В. М. БОГУШ, В. В. БОГУШ, В. Д. БРОВКО, В. П. НАСТРАДІН

ОСНОВИ КІБЕРПРОСТОРУ, КІБЕРБЕЗПЕКИ ТА КІБЕРЗАХИСТУ

Навчальний посібник

Київ
Видавництво Ліра-К
2020

УДК **004.056.5**
О 60

Автори: В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін

Рецензенти:

Бурячок В. В., д-р техн. наук, професор;
Кудін А. М., д-р техн. наук, старший науковий співробітник;
Козюра В. Д., к-т техн. наук, доцент

О 60 **Основи кіберпростору, кібербезпеки та кіберзахисту.** Навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під. ред. В. М. Богуша. — К.: Видавництво Ліра-К, 2020. — 554 с.

ISBN 978-617-7844-54-8

У навчальному посібнику наведена систематизована сукупність відомостей про стан та перспективи розвитку широкого кола методологічних, наукових та технічних основ побудови кіберпростору, процесів протиборства у кіберпросторі, організацію забезпечення безпеки кіберпростору, методи та засоби забезпечення кіберзахисту. Навчальний посібник створений за результатами детального аналітичного вивчення сучасної міжнародної та національної нормативно-правової бази щодо сфери забезпечення кібербезпеки на міжнародному, державному рівні та на рівні організації.

Розрахований на студентів молодших курсів вищих навчальних закладів, які навчаються за всіма освітніми програмами спеціальності 125 Кібербезпека.

ISBN 978-617-7844-54-8 УДК **004.056.5**

ЗМІСТ

ВСТУП

Під впливом швидкого розвитку інформаційних технологій формуються нові — віртуальні — середовища різноманітних просторів, які набувають все більшої значущості як у міжнародних та державних відносинах, так і у зовнішніх та внутрішніх відносинах конкретних організацій. До кола таких віртуальних середовищ належить кіберпростір, що позначає особливу область соціальних взаємодій, опосередкованих сукупністю процесів, що відбуваються в інформаційно-комунікаційних мережах світу, і який перетворився на ще одне середовище буття та діяльності людини.

Крім Інтернету до кіберпростіру належать багато інших мереж, наприклад, транснаціональних, через які відбувається передача даних про фінансові потоки, торги на різних біржах і операції по кредитних лініях.

Крім того, в кіберпросторі функціонують системи управління різноманітними машинами і механізмами, наприклад, панелі керування генераторами, ліфтами, насосами, транспортними та енергетичними системами тощо.

Особлива та дуже важлива частина кіберпростору належить системам та мережі управління воєнною технікою, зокрема безпілотниками (дронами), бойовими роботами, ракетами різного радіусу дії.

Цей короткий і далеко не повний перелік дозволяє дійти висновку, що кіберпростір сьогодні являє собою життєво важливу галузь інформаційної, економічної, політичної, воєнної діяльності окремих людей, корпорацій, держав та їх спільнот, наднаціональних структур і утворень.

Кіберпростір, що не обмежений державними кордонами, став найважливішим полем політичної, економічної, інформаційної та культурної конкуренції держав, суспільств та особистостей, в якому стикаються інтереси різних політичних суб'єктів, різних держав і центрів політичної сили.

Майже відразу ж після свого виникнення кіберпростір перетворився у п'яте (після суші, моря, повітря і космосу) поле битви різних політичних і воєнних сил і залишається таким [68]. Більше того, безліч протистоянь між розвідувальними організаціями різних країн, їх воєнними структурами, а також економічні та інформаційні війни, зокрема шпигунство і диверсії,

розгортаються саме у кіберпросторі. Ця обставина визначає високу значимість процесів, що відбуваються у кіберпросторі, для сучасного стану національної безпеки.

У міру розвитку кіберпростору в ньому виникали та посилювалися різні загрози, а також відповідні заходи щодо протидії цим загрозам і їх нейтралізації.

Згідно з визначенням Міжнародного союзу комунікацій, кібербезпека являє собою набір засобів, стратегій і принципів забезпечення безпеки, гарантії безпеки, підходів до управління ризиками, дії і практичного досвіду для захисту кіберсередовища, ресурсів організації і користувача [112].

Кібербезпека охоплює заходи, які можна здійснити для захисту кіберпростору як у цивільній, так і у воєнній області від загроз, які пов'язані зі сформованими в ньому взаємозалежними мережами та інформаційною інфраструктурою або можуть завдати даній інфраструктурі шкоди.

Очевидно, що кібербезпека не може розглядатися ізольовано від інших аспектів і видів внутрішньої та міжнародної безпеки, а кіберзлочинність тісно пов'язана з іншими видами злочинності, такими як промислове шпигунство, діяльність розвідувальних служб, міжнародний тероризм [116].

У той же час кібербезпека має яскраво виражену специфіку, яка визначається використанням інформаційних технологій, що швидко розвиваються, її необхідно розглядати як особливу сферу національної та міжнародної безпеки з власними тенденціями розвитку та властивим їй інструментарієм.

При цьому однією зі специфічних рис кібербезпеки є те, що межа між кіберзлочинністю, застосуванням кіберзброї і діями різних політичних акторів (наприклад, спецслужб різних держав) досить розмита і невизначена. Наразі виникає складність ідентифікації джерела і характеру загроз для кіберпростору, яка вже стала чинником численних внутрішньополітичних і міжнародних конфліктів, взаємних звинувачень і політичної «боротьби без правил».

У навчальному посібнику наведена систематизована сукупність відомостей про стан та перспективи розвитку широкого кола методологічних, наукових та технічних основ побудови кіберпростору, процесів протиборства у кіберпросторі, організацію забезпечення безпеки кіберпростору, методи та засоби забезпечення кіберзахисту.

Навчальний посібник створений за результатами детального аналітичного вивчення сучасної міжнародної та національної нормативно-правової бази щодо сфери забезпечення кібербезпеки на міжнародному, державному рівні та на рівні організації. Він складається з трьох частин і чотирнадцяти розділів.

У **першій частині** посібника здійснений аналіз основних напрямів розвитку теоретичних основ побудови та дослідження кіберпростору. Сформульовані загальні підходи щодо побудови, розвитку і використання інфраструктури кіберпростору та сервісів кіберпростору, а також методів та засобів дослідження соціологічної та психологічної сфери кіберпростору з метою виявлення загроз безпеці кіберпростору.

У **другій частині** посібника на основі системного підходу викладені методологічні та теоретичні основи забезпечення безпеки особистості, суспільства та держави у кіберпросторі, що охоплює кіберінфраструктуру, кіберсервіси, соціологічні та психологічні сфери, пов'язані з діяльністю людей. Наведені теоретичні та методологічні основи запобігання кіберзлочинності, кібертероризму, кіберконфліктам і кібервійнам на основі впровадження методів та засобів забезпечення кібербезпеки.

У **третій частині** посібника визначені загальні завдання побудови та впровадження технологій та засобів захисту інфраструктури кіберпростору, основні напрями дослідження середовища кібербезпеки організації та розробки загальних підходів її кіберзахисту, загальної методології обґрунтування засобів, заходів та технологій кіберзахисту організації, процесу побудови системи її кіберзахисту.

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

Автори висловлюють щиру вдячність рецензентам: доктору технічних наук, професору В. Л. Бурячку, доктору технічних наук, старшому науковому співробітнику А. М. Кудіну та кандидату технічних наук, доценту В. Д. Козюрі за змістовні зауваження та рекомендації, які безумовно сприяли покращенню книги.

ПЕРЕЛІК АБРЕВІАТУР

Україномовні

АСУ	—	автоматизована система управління
ВВС	—	взаємодія відкритих систем
ЕОМ	—	електронно-обчислювальна машина
ЕЦП	—	електронний цифровий підпис
ІКМ	—	інформаційно-комунікаційна мережа
ІКТ	—	інформаційно-комунікаційна технологія
ІнАУ	—	Інтернет асоціація України
ІПС	—	інформаційно-пошукова система
ІС	—	інформаційна система
ЗКТ	—	засоби комп'ютерної техніки
ЗМІ	—	засоби масової інформації
КВО	—	критично важливий об'єкт
КНШ	—	комітет начальників штабів
МКХ	—	міжнародний класифікатор хвороб
НСД	—	несанкціонований доступ
ОС	—	операційна система
ПК	—	персональний комп'ютер
ПЕМВ	—	побічні електромагнітні випромінювання
РЄ	—	Рада Європи
РЕЗ	—	радіоелектронний засіб
САПР	—	система автоматизованого проєктування
СЗІБ	—	система забезпечення інформаційної безпеки
СЗІ	—	система захисту інформації
СІБ	—	система інформаційної безпеки
СУБД	—	система управління базою даних
СУБМ	—	система управління базою моделей
СУІБ	—	система управління інформаційною безпекою
ТД	—	точка доступу
ТЗ	—	технічний засіб
УНІАН	—	українське незалежне інформаційне агентство новин
ЦС	—	центр сертифікації

Англомовні

API	—	Application Programming Interface (прикладний програмний інтерфейс)
AR	—	Augmented Reality (доповнена реальність)
BcN	—	Broadband convergence Network (мережа конвергенції широкосмугового зв'язку)
C4I2	—	Command, Control, Communications, Computing, Intelligence and Information Systems
C4ISR	—	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (система оперативного (бойового) управління, зв'язку, розвідки та спостереження)
C4IEW	—	Communications, Computers, Intelligence, Electronic Warfare
CDMA	—	Code Division Multiple Access (багатостанційний доступ з кодовим розділенням каналів)
CERT	—	Computer Emergency Response Team (команда реагування на комп'ютерні надзвичайні події)
CIRT	—	Cyber Incident Response Team (команда реагування на інциденти)
CSIRT	—	Computer Security Incident Response Team (команда комп'ютерної безпеки з реагування на інциденти)
CYBEX	—	Cybersecurity Information Exchange techniques (методи обміну інформацією про кібербезпеку)
DNS	—	Domain Name System (система доменних імен)
DoS	—	Denial of Service (відмова в обслуговувані)
DDoS	—	Distributed Denial of Service (розподілена відмова в обслуговані
DSM	—	Diagnostic and Statistical Manual of mental disorders (діагностичний і статистичний посібник з психічних розладів)
DTD	—	— Document Type Definition (визначення типу документа)
DWDM	—	Dense Wavelength Division Multiplexing (щільне мультиплексування з розділенням за довжиною хвилі)
EMS	—	Enterprise Management Systems (система управління підприємством)
FGN	—	Future Generation Network (мережа майбутнього покоління)
ICA	—	InfoCommunication Actor (автор (учасник) кіберінфраструктури)
ICT	—	Information and Communication Technology (інформаційно-комунікаційна технологія)
IDS	—	Intrusion Detection System (система виявлення вторгнень)
IMS	—	IP Multimedia Subsystem (мультимедійна підсистема на основі протоколу IP)
IoT	—	Internet of Things (Інтернет речей)
IP	—	Internet Protocol (міжмережний протокол)
IPO	—	Information Providing Organizations (організація, що є стороною, яка передає інформацію)

IRO	—	Information Receiving Organizations (організація, яка є стороною, що приймає інформацію)
IPTV	—	Internet Protocol Television (цифрове телебачення за протоколом IP
IT	—	Information Technology (інформаційна технологія)
ITU	—	International Telecommunication Union (Міжнародний союз телекомунікацій)
ISMS	—	information security management system (система управління інформаційною безпекою)
ISO	—	International Organization for Standardization (Міжнародна організація стандартизації)
JCS	—	Joint Chiefs of Staff (Комітет начальників штабів)
HTML	—	Hypertext Markup Language (мова розмітки гіпертекстових документів)
HTTP	—	Hyper Text Transfer Protocol (протокол передавання гіпертекстових документів)
LAN	—	Local Area Network (локальна обчислювальна мережа)
LDAP	—	Lightweight Directory Access Protocol (полегшений протокол доступу до директорій/каталогів)
LTE	—	Long Term Evolution («довготерміновий розвиток»)
MIME	—	Multipurpose Internet Mail Extensions (багатоцільові розширення для інтернет-пошти)
NAT	—	Network Address Translation (перетворення мережних адрес)
NOC	—	Network Operations Center (мережний операційний центр)
NGN	—	Next Generation Network (мережа наступного покоління)
OAM&P	—	Operations, Administration, Maintenance, and Provisioning (операції, адміністрування та управління або операції, адміністрування та обслуговування)
OSI	—	Open Systems Interconnection model (модель взаємодії відкритих систем)
PKI	—	Public Key Infrastructure (інфраструктура відкриих ключів)
RADIUS	—	Remote Authentication in Dial-In User Service (протокол для реалізації автентифікації, авторизації та збору відомостей про використані ресурси)
SAM	—	Software Asset Management (менеджмент програмних активів)
SDP	—	Service Delivery Platform (платформа надання послуг)
SEO	—	Search Engine Optimization (пошукова оптимізація)
SMM	—	Social Media Marketing (просування в соціальних мережах)
SMO	—	Social Media Optimization (оптимізація для соціальних мереж)
SSID	—	Service Set Identifier (символьна назва безпрової точки доступа Wi-Fi
SQL	—	Structured Query Language (мова структурованих запитів)

VLAN	—	Virtual Local Area Network (віртуальна локальна мережа)
URL	—	Uniform Resource Locator (універсальний покажчик на ресурс)
VAR	—	Value Added Reseller (реселлер, що надає послуги)
VoIP	—	Voice over IP (передавання голосу за протоколом IP)
VPN	—	Virtual Private Network (віртуальна приватна мережа)
WLAN	—	Wireless Local Area Network (бездротова локальна мережа)
WSW	—	Wireless Sensor Networks (безпровідна сенсорна мережа)
WWW	—	World Wide Web (Всесвітня павутина)

Частина I

ОСНОВИ КІБЕРПРОСТОРУ

Розділ 1

ОСНОВНІ ПОЛОЖЕННЯ ТА ВИЗНАЧЕННЯ КІБЕРПРОСТОРУ

1.1. Загальне визначення простору та інформаційного простору

Простір [space] це одна з основних форм існування матерії (філос.), яка характеризується протяжністю і обсягом. Відповідно до спеціальної теорії відносності існує тісний зв'язок простору і часу.

На рівні практичного сприйняття під простором розуміють місце, у якому можливий рух, різноманітні положення і розташування об'єктів, відношення близькості-дальності, поняття спрямованості, місце, де відбуваються події і дії, що містить всі місця, об'єкти і структури.

Інформаційний простір [information space] — одне з первинних понять, що не може бути точно визначене. Найчастіше термін розуміють як логічне зіставлення об'єктному (предметному, фізичному, матеріальному) світу. З практичної точки зору вважається, що інформаційний простір — це теж саме, що семантичний простір [21].

Для практичного застосування краще використати визначення інформаційного простору як будь-якого середовища, де інформація створюється, через яке передається, приймається, в якому зберігається, обробляється і знищується [86].

Основними компонентами інформаційного простору є:

— інформаційні ресурси;
— засоби інформаційної взаємодії;
— інформаційна інфраструктура.

1.2. Основні положення інформаційного простору

1.2.1. Інформаційні ресурси

У загальному випадку під інформаційними ресурсами розуміють результат об'єктивного цілеспрямованого відображення закономірностей і фактів реалізації будь-яких процесів, що відбуваються у суспільстві та в навколишньому середовищі (природі). Вони являють собою сукупність наукових знань, зафіксованих на паперових чи інших носіях, що зберігають-

ся у довідково-інформаційних фондах інформаційних органів та бібліотек [11].

До інформаційних ресурсів також відносять окремі документи і окремі масиви документів, документи і масиви документів у інформаційних системах (бібліотеках, архівах, фондах, банках, банках даних і т. ін.), що містять інформацію з усіх напрямків життєдіяльності суспільства, а також сукупність даних, які є цінними для установи (організації) і виступають як матеріальні ресурси, зокрема, це основні та допоміжні дані, що зберігаються в зовнішній пам'яті комп'ютерних систем, та вхідні документи.

Класифікація інформаційних ресурсів:

за видом інформації — інформаційні ресурси, що можуть містити інформацію наступних видів:

- правову;
- науково-технічну;
- політичну;
- економічну (фінансово-економічну);
- статистичну;
- інформацію про стандарти і регламенти, метрологічну;
- соціальну;
- інформацію про охорону здоров'я;
- інформацію про надзвичайні ситуації;
- особисту інформацію (персональні дані);
- кадастри (земельний, містобудівний, лісовий, майновий і т. ін.);
- інформацію іншого виду;

за режимом доступу — інформаційні ресурси, що містять відкриту інформацію (без обмежень) або інформацію обмеженого доступу (державну таємницю, конфіденційну інформацію, комерційну таємницю, професійну таємницю, службову таємницю, особисту (персональну) таємницю);

за видом носія — інформаційні ресурси, інформація в яких може бути записана на папері, на машиночитаних носіях, у вигляді зображення на папері, на екрані ЕОМ, в пам'яті ЕОМ, у каналах зв'язку, на інших видах носіїв;

за способом формування і розповсюдження — інформаційні ресурси, що знаходяться у стаціонарному або рухомому (мобільному) стані;

за способом організації зберігання і використання— інформаційні ресурси, для зберігання і використання інформації, в яких можуть використовуватися традиційні форми (масиви документів, фонди документів, архіви) або автоматизовані форми (банки даних, інформаційні системи, бази знань);

за формою власності — інформаційні ресурси, що можуть складати:
— загальнодержавне національне надбання;
— державну власність;
муніципальну власність;
— приватну власність;
— колективну власність.

1.2.2. Засоби інформаційної взаємодії

Умови інформаційної взаємодії

Термін «інформація» походить від лат. informatio, що означає «роз'яснення» і передбачає наявність будь-якої форми діалогу між відправниками і одержувачами інформації.

Усі якісні і кількісні визначення інформації також передбачають наявність відправників і одержувачів інформації, тобто мова йде про деякий вид взаємодії об'єктів.

Взаємодію об'єктів, яка призводить до зміни знань хоч би одного з них, можна назвати **інформаційною взаємодією**, а сукупність засобів, що забезпечують взаємодію об'єктів — засобами інформаційної взаємодії [48].

Умови інформаційної взаємодії на прикладі передачі знань за допомогою усного мовлення можна сформулювати наступним чином.

Для того, щоб процес передачі знань від одного об'єкта до іншого був успішним, слід дотримуватися низки умов. **Процес інформаційної взаємодії** на прикладі передачі знань за допомогою усного мовлення можна уявити п'ятикомпонентною (п'ятивимірною векторною) величиною, що складається з компонентів:

1. фізичної;
2. сигнальної;
3. лінгвістичної;
4. семантичної;
5. прагматичної.

Перша компонента — фізична, тобто необхідна наявність фізичного джерела звуку (голосових зв'язок), фізичного середовища поширення звуку (повітря) і фізичного приймача (вуха).

Друга компонента — сигнальна: амплітудно і частотно модульовані коливання.

Третя компонента — лінгвістична: необхідно, щоб обидва співрозмовники знали хоча б одну спільну мову.

Четверта компонента — семантична, тобто в переданому повідомленні повинен бути присутнім змістовний опис об'єкта або впливу, щоб при отриманні повідомлення могли змінитися знання у того, хто приймає ці повідомлення

П'ята компонента — прагматична: необхідна наявність бажання (мотивації) передавати і приймати повідомлення.

Інформаційна взаємодія відкритих систем

Як приклад класифікації інформаційних взаємодій можна навести протокольні рівні в міжнародних стандартах взаємодії відкритих мереж [93]. При взаємодії двох користувачів в комунікаційній мережі реалізується сукупність протоколів семи рівнів:

1. фізичного;
2. канального;
3. мережного;
4. транспортного;
5. сеансового;
6. представницького;
7. прикладного.

Перші три протокольних рівні визначають такі особливості роботи мережі зв'язку при обслуговуванні користувачів, як стандарт електричних сигналів в мережі, виявлення та виправлення помилок, маршрутизація в транспортній мережі і т. ін.

Наступні чотири рівні визначають такі стандарти взаємодії самих користувачів, як контроль за цілісністю повідомлення, відновлення без втрат сеансу взаємодії в разі переривання, представлення даних на дисплеях і друкуючих пристроях тощо.

Класи взаємодії відкритих систем

Спектр інформаційних взаємодій надзвичайно широкий. Можна умовно розділити досліджувані інформаційні взаємодії по об'єктах на три класи:

1-й клас — взаємодія штучних (технічних) систем;

2-й клас — взаємодія змішаних систем;

3-й клас — взаємодія природних (живих) систем.

До першого класу відносяться інформаційні взаємодії в технічних системах — від найпростіших регуляторів до глобальних комп'ютерних мереж.

До другого класу — інформаційні взаємодії типу «живий організм — штучний орган», «людина — машина», «живий дослідник — неживий об'єкт досліджень» і т. ін.

До третього класу належать інформаційні взаємодії, що діють в межах від молекулярно-генетичного рівня до рівня соціальних спільнот.

При такому різноманітті взаємодіючих об'єктів завдання опису законів інформаційної взаємодії надзвичайно складне, оскільки треба описати як обмін однобітовою інформацією типу «включено — виключено» в технічних системах, так і формування моралі в людських співтовариствах.

При описі кожного з цих рівнів доводиться спиратися на специфічну для відповідного рівня концепцію перетворювача інформації, свої мови опису, закономірності, що розробляються в рамках відповідних дисциплін (наук), які, тим самим, вивчають інформаційну взаємодію на даному рівні.

1.2.3. Інформаційна інфраструктура

Інформаційна інфраструктура [information infrastructure] — система організаційних структур і підсистем, що забезпечують функціонування засобів інформаційної взаємодії в інформаційному просторі.

Вона включає в себе: сукупність інформаційних центрів, підсистем, банків даних і знань, систем комунікацій, центрів управління, апаратно-програмних засобів і технологій, що забезпечують збирання, зберігання, оброблення і передавання інформації, а також доступ споживачів до інформаційних ресурсів [11].

Глобальна інформаційна інфраструктура — інформаційна інфраструктура світового (міждержавного) масштабу. Може створюватися на основі трансформації національних інформаційних інфраструктур при створенні глобального інформаційного суспільства з дотриманням наступних принципів:

- забезпечення справедливої конкуренції;
- заохочення приватних інвестицій;
- визначення й адаптація регулюючих механізмів;
- забезпечення відкритого доступу до мереж;
- створення умов для забезпечення універсального доступу до інформаційних послуг;
- забезпечення рівних можливостей для громадян;
- забезпечення різноманітності змісту, включаючи культурний і мовний.

Ці принципи застосовуються до глобальної інформаційної інфраструктури за допомогою: