МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

В. Л. БУРЯЧОК, В.Б. ТОЛУБКО,
В. О. ХОРОШКО, С.В. ТОЛЮПА

ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА: соціотехнічний аспект

П і д р у ч н и к

Видавництво "Магнолія 2006"

Львів

Б 91
УДК 67.401.212я73

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

Р е ц е н з е н т и :

Щербак Л. М. – доктор технічних наук, професор,
Дудикевич В. Б. – доктор технічних наук, професор,
Самохвалов Ю. Я. – доктор технічних наук, професор,

Бурячок В. Л.
Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник].
Б 91 / В. Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С.В. Толюпа /. – Львів:
«Магнолія 2006»– 320с.

ISBN 978-617-574-126-9

У підручнику висвітлено головні принципи забезпечення інформаційної та кібернетичної безпеки, розкрито їхню сутність, основний зміст та складові.

Значну увагу приділено типовим інцидентам у сфері високих технологій, а також методам і засобам соціального інжинірингу. Докладно розглянуто систему заходів із захисту від соціотехнічних атак. Наведено порядок здійснення процедур із тестування систем захисту інформації в інформаційно-комунікаційних системах на предмет проникнення, а також порядок оцінювання їхніх параметрів на різних рівнях.

Виклад зорієнтовано на майбутніх фахівців у галузі кібернетичної безпеки.

Пропонований матеріал буде корисний науковим і науково-педагогічним працівникам, профіль діяльності яких пов’язаний із забезпеченням інформаційної безпеки, а також аспірантам, магістрантам і студентам вищих навчальних закладів, що спеціалізуються у сфері управління інформаційною безпекою та систем захисту інформації згідно з освітнім напрямом «Інформаційна безпека».

ISBN 978-617-574-126-9

ЗМІСТ

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	–	рзвідка 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

Науково-технічна революція початку XXI сторіччя спричинила в усьому світі глибокі системні перетворення. Передусім завдяки поєднанню досягнень у сфері новітніх інформаційно-комунікаційних технологій (ІКТ) із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем (ІТС), сформувалися принципово нові глобальні субстанції - інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу.

Проте через небачене досі поширення ІКТ та ІТС світова спільнота отримала не лише численні переваги, а й цілу низку проблем, зумовлених дедалі більшою вразливістю інфосфери щодо стороннього кібернетичного впливу. Тому цілком природно постала необхідність контролю та подальшого врегулювання відповідних взаємовідносин, а отже, і невідкладного створення надійної системи кібернетичної безпеки. Натомість відсутність такої системи може призвести до втрати політичної незалежності будь-якої держави світу, бо йтиметься про фактичний програш нею змагання невійськовими засобами та підпорядкування її національних інтересів інтересам протиборчої сторони. Оскільки саме ці обставини відіграють останнім часом важливу роль у геополітичній конкуренції більшості країн світу, то забезпечення кібербезпеки та злагоди в кіберпросторі стає головним завданням нашої інформаційної епохи.

Протягом останніх років Україна, як і більшість інших країн світу, робить впевнені кроки в напрямку розбудови інформаційного суспільства, забезпечення кібербезпеки та боротьби з кіберзлочинністю. Нормативно-правову базу в цих сферах діяльності становлять Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 07.09.2005 року № 2824-IV, а також відповідні закони України та Укази Президента України, присвячені цій проблемі, положення Кримінального кодексу України, окремі постанови Кабінету Міністрів та рішення РНБО України. Важливий практичний крок у реалізації наявної нормативно-правової бази було зроблено створенням 2007 року Центру реагування на комп’ютерні інциденти, що ввійшов до складу Державної служби спеціального зв’язку та захисту інформації України. На виконання статті 35 згаданої Конвенції про кіберзлочинність у червні 2009 року при Службі безпеки (СБ) України на базі спеціального підрозділу для боротьби з кіберзагрозами запрацював Національний контактний пункт формату 24/7 із реагування та обміну терміновою інформацією про вчинені кіберзлочини.

Окрім того, Указом Президента України «Про виклики та загрози національній безпеці України у 2011 році» від 10 грудня 2010 року № 1119/2010 ухвалено рішення про початок створення Єдиної загальнодержавної системи протидії кіберзлочинності. Іншим Указом Президента України «Про внесення змін до деяких законів України про структуру і порядок обліку кадрів Служби безпеки України» від 25 січня 2012 року № 34 у структурі СБ України створено Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки. З огляду на динаміку поширення комп'ютерних інцидентів теренами України в липні 2010 року у структурі МВС України на базі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, утворено новий структурний підрозділ - Департамент боротьби з кіберзлочинністю та торгівлею людьми.

Такий стан справ фактично означає, що Україна поступово нагромаджує важливий досвід у захисті власної ІТ-інфраструктури від кіберзагроз сучасності та протидії проявам кібертероризму. Утім протистояти фізичному руйнуванню технічних засобів, дезорганізації роботи інформаційних систем і мереж, порушенню функціонування об'єктів нападу, а також протиправній діяльності соціальних інженерів в умовах інтенсифікації кібервтручань з дня на день стає все важче. Одна з головних причин цих негараздів полягає в «незадовільному кадровому забезпеченні відомств відповідними фахівцями у сфері інформаційної безпеки», як наголошується в аналітичній доповіді Національного інституту стратегічних досліджень при Президентові України «Кібербезпека: світові тенденції та виклики для України». Отже, найбільшу загрозу вітчизняним установам і відомствам становить відчутна нестача професіоналів з інформаційної та кібербезпеки, здатних:

відшукувати, збирати або добувати інформацію про ІТ-системи й мережі протиборчих сторін, а також про технології та засоби їхнього впливу на власну інфосферу;

виявляти ознаки стороннього кібервпливу й моделювати можливі ситуації такого впливу, прогнозуючи відповідні наслідки;

протидіяти несанкціонованому проникненню протиборчих сторін у власні ІТ-системи й мережі, забезпечуючи стійкість їхньої роботи, а також відновлення нормального функціонування після здійснення кібернападів тощо.

Дедалі вища активність так званого когнітивного базису – звичайних користувачів, професійних шпигунів і/або хакерів (порушників), поряд зі стрімко зростаючою кількістю способів і методів, до яких вони вдаються з метою пошуку й збору інформації з відкритих і відносно відкритих джерел та її

добування із закритих електронних джерел, потужний сплеск розвитку соціальних мереж - це ті чинники, що активізують кіберзлочинність, особливо з огляду на тенденції розвитку інтернету в напрямку інтеграції та об'єднання наявних можливостей у рамках єдиних багатокористувальницьких веб-платформ. Саме тому глобальна мережа перетворюється на засіб організації різного роду кібернетичних і соціотехнічних атак, несанкціонованого доступу (НСД) до чужих сайтів, створення сайтів-двійників тощо. Останнім часом такі дії неухильно виходять за межі окремих країн, випереджаючи за темпами зростання всі інші види організованої злочинності.

Вочевидь, чинити дієвий опір таким агресивним діям дуже складно. Адже заходи з ефективного запобігання небажаним витокам інформації мають крім суто технічних механізмів спиратися на методи й засоби соціального інжинірингу, систематизований виклад яких — одне з головних завдань пропонованого підручника. У кожному з п'яти його розділів поряд із теоретичними засадами забезпечення інформаційної та кібернетичної безпеки (розкриття змісту основних термінів і понять, визначень та математичних моделей процесів захисту від несакціонованого доступу тощо) висвітлюються найважливіші аспекти відповідної діяльності, здійснюваної на базі чинних законодавчих і нормативних документів. Особливо важливі витяги з них наводяться в тексті.

Підручник має передусім спонукати читачів до самостійного пошуку практичних заходів із протидії сторонньому кібернетичному впливу за тих чи інших конкретних умов.

Поглибленому опрацюванню матеріалу підручника посприяє добірка питань для самоконтролю, якою завершується кожний його розділ.

Практичну спрямованість підручника підсилюють шість тематичних додатків, що охоплюють найширше коло споріднених питань.

НАВЧАЛЬНЕ ВИДАННЯ

Володимир Леонідович БУРЯЧОК
Володимир Борисович ТОЛУБКО
Володимир Олексійович ХОРОШКО
Сергій Васильович ТОЛЮПА

ІНФОРМАЦІЙНА І КІБЕРБЕЗПЕКА:
соціотехнічний аспект

підручник
(українською мовою)

Формат 60x84/16. Папір офсетний. Гарнітура Times New Roman Умовн. друк. арк. 18,6.

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»