошуку, збору, добування, оброблення тощо). Розглядається процес захисту національної інфосфери від стороннього кібернетичного впливу, а також пропонується відповідний нормативний апарат.

Монографія розрахована на широке коло фахівців у галузі інформаційної і кібербезпеки. Викладений матеріал має стати у пригоді науково-педагогічним працівникам, які займаються плануванням і прогнозуванням процесів розвідки інформації та її захисту, а також аспірантам і студентам вищих навчальних закладів, які навчаються за спеціальностями освітнього напрямку “Інформаційна безпека”.

ISBN 978-617-574-129-0

© Бурячок В.Л.

© «Магнолія 2006»

ЗМІСТ

	стор.
ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	6
ПЕРЕДМОВА	7
РОЗДІЛ 1 АНАЛІЗ СТАНУ БОРОТЬБИ У КІБЕРПРОСТОРИ	8
1.1 Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства	10
1.2 Інформаційне протиборство, як закономірний та об’єктивний процес у досягненні цілей державної політики в мирний і воєнний час. Кібернетична війна, як основна форма сучасного протиборства в інформаційній сфері	23
1.3 Еволюція та особливості реалізації атак у кіберпросторі. Основні заходи щодо послаблення їх деструктивного впливу	36
РОЗДІЛ 2 РОЛЬ І МІСЦЕ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ В ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА У КІБЕРПРОСТОРИ	62
2.1 Структура СІТС та призначення її основних підсистем і компонент. Місце комп’ютерних мереж СІТС у розвитку сучасного інформаційного суспільства	63
2.2 Метод аналізу рівня захищеності СІТС від стороннього кібернетичного впливу: механізм виявлення загроз та реагування на їх можливі прояви. Оцінювання ступеня порушення системи захисту інформації у СІТС за метою реалізації	71
2.3 Методи і засоби несанкціонованого отримання інформації з СІТС	87
2.4 Критерії і показники оцінювання якості функціонування СІТС	95
РОЗДІЛ 3 ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ І ПРОВЕДЕННЯ РОЗВІДУВАЛЬНОЇ ДІЯЛЬНОСТІ У КІБЕРПРОСТОРИ	104
3.1 Розвідка систем телекомунікацій. Технологія проведення атак на програмну реалізацію криптосистеми шляхом перехоплення звернень CPU до RAM	105
3.2 Мережева розвідка інформаційно-телекомунікаційних систем. Технологія організації і проведення МР з використанням уразливостей Web-ресурсів	116
3.3 Кібернетична розвідка ІТС: складові, технологія організації і проведення кіберрозвідки	124
3.4 Технологія організації збору та добування інформації у	

	кіберпросторі: метод проведення інформаційного пошуку та процедура його реалізації. Роль і місце у цьому процесі роботизованих “процесорів” (спайдер-комплексів)	147
3.5	Технологія організації обробки, аналізу і синтезу інформації про об’єкт розвідки у кіберпросторі: метод обробки інформаційних матеріалів ЗМІ	162
3.6	Критерії і показники оцінювання ефективності розвідки у кіберпросторі.....	171
РОЗДІЛ 4 ШЛЯХИ ПОБУДОВИ СПЕЦІАЛЬНИХ ПРОГРАМНО-АПАРАТНИХ КОМПЛЕКСІВ РОЗВІДКИ У КІБЕРПРОСТОРИ		175
4.1	Склад і функціональна структура перспективного спеціального програмно-апаратного комплексу кібернетичної розвідки	176
4.2	Метод оцінювання технічних засобів перспективного СПАККР та вибору серед них раціонального варіанту для комплектування технічної компоненти комплексу	189
4.3	Методика формування раціонального кошика замовлень програмних засобів перспективного СПАККР та вибору серед них раціонального варіанту для комплектування програмної компоненти комплексу	197
4.3.1	Формування набору показників для оцінювання якості ПЗ перспективного СПАККР	198
4.3.2	Метод порівняльного оцінювання якості ПЗ перспективного СПАККР за змішаними показниками	206
4.3.3	Пропозиції щодо впровадження до складу перспективного СПАККР програмних (програмно-апаратних) засобів ведення розвідки у кіберпросторі	218
4.4	Метод порівняльного оцінювання альтернативних варіантів побудови перспективного СПАККР	223
РОЗДІЛ 5 МЕТОДИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У СОЦІОТЕХНІЧНИХ СИСТЕМАХ КІБЕРПРОСТОРИ		230
5.1	Методи прийняття рішень в умовах повної визначеності	233
5.2	Методи прийняття рішень в умовах активної, пасивної і компромісної невизначеності	268
5.3	Методи оцінювання ризику при прийнятті управлінських рішень	283
5.4	Методи комплексного оцінювання результатів прийнятих рішень	291
РОЗДІЛ 6 НАПРЯМИ ОРГАНІЗАЦІЇ І ПРОВЕДЕННЯ ЕКСПЕРТНОГО ОЦІНЮВАННЯ ІНФОРМАЦІЇ У СОЦІОТЕХНІЧНИХ		

	СИСТЕМАХ КІБЕРПРОСТОРУ	295
6.1	Формування задачі експертного оцінювання. Головні етапи її реалізації	298
6.2	Процедура формування експертної групи та методи оцінювання компетентності її представників	301
6.3	Методи індивідуального і колективного одержання вихідної інформації евристичного походження. Їх основні переваги та недоліки	310
6.4	Математичні методи опрацювання вихідної інформації евристичного походження	325
6.5	Аналіз матеріалів експертного оцінювання. Визначення ступеня погодженості суджень групи експертів та їх статистичної достовірності	338
6.6	Парето-аналіз множини альтернатив	346
	РОЗДІЛ 7 ТЕХНОЛОГІЯ ЗАХИСТУ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ СФЕРИ ВІД СТОРОННЬОГО КІБЕРНЕТИЧНОГО ВПЛИВУ	349
7.1	Основні суб'єкти державної інформаційної інфраструктури. Співробітництво України з провідними державами світу в сфері кіберзахисту	351
7.2	Технологія захисту інфосфери України від стороннього кібернетичного впливу: формування національної стратегії кібернетичної безпеки, завдання суб'єктам інформаційної інфраструктури з питань своєчасного виявлення та адекватного реагування на комп'ютерні інциденти	358
7.3	Формування вимог до системи кібернетичної безпеки об'єкту інформаційної діяльності: стратегія оцінювання рівня кіберпотужності ОІД в умовах стороннього кібервпливу та реагування на його прояви	373
7.4	Техніко-економічний аналіз рішень, що приймаються при створенні системи кібербезпеки об'єкту інформаційної діяльності та види витрат, необхідних для цього	387
	ПІСЛЯМОВА	392
	СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	394
Додаток А	Перелік можливих загроз інформації, що обробляється в СІТС та циркулює у відповідних приміщеннях	421
Додаток Б	Навчання Cyber Storm та Cyber Europe: мета, хід і результати	425
Додаток В	Перелік основних термінів та визначень	428

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АРМ	–	автоматизоване робоче місце
АС	–	абонентська система
АСУ	–	автоматизована система управління
БД (БнД)	–	база даних (банк даних)
ЕМВ	–	електромагнітні випромінювання
ЕОТ	–	електронна обчислювальна техніка
ЗМІ	–	засоби масової інформації
ЗПЗ	–	загальне програмне забезпечення
ІзОД	–	інформація з обмеженим доступом
ІКТ	–	інформаційно-комунікаційна технологія
ІОС	–	інформаційно-обчислювальна система
ІПД	–	інформаційно-пошукові дослідження
ІПС	–	інформаційно-пошукова система
ІР	–	інформаційний ресурс
ІРМ	–	інформаційні і розвідувальні матеріали
ІТС	–	інформаційно-телекомунікаційна система
КМ	–	комп'ютерна мережа
КР	–	кіберрозвідка
ЛОМ	–	локальна обчислювальна мережа
МПЗ	–	мережеве програмне забезпечення
МР	–	мережева розвідка
НСД	–	несанкціонований доступ
ОС	–	операційна система
ПЕОМ	–	персональна ЕОМ
ПОД	–	пошуковий образ документа
ПОЗ	–	пошуковий образ запиту
ПСП	–	підрозділи спеціального призначення
РСт	–	розвідка систем телекомунікацій
СЗІ	–	система захисту інформації
СІТС	–	ІТС спеціального призначення
СПАККР	–	спеціальний програмно-апаратний комплекс кіберрозвідки
СПЗ	–	спеціальне програмне забезпечення
СУБД	–	системи управління базами даних
ТЗ	–	технічний засіб
ФІП	–	формула інформаційного пошуку

ПЕРЕДМОВА

Події кінця XX – початку XXI сторіччя проходять на фоні трансформації суспільства від постіндустріального до інформаційного. Відбувається бурхливий розвиток та формування глобальної інфраструктури інформаційних технологій (ІТ), що супроводжується інтенсифікацією інформаційних процесів та їх проникненням у всі сфери діяльності людини – соціальну, економічну, політичну тощо, збільшенням залежності приватних осіб, організацій та переважної більшості країн світу від інформаційних систем і мереж, а також підвищенням ступеня їх уразливості від стороннього кібернетичного впливу. Завдяки революції в області інформатизації і комунікацій відбуваються значні зміни у військовій справі. З'являються нові види озброєння, засновані на застосуванні ІТ, які дозволяють вести неконтактні бойові дії. Розвиваються засоби розвідки та захисту інформації, автоматизовані системи управління військами і зброєю. Розробляються нові концепції ведення воєнних конфліктів, удосконалюються форми і способи застосування військ. Все це, як результат:

по-перше, веде до зміни сучасної картини світу інформатизації, а також до появи нових технологічних і комп'ютерних ризиків безпеки;

по-друге, примушує більшість країн світу до формування наряду з існуючими інформаційними власних систем кібернетичної безпеки (кібербезпеки).

Зважаючи на відсутність відповідного нормативно-правового базису та системних досліджень у цьому напрямку, а також недостатньо формалізовані основи такої діяльності проблема з розроблення основ формування системи кібербезпеки України, яка б забезпечувала захист національних інтересів в інформаційній сфері та окремої особистості нашої держави і суспільства у цілому від стороннього кібернетичного впливу – є надзвичайно актуальною. У монографії запропоновано широкий спектр понять і визначень з кіберпроблематики, системно і послідовно описано низку завдань, які мають бути враховані при розробленні стратегії і концепції кібернетичної безпеки України, формалізовано процес захисту інфосфери України від стороннього кібервпливу за рахунок удосконалення існуючих методів оцінювання рівня захищеності власних ІТ систем від внутрішніх і зовнішніх кібернетичних втручань та загроз, а також злову систем захисту протидіючих, розроблення нових методів отримання суспільно значущої інформації з відкритих, відносно відкритих і закритих електронних джерел та автоматизації усіх, супутніх цьому процесів.

Автор висловлює щиро подяку професорам Козловському В.В. (Інститут спеціального зв'язку та захисту інформації НТУУ “КПІ”), Рибальському О.В. (Національна академія внутрішніх справ) і Хорошко В.О. (Національний авіаційний університет), зауваження і поради яких дали можливість суттєво покращити роботу та уникнути ряду помилок.

НАУКОВЕ ВИДАННЯ

Володимир Леонідович Бурячок

**ОСНОВИ ФОРМУВАННЯ ДЕРЖАВНОЇ СИСТЕМИ
КІБЕРНЕТИЧНОЇ БЕЗПЕКИ**

Монографія

(українською мовою)

Формат 60x84/16. Папір офсетний. Друк цифровий.
Гарнітура Times New Roman

Умовн. друк. арк. 25,11

ПП «Магнолія 2006»

м. Львів-53, 79053, Україна, тел.+380503701957

e-mail: magnol06@ukr.net

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції: серія ДК № 2534 від 21.06.2006 року, видане Державним комітетом інформаційної політики, телебачення та радіомовлення України

Надруковано у друкарні видавництва «Магнолія 2006»