

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДНП “Державний університет “Київський авіаційний інститут”
Факультет комп’ютерних наук та технологій

Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед та ін.

СИСТЕМИ ІНФОРМАЦІЙНОЇ ЗБРОЇ ТА ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОЇ ВІЙНИ

Підручник

Видання 2-е, виправлене та перероблене

За загальною редакцією

кандидата наук з державного управління, доцента,
члена-кореспондента Міжнародної академії богословських наук
ПЕТРИКА Валентина Михайловича

кандидата технічних наук, старшого наукового співробітника
ПРИСЯЖНЮКА Миколи Миколайовича

доктора технічних наук у галузі кібербезпеки (Dr.Sc), PhD
АЛЬ-ФАЙЮМІ Халеда

Київ – 2026

УДК 342.9 (477)
П 29

Рекомендовано Вченою радою
факультету комп'ютерних наук та технологій КАІ,
протокол № 2 від 21 лютого 2026 року

РЕЦЕНЗЕНТИ:

НОВИЦЬКИЙ Андрій Миколайович – доктор юридичних наук, професор;
НОВИЦЬКА Наталія Борисівна – доктор юридичних наук, професор

Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед та ін.

П 29 Системи інформаційної зброї та технології інформаційної війни: підручник. Видання 2-е, виправлене та перероблене / За заг. ред. В. М. Петрика, М. М. Присяжнюка, Аль-Файюмі Халеда. – К.: Видавничий центр “Кафедра”, 2026. – 316 с.

ISBN 978-966-370-306-0

У підручнику розкриваються особливості використання систем інформаційної зброї, сучасні технології та практика їх застосування у проведенні інформаційних війн, спеціальних інформаційних операцій і акцій інформаційного впливу проти України. Також розглядаються історія інформаційно-психологічного протиборства, також засоби, методи та сучасні технології соціальної інженерії і особливості захисту інформації від атак соціальної інженерії з врахуванням людського фактору.

Підручник рекомендується для викладання навчальних дисциплін “Системи інформаційної зброї та технології інформаційної війни” “Інформаційно-психологічне протиборство”, “Інформаційна безпека”, “Інформаційна безпека держави”, “Забезпечення інформаційної безпеки держави”, “Управління інформаційною безпекою”, “Кібергігієна”, “Інцидент-менеджмент у кіберпросторі”. Також може використовуватися для викладання таких дисциплін, як: “Психологія” та “Безпека життєдіяльності”.

Авторський колектив:

Петрик В. М.: задум, *Частина 1* (розділи 1-3, 5), *Частина 3* (розділ 4), додаток;
Присяжнюк М. М.: *Частина 1* (розділ 4), *Частина 2* (розділи 3-4), іменний і тематичний покажчики; Жарков Я. М.: *Частина 2* (підрозділи 1.1-1.2, розділ 2); Стайкуца С.В.: *Частина 3* (підрозділ 1.1); Цибулькін В.В.: *Частина 2* (підрозділ 1.3); Івахненко М.С.: *Частина 3* (підрозділ 1.2); Кононович В. Г.: *Частина 3* (підрозділ 1.3); Аль-Файюмі Халед: вступ, *Частина 3* (підрозділ 2.1); Корчинский В. В.: *Частина 3* (підрозділ 2.2); Давидюк А. В.: *Частина 3* (розділ 3); Фесенко А. О.: *Частина 3* (підрозділ 2.3).

УДК 342.9 (477)

ISBN 978-966-370-306-0

© Петрик В. М., Присяжнюк М. М.,
Аль-Файюмі Халед та ін., 2026
© Видавничий центр “Кафедра”, 2026

ЗМІСТ

ВСТУП.....	6
ЧАСТИНА 1.	
ТЕОРЕТИЧНІ ЗАСАДИ ТА СУЧАСНИЙ СТАН ЗАСТОСУВАННЯ ІНФОРМАЦІЙНОЇ ЗБРОЇ ТА ТЕХНОЛОГІЙ ІНФОРМАЦІЙНОЇ ВІЙНИ	
РОЗДІЛ 1. Визначення базових понять, що пов’язані з інформаційною війною та інформаційною зброєю.....	9
1.1. Інформаційна безпека та її різновиди.....	9
1.2. Базові поняття щодо інформаційних впливів.....	11
1.3. Характеристика інформаційно-психологічних впливів та основні поняття, які пов’язані з маніпулюванням.....	21
РОЗДІЛ 2. Інформаційна війна як форма інформаційного протиборства російської федерації проти України.....	30
2.1. Форми і види інформаційного протиборства. Завдання інформаційних війн.....	30
2.2. Об’єкти посягань, об’єкти деструктивного інформаційного впливу та форми інформаційних війн.....	32
2.3. Стратегія і тактика проведення гібридної війни рф проти України.....	36
2.3.1. Теорія гібридної війни В. Герасимова.....	36
2.3.2. Особливості гібридної війни, яку проводить рф проти України.....	39
РОЗДІЛ 3. Сучасні технології проведення спеціальних інформаційних операцій російської федерації проти України.....	46
3.1. Етапи, ознаки, суб’єкти спеціальних інформаційних операцій.....	46
3.2. Методи проведення спеціальних інформаційних операцій.....	50
РОЗДІЛ 4. Інформаційна зброя в сучасних умовах.....	77
4.1. Інформаційний простір як театр сучасних воєнних дій.....	77
4.2. Класифікація сучасної інформаційної зброї.....	81
4.3. Основні способи й методи застосування інформаційної зброї.....	91
РОЗДІЛ 5. Особливості впливу на інформаційний простір України російських та проросійських неурядових організацій.....	96
5.1. Характеристика діяльності російських і проросійських неурядових організацій в Україні.....	96
5.2. Особливості російської шовіністичної ідеології І. Ільїна.....	105
5.2.1. Філософсько-політичні ідеї Івана Ільїна: шлях до шовінізму.....	106
5.2.2. Вплив Івана Ільїна на Олександра Дугіна та володимира путіна: порівняльний аналіз ідеологій.....	109

5.3. Особливості російської неосоціалістичної ідеології О. Дугіна та її історичне підґрунтя.....	112
5.4. Аналіз підривної діяльності проросійських неурядових об'єднань як інструмент анексії Криму.....	129

ЧАСТИНА 2.

ІСТОРІЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ПРОТИБОРСТВА

РОЗДІЛ 1. Становлення та розвиток інформаційно-психологічного протиборства.....	137
1.1. Інформаційно-психологічне протиборство у стародавньому світі та в епоху Середньовіччя.....	137
1.2. Розвиток інформаційно-психологічного протиборства у воєнних конфліктах XIX ст.....	146
1.3. Військові хитрощі українського козацтва.....	152
РОЗДІЛ 2. Формування основ теорії і практики інформаційно-психологічного протиборства в роки Першої світової війни та в міжвоєнний період.....	161
2.1. Інформаційно-психологічне протиборство під час Першої світової війни.....	161
2.2. Діяльність політорганів Червоної Армії серед військ противника в міжвоєнний період.....	165
2.3. Особливості пропаганди фашистської Німеччини в міжвоєнний період.....	171
РОЗДІЛ 3. Інформаційно-психологічне протиборство в роки Другої світової війни.....	183
3.1. Особливості ведення пропаганди Німеччиною і СРСР серед військ та населення противника в роки Другої світової війни.....	183
3.2. Ведення пропаганди США, Англією та Японією в роки Другої світової війни.....	191
РОЗДІЛ 4. Інформаційно-психологічне протиборство часів “холодної війни”.....	198
4.1. Психологічні операції США у війнах і збройних конфліктах.....	198
4.2. Спеціальна пропаганда СРСР в Афганістані у 1979–1989 рр.....	210
4.3. Історичні передумови розвалу СРСР.....	212
4.3.1. Зовнішній вплив, направлений на розвал СРСР.....	216

ЧАСТИНА 3.
СОЦІАЛЬНА ІНЖЕНЕРІЯ: СУЧАСНІ ТЕХНОЛОГІЇ ТА
ШЛЯХИ ЗАХИСТУ

РОЗДІЛ 1. Теоретико-методологічні основи соціальної інженерії.....	232
1.1. Аналітичний розгляд літератури.....	232
1.2. Сучасне застосування соціальної інженерії.....	233
1.3. Людський фактор як вразливість інформаційної безпеки.....	237
 РОЗДІЛ 2. Засоби та методи соціальної інженерії.....	 241
2.1. Головні вектори нападу при проведенні атак за допомогою методів соціальної інженерії.....	241
2.2. Характеристика основних методів соціальної інженерії.....	245
2.3. Види атак із використанням соціальної інженерії.....	248
 РОЗДІЛ 3. Соціальна інженерія як складова складної кібернетичної атаки.....	 255
3.1. Соціально-технічний контекст системи забезпечення кібербезпеки.....	255
3.2. Історична та термінологічна динаміка систем захисту інформації.....	256
3.3. Вразливості та загрози кіберсистемам від соціальної інженерії.....	260
 РОЗДІЛ 4. Особливості захисту інформації від соціальної інженерії з врахуванням людського фактору.....	 273
4.1. Базові методи захисту від атак за допомогою методів соціальної інженерії.....	273
4.2. Організаційні заходи.....	273
4.3. Питання, які повинні бути розглянуті в політиці ІБ.....	276
4.4. Особистісно-психологічний захист від застосування методів соціальної інженерії.....	283
 СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	 299
 ІМЕННИЙ ПОКАЖЧИК.....	 309
 ТЕМАТИЧНИЙ ПОКАЖЧИК (з умовними скороченнями)	 311

ВСТУП

Характерною рисою сучасної цивілізації є її детермінованість інформаційними процесами. Потенційні можливості розвитку основних сфер життя сучасного суспільства зокрема залежать від стану цих процесів. На сьогодні інформація вважається стратегічним національним ресурсом, одним із основних багатств країни. Повсюдне впровадження інформаційних технологій, сучасних засобів оброблення й передавання інформації в різні сфери діяльності започаткувало новий еволюційний процес у розвитку людства – інформатизацію.

На сучасному етапі наука має в розпорядженні теоретичні побудови, на базі яких здійснюється технологізація інформаційного протиборства, тобто відповідні державні й недержавні структури, що причетні до такої діяльності, проводять розроблення та апробацію нових інформаційних технологій, прийомів, технічних засобів, методів здійснення психологічного впливу. Подібні зрушення не могли не відбитися на зростанні ефективності застосування інформаційних технологій, яке може приводити до кардинальних змін у суспільній, економічній, політичній та інших сферах у масштабі окремої країни або ж світу загалом.

Сучасний етап науково-технічного розвитку породив справжню революцію у військовій справі. Концепція тотальної війни, що збереглася в основі стратегічних установок багатьох держав, історично себе вичерпала. Подальше широкомасштабне використання зброї проти армій і народів у війнах веде до глобальної катастрофи, загибелі цивілізації й навколишнього середовища. Є серйозні підстави думати, що світ вступає в смугу воєн нового покоління (гібридних), спрямованих не стільки на безпосереднє знищення противника, скільки на досягнення політичних цілей війни без застосування масових армій. Тому війну нині варто розглядати як складне суспільно-політичне явище, яке включає сукупність різних форм боротьби: політичної, економічної, збройної, інформаційної, психологічної й ін., – що ведуть між собою держави або їхні коаліції. Збройна боротьба перестає бути неодмінним атрибутом війни.

Історичний досвід показав, що останнім часом критично важливим державним ресурсом, який чинить усе більший вплив на національну безпеку, стає інформація, що циркулює в автоматизованих системах управління та зв'язку, які є невід'ємними компонентами структури управління державою, економікою, фінансами й обороною. Усе це веде до того, що суперництво, яке розгортається довкола інформаційного ресурсу, боротьба за володіння останнім, досягнення та утримання інформаційної переваги сьогодні займають значне місце в геополітичній конкуренції розвинутих країн.

Інформаційний простір стає, з одного боку, ареною запеклої геополітичної конкуренції, з іншого – однією з найважливіших сфер життєдіяльності сучасного співтовариства; найважливішим інструментом впливу на світову громадську думку.

Сучасні інформаційно-комунікаційні технології орієнтовані на акумулювання таких обсягів інформації, які при відповідних методах її оброблення дозволяють *прогнозувати* сукупність можливих сценаріїв розвитку соціальних і політичних явищ із метою визначення найбільш імовірного з них; *формувати* інформаційне поле такої концентрації, яка б перевищувала інформаційний рівень структури, що має вплив на ці сценарії. Наведена схема розкриває *сутність* так званого *інформаційного домінування в геополітичних відносинах*.

Зазначені обставини безпосередньо стосуються наукової та прикладної проблеми, що полягає в необхідності усвідомлення суперечностей, специфіки та складності побудови інформаційного суспільства в умовах недружного інформаційного впливу ззовні.

Варто також урахувувати, що в інформаційному суспільстві традиційна боротьба за володіння матеріальними цінностями також зазнаватиме глибокої трансформації та зміщуватиметься більше в інформаційну сферу, що, звичайно, призведе до посилення інформаційного протиборства.

У наш час керівники низки держав вважають інформаційну війну ефективним інструментом реалізації зовнішньої політики. Найповніше ця тенденція проглядається в концепціях інформаційних воєн, які розробляються провідними у військовому відношенні країнами. Інформаційна війна розглядається під різними кутами як один з основних чинників забезпечення національної безпеки та національних інтересів у життєво важливих сферах державної й суспільної діяльності, зокрема у військовій.

З урахуванням цих чинників інформаційний розвиток України має здійснюватися в рамках системної та збалансованої державної політики, здатної забезпечити захист суспільства, держави і громадян від інформаційно-психологічної експансії суб'єктів геополітичної конкуренції.

На сьогодні є певна кількість навчальної та наукової літератури щодо інформаційної безпеки, де здебільшого розглянуто інформаційно-технічні аспекти, правові й загальні положення зазначеної проблематики. Пропонований підручник є першим вітчизняним навчальним виданням, яке розкриває широкий спектр питань з історії й сучасності інформаційно-психологічного протиборства, розкриття сучасних технологій інформаційно-психологічного впливу, форм та способів застосування інформаційної зброї, особливостей психологічного та технічного захисту від інформаційних впливів.

Згідно з вимогами освітньо-професійної програми студенти та курсанти після засвоєння навчальної дисципліни ***“Системи інформаційної зброї та технології інформаційної війни”*** мають продемонструвати такі результати навчання:

Знання:

розширити і систематизувати знання щодо застосування інформаційної зброї;

набути знання щодо історії та сучасності проведення акцій інформаційного впливу, спеціальних інформаційних операцій, інформаційних війн;

сформувати критичне мислення для набуття навичок із захисту від маніпулятивного впливу;

розвинути вміння щодо управління інформаційною безпекою держави.

базові поняття щодо інформаційної безпеки держави, суспільства і особи;

види та сучасні технології інформаційних впливів;

сутність форми і види інформаційного протистояння;

етапи, ознаки, суб'єкти та методи проведення спеціальних інформаційних операцій;

завдання, об'єкти посягань, форми проведення інформаційної війни;

історію і особливості сучасного стану інформаційно-психологічного протистояння;

основні методи, головні вектори та види атак з використанням соціальної інженерії;

Уміння:

узагальнювати теоретичні уявлення щодо сутності інформаційної безпеки;

виявляти існуючі та потенційні загрози національній безпеці України в інформаційній сфері;

виявляти приховані та шкідливі інформаційно-психологічні впливи;

здійснювати порівняльний аналіз форм, методів, засобів та технологій проведення інформаційних війн, акцій інформаційного впливу та спеціальних інформаційних операцій;

здійснювати прогнози щодо можливих небезпек інформаційному простору держави;

використовувати світовий досвід щодо захисту інформаційного простору для його творчого впровадження на українських теренах;

Досвід:

проводити аналітичні дослідження у сфері інформаційної безпеки України;

приймати участь у заходах захисту від атак, які проводяться за допомогою Інтернету.