УДК 35:004.056.5

Панченко Н.А., здобувач,
Ткачук Р.Л., д.т.н., професор,
Полотай О.І., к.т.н., доцент
Львівський державний університет безпеки життєдіяльності

КІБЕРТЕРОРИЗМ, ДЕЗІНФОРМАЦІЯ ТА ІНФОРМАЦІЙНІ ОБМЕЖЕННЯ ЯК ЗАГРОЗИ ДЕРЖБЕЗПЕЦІ

У сучасних умовах цифровізації та зростання ролі інформаційного простору забезпечення інформаційної безпеки держави набуває стратегічного значення. Інформація перетворилась на критичний ресурс, від ефективного захисту якого залежить стабільність політичних інститутів, функціонування державних систем та довіра суспільства. З урахуванням інтенсивного розвитку гібридних форм протидії, держава стикається з новими типами загроз, серед яких ключовими виступають кібертероризм, дезінформація та штучні обмеження доступу до публічної інформації. Ці фактори здатні порушувати цілісність інформаційного простору, маніпулювати суспільною думкою та підривати національну безпеку, що зумовлює необхідність їх комплексного аналізу та системної протидії.

Важливо розуміти, що інформаційна безпека є однією зі складових національної безпеки держави нарівні з економічною, енергетичною, військовою, соціальною та іншими. При цьому цілком очевидно, що роль інформаційної безпеки та її місце в системі національної безпеки держави стає все значнішою.

У сучасних умовах цифрової трансформації кібербезпека є ключовим компонентом державної безпеки, що забезпечує захист кіберпростору та критичної інфраструктури від зовнішніх і внутрішніх кібервпливів. Зростання кіберзлочинності, інтенсифікація гібридних атак та використання ІКТ, як інструментів впливу формують спектр загроз, серед яких найбільш небезпечними виступають кібертероризм, дезінформація та штучні обмеження доступу до публічної інформації. Ці явища здатні дестабілізувати систему державного управління, впливати на суспільну свідомість, порушувати функціонування критичних сервісів та підривати національну безпеку.

В умовах триваючої гібридної війни Україна накопичила значний досвід протидії кібератакам та інформаційно-психологічному впливу, однак ефективна нейтралізація сучасних загроз вимагає запровадження комплексної моделі національної кіберстійкості. Така модель має спиратися на принципи управління ризиками та поєднувати

превентивні, технічні, організаційні й правові заходи, що мають реалізуватися за чотирма ключовими напрямами:

1. *Розвиток національної кіберінфраструктури та кіберстійкості*: посилення захисту критичних об'єктів; впровадження систем раннього виявлення та реагування на кібератаки; регулярний аудит та тестування безпеки.

2. *Превентивні та правові заходи:* удосконалення законодавства у сфері кібербезпеки та інформаційного захисту; посилення механізмів відповідальності за кібератаки й інформаційні диверсії; формування єдиної державної політики протидії дезінформації.

3. *Інформаційна стійкість суспільства*: розвиток медіаграмотності населення; підвищення прозорості державних комунікацій для мінімізації ризиків інформаційних маніпуляцій; створення ефективних механізмів перевірки та спростування фейкових повідомлень.

4. *Міжнародна кооперація*: участь у глобальних програмах кіберзахисту; обмін даними про кіберзагрози з країнами-партнерами та міжнародними організаціями; уніфікація стандартів і процедур реагування на кібератаки.

Таким чином, ефективне протистояння кібертероризму, дезінформації та інформаційним обмеженням можливе лише за умови формування комплексного, багаторівневого механізму, який поєднує технологічні рішення, правове регулювання, інституційну взаємодію та підвищення стійкості суспільства до інформаційних впливів.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 15.10.2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

2. Крикун В., Бауліна Т. Дезінформація як засіб гібридної війни : сутність і наслідки. Вісник Київського національного університету імені Тараса Шевченка. Філософія. 2022, Вип. 2. С. 30–33. URL : http://nbuv.gov.ua/UJRN/ VKNUF_2022_2_7

3. Івануса А. І., Ткачук Р. Л., Брич Т. Б. Удосконалення методів управління процесами інформаційної безпеки. Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : матеріали III Міжнародної науково-практичної конференції (Хмельницьк, 21 листопада 2024 р.). Хмельницький: НАДПСУ, 2024. С. 1136–1138.