В. Л. БУРЯЧОК, Г.М.ГУЛАК, В.Б.ТОЛУБКО

ІНФОРМАЦІЙНИЙ ТА КІБЕРПРОСТОРИ: проблеми безпеки, методи та засоби боротьби

П і д р у ч н и к

Видавництво ПП "Магнолія 2006"

Львів

Б 91
УДК 004.7.056.5(477)(075.8)

Гриф надано Міністерством освіти і науки України

Рекомендовано вченою радою
Державного університету телекомунікацій
до друку та використання в навчальному процесі

А в то р и:
В.Л.Бурячок, доктор технічних наук, с.н.с.;
Г.М.Гулак, кандидат технічних наук, доцент;
В.Б.Толубко, доктор технічних наук, професор

Р е ц е н з е н т и:
доктор технічних наук, професор В.А.Лужецький;
доктор технічних наук, професор О.В. Рибальський

Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки,
Б 91 методи та засоби боротьби. [Підручник]. / В. Л. Бурячок,
Г.М.Гулак, В.Б. Толубко. – Львів: «Магнолія 2006» – 448 с.

ISBN 978-617-574-127-6

У підручнику висвітлено головні ознаки таких понять, як інформаційне суспільство, інформаційний і кіберпростори, інформаційна та кібербезпека. Розкрито основи їх формування та розвитку, досліджено їх сутність, основний зміст та складові. Значну увагу приділено типовим інцидентам у сфері високих технологій, методам і засобам реалізації атак на інформаційний і кіберпростори та тим заходам, які можуть послабити їх деструктивний вплив. Розглянуто методи та засоби боротьби в інформаційному і кіберпросторах, а також досліджено особливості захисту сучасної інфосфери в умовах стороннього кібернетичного впливу.

Виклад зорієнтовано на фахівців у галузі кібернетичної безпеки. Пропонований матеріал буде корисний науковим та науково-педагогічним працівникам, профіль діяльності яких пов’язаний з питаннями забезпечення інформаційної безпеки, а також аспірантам, магістрантам і студенам вищих навчальних закладів, що спеціалізуються у сфері організації та управління інформаційною і кібербезпекою згідно з освітнім напрямому “Інформаційна безпека”.

ISBN 978-617-574-127-6

ЗМІСТ

стор.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ ……..……...… *6*

ПЕРЕДМОВА ……..……. *7*

ГЛАВА 1 ОЗНАКИ, ПРИНЦИПИ СТАНОВЛЕННЯ ТА РОЗВИТКУ СУЧАСНОГО ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА ……. *9*

1.1 Інформаційне суспільство: визначення, проблемні питання формування та розвитку ……..... *9*

1.1.1 Інформаційне суспільство – новий етап розвитку цивілізації ……. *9*

1.1.2 Інформаційне суспільство – як мета України …… *16*

1.2 Інформаційний простір – головна субстанція сучасного інформаційного суспільства …… *24*

1.2.1 Основні види інформаційного простору, його ознаки, складові та функції …….. *26*

1.2.2 Основні характеристики інформаційного простору …….... *27*

1.2.3 Основи формування єдиного інформаційного простору …….. *35*

1.3 Роль та місце інформації в системі забезпечення функціонування сучасного інформаційного суспільства …… *41*

1.3.1 Категорії інформації та її способи її класифікація …… *44*

1.3.2 Властивості інформації та міри її вимірювання …… *51*

1.3.3 Загрози безпеки інформації та можливі методи їх реалізації ……... *56*

1.4 Інформаційні системи та їх внесок у становлення сучасного інформаційного суспільства …… *60*

1.4.1 Підходи до класифікації ІС за функціональною ознакою та ознакою структурованості завдань …… *62*

1.4.2 Мета та принципи створення АІС. Їх основні завдання і функції *67*

1.4.3 Типова структура та склад АІС ……..... 71

1.5 Інформаційні технології в системі функціонування сучасного інформаційного суспільства ……..... *80*

1.5.1 Рівні розгляду та методології застосування ІТ. Їх переваги і недоліки …… *84*

1.5.2 Класифікація автоматизованих інформаційних технологій …….. *87*

Висновки до першої глави ……..……... *100*

Запитання для самоконтролю ……... *102*

ГЛАВА 2 КІБЕРПРОСТІР ТА МЕРЕЖА INTERNET: СТАНОВЛЕННЯ, СТРУКТУРА, ПРОБЛЕМНІ АСПЕКТИ ФУНКЦІОНУВАННЯ … *105*

2.1 Кіберпростір: визначення, система відношень, загрози та актори …… *106*

2.1.1 *Кібернетичне протиборство, як головна ознака сучасного кіберпростору ……* *115*

2.2 Глобальна комп’ютерна мережа Internet, як передвісник формування

кіберпростору та його головних компонент …… *123*
2.2.1 Історія створення й становлення мережі Інтернет …..…..…..….. *124*
2.2.2 Технологічні особливості та організаційна структура Інтернету . *129*
2.2.3 Територіальна структура Інтернет ……..…..…..…..…..…..…..…..….. *137*
2.2.4 Причини уразливості мережі Інтернет ……..…..…..…..…..…..…..….. *142*
2.3 Організація пошуку, збору і добування інформації в мережі Інтернет .. *144*
2.3.1 Засоби пошуку, збору та добування інформації ……..…..…..…..…..…..… *144*
2.3.2 Метод проведення інформаційного пошуку та процедура його реалізації ……..…..…..…..…..…..…..…..…..…..…..…..…..…..…..…..…..….. *162*
2.4 Процедури первинної обробки відкритої та відносно відкритої інформації, її аналізу і синтезу …….. *169*
2.4.1 Методи підтримки прийняття інформаційних рішень …….. *179*
2.4.2 Засоби та алгоритм обробки інформаційних матеріалів ЗМІ …….. *187*
2.5 Автоматизація процесів збереження і розповсюдження інформації. Класифікація та принципи створення систем електронного документообігу …….. *190*
2.5.1 Призначення, завдання, та принципи створення СЕД ……..…..…..…..….. *192*
2.5.2 Класифікація систем електронного документообігу ……..…..…..…..….. *193*
2.5.3 Особливості вибору та впровадження СЕД ……..…..…..…..…..…..….. *198*
Висновки до другої глави …… *215*
Запитання для самоконтролю ……... *218*
ГЛАВА 3 СИСТЕМА БЕЗПЕКИ ІНФОРМАЦІЙНОГО І КІБЕРПРОСТОРІВ: ФОРМУВАННЯ ТА РОЗВИТОК …… *220*
3.1 Національна безпека України: реалії та перспективи …….. *222*
3.1.1 Визначення та основні категорії теорії національної безпеки ……..….. *223*
3.1.2 Характеристика основних рівнів та видів національної безпеки.….. *233*
3.2 Роль і місце інформаційної безпеки у загальній системі нацбезпеки . *237*
3.2.1 Концептуальна модель ІБ, етапи її реалізації та методи вирішення *239*
3.2.2 Загрози інформаційній безпеці. Класифікація та методи реалізації *242*
3.2.3 Критерії класифікації загроз ІБ та функціональних послуг …… *246*
3.3 Роль та місце кібернетичної безпеки у загальній системі нацбезпеки ... *251*
3.3.1 Заходи України щодо створення сучасної системи кібербезпеки ….. *258*
3.4 Інциденти інформаційної і кібербезпеки: характерні ознаки та проблемні аспекти ……..……..…….. *273*
3.4.1 Поняття, ознаки та основні метрики оцінювання інцидентів інформаційної безпеки ……..…..…..…..…..…..…..…..…..…..…..…..…..….. *273*
3.4.2 Аналіз впливу інцидентів на функціонування сучасної інфосфери … *281*
3.4.3 Процес управління інцидентами інформаційної безпеки в організаційно-технічних системах ……..…..…..…..…..…..…..…..…..…..….. *287*
3.4.4 Нормативно-правове забезпечення процесу управління

інцидентами ІБ *305*
3.5 Еволюція та особливості реалізації атак в ІКС. Основні напрями захисту інформації в інформаційному і кіберпросторах *308*
3.5.1 Класифікація кібератак *309*
3.5.2 Заходи протидії деструктивному впливу кібератак *324*
Висновки до третьої глави *330*
Запитання для самоконтролю *331*
ГЛАВА 4 ЗАСОБИ ТА СПОСОБИ БОРОТЬБИ В ІНФОРМАЦІЙНОМУ І КІБЕРПРОСТОРАХ *334*
4.1 Інформаційна боротьба: основні цілі та методи їх досягнення ... *335*
4.1.1 Аспекти інформаційної боротьби *335*
4.1.2 Інформаційне протиборство, як головна форма інформаційної боротьби *338*
4.1.3 Оцінка ефективності інформаційної боротьби *349*
4.2 Кібервійна та кібертероризм, як одні з найбільших загроз сучасності *351*
4.2.1 Визначення та головні аспекти ведення кібервоєн *351*
4.2.2 Кібертерроризм: прояви і тенденції поширення, можливі заходи протидії *360*
4.3 Досвід застосування інформаційної та кібернетичної зброї у ході останніх конфліктів сучасності *371*
4.3.1 Участь КНР у світовому протистоянні в інформаційній сфері *372*
4.3.2 Участь Росії в інформаційних і кіберконфліктах сучасності: Чечня, Грузія, Естонія, Україна *375*
4.3.3 Інформаційне і кіберпротиборство між США, Росією та Китаєм *388*
4.4 Заходи провідних країн світу щодо захисту власної інформаційної сфери від деструктивного кібернетичного впливу *391*
4.4.1 Заходи США щодо захисту власного кібернетичного простору ... *391*
4.4.2 Заходи керівництва НАТО щодо захисту кібернетичного простору Північноатлантичного альянсу *401*
Висновки до четвертої глави *413*
Запитання для самоконтролю *416*
ПІСЛЯМОВА *418*
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ *420*
Додаток А Проблемні питання у розвитку інформаційого суспільства України та пропозиції щодо їх вирішення (витяг) *432*
Додаток В Перелік основних термінів та визначень *444*

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АРМ	–	автоматизоване робоче місце
АСУ	–	автоматизована система управління
БД (БнД)	–	база даних (банк даних)
ДРР	–	дешифрувально-розвідувальна робота
ЕОМ	–	електронна обчислювальна машина
ЗІ	–	захист інформації
ЗПЗ	–	загальне програмне забезпечення
ІзОД	–	інформація з обмеженим доступом
ІКТ	–	інформаційно-комунікаційна технологія
ІБ	–	інформаційна безпека
ІТ	–	інформаційна технологія
ІР	–	інформаційний ресурс
ІТС	–	інформаційно-телекомунікаційна система
ІС	–	інформаційна система
КБ	–	кібернетична безпека
КР	–	кібернетична розвідка
КСЗІ	–	комплексна система захисту інформації
ЛОМ	–	локальна обчислювальна мережа
МР	–	мережева розвідка
НСД	–	несанкціонований доступ
ОС	–	операційна система
ПАК	–	програмно-апаратний комплекс
ПЕОМ	–	персональна ЕОМ
ПІБ	–	політика інформаційної безпеки
ПЗ	–	програмне забезпечення
РІ	–	розвідувальна інформація
РІТС	–	розвідка інформаційно-телекомунікаційних систем
Рст	–	робоча станція
СІ	–	соціальний інжиніринг
СЗІ	–	система захисту інформації
СПЗ	–	спеціальне програмне забезпечення
СУБД	–	системи управління базами даних
ТЗІ	–	технічний захист інформації

ПЕРЕДМОВА

Глобальна інформатизація останнім час активно управляє існуванням і життєдіяльністю держав світового співтовариства, а інформаційні технології все частіше застосовуються при рішенні завдань забезпечення національної безпеки. Одним з фундаментальних наслідків цих процесів стало виникнення принципово нового середовища – кіберпростору.

Стрімко наростаючий у світі інтерес до проблематики кіберпростору багато в чому пов'язаний з активністю найбільш розвинених країн світу в питаннях тактики і стратегії ведення збройної боротьби, а також забезпечення безпеки критично важливих об'єктів їхньої економіки від внутрішніх і зовнішніх інформаційних та кібернетичних загроз. І якщо сьогодні між провідними у військовому і економічному відношенні світовими державами зложився певний паритет в області застосування звичайних озброєнь і зброї масового ураження, у міжнародному праві зафіксовані основні принципи взаємин цих держав у рамках таких просторів, як наземне, морське, повітряне та космічне, то питання про міждержавний паритет і взаємини в кіберпросторі на теперішній час продовжують залишатися відкритими. Це пояснюється насамперед наявністю факторів невизначеності вихідної інформації про розвиток науково-технічного прогресу, переходом від екстенсивних до інтенсивних шляхів підвищення ефективності розвитку інформаційного суспільства, а також доволі справедливим твердженням про те, що війни XXI століття будуть кібернетичними за своєю основною суттю.

У процесі формування глобального кіберпростору відбувається конвергенція військових і цивільних комп'ютерних технологій, у провідних закордонних державах інтенсивно розробляються нові засоби й методи активного впливу на інформаційну інфраструктуру потенційних супротивників, створюються різні спеціалізовані кібернетичні центри і підрозділи керування (командування), основним завданням яких є підготовка й проведення активних деструктивних дій в інформаційних системах супротивника, а також захист власних систем від подібного впливу. Терміни й визначення із приставкою «кібер...» останнім часом широко використовуються як у міжнародних, так і у внутрішньодержавних дискусіях і документах. Останнім часом вони знайшли своє відбиття в стратегічних доктринах окремих держав і міжнародних організацій, включаючи НАТО. Так, наприклад, Пентагон офіційно визнав кіберпростір новим полем можливих бойових дій, НАТО дорівнює кібератаки на країну-члена альянсу до збройного нападу, а їх фахівці в області інформаційних технологій одностайно відзначають той факт, що

«держава, яка контролює кіберпростір, буде контролювати війну й мир».

Як наслідок, для будь-якої держави безпека в кіберпросторі й насамперед кібернетична безпека (кібербезпека) стають гострою й специфічною проблемою в забезпеченні своєї національної безпеки й захисті своїх інтересів. Це приводить до того, що кібербезпека все частіше розглядається, як стратегічна проблема, яка комплексно зачіпає економіку країни, у тому числі взаємодію національних розроблювачів програмного забезпечення й систем керування, виробників устаткування й компонентів для забезпечення інформаційно-комунікаційної інфраструктури, низька ринкова конкурентоспроможність яких приводить до необхідності використання рішень від іноземних виробників. На практиці дане явище приводить до стрімкого зростання залежності від ринку іноземних товарів і послуг, а також до зниження рівня інформаційного захисту у виді змушеного використання «закритого» програмного й апаратного забезпечення у всіх сегментах інфраструктури як для спеціальних державних відомств, так і цивільного сектора. З погляду економіки дане явище, позитивно впливаючи на розвиток електронної промисловості й реального сектора, створює реальну загрозу для національної безпеки, переводячи її під контроль іноземних спеціальних служб.

Для того щоб національна безпека України могла відповідати рівню провідних економічних держав, необхідні як послідовні дії з боку держави, спрямовані на підвищення ефективності й розвиток системи взаємодії учасників ІКТ-галузі та забезпечення безпеки критично важливих об’єктів інформаційної та кіберінфраструктур, так й приділення підприємствами та організаціями нашої держави більшої уваги до питань власної інформаційної і кібербезпеки.

Автори висловлюють щиру вдячність професорам Лужецькому В.А. (Вінницький Національний технічний університет) та Рибальському О.В. (Національна академія Міністерства внутрішніх справ України), зауваження і поради яких сприяли значному покращенню та поглибленню викладеного у підручнику матеріалу. Крім того автори висловлюють подяку за співробітництво та поради спеціалістам СБ України, Служби зовнішньої розвідки, а також Державної служби спеціального зв’язку та захисту інформації.

НАВЧАЛЬНЕ ВИДАННЯ

Володимир Леонідович БУРЯЧОК
Геннадій Миколайович ГУЛАК
Володимир Борисович ТОЛУБКО

ІНФОРМАЦІЙНИЙ ТА КІБЕРПРОСТОРИ: проблеми безпеки, методи та засоби боротьби

Підручник

(українською мовою)

Формат 60x84/16. Папір офсетний. Гарнітура
Times New Roman
Умовн. друк. арк. 26,04.

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»