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

Петрик В.М., Музиченко К.М., Аль-Файюмі Халед та ін.

СУЧАСНІ ПРИЙОМИ МАНІПУЛЮВАННЯ

Навчальний посібник

За загальною редакцією

кандидата наук з державного управління, доцента,
члена-кореспондента Міжнародної академії богословських наук
ПЕТРИКА Валентина Михайловича
та
доктора технічних наук у галузі кібербезпеки (Dr.Sc), PhD
АЛЬ-ФАЙЮМІ Халеда

Київ – 2026

УДК 316.625 (075.8)
П 29

Рекомендовано Вченою радою
факультету комп'ютерних наук та технологій КАІ,
протокол № 2 від 23 лютого 2026 року

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

Петрик В. М., Музиченко К. М., Аль-Файюмі Халед та ін.
П 29 Сучасні прийоми маніпулювання: Навчальний посібник / За заг. ред. В. М. Петрика та Аль-Файюмі Халеда. – К.: Видавничий центр "Кафедра", 2026. – 280 с.

ISBN 978-966-370-320-6

У посібнику розглядаються сучасні прийоми та засоби маніпулювання у різних сферах життєдіяльності людини, суспільства і держави. Розкрито теоретичні засади функціонування ботоферм та ферм інтернет тролів. Проведено системний аналіз нейролінгвістичного програмування та окреслено можливі сфери його застосування. Окрему увагу приділено засобам, методам і сучасним технологіям соціальної інженерії, а також питанням захисту інформації від атак соціальної інженерії з урахуванням людського фактору. Штучний інтелект розглядається як інструмент сучасного маніпулювання свідомістю та як механізм захисту від шкідливих інформаційно-психологічних впливів.

Навчальний посібник рекомендовано для викладання дисциплін: «*Системи інформаційної зброї та технології інформаційної війни», «Інформаційно-психологічне протиборство», «Інформаційна безпека», «Інформаційна безпека держави», «Забезпечення інформаційної безпеки держави», «Основи інформаційної безпеки», «Основи кібербезпеки та захисту інформації», «Управління інформаційною безпекою», «Кібергігієна», «Інцидент-менеджмент у кіберпросторі»*. Посібник також може бути використаний у процесі викладання дисциплін *«Психологія» та «Безпека життєдіяльності».*

Внесок авторів:

Петрик В.М.: задум, розділи 1, 8; Музиченко К.М: вступ, розділи 2, 9; Аль-Файюмі Халед: розділи 5, 6; Черненко О.Є.: підрозділ 3.2, 3.3; Гурєєв В.О.: підрозділ 3.4; Кальниш В. В.: підрозділ 4.1, 4.3; Давидюк А. В.: розділ 7; Цибулькін В.В.: підрозділ 3.1; Сердюченко М. М.: 4.2.

ISBN 978-966-370-320-6

УДК 316.625 (075.8)

ЗМІСТ

ВСТУП

Сучасний етап розвитку інформаційного суспільства характеризується стрімким поширенням цифрових технологій, глобалізацією інформаційного простору та зростанням ролі інформації як одного з ключових ресурсів держави, суспільства й особистості. Поряд із позитивними наслідками цифрової трансформації дедалі більшої актуальності набувають загрози, пов'язані з маніпулятивним впливом на свідомість людини, інформаційно-психологічними операціями, використанням технологій соціальної інженерії, діяльністю ботоферм, інтернет-тролів, а також застосуванням штучного інтелекту для деструктивного впливу на громадську думку.

Особливої актуальності зазначені проблеми набувають в умовах гібридних конфліктів, інформаційних війн та високого рівня залежності сучасного суспільства від інформаційно-комунікаційних технологій. Маніпулювання суспільною свідомістю стало одним із найефективніших інструментів впливу на політичні процеси, соціальну поведінку, міжособистісні відносини та функціонування державних інституцій. Сучасні інформаційні технології дозволяють здійснювати прихований вплив на масову аудиторію, формувати необхідні наративи, провокувати панічні настрої, дестабілізувати суспільство та впливати на прийняття рішень окремими особами й соціальними групами.

Значна частина сучасних маніпулятивних технологій базується на використанні психологічних механізмів впливу, когнітивних викривлень, методів нейролінгвістичного програмування, технологій соціальної інженерії та автоматизованих інформаційних систем. Окрему небезпеку становить використання генеративного штучного інтелекту, систем deepfake, алгоритмів персоналізованого контенту та нейромережевого профілювання, які здатні створювати надзвичайно реалістичний контент і значно підвищують ефективність інформаційно-психологічних операцій.

У сучасних умовах проблема забезпечення інформаційної безпеки виходить далеко за межі суто технічного захисту інформаційних систем. Вона охоплює комплекс питань, пов'язаних із захистом особистості, суспільства та держави від маніпулятивних впливів, дезінформації, психологічного тиску, кіберсоціальних загроз та інших форм деструктивного інформаційного впливу. Саме тому виникає необхідність комплексного дослідження теоретичних і практичних аспектів маніпулювання, функціонування ботоферм і тролеферм, технологій соціальної інженерії, психологічних механізмів впливу на натовп, а також сучасних загроз, пов'язаних із використанням штучного інтелекту.

Метою цього посібника є формування у здобувачів освіти системного розуміння сутності маніпулятивних технологій, механізмів інформаційно-психологічного впливу, особливостей функціонування сучасних кіберсоціальних загроз та методів захисту від них. Навчальний посібник спрямований на розвиток у читачів критичного мислення, навичок виявлення

маніпулятивного впливу, аналізу інформаційних загроз і застосування ефективних засобів протидії.

У навчальному посібнику розглянуто понятійний апарат, пов'язаний із маніпулюванням та інформаційно-психологічними впливами; теоретичні засади функціонування ботоферм і ферм інтернет-тролів; особливості нейролінгвістичного програмування як інструменту когнітивного впливу; закономірності формування та поведінки натовпу; теоретико-методологічні основи соціальної інженерії; засоби та методи реалізації соціотехнічних атак; особливості забезпечення захисту інформації з урахуванням людського фактору; а також сучасні аспекти використання штучного інтелекту як інструменту маніпулювання свідомістю та механізми захисту від AI-індукованих маніпуляцій.

Структура посібника побудована за принципом послідовного переходу від базових понять і теоретичних положень до аналізу сучасних технологій маніпулятивного впливу та практичних аспектів забезпечення інформаційної безпеки. Матеріал орієнтований на здобувачів вищої освіти, науково-педагогічних працівників, фахівців у сфері кібербезпеки, інформаційної безпеки, психології, державного управління, правоохоронної діяльності та всіх, хто цікавиться проблематикою сучасних інформаційних загроз і засобів протидії їм.

Навчальний посібник підготовлено з урахуванням сучасних наукових підходів, міжнародного досвіду, актуальних тенденцій розвитку інформаційного середовища та новітніх викликів у сфері інформаційної і кібернетичної безпеки.