Антон БОЙЧЕНКО
здобувач вищої освіти 1 курсу ОС «Бакалавр»
спеціальності 126 «Інформаційні системи і технології»
Науковий керівник:
канд. екон. наук, доцент Ірина МУШЕНИК
Заклад вищої освіти «Подільський державний університет»
м. Кам'янець-Подільський

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ

У наукових виданнях подекуди їх ототожнюють або, навпаки, наводять розгалужені їх класифікації за різноманітними критеріями. Загрози інформаційній безпеці України розглядаються нами як детермінуючі фактори, що зумовлюють і породжують негативні явища, які посягають на національні інтереси в інформаційній сфері, організацію та функціонування національного інформаційного простору загалом. Вони можуть мати широкомасштабне транскордонне чи глобальне значення, пов'язані із ризиками і небезпеками в інших сферах, посягаючи на національний інформаційний простір держави або міжнародну інформаційну безпеку.

З метою попередження і протидії існуючим та ймовірним загрозам інформаційній безпеці стратегічне завдання держави потягає у створенні та функціонуванні механізму забезпечення інформаційної безпеки. Він передбачає послідовну системну діяльність, сукупність заходів і державно-правових інституцій, що покликані гарантувати безперешкодну реалізацію національних інтересів держави в інформаційній сфері, відповідних інтересів людини і суспільства, попередження інформаційних конфліктів та оперативне їх подолання.

Сучасні інформаційні війни, поряд з іншими формами інформаційної боротьби і видами інформаційних конфліктів, є проявами більш широкої категорії – загроз національним інтересам та національній безпеці. Безумовно, предмет нашого вивчення становить не весь комплекс загроз, а власне загрози в інформаційній сфері, загрози інформаційній безпеці держави.

Якщо поняття, сутність і зміст такого феномену як інформаційна безпека зазвичай аналізують дослідники належною мірою, то набагато менше уваги приділяється питанням небезпеки і загрозам сучасних держав. Прикметно, що не дивлячись на виокремлення самостійного напряму наукових досліджень – націобезпекознавства, порушена проблематика іноді актуалізується представниками науки міжнародного права, конституційного та адміністратив-ного права, кримінального права, інформаційного права, державного управління, політології, історії, державної безпеки [2].

Враховуючи відсутність єдиного загальноприйнятого підходу до розкриття розуміння понять «інформаційна безпека»; «загрози інформаційній безпеці», а також їх активне поширення у суспільно-державному житті та на міжнародній

арені з непередбачуваними переважно негативними наслідками, вважаємо доцільним привернення уваги наукової спільноти до даної проблематики. Насамперед, потребують розмежування однорідні та споріднені поняття «загроза», «ризик», «небезпека», «виклик» і т.д., а також «інформаційна загроза», інформаційний конфлікт», інформаційна війна», «інформаційне. протистояння», «інформаційне протиборство», «інформаційний тероризм» тощо[1].

Ще Законом України «Про основи національної безпеки України» у ст. 7 (втратив чинність на підставі Закону № 2469-VIII від 21.06.2018) до загроз національним інтересам і національній безпеці в інформаційній сфері було віднесено наступні:

- прояви обмеження свободи слова та доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що е власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

У Доктрині інформаційної безпеки України», затвердженій Указом Президента України №47/2017 від 25 лютого 2017 року перелічено актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері:

- здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів,
- підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;
- проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;
- інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;
- недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;
- неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства[3].

Висновок. Необхідність подальшого вивчення і розроблення чіткого поняття «загроза» є нагальною і має бути спрямована на формування ефективної і реальної системи моніторингу та управління загрозами, та іншими ризиками для інформаційної безпеки держави.

Список використаних джерел

1. Про основи національної безпеки України: Закон України від 19 червня 2003 року № 964-IV URL: https://zakon.rada.gov.ua/laws/show/964-15/#Text (дата звернення 12.10. 2023).
2. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. Офіційний вісник України. 2017. № 91. Ст. 2765.
3. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. К.: КНТ, 2006. 280 с.

Ілля БУЧАРСЬКИЙ
здобувач вищої освіти
Науковий керівник:
канд. екон. наук, доцент Ірина МУШЕНИК
Заклад вищої освіти «Подільський державний університет»
м. Кам'янець-Подільський

ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАТИВНИХ ТЕХНОЛОГІЙ ПРИ ВИВЧЕННІ ДИСЦИПЛІН ТЕХНІЧНОГО НАПРЯМКУ

На початку XXI століття людство увійшло в нову стадію свого розвитку – вчені й політики, підприємці й педагоги дедалі частіше говорять про настання інформаційної ери. Сучасний стан розвитку освіти передбачає використання комп'ютерних технологій, які є основою інформаційних засобів навчання. В умовах збільшення кількості та об'єму інформації, навчальні підручники не здатні ефективно виконувати такі освітні завдання, як оновлення змісту освіти, забезпечення особисто-орієнтованого навчання та розвитку інформаційно-комунікаційної компетентності.

Впровадження ІКТ у процесі викладання історії має низку переваг, а саме:

1. ІКТ дозволяють представляти знання історичних фактів, подій, документів, коментарів та інтерпретацій у взаємозв'язку;
2. Знання постають у певному контексті. Контекстом слугують не тільки коментарі, а й багато інших матеріалів (малюнки, звукові вставки, анімація, портрети тощо), які подають інформацію про історичні явища з різних боків. Створюється мережева структура інформації, з великою інформаційною насиченістю і додатковим смисловим потенціалом;
3. Знання формуються завдяки залученню різних каналів сприйняття;
4. Сприйняття, інтерпретація та засвоєння історичних знань за умови використання ІКТ відбувається не тільки когнітивним способом, але й споглядальним шляхом;