**ЗМІСТ**

**ВСТУП………………………………………………………………………...3**

**РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ…………………………………………...………....5**

1.1. Поняття інформаційних загроз та інформаційної війни……………...5

1.2. Види загроз національній безпеці в інформаційній сфері…………....9

**РОЗДІЛ 2. Характеристика загроз інформаційного характеру в окремих сферах національної безпеки України…………………………..….11**

2.1. Загрози інформаційного характеру у політичній та соціально-гуманітарній сферах………………………………………………………..……..11

2.2. Загрози інформаційного характеру у воєнній сфері……………..….13

**РОЗДІЛ 3. Протидія загрозам інформаційного характеру в контексті забезпечення національної безпеки України………………………………....18**

3.1. Напрями протидії загрозам інформаційного характеру у політичній та соціально-гуманітарній сферах……………………………………………..…....18

3.2. Подолання загроз інформаційного характеру у воєнній сфері……..23

**ВИСНОВКИ………………………………………………………………..26**

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…………………………….....28**

**ВСТУП**

**Актуальність теми.** Інтереси держави в інформаційній сфері в основному зводяться до гармонійного розвитку інформаційної структури держави. Інформаційна безпека держави – це стан її захищеності, при якій спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, неза-конне зняття інформації за допомогою спеціальних технічних засобів, комп'ю-терні злочини та інший деструктивний інформаційний вплив не завдає істотної шкоди національним інтересам.

**Мета курсової роботи** полягає у комплексному та об'єктивному дослідженні впливу загроз інформаційного характеру на складові національної безпеки.

**Об’єктом дослідження** є суспільні відносини інформаційного характеру, що охоплюють сферу національної безпеки.

**Предметом дослідження** є характеристика загроз інформаційного характеру в окремих сферах національної безпеки України.

**Структура та обсяг курсової роботи.** Курсова робота складається зі вступу, трьох розділів, висновків, та списку використаної літератури. Загальний обсяг роботи – 30 сторінок.

**РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ**

**1.1. Поняття інформаційних загроз та інформаційної війни**

Розуміючи інформаційну безпеку як «стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій», правомірно визначити загрози безпеки інформації, джерела цих загроз, способи їх реалізації та мети, а також інші умови і дії, що порушують безпеку . При цьому, природно, слід розглядати і заходи захисту інформації від неправомірних дій, що призводять до нанесення збитку [1].

Загроза – сукупність факторів та умов, що виникають в процесі взаємодії об'єкта безпеки з іншими об'єктами, а також складових його компонентів між собою і здатних чинити на нього негативний вплив. Вона виступає в якості можливості вирішення протиріччя у взаємодії об'єкта безпеки з іншими об'єктами, компонентів об'єкта безпеки, що у стадії дисгармонії чи конфлікту, шляхом насильницької зміни в бік погіршення властивостей об'єкта безпеки, або його компонентів, тобто шляхом нанесення шкоди [1].

**1.2. Види загроз національній безпеці в інформаційній сфері**

Стаття 7 Закону України «Про основи національної безпеки» виділяє такі загрози національним інтересам і національній безпеці України в інформаційній сфері такі:

прояви обмеження свободи слова та доступу до публічної інформації;

поширення засобами масової інформації культу насильства, жорстокості, порнографії;

комп'ютерна злочинність та комп'ютерний тероризм;

розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави;

намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [8].

Відповідно до Стратегії національної безпеки України загрозами інформаційній безпеці виступають:

ведення інформаційної війни проти України;

відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства [9].

Згідно Доктрини інформаційної безпеки України актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є:

**РОЗДІЛ 2**

**ХАРАКТЕРИСТИКА ЗАГРОЗ ІНФОРМАЦІЙНОГО ХАРАКТЕРУ В ОКРЕМИХ СФЕРАХ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ**

**2.1. Загрози інформаційного характеру у політичній та соціально-гуманітарній сферах**

Інтереси особистості в інформаційній сфері полягають в реалізації конституційних прав людини і громадянина на доступ до інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного та інтелектуального розвитку, а також у захисті інформації, що забезпечує особисту безпеку. Інтереси суспільства в інформаційній сфері полягають у захисті життєво важливих інтересів особистості в цій сфері, забезпеченні реалізації конституційних прав і свобод людини та громадянина в інтересах зміцнення демократії, створенні правової соціальної держави, досягненні і підтримці суспільної злагоди, в духовному оновленні України, досягненні і підтримці громадської згоди, підвищенні творчої активності населення. Інтереси держави в інформаційній сфері визначаються створенням умов для гармонійного розвитку української інформаційної інфраструктури, для реалізації конституційних прав і свобод людини та громадянина у сфері отримання інформації, користування нею з метою забезпечення непорушності конституційного ладу, суверенітету і територіальної цілісності України, встановлення політичної, економічної та соціальної стабільності, в безумовному забезпеченні законності і правопорядку, розвитку рівноправного і взаємовигідного міжнародного співробітництва на основі партнерства [11].

**2.2. Загрози інформаційного характеру у воєнній сфері**

Загалом, у Законі України «Про основи національної безпеки» виділяються такі загрози у воєнній сфері та сфері безпеки державного кордону України:

поширення зброї масового ураження і засобів її доставки;

недостатня ефективність існуючих структур і механізмів забезпечення міжнародної безпеки та глобальної стабільності;

нелегальна міграція;

можливість втягування України в регіональні збройні конфлікти чи у протистояння з іншими державами;

нарощування іншими державами поблизу кордонів України угруповань військ та озброєнь, які порушують співвідношення сил, що склалося;

небезпечне зниження рівня забезпечення військовою та спеціальною технікою та озброєнням нового покоління Збройних Сил України, інших військових формувань, що загрожує зниженням їх боєздатності;

повільність у здійсненні та недостатнє фінансове забезпечення програм реформування Воєнної організації та оборонно-промислового комплексу України;

**РОЗДІЛ 3**

**ПРОТИДІЯ ЗАГРОЗАМ ІНФОРМАЦІЙНОГО ХАРАКТЕРУ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ**

**3.1. Напрями протидії загрозам інформаційного характеру у політичній та соціально-гуманітарній сферах**

Підходи щодо забезпечення безпеки ба-зуються на вже сформованій залежності всіх сфер життєдіяльності суспільства і держави – економіки, політики, науки, культури, забезпечення національної та міжнародної без-пеки – від нормального обміну інформацією, надійного функціонування інформаційних і телекомунікаційних систем. Тим самим для розвинених країн створюється спокуса використовувати наявні у них переваги (електронно-цифровий розрив) в інформа-ційних технологіях і засобах маніпулювання суспільною свідомістю для експансії у ви-щевказаних сферах життєдіяльності, вико-ристовуючи поки не обмежений ніякими по-ложеннями міжнародного права абсолютно новий вид зброї – інформаційної. У сучасних умовах застосування інформаційної зброї як засобу ведення війн може викликати наслідки, цілком порівнянні за силою своєї дії з «традиційною» зброєю масового знищення. Дана теза аж ніяк не випадкова. Аналіз використання сучасних технологій іншими державами вимагає здійснення системи спеціальних заходів щодо забезпечення інформаційної безпеки, в т. ч. міжнародної. На тлі стрімкої глобалізації у світі, де панують новітні технології та інформаційна уніфікованість, досі не подолане відставання у сфері комунікаційних технологій – особливо важливій в епоху інформаційних суспільств. Це загрожує національній безпеці України, бо вже призвело до значної інформаційної та технологічної залежності від іноземних держав та міжнародних медіа-структур. Для подолання цих явищ необхідне:

**3.2. Подолання загроз інформаційного характеру у воєнній сфері**

Рішенням Ради національної безпеки і оборони України від 2 вересня 2015 року "Про нову редакцію Воєнної доктрини України" визначено такі напрямки державної політики:

удосконалення державної інформаційної політики у воєнній сфері;

попередження та ефективна протидія інформаційно-психологічним впливам іноземних держав, спрямованим на підрив обороноздатності, порушення суверенітету і територіальної цілісності України, дестабілізацію внутрішньої соціально-політичної обстановки, провокування міжетнічних та міжконфесійних конфліктів в Україні [17].

До джерел загроз і небезпек інформаційній безпеці системі управління національною безпекою належать:розкриття інформаційних ресурсів;пору-шення їх цілісності;збій в роботі самого обладнання [18].

Ю. П. Лісовська визначає, що нагальною потребою є необхідність прийняття Закону України «Про інформаційну безпеку України». Визначено систему правового регулювання стосовно недержавного забезпечення національної безпеки та її інформаційної складової, а також засад громадського контролю за діяльністю органів державної влади і місцевого самоврядування [19, с. 12].

**ВИСНОВКИ**

Загрози інформаційній безпеці – це можливі дії або події, які можуть вести до порушень ІБ. Види загроз інформаційній безпеці дуже різноманітні і мають безліч класифікацій.

До основних інформаційних загроз відносяться:

• надання цілеспрямованого інформаційного впливу на населення через засоби масової інформації, Інтернет, яке може привести до негативних соціально-політичних наслідків;

• неповна реалізація прав громадян у сфері отримання та обміну достовірної інформації;

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Черевко О. В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту. URL: http://www.economy.nayka.com.ua/ ?op=1&z=3304 (дата звернення: 10.12.2020).

2. Інформаційні загрози. URL: <http://stud.com.ua/550/bzhd/informatsiyni_zagrozi> (дата звернення: 10.12.2020).

3. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.

4. Горбенко І. Д., Долгов В. І., Гріненко Т. О. Інформаційна війна – сутність, методи та засоби ведення. URL: http://www.bezpeka.com/ru/ lib/spec/law/methods-information-warfare.html (дата звернення: 10.12.2020).

5. Сидор Ю. В., Романюк Н.І Інформаційні війни як виклик міжнародній безпеці. URL: https://internationalconference2014.wordpress.com/ 2014/10/10/інформаційні-війни-як-виклик-міжнаро/ (дата звернення: 10.12.2020).

6. Шпига П. С., Рудник Р.М. Основні технології та закономірності інформаційної війни. URL: <http://www.kymu.edu.ua/vmv/v/p08/22.pdf> (дата звернення: 10.12.2020).

7. Ліпкан В.А. Національна безпека України: Навчальний посібник. К.: КНТ, 2009. 576 с.

8. Про основи національної безпеки України : Закон від 19.06.2003 № 964-IV : Редакція від 07.08.2015. URL: <http://zakon3.rada.gov.ua/laws/show/964-15> (дата звернення: 10.12.2020).

9. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України" : Президент України; Указ, Стратегія від 26.05.2015 № 287/2015. URL: http://zakon3.rada.gov.ua/laws/ show/287/2015/ paran14#n14 (дата звернення: 10.12.2020).

10. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Президент України; Указ, Доктрина від 25.02.2017 № 47/2017. URL: http://zakon3.rada.gov.ua/laws/show/47/2017

11. Степанов В. Ю. Інформаційна безпека як складова державної інформаційної політики. *Державне будівництво.* 2016. № 2. С. 1-9.

12. Пилипчук В., Дзьобань О. Глобальні виклики й загрози національній безпеці. *Вісник Національної академії правових наук України.* 2014. № 3 (78) С. 43-52

13. Косогов О.М. Інформаційна безпека у сфері оборони як складова воєнної безпеки України. *Системи обробки інформації.* 2016. № 8 (145). С. 115-117

14. Реалії інформаційної війни в Україні. URL: http://www.milnavigator.com/uk/reali%D1%97-informacijno% D1%97-vijni-v-ukra%D1%97ni/ (дата звернення: 10.12.2020).

15. Нашинець-Наумова А. Концептуальні підходи щодо забезпечення національної безпеки: інформаційно-правові та інституційні засади. *Підприємництво, господарство і право*. 2017. № 1. С. 34-39.

16. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політичні науки.* 2016. № 1. С. 27-32.

17. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року "Про нову редакцію Воєнної доктрини України": Президент України; Указ, Доктрина від 24.09.2015 № 555/2015. URL: <http://zakon3.rada.gov.ua/laws/show/555/2015/page> (дата звернення: 10.12.2020).

18. Чудінова Н.В., Грицюк Ю.І. Інформаційна безпека України та види джерел загроз і небезпек. URL: http://virt.ldubgd.edu.ua/pluginfile.php/ 14209/mod\_folder/ content/0/%D0%9A%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B0%20%D0%A3%D0%86%D0%91/%D0%93%D1%80%D0%B8%D1%86%D1%8E%D0%BA%20%D0%AE.%D0%86/Chudinova.pdf?forcedownload=1 (дата звернення: 10.12.2020).

19. Лісовська Ю. П. Адміністравтивно-правовн забезпечення інформаційної безпеки в Україні : автореф. дис. на здобуття наук. ступеня канд. юр. наук : спец. 12.00.07. Київ, 2017. 21 с.

20. Концептуальна стаття Горбуліна: "Гібридна війна" як ключовий інструмент російської геостратегії реваншу. URL: <http://texty.org.ua/pg/news/editorial/read/58061/Konceptualna_statta_Gorbulina_Gibrydna_vijna_jak_kluchovyj> (дата звернення: 10.12.2020).

21. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів. *Резонанс.* 2017. № 18. URL: http://nbuviap.gov.ua/images/ rezonans/2017/rez18.pdf. (дата звернення: 10.12.2020).