МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Державний університет телекомунікацій

Київський національний університет імені Тараса Шевченка

В. Л. БУРЯЧОК, С. В. ТОЛЮПА, В. В. СЕМКО,
П. М. СКЛАДАННИЙ, Л.В.БУРЯЧОК, Н.В.ЛУКОВА-ЧУЙКО

ІНФОРМАЦІЙНИЙ ТА КІБЕРПРОСТОРИ:

проблеми безпеки, методи та засоби боротьби

ПОСІБНИК

(л а б о р а т о р н и й п р а к т и к у м)

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

Київ ДУТ 2016

БКК 32.973-018.2я.73
БІ-74
УДК 004.056(075.8)

Гриф надано Міністерством освіти і науки України
згідно з листом №1/11-8662 від 22.06.2015

Рекомендовано до друку та використання в навчальному процесі
вченими радами

Державного університету телекомунікацій
(протокол № 24 від 17.06.2015 року)
Київського національного університету імені Тараса Шевченка
(протокол № 11 від 17.11.2015 року)

А в то р и:
В.Л.Бурячок, доктор технічних наук, професор;
С.В.Толюпа, доктор технічних наук, профессор;
В.В.Семко, кандидат технічних наук, доцент;
П.М.Складанний, аспірант;
Л.В.Бурячок, аспірант;
Лукова-Чуйко Н.В., кандидат фізико-математичних наук, доцент

Р е ц е н з е н т и:
доктор технічних наук, с.н.с. Р.В.Грищук;
доктор технічних наук, доцент І.Ю. Субач

Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В. Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний Н.В. Лукова-Чуйко – К. : ДУТ - КНУ, 2016. – 178 с.
БІ-74
ISBN 978–617–7092–78–9

У посібнику представлено низку лабораторних робіт за такими темами: ознаки, принципи становлення та розвитку сучасного інформаційного суспільства; кіберпростір та мережа Internet: становлення, структура, проблемні аспекти функціонування; система безпеки інформаційного і кіберпросторів: формування та розвиток, а також засоби та способи боротьби в інформаційному і кіберпросторах. Їх засвоєння дозволить більш глибоко та детально розглянути основні положення, поняття й визначення щодо базових аспектів захисту інформації, створення та експлуатації захищених інформаційних та комунікаційних систем.

Посібник буде корисний науковим та науково-педагогічним працівникам, аспірантам, магістрантам і студенам вищих навчальних закладів, що навчаються за спеціальністю 125 «Кібернетична безпека».

ISBN 978–617–7092–78–9

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АРМ	–	автоматизоване робоче місце
АСУ	–	автоматизована система управління
БД (БнД)	–	база даних (банк даних)
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
КСЗІ	–	комплексна система захисту інформації
ЛОМ	–	локальна обчислювальна мережа
НСД	–	несанкціонований доступ
ОС	–	операційна система
ПЕОМ	–	персональна ЕОМ
ПІБ	–	політика інформаційної безпеки
ПЗ	–	програмне забезпечення
СЗІ	–	система захисту інформації
СПЗ	–	спеціальне програмне забезпечення
СУБД	–	системи управління базами даних
ТЗІ	–	технічний захист інформації

ПЕРЕДМОВА

Глобальна інформатизація останнім часом 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 й 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 й 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 прирівнює 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 та кібернетичної безпеки.

Автори висловлюють щиру вдячність доценту Субачу І.Ю. (Військовий інститут телекомунікацій та інформатизації, м.Київ) та Грищуку Р.В. (Житомирський військовий інститут ім. С.П.Корольова, м. Житомир), зауваження і поради яких сприяли значному покращенню та поглибленню викладеного у посібнику матеріалу.

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

1. Почепцов Г. Г. Інформаційна політика / Г.Г.Почепцов. С.А.Чукут. - К.: Знання. 2008. – 663 с.
2. Силаенков А.Н. Проектирование системы информационной безопасности: учеб. пособие – Омск: Изд-во ОмГТУ, 2009. – 128 с.
3. Богуш В.М. Основи інформаційної культури (електронний варіант). - К.: ДУІКТ, 2002. – 244 стор.
4. Бурячок В.Л. Варіант механізму злому інформаційно-телекомунікаційних систем та їх захисту від стороннього кібернетичного впливу. // Науково-технічний журнал «Сучасний захист інформації» ДУІКТ України, № 4, 2011, с. 76 – 84
5. Соколов Д.Н., Степанюк А.Д. Защита от компьютерного терроризма. – М.: БХВ-Петербург, Арлит, 2002. – 456 с.
6. Леваков Г.Н. Анатомия информационной безопасности. – М.: ТК Велби, издательство Проспект, 2004. – 256 с.
7. Сыч О.С. Комплексная антивирусная защита локальной сети. – М.: финансы и статистика, 2006. – 736 с.
8. Бурячок В.Л. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу. // В.Л.Бурячок, О.Г. Корченко, В.О., Хорошко, В.А. Кудінов / Науково-технічний журнал «Захист інформації» Національного авіаційного університету. Том 15, № 1, 2013, с. 5 – 14
9. Грязнов Е.С., Панасенко С.А. Безопасность локальных сетей. – М.: Вузовский учебник, 2006.- 525 с.
10. Козлачков П.С. Основные направления развития систем информационной безопасности. – М.: финансы и статистика, 2004. – 736 с.
11. Бурячок В.Л. Сучасні системи виявлення атак в інформаційно-телекомунікаційних системах і мережах. Модель вибору раціонального варіанта реагування на прояви стороннього кібернетичного впливу. // Науковий журнал «Інформаційна безпека» Східноукраїнського національного університету ім. В.Даля, № 1(9), 2013, с. 33 – 40
12. 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.
13. Перфильев Ю.Ю. Российское Интернет-пространство: развитие и структура / Перфильев Ю.Ю. - М.:Гардарики. 2003. - 272с.

14. 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=bef81c55bc3cb65d2076769b3ba3e52
15. Бурячок В.Л. Модель формування дерева атак для одержання інформації в інформаційно-телекомунікаційних системах і мережах при вилученому доступі. // Науковий журнал «Інформатика та математичні методи в моделюванні» Одеського національного політехнічного університету, № 2, 2013, с. 123 – 131
16. Черняк В.З. Тайны промышленного шпионажа. / В.З. Черняк. – М.: Вече, 2002. – 512 с.
17. 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.
18. Бурячок В.Л. Практичні аспекти методології сучасного інформаційного пошуку // Інформаційна безпека. – 2011. – № 2(6). – С. 149–154.
19. 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.
20. 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.
21. Ярочкин В.И. Технические каналы утечки информации. / В.И. Ярочкин. – М.: ИПКИР, 1994. – 112 с.
22. 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.
23. 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.
24. Богуш В.М., Кудін А.М. Інформаційна безпека від А до Я: 3000 термінів і понять. - К.: МОУ, 1999. - 456 с.
25. Бурячок В.Л. Технологія використання уразливостей Web ресурсів у процесі організації та проведення мережевої розвідки інформаційно-телекомунікаційних систем // Науковий журнал "Безпека інформації" Національного авіаційного університету. Том 19#2, 2013. с. 83 – 87

26. Гнатюк С.О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. // Безпека інформації. – 2013. – Том 19, № 2 (2013) – С. 118-129.
27. 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.
28. 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.
29. 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.
30. 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.
31. Практика ИБ \ SANS - Топ 20 наиболее критичных защитных мер и средств. https://www.sugarsync.com/pf/D6870693_7400982_60553
32. Бурячок В.Л. Застосування бездротових мереж в ході організації та проведення розвідки систем телекомунікацій // Науково-технічний журнал «Сучасний захист інформації» Державного університету телекомунікацій. № 4, 2013, с. 57 – 67
33. Семенов Ю.А. Обзор по материалам ведущих фирм, работающих в сфере сетевой безопасности. [Електронний ресурс]. – Режим доступу: http://book.itep.ru/10/2012.htm
34. Competitive intelligence. [Електронний ресурс]. – Режим доступу: http://en.wikipedia.org/wiki/Competitive_intelligence.
35. 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.
36. Аносов А.О. Моделювання DDos атак на комп'ютерні мережі для визначення ознак їх проведення / А.О. Аносов // Науково-технічний журнал «Сучасний захист інформації» – 2015. – № 3. – С. 13 – 17.
37. Бурячок В.Л.. Оценка живучести систем защиты информационного пространства систем управления воздушным движением // В.Л. Бурячок, С.О. Гнатюк / Безпека інформації. – Том 19, №1. – 2013. – С. 40-45.
38. Словник термінів з кібербезпеки / За загальною редакцією Копана О.В., Скулиша Є.Д. – К. : ВБ «Аванпост-Прим». – 2012. – 214 с.
39. Почепцов Г.Г. Информационные войны.- М.: Рефл-бук, К.: Ваклер, 2001.- 576 с.

40. Гриняев С. Н. Поле битвы – киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны. – Мн.: Харвест, 2004. – 448 с.
41. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.:НАУ, 2013. – 432 с.
42. 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.
43. 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.
44. Конкурентная разведка в Internet / В.В.Дудихин, О.В.Дудихина. 2-е изд. испр. и доп. – М.: ООО "Издательство АСТ", 2004. – 229 с.
45. М.Левин. E-mail "безопасная": взлом, "спам" и "хакерские" атаки на системы электронной почты Internet. – М.: Бук-пресс, 2006. – 192 с.
46. Peter Neumann, Donald Parker. A summary of computer misuse techniques. In 12th National Computer Security Conference, 1989.
47. Peter Neumann. Computer-Related Risk. ACM Press/Addison Wesley, 1995.
48. Гриняев С.Н. Интеллектуальное противодействие информационному оружию. – М.: СИНТЕГ, 1999. – 232 с.

НАВЧАЛЬНЕ ВИДАННЯ

Володимир Леонідович БУРЯЧОК
Сергій Васильович ТОЛЮПА
Віктор Володимирович СЕМКО
Павло Миколайович СКЛАДАННИЙ
Лідія Володимирівна БУРЯЧОК
Наталія Вікторівна ЛУКОВА-ЧУЙКО

ІНФОРМАЦІЙНИЙ ТА КІБЕРПРОСТОРИ:
проблеми безпеки, методи та засоби боротьби
Посібник
(л а б о р а т о р н и й п р а к т и к у м)

(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 11.1. Наклад 350 прим.
Віддруковано ТОВ «Наш формат»
м. Київ, пр. Миру, 7, к.45