МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Державний університет телекомунікацій

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

Затверджено Міністерством освіти і науки України
як підручник для студентів вищих навчальних закладів

Київ ДУТ 2015

БКК 39.973.26-018.2(4Укр)я73
Б 91
УДК 004.7.056.5(477)(075.8)

Гриф надано Міністерством освіти і науки України
згідно з листом №1/11-8664 від 22.06.2015 р.

Рекомендовано вченою радою
Державного університету телекомунікацій
до друку та використання в навчальному процесі
(протокол № 24 від 17.06.2015 року)

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. – К. : ТОВ «СІК ГРУП Україна», 2015. – 449 с.
ISBN 978–617–7092–64–2

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 978–617–7092–64–2

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	–	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.

ПІСЛЯМОВА

За матеріалом, викладеним в підручнику, можна зробити такі висновки.

1. Інформаційне суспільство – якісно новий етап соціотехнологічної еволюції суспільства, одним з головних напрямків формування якого є розбудова динамічного, структурованого, високотехнологічного та завжди захищеного інформаційного простору. Це висуває на передній план необхідність змістовного дослідження інформації, яка стає третім і все більш важливим видом ресурсів, доповнюючим і багато в чому замінюючим такі традиційні ресурси як матерія та енергія.

2. Найбільш раціональними засобами, які дають можливість працювати з інформацією поступово стають сучасні інформаційно-комунікаційні технології. Саме застосування світовою спільнотою для забезпечення процесів своєї життєдіяльності та впливу на окремих осіб або суспільство в цілому сучасних засобів обчислювальної техніки, а також програмно-технічних засобів пошуку, збору та реєстрації інформації поступово обумовило появу так званого віртуального простору, доволі умовне поєднання якого з простором реальним призвело до формування простору кібернетичного.

3. Враховуючи появу нових викликів, кібервтручань і фактично неприхованих кіберзагроз, які майже постійно відчуває на собі сучасна інфосфера та які, як результат, впливають на погіршення безпеки світового інформаційного і кіберпросторів, провідні країни світу такі, як США, Японія, Франція, Велика Британія, Росія, Китай та багато інших протягом останніх років активно модернізують власні сектори безпеки й, передусім, безпеки інформаційної та кібернетичної, віддаючи при цьому головну роль проблемі завоювання інформаційної переваги в управлінні військами (силами) і зброєю, а також удосконаленню відповідної нормативно-правової бази.

4. В практику збройної боротьби провідними країнами світу активно впроваджуються концепції інформаційного та кіберпротиборства, що розгортаються навколо IP, ІКТ та ІТС й передбачають ведення активних розвідувальних дій щодо об’єкта нападу або потенційного порушника та дій, спрямованих на захист національних інтересів від стороннього кібернетичного впливу. Головними критеріальними ознаками цих процесів нині варто вважати: *критерій цілеполагання* – регламентує, що вищою метою протиборства сторін у кіберпросторі є переслідування особливих, насамперед політичних цілей;

міжнародно-правовий критерій – передбачає, що вищою формою протиборства у кіберпросторі є «агресія»; «*граничний критерій*» – означає, що перевищення певного порога збитку є відправною точкою для переходу протиборства сторін у кіберпросторі в статус військового конфлікту.

5. Подальше розширення кола країн, керівництво яких здійснюватиме активні заходи у напрямі нарощування оборонного і наступального потенціалів в інформаційному і кіберпросторах може призвести до загострення міждержавних суперечностей. Це вимагатиме активізації заходів міжнародного співробітництва щодо гарантування глобальної інформаційної і кібербезпеки, прискорення процесу розробки ефективних механізмів захисту власних об'єктів критичної інфраструктури від стороннього кібернетичного впливу та створення дієвих і високо надійних систем кібербезпеки як важливих складових їх загальнодержавних систем ІБ, відсутність яких може призвести до втрати політичної незалежності будь-якою з них, тобто до фактичного програшу війни невійськовими засобами й підпорядкування власних національних інтересів інтересам іншої (протиборчої) сторони.

6. Україні, щоб ефективно протидіяти деструктивному інформаційному і кібервпливу, на найближчу перспективу необхідно: провести коректування в застосуванні принципу свободи слова; вжити заходів до захисту людей – потенційних жертв інформаційної та кіберагресії; здійснювати контр-дезінформаційні заходи й створювати спеціальні контр-дезінформаційні служби; пам'ятати про найважливіше «правило ведення інформаційного бою» – у жодному разі не здавати інформаційний і кіберпростір інформаційним або кібер агресорам та терористам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

До першої глави

1. Бебик В. Інформаційно-комунікаційний менеджмент у глобальному суспільстві: психологія, технологі, техніка паблік рілейшнз / В. Бебик. – К. : МАУП, 2005. – 440 с.
2. Власенко Н.А., Зорько С.В., Сиротич М.Р. Україна на шляху до інформаційного суспільства: проблеми та здобутки. Інформаційно-аналітичний огляд Національного інституту стратегічних досліджень. – К. : НІСД, 1995. – № 5
3. Макаренко Є. А. Європейська інформаційна політика: Монографія. – К.: Наша культура і наука, 2000. – 368 с.
4. Брыжко В. М., Цимбалюк В. С., Орехов А. А., Гальченко О. Н. Е-будущее и информационное право. / Под ред. Р. А. Калюжного и М. Я. Швеца. - К.: „Интеграл", 2002. – 264 с.
5. Григор О.О. Формування інформаційного суспільства в Україні в контексті інтеграції в Європейський Союз (державно-управлінський аспект): Автореф. дис. ... канд. наук з державного управління: 25.00.01 / Львівський регіональний інститут державного управління Національної академії державного управління при Президентові України. – Львів, 2003. – 20 с.
6. Делягин М. Мировой кризис: Общая теория глобализации. – М.: ИНФРА-М, 2003. – 767 с.
7. Копылов В.А. Информационное право: вопросы теории и практики. – М.: Юристъ, 2003. – 623 с.
8. Чернов А.А. Становление глобального информационного общества: проблемы и перспективы: Монография. – М.: «Дашков и К°», 2003. – 232 с.
9. Чиж І.С. Україна: шлях до інформаційного суспільства. – К.: Либідь, 2004. – 287 с.
10. Про основні засади розвитку інформаційного суспільства в Україні на 2007 - 2015 роки: Закон України, 2007. -№12. - Режим доступу: http://zakon.rada.gov.ua/
11. Про концепцію (основи державної політики) національної безпеки України. Постанова ВР України. Відомості Верховної Ради, 1997, № 10.
12. Богуш В.М. Інформаційна безпека держави: Вступ до спеціальності. - К.: ДУІКТ, 2002. (електронний варіант).
13. Данільян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: структура та напрямки реалізації: Навчальний посібник. - Харків: Фоліо, 2002. - 285 с.
14. Машлыкин В.Г. Европейское информационное пространство. М.: Наука, 1999. http://isn.rsuh.ru/iu/m4.htm.

15. Зуев С.Э. Измерения информационного пространства (политики, технологии, возможности). http://future.museum.ru/part01/010601.htm
16. Бортко Г. Н. Национальные стратегии информационного общества: преимущества и условия реализации в Украине / Г. Н. Бортко // Информационное общество. - 2004. - № 2. – С. 25-29.
17. Дюжев Д. Б. Інформаційне суспільство: сощально-правові аспекта суспільного розвитку / Д В. Дюжев // Наука. Релігія. Суспільство. - 2004. - № 1. – С. 116-122.
18. Клименко І. В. Технології елекгронного урядування. /І.В.Клименко, К.О.Линьов. - К.: Центр сприяння інституційному розвитку державної' служби, 2006. – 192 с.
19. Окинавська хартія глобального інформаційного суспільства // Дипломатичний вісник - 2000. - № 8. – С. 51-56.
20. Почепцов Г. Г. Інформаційна політика / Г.Г.Почепцов. С.А.Чукут. - К.: Знання. 2008. – 663 с.
21. Проценко П.П. Проблематика переходу до інформаційного суспільства / П.П.Проценко // Політичний менеджмент. - 2004. - № 6 (9). - С. 129-137.
22. Силаенков А.Н. Проектирование системы информационной безопасности: учеб. пособие – Омск: Изд-во ОмГТУ, 2009. – 128 с.
23. Богуш В.М. Основи інформаційної культури (електронний варіант). - К.: ДУІКТ, 2002. – 244 стор.
24. Грязнов Е.С., Панасенко С.А. Безопасность локальных сетей. – М.: Вузовский учебник, 2006.- 525 с.
25. Козлачков П.С. Основные направления развития систем информационной безопасности. – М.: финансы и статистика, 2004. – 736 с.
26. Леваков Г.Н. Анатомия информационной безопасности. – М.: ТК Велби, издательство Проспект, 2004. – 256 с.
27. Соколов Д.Н., Степанюк А.Д. Защита от компьютерного терроризма. – М.: БХВ-Петербург, Арлит, 2002. – 456 с.
28. Сыч О.С. Комплексная антивирусная защита локальной сети. – М.: финансы и статистика, 2006. – 736 с.
29. Швецова Н.Д. Системы технической безопасности: актуальные реалии. Спб: Питер, 2004. – 340 с.
30. http://www.lghost.ru/lib/security/kurs5/theme01_chapter04.htm
31. http://www.globaltrust.ru/
32. http://www.arnis.ru/gost_17799_common.htm
33. Башмаков А.И., Башмаков И.А. Интеллектуальные информационные технологии. – М.: МГТУ имени Н.Э. Баумана, 2005. – 302 с.

34. Белоногов Г.Г. Компьютерная лингвистика и перспективы информационной технологии. – М.: Русский дом, 2004.
35. Бурячок В.Л. Використання методу експертного аналізу для визначення якості автоматизованих інформаційних систем та їхньої порівняльної оцінки. //Збірник наукових праць/ ЦНДІ ОВТ ЗС України. Вип. 15. – К.: ЦНДІ ОВТ, 2006. – С. 18 - 30.
36. Дружинин Г. В., Сергеева И. В. Качество информации. – М.: Радио и связь, 1990.
37. Синицын Н.В., Петропавловский В.П., Никитин А.М. Автоматизированные системы научных исследований. – М.: Знание, 1987, – 64 с.
38. Богуславський Л.Б., Дрожжинов В.И. Основы построения вычислительных сетей для автоматизированных систем. – М.: Энергоатомиздат, 1990. – 256 с.
39. Диго С.М. Базы данных. – М.: Московский международный інститут эконометрики, информатики, финансов и права, 2004. – 177 с.
40. Кузьмин В. Microsoft Office Excel 2003. Учебный курс. – СПб.: Питер; Киев: Издательская группа BHV, 2004. – 493 с.
41. Інформаційні системи в менеджменті: Навчальний посібник // Батюк А.Є., Двуліт З.П., Обельовська К.М., Огородник І.М. та ін. – К.: Інтелект-Захід, 2004. – 520 с.
42. Інформаційне забезпечення менеджменту // Новак В.О., Макаренко Л.Г., Луцький И.Г. – К.: Кондор, 2006. – 462 с.
43. Тлумачний словник з інформатики / Г.Г.Півняк, Б.С.Бусигін, М.М.Дівізінюк та ін. – Дніпропетровськ: Нац. гірн. ун-т, 2008. – 599 с.
44. Информационные системы: Учебное пособие для вузов / Под ред. В.Н.Волковой, Б.И.Кузина. – СПб.: Изд-во СПбГТУ, 1998. – 213 с.
45. Информационные системы в экономике / Под ред. В.В.Дика. – М.: Финансы и статистика, 1996. – 374 с.
46. Харитонова И.А. Microsoft Access 2007. Учебный курс. – СПб.: Питер; Издательская группа BHV, 2008. – 580 с.

До другої глави

47. Gibson W. Neuromancer / W. Gibson. – London: HarperCollins, 1994. – 271 p. № 49, ст. 420.
48. Грунин О. А., Грунин С.О. Экономическая безопасность организации - СПб.: Питер, 2002. - 160 с. ил. - (Серия “Учебные пособия”).
49. Пастернак-Таранущенко Г. Економічна безпека держави. Статика процесу забезпечення. Підручник для державних службовців, науковців, студентів і аспірантів вищих навчальних закладів економічного профілю / За ред. професора Богдана Кравченка. - К.: "Кондор”, 2002. - 302 с.
50. Про концепцію (основи державної політики) національної безпеки України. Постанова

Верховної ради України). Відомості Верховної Ради (ВВР), 1997, № 10, ст. 85 (Із змінами, внесеними згідно із Законом ж 2171-III від 21.12.2000, ВВР, №9, ст.38).

51. Пашнев Д.В. Виды и классификация преступлений, совершаемых с помощью компьютерных технологий / Д.В. Пашнев // Компьютерная преступность и кибертерроризм : Сборник научных статей ; под ред. В.А. Голубева, Н.Н. Ахтырской. – Запорожье : Центр исследования компьютерной преступности, 2004. – Вып. 2. – С. 42–46.
52. Кiберманьячка окажется на скамье подсудимых. [Електронний ресурс]. – 17.05.2008. – Режим доступу : http://news.ntv.ru/132383/video/.
53. Жителя Сочи довели до суицида с помощью сайта «Одноклассники». [Електронний ресурс]. – 22 декабря, 2011. – Режим доступу : http://www.securitylab.ru/news/412942.php.
54. Robertson N. Documents reveal al Qaeda's plans for seizing cruise ships, carnage in Europe [Електроннийресурс] / N. Robertson, P. Cruickshank, T. Lister. – Режимдоступу : http://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future/?hpt=hp_c1.
55. Shelley L. Organized Crime, Terrorism and Cybercrime [Електроннийресурс] / L. Shelley;переводисследователяВЦИОПТропининойТ.Л. – Режимдоступу : http://www.crime.vl.ru/index.php?p=928&more=1&c=1&tb=1&pb=1.
56. Алисов Н.В. География мировой телекоммуникационной связи / Н.В.Алисов // Вестник Моск. ун-та. - Сер. 5. Геогр. - 1996. - №3. - С.9-15
57. Перфильев Ю.Ю. Российское Интернет-пространство: развитие и структура / Перфильев Ю.Ю. - М.:Гардарики. 2003. - 272с.
58. Росич Ю.Ю. География развития Интернета в России: канд. геогр. наук / Росич Ю.Ю. - М., 2005. - 167с.
59. Шестак Н.В. География Интернета. Основные факторы и показатели развития Интернета, виды интернет-услуг: материалы межрегиональной научно-практической конференции «Профессиональное образование в условиях дистанционного обучения. Достижения, проблемы, перспективы» [Электронный ресурс] / Шестак Н.В.-М.,СГА, 2004. - Режим доступа: http://www.muh.ni/arcli/konf_mSliestak.htm?user=bef81 c55bc 13cb65d2076769b3ba3e52
60. Новости. Глобальная статистика украинского Интернета за октябрь 2010 г. /- Bigmir-interaet. - http://bigmir-interaet.com.ua/news/1032/. - 30.11.2010.
61. Measuring the Information Society 2010 - International Telecommunication Union. - http://www.itu.int/ITU-D/ict/publications/idi/2010/Material/MIS_2010 _witliout% 20annex%204-e.pdf. - 15.11.2010.
62. Торокин А.А. Инженерно-техническая защита информации: учеб. пособие для

студентов, обучающихся по специальностям в области информационной безопасности. / А.А. Торокин. – М.: Гелиос АРВ, 2005. – 960 с.
63. Черняк В.З. Тайны промышленного шпионажа. / В.З. Черняк. – М.: Вече, 2002. – 512 с.
64. Ландэ Д.В. Конкурентная разведка в WEB. [Електронний ресурс] / Д.В. Ландэ, В.В. Прищепа. – Режим доступу: http://z-filez.info/story/konkurentnaya-razvedka-v-web.
65. Бурячок В.Л. Практичні аспекти методології сучасного інформаційного пошуку // Інформаційна безпека. – 2011. – № 2(6). – С. 149–154.
66. Ярочкин В.И. Технические каналы утечки информации. / В.И. Ярочкин. – М.: ИПКИР, 1994. – 112 с.
67. Доронин А.И. Аналитическая разведка средствами Інтернет. [Електронний ресурс] / А.И. Доронин. – Режим доступу: http://www.agentura.ru.
68. Леваков А. Новые приоритеты в информационной безопасности США. [Електронний ресурс] / Александр Леваков. – Режим доступу: http://www.agentura.ru/equipment/psih/info/prioritet.
69. Шевчук Д.А. Экономическая журналистика. [Електронний ресурс]. / Д.А. Шевчук. – Режим доступу: http://svoikrug.narod.ru/young_a.htm.
70. Significant New FBI Carnivore Documents Obtained by EPIC (Released January 14, 2005). [Електронний ресурс]. – Режим доступу: www.epic.org/privacy/carnivore.
71. Ландау Э. Службы безопасности создают собственную сеть. [Електронний ресурс]/ Эдмунд Ландау. – Режим доступу: http://www.osp.ru/cw/1998/11/28107.
72. Кузнєцов И.Н. Информация: сбор, защита, анализ. Учебник по информацион- но-аналитической работе. / И.Н. Кузнєцов. – М.: ООО Изд. Яуза, 2001. – 92 с.
73. Макнамара Д. Секреты компьютерного шпионажа. Тактика и контрмеры / Д. Макнамара; пер.с англ.; под ред. С.М. Молявко. – М.: БИНОМ. Лаборатория знаний, 2004. – 536 с.
74. Меньшаков Ю.К. Теоретические основы технических разведок: Учебное пособие / Ю.К. Меньшаков; под ред. Ю.Н.Лаврухина. – М.: Узд-во МГТУ им. Н.Э. Баумана, 2008. – 524 с.
75. Максимович Г.Ю., Андреев А.М. Новые возможности автоматизации делопроизводства // Секретарское дело, 1999. № 4.
76. Максимович Г.Ю., Берестова В.П. Как создать информационную документальную систему // Секретарское дело, 2000. № 1.
77. Кузнецов С.Л. Проблема выбора программного обеспечения для комплексной автоматизации работы офиса // Секретарское дело 2000. № 4.
78. Кузнецов С.Л. Российские программы комплексной автоматизации делопроизводства // Делопроизводство, 2001. № 2.
79. Задорожна Н.Т. Аналіз стану та тенденції розвитку інформаційних технологій

підтримки діяльності органів державного управління //Проблеми програмування, 2001. – №3-4. – С.125–138.
80. Ефимова О.А. Современные системы автоматизации делопроизводства попытка анализа и классификации. // Секретарское дело 2003. № 5.
81. Ферова С.М. Современные программные системы в обеспечении работы секретаря. - М., 2004.
82. Рогов А.К. Применение современных программных систем в документообороте организаций. - СПб, 2005.
83. М.Зырьянов. Все об электронном документообороте, "Computerworld". №23, 2002 г.
84. «Российские системы электронного документооборота ждет большое будущее». Интернет-издание C-News, 7 февраля 2003 г.
85. Бобылева М.П. "Эффективный документооборот: от традиционного к электронному" Изд.: ТЕРМИКА, 2004.
86. Белов А.Н., Белов А.А. Делопроизводство и документооборот. Издательство "Эксмо-Пресс", 2006.
87. IDC, Collaborative ApplicationsMarket Forecast and Analysis, 2000-2004.
88. GartnerGroup, "The impact of Knowledge Management on Enterprise Archtecture".
89. Серія ДСТУ 3719-1-98 - ДСТУ 3719-10-98. Інформаційні технології. Електронний документообіг. Архітектура службових документів (ODA) та обмінний формат. Частини з 1 по 10.
89. Серія ДСТУ 3873-1-99 - ДСТУ 3873-2-99. Інформаційні технології. Електронний документообіг. Файлування та відбирання документів (DFR). Частини 1 та 2.
90. ДСТУ 3986-2000 (ISO 8879:1986). Інформаційні технології. Електронний документообіг. Стандартна мова узагальненої розмітки (SGML).
91. Ловцов Д.А. Информационная теория эргасистем: Тезаурус. - М.: Наука, 2005.
92. Сухов А.В. Динамика информационных потоков в системе управления сложным техническим комплексом //Теория и системы управления. - М. 2000, № 4. С. 111 – 119
93. Бурячок В.Л. Обґрунтування вибору раціональної системи електронного документообігу для державних структур спеціального призначення / В. Л. Бурячок, Т.Я. Костюк, Л.В. Бурячок // Вісник воєнної розвідки, ВДА ГУР МО України 2011, № 24, с. 67 - 74.

До третьої глави

94. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.:НАУ, 2013. – 432 с.
95. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник]. / В. Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С.В. Толюпа /. За заг. ред. докт. техн.

наук, проф. В.Б. Толубко. – К. : ПВП «Задруга», 2014. – 320 с.
96. Про раду національної безпеки України. Закон України. Відомості Верховної Ради (ВВР), 1998, № 35, ст.237.
97. Про концепцію (основи державної політики) національної безпеки України. Постанова Верховної ради України). Відомості Верховної Ради (ВВР), 1997, № 10, ст. 85 (Із змінами, внесеними згідно із Законом ж 2171-III від 21.12.2000, ВВР, №9, ст.38).
98. Богуш В.М., Кудін А.М. Інформаційна безпека від А до Я: 3000 термінів і понять. - К.: МОУ, 1999. - 456 с.
99. Грунин О. А., Грунин С.О. Экономическая безопасность организации - СПб.: Питер, 2002. - 160 с. ил. - (Серия "Учебные пособия").
100. Пастернак-Таранущенко Г. Економічна безпека держави. Статика процесу забезпечення. Підручник для державних службовців, науковців, студентів і аспірантів вищих навчальних закладів економічного профілю / За ред. професора Богдана Кравченка. - К.: "Кондор", 2002. - 302 с.
101. Про Воєнну доктрину України. Постанова Верховної Ради України. Відомості Верховної Ради (ВВР), 1993, № 43, ст. 409 (Із змінами, внесеними згідно із Законом № 2171-III від 21.12.2000, ВВР, №9, ст.38).
102. Про оборону України. Закон України. В редакції Закону № 2020-III від 05.10.2000, ВВР, 2000, № 49, ст. 420.
103. Про інформацію: за станом на 09.05.2011 р. / Закон, затверджений ВР України 02.10.1992, № 2657-XII. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Відомості Верховної Ради України від 01.12.1992.
104. Про основи національної безпеки України: за станом на 20.07.2010 р. / Закон, затверджений ВР України 19 червня 2003 р., № 964-IV. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Урядовий кур'єр від 30.07.2003, № 139.
105. Про державну службу спеціального зв'язка та захисту інформації: за станом на 07.08.2011 р. / Закон, затверджений ВР України 23 лютого 2006 року, № 3475-IV. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Урядовий кур'єр від 11.04.2006, № 68.
106. Про телекомунікації: за станом на 15.10.2011 р. / Закон, затверджений ВР України, 18.11.2003, № 1280-IV. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Урядовий кур'єр від 24.12.2003, № 243.
107. Про захист інформації в інформаційно-телекомунікаційних системах: за станом на 30.04.2009 р. / Закон, затверджений ВР України 05.07.1994, № 80/94-ВР.

[Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Відомості Верховної Ради України від 02.08.1994.

108. Про об'єкти підвищеної небезпеки: за станом на 18.11.2012 р. / Закон, затверджений ВР України 18.01.2001, № 2245-III. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2245-14. – Офіц. вид. – К.: Відомості Верховної Ради України від 13.04.2001.
109. Про Доктрину інформаційної безпеки України: за станом на 08.07.2009 р. / Указ Президента України від 8.02.2009 р., № 514/2009. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Офіційний вісник України від 20.07.2009.
110. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: за станом на 09.01.2007р. / Закон, затверджений ВР України 09.01.2007 № 537-V. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/537-16. – Офіц. вид. – К.: Відомості Верховної Ради України від 23.03.2007.
111. Про внесення змін до Закону України "Про основи національної безпеки України" щодо кібернетичної безпеки України: проект за станом на 06.03.2013 р. № 2483. [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45998
112. Про Стратегію національної безпеки України: за станом на 12.02.2007 р. / Указ Президента України від 12.02.2007 р., № 105/2007. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Урядовий кур'єр від 07.03.2007, № 43.
113. William Gibson, Neuromancer. New York: Ace Books, 1984.
114. David Clark, Characterizing cyberspace: past, present and future, MIT/CSAIL Working Paper, 12 March 2010.
115. Гнатюк С.О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. // Безпека інформації. – 2013. – Том 19, № 2 (2013) – С. 118-129.
116. GAO-10-606. CYBERSPASE United States Faces Challenges in Addressing Global Cybersecurity and Governance, Washington, July 2010. [Електронний ресурс]. – Режим доступу: http://web.ebscohost.com.
117. GAO-10-628. Key Private and Public Cyber Expectations Need to Be Consistently Addressed United States Government Accountability Office, Washington, July 2010. [Електронний ресурс]. – Режим доступу: http://web.ebscohost.com.
118. Рада національної безпеки і оборони України: Експертні консультації Україна – НАТО з питань кібернетичного захисту. [Електронний ресурс]. – Режим доступу: http://www.rainbow.gov.ua/news/ 1076.html

119. Корченко О.Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти // О.Г. Корченко, В.Л. Бурячок, С.О. Гнатюк / Безпека інформації. – Том 19, №1. – 2013. – С. 40-45.
120. Мельник С.В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С.В. Мельник, О.О. Тихомиров, О.С. Лєнков // Збірник наукових праць Військового інституту КНУ ім. Тараса Шевченка. – К. : ВІКНУ, 2011. – Вип. 30. – С. 159-165.
121. Словник термінів з кібербезпеки / За загальною редакцією Копана О.В., Скулиша Є.Д. – К. : ВБ «Аванпост-Прим». – 2012. – 214 с.
122. Бурячок В.Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства // Сучасна спеціальна техніка. – 2011. – № 3 (26). – С. 104–114.
123. Про ратифікацію Конвенції про кіберзлочинність: за станом на 14.10.2010 р. / Закон, затверджений ВР України 07.09.2005, № 284-IV. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2824-15. Офіц. вид. – К.: Відомості Верховної Ради України від 10.02.2006.
124. 11–12 лютого в Україні пройшли Консультації експертів "Україна-НАТО" з питань кібернетичного захисту. [Електронний ресурс]. – Режим доступу: http://zik.com.ua/ua/news/2010/02/12/216707.
125. Шеломенцев В.П.Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення. [Електронний ресурс]. – Режим доступу: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&Z21ID=&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/boz_2012_2_36.pdf
126. Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства. [Електронний ресурс]. – Режим доступу: http://www.osce.org/ru/secretariat/110472?download=true
127. Практика ИБ \ SANS - Топ 20 наиболее критичных защитных мер и средств. https://www.sugarsync.com/pf/D6870693_7400982_60553
128. Семенов Ю.А. Обзор по материалам ведущих фирм, работающих в сфере сетевой безопасности. [Електронний ресурс]. – Режим доступу: http://book.itep.ru/10/2012.htm
129. Competitive intelligence. [Електронний ресурс]. – Режим доступу: http://en.wikipedia.org/wiki/Competitive_intelligence.
130. Карпов Г. Атака на DNS или ночной кошмар сетевого администратора. [Електронний ресурс] / Геннадий Карпов. – Режим доступу: http://www.hackzone.ru/articles/dns-poison.html, 02.06.2007.

131. Examining port scan methods - Analyzing Audible Techniques. [Електронний ресурс]. – Режим доступу: http://www.windowsecurity.com/whitepapers/xamining_port_scan_ methods_Analyzing_ Audible_Techniques.html.
132. Инциденты информационной безопасности. Рекомендации по реагированию. – М.: Group-IB и LETA, 2011. – 20 с.
133. Мир вступил в эпоху сетевых войн и конфликтов. [Електронний ресурс]. – Режим доступу: http://www.rodon.org/polit-100408112419
134. Гнатюк В.О. Аналіз дефініцій поняття «інцидент» та його інтерпретація у кіберпросторі // В.О. Гнатюк / Безпека інформації. - 2013. - Т.19.-№3.-С. 175-180.
135. Бон Я.В. ИТ Сервис-менеджмент, введение / под ред. Яна Ван Бона; пер. с англ. «IT Expert», 2003. - 240 с.
136. Метрики для управления ИТ-услугами / Питер Брукс; пер. с англ. - М. : Альпина Бизнес Букс, 2008. - 283 с.

До четвертої глави

137. Мир вступил в эпоху сетевых войн и конфликтов. [Електронний ресурс]. – Режим доступу: http://www.rodon.org/polit-100408112419
138. Прокофьев В. Ф. Тайное оружие информационной войны: атака на подсознание. Издание второе, расширенное и доработанное. Серия "Информационные войны". – М.: СИНТЕГ, 2003. - 408 с.
139. Почепцов Г.Г. Информационные войны.- М.: Рефл-бук, К.: Ваклер, 2001.- 576 с.
140. Словарь “Геополитика и национальная безопасность”// Вестник военной информации.-1998.-№10.-С.13-15.
141. Ерёменко С. По возможностям информационная война куда опаснее, чем ядерное оружие //Defense express.-2002.- №8.- С.12.
142. Варюхін В.О., Замураєва І., Рось А. Глосарій з предметних галузей “Інформаційна війна”, “Інформаційна безпека” та “Інформаційна боротьба” //Труди Академії.-2000.- №20.- С.24.
143. Факадей Р. Тенденція розвитку збройної боротьби на сучасному етапі та її вплив на розвиток теорії і практики управління військами (силами) //Труди Академії.-2001.-№31.-С.29.
144. Пожидаев Д. Информационная война в планах Пентагона //Зарубежное военное обозрение, 1996.- №2. - С.2.
145. Гриняев С.Н. Интеллектуальное противодействие информационному оружию. – М.: СИНТЕГ, 1999. – 232 с.
146. Гриняев С. Н. Поле битвы – киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны. – Мн.: Харвест, 2004. – 448 с.

147. Урван Парфентьев. Возможен ли безопасный Інтернет. [Електронний ресурс]. – Режим доступу: http://rus.ruvr.ru/2010/02/12/4403044.html
148. Киберпространство вооружается. [Електронний ресурс]. – Режим доступу: http://inosmi.ru/world/20101115/164256611.html
149. Конкурентная разведка в Internet / В.В.Дудихин, О.В.Дудихина. 2-е изд. испр. и доп. – М.: ООО "Издательство АСТ", 2004. – 229 с.
150. "Cyberwar: War in the Fifth Domain". The Economist, Jul 1st 2010.
151. Clarke, Richard A. Cyber War, HarperCollins (2010).
152. А.А. Мережко. Конвенция о запрещении использования кибервойны в глобальной информационной сети информационных и вычислительных ресурсов (Интернете). [Електронний ресурс]. – Режим доступу: http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57
153. О. Мережко. Проблеми кібервійни та кібербезпеки в міжнародному праві. [Електронний ресурс]. – Режим доступу: http://www.politik.org.ua/vid/publcontent.php3?y=7&p=58, 05.06.2009
154. В.Ф. Комарович, И. Б. Саенко. Компьютерные информационные войны. Концепция и реалии. [Електронний ресурс]. – Режим доступу: http://www.cprspb.ru/bibl/opv/komarovich.doc
155. Е. А. Роговский, П. А. Шариков. Пентагон усиливает кибероборону. США - Канада. Экономика, политика, культура, № 1, Январь 2011, С. 51-60. [Електронний ресурс]. – Режим доступу: http://www.ebiblioteka.ru/browse/doc/24224548
156. Бурячок В.Л., Гулак Г.М., Хорошко В.О. Завдання, форми та способи ведення воєн у кібернетичному просторі // Наука і оборона. – 2011. – № 3. – С. 35–42.
157. Бурячок В.Л. Поняття кібервійни та розвідки інформаційно-телекомунікаційних систем у контексті захисту держави від стороннього кібернетичного впливу / В.Л. Бурячок, О.А. Ільяшов, Г.М. Гулак // Актуальні питання підготовки фахівців із розслідування кіберзлочинів: круглий стіл НА СБ України, 25.11.2011 р.: доповіді та тези доповідей. – К.:, 2012. – С. 27–32.
158. І. О. Ляшенко, В. А. Кириленко. Кібернетичні операції - майбутня форма збройної боротьби. [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/portal/soc_gum/znpnapv_vtn/2010_53/ 10liofzb.pdf
159. Крупин А. ESET сообщает об угрозе червя Win32/Stuxnet, использующего брешь в Windows. [Електронний ресурс] / Андрей Крупин. – Режим доступу: http://www.3dnews.ru/software-news/ESET-soobshchaet-ob-ugroze-chervya-Win32Stuxnet-ispolzuyushchego-bresh-v-Windows/, 20.07.2010.
160. СМИ внезапно вспомнили о черве WIN32/Stuxnet. [Електронний ресурс]. – Режим доступу: [Електронний ресурс]. – Режим доступу: http://purogok.ucoz.

ua/news/smi_vnezapno_vspomnili_o_cherve_win32_stuxnet/2010-09-30-501.

161. Eset: Истинные цели червя Stuxnet до сих пор неясны. [Електронний ресурс]. – Режим доступу: http://www.esetnod32.ru/.company/news/ ?id=8047&year =2010, 27.09.2010.
162. Крупин А. “Лаборатория Касперского”: червь Stuxnet знаменует собой начало новой эры кибервойн. [Електронний ресурс] / Андрей Крупин. – Режим доступу: http://www.liveinternet.ru/users/sintalsa/post135961823/, 26.09.2010.
163. Иранские власти задержали кибертеррористов. [Електронний ресурс]. – Режим доступу: http://itgator.ru/2010/10/04/iranskie-vlasti-zaderzhali-kiberterroristov/, 04.10.2010.
164. Мир вступил в эпоху сетевых войн и конфликтов. [Електронний ресурс]. – Режим доступу: http://www.rodon.org/polit-100408112419.
165. Каждые 15 секунд в мире появляется новый вирус. [Електронний ресурс]. – Режим доступу: http://www.cnews.ru/reviews
166. Тимофей Сайтарлы. Киберпреступность: программное обеспечение в роли “оружия массового сбоя”. [Електронний ресурс]. – Режим доступу: http://www.crime-research.ru
167. За 97% кибернападений ответственны всего 20 стран. [Електронний ресурс]. – Режим доступу: http://soft.compulenta.ru/499115/
168. Рыбаков Ф.И. Системы эффективного взаимодействия человека и ЭВМ. – М.:Радио и связь, 1985. – 200 с.
169. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. В.Л. Бройдо. – СПб.: Питер, 2004. – 703 с.
170. Семенов Ю.А. Обзор уязвимостей, некоторых видов атак и средств защиты. [Електронний ресурс]. – Режим доступу: http://book.itep.ru/6/intrusion.htm
171. М.Левин. E-mail “безопасная”: взлом, “спам” и “хакерские” атаки на системы электронной почты Internet. – М.: Бук-пресс, 2006. – 192 с.
172. Peter Neumann, Donald Parker. A summary of computer misuse techniques. In 12th National Computer Security Conference, 1989.
173. Peter Neumann. Computer-Related Risk. ACM Press/Addison Wesley, 1995.
174. Сергей Пахомов. Проблемы сетевой безопасности. [Електронний ресурс]. – Режим доступу: http://www.compress.ru/article.aspx?id=10462&iid=429
175. Атака через Internet. Содержание. [Електронний ресурс]. – Режим доступу: http://citforum.vision.am/internet/attack/toc.shtml

Додаток В

Перелік основних термінів та визначень

Таблиця В1

№ з/п	Термін	Визначення
1.	Автоматизоване робоче місце	діалогова професійно-орієнтована індивідуальна або групова (колективна) система обробки інформації, призначена для автоматизації діяльності обслуговуючого персоналу і користувачів АС шляхом реалізації ІКТ у процесах виконання ними встановлених (визначених) функцій
2.	Безпека інформації	стан інформації, за якого забезпечується збереження її властивостей, визначених обраною (сформованою) політикою безпеки
3.	Ботнет	комп'ютерна мережа, що складається із заражених запущеними ботами (шкідливими програмами, що автоматично за заданим розкладом виконують певні деструктивні дії) комп'ютерів
4.	Дійові особи кіберпростору	легальні (легітимні) користувачі, хакери, мережеві комбатанти, кіберзлочинці (кібертерористи), кібервійська, а також інші спеціалізовані державні та недержавні формування
5.	Загроза безпеки ІТС	подія, яка шляхом потенційно можливого впливу на ІТС прямо та/або опосередковано завдає збитку її власникам і користувачам
6.	Захист інформації	сукупність організаційно-технічних заходів та правових норм з попередження і нейтралізації загроз ІР, ІТ системам та мережам, а також усунення їх наслідків
7.	Інсайдер	особа, яка в силу свого службового стану має доступ до конфіденційної інформації корпорації (установи) й використовує її у власних інтересах з метою збагачення
8.	Інформація (information)	універсальна субстанція, яка у виді знаків, сигналів, звуків, зображень і текстових повідомлень будь-якого роду пронизує усі сфери діяльності людства та слугує провідником його знань і умінь, інструментом спілкування, взаєморозуміння та співробітництва
9.	Інформаційна безпека	стан захищеності інформаційного середовища, який забезпечує його формування, використання і розвиток в інтересах оборони держави
10.	Інформаційна війна	інформаційне протиборство, що охоплює весь інформаційний простір супротивних сторін та може приймати форми як дипломатичної, так економічної і збройної боротьби
11.	Інформаційна (кібернетична) інфраструктура	сукупність організацийн-технічних структур і об'єктів, а також засобів їх взаємодії, що складають основу та забезпечують функціонування і розвиток інформаційного (кібер) простору
12.	Інформаційно-комунікаційна технологія	методи і засоби функціональних, змістовних та забезпечувальних компонент інформаційної (кібер) інфраструктури які, будучи об'єднаними засобами ЕОТ підтримують процеси пошуку, збору, добування, опрацювання, накопичення, передачі та зберігання інформації, визначають хід використання ІР, а також впливають на надійність та оперативність виконання процесів планування, управління, структуризації і постановки інформаційних завдань
13.	Інформаційний простір	глобальне інформаційне середовище, яке в реальному масштабі часу забезпечує комплексну обробку відомостей про протиборчі сторони та їх навколишнє оточення в інтересах підтримки прийняття рішень по створенню оптимального, для досягнення поставлених цілей, складу сил і засобів та їх ефективного застосування в різних умовах обстановки
14.	Інформаційне протиборство	об'єктивний процес у стосунках між протиборчими сторонами, спрямований на досягнення ними цілей власної державної політики у мирний та/або воєнний час, за рахунок комплексного впливу на систему державного і військового управління супротивної сторони та її військово-політичне керівництво, а також захисту власних від подібного впливу
15.	Інформаційний ресурс	організована сукупність інформаційних продуктів – матеріалів, відомостей, даних та знань, зафіксованих в ІС або на відповідних носіях інформації й призначених для забезпечення реалізації певних інформаційних потреб

Продовження табл. В1

№ з/п	Термін	Визначення
16.	Інформаційно-телекому-нікаційна система	сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле
17.	Інформаційно-телекомунікаційна сфера (середовище)	сукупність суб'єктів, що приймають участь в інформаційній взаємодії та інформації, призначеної для використання цими суб'єктами, а також технологій, що забезпечують цю взаємодію з точки зору обробки, зберігання й обміну інформацією між суб'єктами
18.	Канал зв'язку	сукупність технічних засобів, призначених для перенесення електричних сигналів між двома пунктами телекомунікаційної мережі, що характеризується смугою частот та/або швидкістю передачі
19.	Кібератака	сукупність узгоджених за метою, змістом і часом дій або заходів – так званих кіберакцій, спрямованих на певний об'єкт впливу з метою порушення конфіденційності, цілісності, доступності, спостережності та/або авторства циркулюючої в ньому інформації, а також порушення роботи його ІТ систем та мереж
20.	Кібербезпека	стан захищеності кіберпростору держави в цілому або окремих об'єктів його інфраструктури (ІТС тощо) від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним та/або національним інтересам
21.	Кіберборотьба	комплекс заходів, спрямованих на здійснення управлінського та/або деструктивного впливу на автоматизовані ІТС протиборчої сторони й захисту від такого впливу власних інформаційно-обчислювальних ресурсів
22.	Кібервійна	активне протистояння між державами, політичними групами, соціальними утвореннями, приватними і комерційними установами та іншими державними і позадержавними суб'єктами, метою якого є заподіяння шкоди один одному в ІТ сфері за рахунок проведення як оборонних (захист власних ІТС від деструктивного впливу), так і наступальних (встановлення контролю над ІТС протиборчої сторони) дій
23.	Кібервплив	деструктивних дії, що в процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо ІР, ІКТ та ІТС
24.	Кібервтручання	спроба впливу протиборчих сторін на інформаційний і кіберпростори один одного за рахунок використання засобів сучасної обчислювальної та/або спеціальної техніки й відповідного програмного забезпечення
25.	Кіберзагроза	прояв дестабілізуючого негативного впливу протиборчих сторін на певний об'єкт, що реалізуються за рахунок використання технологічних можливостей інформаційного й кіберпросторів, створюючи при цьому небезпеку як для них самих, так й для свідомості людини у цілому
26.	Кіберзахист	сукупність методів і заходів організаційного, нормативно-правового та технічного характеру, спрямованих на забезпечення кібербезпеки
27.	Кіберзброя	спеціальні атакові та оборонні засоби ураження, що дають можливість цілеспрямовано змінювати, знищувати, копіювати і блокувати інформацію, долати системи захисту, обмежувати доступ законних користувачів, порушувати функціонування носіїв інформації для дезорганізації роботи технічних засобів ІТ систем і мереж тощо
28.	Кіберзлочинець	особа яка, володіючи спеціальними знаннями в галузі інформаційних технологій, робить деяке протиправне діяння, спрямоване на одержання несанкціонованого доступу до певної інформації з метою її використання
29.	Кіберпростір	комунікаційне середовище, утворене системою зв'язків між об'єктами кіберінфраструктури – ЕОМ, КМ, ПЗ та ІР, що використовується для забезпечення певних інформаційних потреб
30.	Кіберсередовшце	сукупність суб'єктів кіберпростору, які приймають участь у інформаційній взаємодії та об'єктів, які цю взаємодію забезпечують

Продовження табл. В1

№ з/п	Термін	Визначення
31.	Кіберрозвідка (комп'ютерна розвідка)	комплекс заходів, спрямованих на систематичний та цілеспрямований пошук, збір і добування інформації про об'єкти розвідки з відкритих і відносно відкритих електронних джерел, а також подальший облік і накопичення такої інформації, її верифікацію, вивчення та аналітичну обробку
32.	Комп'ютерна мережа	будь-які взаємозв'язані комунікаційними чи телекомунікаційними лініями зв'язку абонентські системи (АРМ, РСт), ПЕОМ та віддалені термінали
33.	Критична інформаційна (кібер) інфраструктура	критично важливі об'єкти інформаційної (кібер) інфраструктури, ураження або знищення яких може призвести до втрати інформаційним (кібер) простором працездатності та/або поставити під загрозу суспільну і державну безпеку в цілому
34.	Об'єкт критично важливої інформаційної інфраструктури	IP і технології, а також IT системи та мережі усіх форм власності, що керуються АСУ й використовуються як для передавання інформації, яка в них циркулює, так й для впливу на аналогічні об'єкти протилежної сторони
35.	Об'єкти посягань кібервоєн	суспільство, органи влади та управління, збройні сили, органи безпеки і правопорядку, політичні партії та блоки, громадські організації, ЗМІ, наукові підрозділи та установи тощо
36.	Програмна закладка	спеціальне ПЗ або програмно-математичний алгоритм, призначені для виконання прихованих несанкціонованих дій (обхід контролю доступу, знищення, блокування, модифікація або копіювання даних, порушення штатного режиму функціонування тощо) в ІС
37.	Системний моніторинг відкритих і відносно відкритих джерел	процес постійного збору з таких джерел широкого спектра інформації про одне й те ж явище, подію чи об'єкт розвідки, її обробки та приведення у структуровану і логічно обґрунтовану систему залежностей (просторово-часових, причинно-наслідкових та інших) для підготовки оперативних і виважених рішень за визначеною тематикою
38.	Соціальна інженерія	комплекс заходів, спрямованих на одержання неавторизованим користувачем НСД до інформації про призначення, структуру, встановлені права доступу, систему захисту, реєстраційні імена і паролі, а також іншої конфіденційної інформації про об'єкт атаки – людину (їх групу), використовуючи його (їх) слабкість або некомпетентність, непрофесіоналізм або недбалість та керуючи його (їх) діями
39.	Суб'єкти інформаційної інфраструктури	держави або їх коаліції, угруповання військ, окремі фахівці або їх групи – інакше користувачі або так звані активні компоненти, що ведуть боротьбу в інформаційному та кіберпросторах
40.	Телекомунікаційна мережа	комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням
41.	Телекомунікаційна система	сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб

PS: запропонований понятійний апарат у сфері забезпечення кібернетичної безпеки є довідковим. Він сформований за алфавітним порядком з урахуванням узагальнення змісту основних понять та їх неофіційного перекладу, визначених зарубіжними експертами та окремими нормативно-правовими документами іноземних країн (зокрема, США, Великобританії, Росії та Польщі).

НАВЧАЛЬНЕ ВИДАННЯ

Володимир Леонідович БУРЯЧОК
Геннадій Миколайович ГУЛАК
Володимир Борисович ТОЛУБКО

ІНФОРМАЦІЙНИЙ ТА КІБЕРПРОСТОРИ: проблеми безпеки, методи та засоби боротьби

Підручник

(українською мовою)

Видається у авторській редакції
Надруковано з оригінал макета замовника

художник-дизайнер Л.В. Бурячок
комп'ютерна верстка П.М. Складанний

Підписано до друку 30 жовтня.2015 р.
Формат 60х84/16. Друк офсетний. Папір офсетний. Гарнітура Таймс.
Ум. друк. аркушів 28.1. Наклад 350 прим.
Віддруковано ТОВ «Наш формат»
м. Київ, пр. Миру, 7, к.45