В.М. Богуш
О.К. Юдін

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

WWW.MK-PRESS.COM

В. М. Богуш, О. К. Юдін

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

"МК-Прес"
Київ, 2005

ББК 32.973
Б74
УДК 355.40

Рецензенти

- Академік Академії зв'язку України, академік Міжнародної академії інформатизації асоційованого члену ООН, завідувач кафедрою УДАЗТ, д т н., професор Поляков П.Ф.
- Професор кафедри організації розслідування злочинів НАВСУ, к.ю.н., доц., полковник міліції Біленчук П.Д.

Рекомендовано Міністерством освіти і науки України як навчальний посібник за напрямом 1601 "Інформаційна безпека"

Богуш В. М., Юдін О. К.

Б74 Інформаційна безпека держави. — К.: "МК-Прес", 2005. — 432с., іл.

ISBN 966-8806-05-0

В книзі наведена систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення. Визначене місце інформаційної безпеки в загальній системі національної безпеки, вплив дестабілізуючих факторів та інформаційних загроз на безпеку особистості, суспільства та держави, основи інформаційного протиборства та інформаційної боротьби, зміст і форми психологічних операцій та інформаційно-психологічної безпеки, а також загальні підходи до забезпечення безпеки інформаційних технологій. Детально розглядаються основні положення інформаційної безпеки України, способи та форми її забезпечення.

Призначається для студентів, що навчаються за усіма спеціальностями освітнього напряму "Інформаційна безпека".

ББК 32.973

Богуш Володимир Михайлович
Юдін Олександр Костянтинович

Інформаційна безпека держави

Головний редактор: Ю. О. Шпак

Підписано до друку 06.09.2005. Формат 60 × 90 1/16. Папір газетний. Друк офсетний. Ум. друк. л. 27. Обл.-вид. л. 25,8. Тираж 1000 екз. Замовлення № 5-1523

ПП Савченко Л.О., Україна, м.Київ, тел./ф.: (044) 517-73-77; e-mail: info@mk-press.com.
Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавників, виготівників та розповсюджувачів видавничої продукції:
серія ДК №51582 від 28.11.2003 р.

Надруковано в ЗАТ "ВІПОЛ". 03151, м. Київ, вул. Волинська, 60

ISBN 966–8806-05-0

Зміст

Вступ

На початок XI сторіччя припадає революційна фаза розвитку суспільства — на зміну індустріальному суспільству приходить інформаційно-індустріальне суспільство, в якому велике значення набувають системи розповсюдження, зберігання і обробки інформації. Відображаючи реальну дійсність, інформація проникає в усі напрямки діяльності держави, суспільства, громадянина.

З появою нових інформаційних технологій, заснованих на широкому впровадженні засобів обчислювальної техніки, зв'язку, систем телекомунікації, вона стає постійним і необхідним атрибутом забезпечення діяльності держави, юридичних осіб, суспільних об'єднань і навіть пересічних громадян. Дійсно, системи електронного документообігу в державних установах, система електронних платежів, карткова система сплати телефонних дзвінків, телевізор із телетекстом або телефонні та відеотелефонні розмови через Internet уже стали часткою повсякденного життя.

Іншою стороною цих процесів є збільшення кількості цінної інформації, яка обробляється в автоматизованих системах, від якості, достовірності і оперативності одержання якої залежить більшість важливих рішень, що приймаються на різних рівнях — від голови держави до громадянина. Як наслідок — нормальне життя суспільства все більше залежить від правильності функціонування таких інформаційних систем. Більш того, вони стають і найважливішим об'єктом для атаки з боку сил, ворожих для суспільства (або окремої держави). Інформаційна сфера стає не тільки однією з найважливіших сфер міжнародного співробітництва, але і об'єктом суперництва.

Інформаційний вплив на державу, суспільство, громадянина зараз більш ефективний і економний, ніж політичний, економічний і навіть воєнний. Країни з більш розвиненою інформаційною інфраструктурою, установлюючи технологічні стандарти й, надаючи покупцям свої ресурси, визначають умови формування і діяльності інформаційних структур в інших країнах, здійснюють суттєвий вплив на розвиток їхніх інформаційних сфер. При формуванні державної інформаційної політики і програми входження в інформаційне суспільство одним із найбільших пріоритетів стає розвиток і гарантування безпеки інформаційної сфери на основі створення державної системи інформаційної безпеки.

Навчальний посібник відображає сучасні погляди на стан та забезпечення інформаційної безпеки особистості, суспільства та держави. Причому інформаційна безпека особистості це, насамперед, захищеність психіки і свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до самогубства, образ і т.ін. Інформаційна безпека держави (суспільства) характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (політики, економіки, науки, техносфери, сфери управління, воєнної сфери і т.ін.) відносно небезпечних (дестабілізуючих, деструктивних, що уражають

державні інтереси і т.ін.) інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека держави визначається як здатність нейтралізувати такі впливи.

Перша частина посібника присвячена розгляду сучасних основ інформаційної безпеки держави.

Докладно окреслене місце й роль інформаційної безпеки в загальній системі національної безпеки:

- визначене поняття національної безпеки, основні категорії національної безпеки, фактори й засоби національної безпеки;
- наведена характеристика основних видів національної безпеки відповідно до її рівнів (безпека особистості, суспільства, держави) та змісту (безпека політична, економічна, соціальна, воєнна, екологічна, науково-технічна, безпека інформаційної сфери);
- визначена система забезпечення національної безпеки, функції системи та повноваження суб'єктів національної безпеки.

До основних положень інформаційної безпеки віднесені:

- визначення поняття інформаційної безпеки як інформаційної безпеки особистості, держави, суспільства та концепції інформаційної безпеки держави як систематизованої сукупності відомостей про інформаційну безпеку держави та шляхи її забезпечення;
- дестабілізуючі фактори, загрози інформаційній безпеці держави та їхні джерела;
- забезпечення інформаційної безпеки держави, методи та засоби забезпечення у формах інформаційного патронату, інформаційної кооперації та у формі інформаційного протиборства.

Інформаційне протиборство характеризується, з однієї сторони, впливом на системи добування, обробки, розповсюдження та зберігання інформації противника, а з іншої — застосуванням заходів захисту своїх подібних систем від деструктивного та керуючого впливу. Наведена загальна характеристика основних форм інформаційного протиборства: інформаційної війни, інформаційного тероризму, інформаційної злочинності.

Інформаційна війна розглядається як комплексний вплив на інформаційну сферу противника, який має за мету створення умов для ведення бойових дій (інформаційна боротьба), або як самостійний фактор, що змушує конфронтуючу державу (а не окремі державні органи) відмовитися від намічених політичних, економічних та інших цілей.

Визначені основні поняття інформаційної війни. Сформульоване поняття концепції інформаційної війни як системи поглядів на інформаційну війну та шляхи її ведення. Наведені поняття органів інформаційної війни, їхні функції та завдання, а також загальна характеристика основних форм ведення інформаційної війни на державному та воєнному рівнях.

Основи теорії інформаційної боротьби можуть бути подані загальними основами теорії інформаційної боротьби, теорією ураження інформації та теорією захисту інформації.

Власне інформаційна боротьба включає комплекс заходів інформаційного забезпечення, інформаційного захисту та інформаційної протидії, які

здійснюються за єдиним замислом і планом з метою захоплення й утримання інформаційної переваги.

Порядок і прийоми застосування сил і засобів інформаційної боротьби для захоплення й утримання інформаційної переваги над противником при підготовці і проведенні бойових дій визначається способами інформаційної боротьби, що поділяються на три основні категорії: силові, інтелектуальні та комбіновані, а також за аналогією із збройною боротьбою вони можуть бути як наступальними, так і оборонними.

Оцінка ефективності інформаційної боротьби розглядається як сукупність способів, прийомів визначення кількісних значень показників інформованості протидіючих сторін та розрахунку ступеня інформаційної переваги однієї з них над іншою у відповідності до мети інформаційної боротьби.

В окремому розділі розглядаються основи психологічної війни та інформаційно-психологічної безпеки держави:

- основні поняття психологічної війни, як складової частини інформаційної війни на державному та воєнному рівнях, складають види та закономірності психологічних впливів, зміст психологічних впливів, ефективність психологічних впливів, зміст психологічних операцій, засоби психологічних впливів та органи психологічної війни;
- технології психологічної війни, що включають вивчення особливостей об'єктів психологічних операцій, форми психологічної війни (вплив усного мовлення, друкованих та образотворчих засобів, радіо та телебачення), методи переконуючого та навіюючого впливів, а також особливі способи та прийоми, засновані на дезінформуванні, маніпулюванні свідомістю та розповсюдженні чуток та міфів;
- забезпечення інформаційно-психологічної безпеки на основі створення державної системи інформаційно-психологічної безпеки, визначення її функцій, структури, сил та засобів, а також напрямів діяльності: ліцензування, сертифікації, експертизи в галузі інформаційно-психологічної діяльності та контролю за її станом.

В заключному розділі першої частини посібника наведені основи державної інформаційної політики, які полягають у визначенні головних напрямів діяльності держави в основних галузях інформаційної сфери, змісту програми входження держави в інформаційне суспільство та політики забезпечення інформаційної безпеки.

У другій частині посібника викладені загальні основи безпеки інформаційних технологій.

В окремому розділі розглядаються основні властивості інформації як предмета захисту, основні характеристики інформаційних систем як об'єктів безпеки та основні проблеми безпеки інформаційних технологій.

Детально розглядаються фундаментальні основи безпеки інформаційних ресурсів:

- в основу класифікації загроз безпеці інформаційних ресурсів покладені збитки від реалізації загроз, наведена класифікація загроз, класифікація та ранжирування джерел загроз і уразливостей безпеці;

- як основні напрями забезпечення безпеки інформаційних ресурсів розглядаються методи та способи правового, організаційного та інженерно-технічного захисту;
- безпека мереж телекомунікації подається на основі рекомендацій міжнародної спілки електрозв'язку X.800 та стандарту міжнародної організації стандартизації ISO 7498-2 щодо архітектури безпеки в моделі взаємодії відкритих систем, приводиться опис процедур захисту та сервісних служб захисту.

Стандарти вимог і критерії оцінки захищеності інформаційних технологій призначені для взаємодії між виробниками, споживачами і експертами з кваліфікації продуктів інформаційних технологій у процесі створення та експлуатації захищених систем обробки інформації.

У посібнику надається (у хронологічному порядку) загальна характеристика критеріїв оцінки захищеності інформаційних технологій:

- Критерії безпеки комп'ютерних систем;
- Європейські критерії безпеки інформаційних технологій;
- Федеральні критерії безпеки інформаційних технологій;
- Канадські критерії безпеки комп'ютерних систем;
- Загальні критерії безпеки інформаційних технологій.

Розглядаються основні положення та складові частини Загальних критеріїв:

- потенційні загрози та типові завдання захисту;
- політика безпеки;
- продукт інформаційних технологій;
- профіль захисту;
- проект захисту;
- функціональні вимоги безпеки;
- вимоги гарантій та рівні гарантій безпеки;
- шляхи та перспективи застосування Загальних критеріїв в Україні.

В останньому розділі другої частини посібника розглядається проблема створення ефективних систем інформаційної безпеки на основі сучасних методів менеджменту, основною метою яких стало б скорочення матеріальних втрат, пов'язаних з порушенням інформаційної безпеки. Наводяться основні положення міжнародного стандарту ISO 17799, основна ідея якого — допомогти державним та комерційним організаціям вирішити достатньо складне завдання: не тільки забезпечити надійний захист інформації, але також організувати ефективний доступ до даних та нормальну роботу з ними.

У третій частині посібника розглядаються підходи до забезпечення інформаційної безпеки України.

Проведений аналіз інформаційної безпеки України:

- визначені зміст національних інтересів України в інформаційній сфері та шляхи їх забезпечення;

- наведена система загроз та їхніх джерел для інформаційної безпеки України;
- окреслений стан інформаційної безпеки в Україні та сформульовані основні завдання з її забезпечення.

Система методів та заходів забезпечення інформаційної безпеки України повинна включати загальні правові, організаційно-технічні й економічні методи та заходи, а також методи та заходи, які можуть застосовуватися у різноманітних сферах життєдіяльності держави та суспільства: у сфері економіки, внутрішньої та зовнішньої політики, оборони, духовного життя, у галузі науки і техніки, в загальнодержавних інформаційних і телекомунікаційних системах, у правоохоронній і судовій сферах, в умовах надзвичайних ситуацій.

Невід'ємною частиною інформаційної безпеки України повинне стати міжнародне співробітництво в галузі забезпечення інформаційної безпеки як складової частини політичної, воєнної, економічної, культурної та інших видів взаємодії країн, що входять до світового співтовариства.

У посібнику наведені основні функції та основні елементи організаційних основ системи забезпечення інформаційної безпеки України. Сформульовані основні положення політики інформаційної безпеки України та перелік першочергових заходів щодо її реалізації.

Посібник містить також словник додаткових термінів і понять та покажчик ключових термінів і понять. Ключові терміни та поняття інформаційної безпеки, які формулюються у основному тексті посібника та у словнику додаткових термінів і понять, виділені жирним шрифтом, а посилання на них — курсивом. Наведені англійські еквіваленти термінів і понять, а також їхня етимологія, тобто визначення походження слова шляхом зіставлення його із спорідненими словами тієї або іншої мови. Це дозволяє досить докладно окреслити предметну частину інформаційної безпеки держави та використовувати посібник як тлумачний словник.

Перелік абревіатур і скорочень

Українська мова

АСК	автоматизована система керування
ВГБ	вимога гарантій безпеки
ІПБ	інформаційно-психологічна безпека
ІС	інформаційна система
ІТ	інформаційна технологія
ЗМІ	засоби масової інформації
ЕОМ	електронно-обчислювальна машина
КПП	контрольно-пропускний пункт
МВВС	модель взаємодії відкритих систем
МОІ	мережа обміну інформацією
МОС	Міжнародна організація стандартизації
МСЕ	Міжнародна спілка електрозв'язку
НСД	несанкціонований доступ
ОЗП	оперативний запам'ятовуючий пристрій
ПЕОМ	персональна електронно-обчислювальна машина
ПРД	правила розмежування доступу
РЕЗ	радіоелектронні засоби
СЗІБ	система забезпечення інформаційної безпеки
ФВБ	функціональна вимога безпеки
ЦП	центральний процесор

Англійська мова

BIOS	Basic Input/Output System — базова система вводу-виводу
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria — Канадські критерії безпеки комп'ютерних систем
DAA	Designated Approving Authority — орган сертифікації
FCITS	Federal Criteria for Information Technology Security — Федеральні критерії безпеки інформаційних технологій
ICMP	Internet Control Message Protocol — міжмережний протокол керуючих повідомлень
IEC	International Electrotechnical Commission — Міжнародна електротехнічна комісія
IP	Internet Protocol — міжмережний протокол
ISO	International Organization for Standardization — Міжнародна організація стандартизації
IT	Information Technology — інформаційні технології

В.М. Богуш О.К. Юдін

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

Юдін Олександр Костянтинович

Кандидат технічних наук, доцент.

У 1989 р. закінчив Київський інститут інженерів цивільної авіації з напряму "Радіотехніка".

Заступник директора Інституту ІДС Національного авіаційного університету.

Член-кореспондент Академії зв`язку України.

Член експертної та науково-методичної ради Міністерства освіти та науки України в галузі "Національна безпека" (напрям 1601 "Інформаційна безпека").

Богуш Володимир Михайлович

Кандидат технічних наук, доцент.

У 1972 р. закінчив Київське вище інженерне радіотехнічне училище ППО.

Заступник директора Інституту захисту інформації Державного університету інформаційно-телекомунікаційних технологій, завідувач кафедрою Безпеки інформаційних технологій ДУІКТ.

Пресс