Смик І. А.,
здобувач вищої освіти
факультету забезпечення державної безпеки
Київського інституту Національної гвардії України

Науковий керівник:
Дручек О. В.,
кандидат юридичних наук, доцент,
професор кафедри правового
забезпечення та правоохоронної діяльності
факультету забезпечення державної безпеки
Київського інституту Національної гвардії України
(м. Київ, Україна)

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

У сучасному світі, що характеризується стрімким розвитком інформаційних технологій та глобалізацією суспільства, інформаційна безпека набуває вирішального значення для стабільності та розвитку держави.

Розповсюдження цифрових технологій створює нові можливості для економічного зростання, але водночас породжує низку ризиків, пов'язаних із кіберзагрозами, дезінформацією та інформаційними маніпуляціями. У цьому контексті забезпечення інформаційної безпеки є невід'ємною складовою загальної системи національної безпеки України, оскільки від її ефективності залежить здатність держави протистояти зовнішнім та внутрішнім загрозам [3, с. 45; 4, с. 78]. Відтак, аналіз ролі інформаційної безпеки у забезпеченні національної безпеки, визначення основних напрямів її розвитку та інтеграції сучасних технологічних і правових рішень для протидії кіберзагрозам є важливою науковою проблемою.

Основою для регулювання інформаційних відносин в Україні є комплекс нормативно-правових актів, серед яких найбільш важливими є Конституція України, Закон України «Про національну безпеку України» та Закон України «Про інформацію». Конституція встановлює основні принципи державного устрою та гарантує право на інформаційну свободу, що є фундаментом для подальшого законодавчого регулювання [1]. Закон України «Про національну безпеку України» формує стратегічні підходи до захисту суверенітету та територіальної цілісності держави, в тому числі і в інформаційному просторі [2]. Норми Закону України «Про інформацію» [6, с. 210] визначають правові засади регулювання інформаційних процесів, що є особливо актуальним в умовах ведення російсько-української війни, яка має, у тому числі, і інформаційний вимір, за якого точність і достовірність інформації набувають критичного значення.

Зазначена нормативно-правова база дозволяє створити механізми для своєчасного виявлення та нейтралізації загроз інформаційному простору.

Сучасна наука розглядає інформаційну безпеку як комплексний процес управління ризиками, що виникають у цифровому середовищі. Серед основних методів захисту інформації – використання криптографічних засобів, систем моніторингу кіберпростору, алгоритмів аналізу кіберзагроз та технологій штучного інтелекту, які дозволяють проводити прогнозування та оперативну реакцію на кіберінциденти [3, с. 67].

На думку фахівців у галузі національної безпеки України О. Г. Данільяна, О. П. Дзьобаня, М. І. Панова, такі технології дозволяють не тільки забезпечити конфіденційність, цілісність та доступність даних, але й оптимізувати процеси управління інформаційною безпекою на державному рівні. Системний підхід у цьому контексті включає розробку моделей ризик-менеджменту, що дозволяють проводити комплексну оцінку вразливостей інформаційної інфраструктури та оперативно реагувати на зміни в інформаційному середовищі [4, с. 90].

Окрім технологічних рішень, важливим компонентом інформаційної безпеки є правове та організаційне забезпечення.

Забезпечення ефективного правового регулювання сприяє встановленню чітких нормативних вимог до суб’єктів інформаційних відносин, визначає відповідальність за порушення інформаційної безпеки та створює правові умови для захисту критичної інфраструктури.

На думку С. М. Домбровської, організаційні заходи, спрямовані на координацію діяльності державних органів, наукових установ та приватного сектору, дозволяють створити інтегровану систему реагування на інформаційні загрози. Наприклад, створення міжвідомчих комітетів та робочих груп сприяє обміну інформацією про поточні кіберзагрози, що підвищує та зменшує ризики їх негативного впливу [5, с. 112].

Формування високого рівня інформаційної культури як у цілому, так і у військово-професійному середовищі, є одним із запорук успішної протидії дезінформації та кіберзагрозам. Освітні програми, наукові конференції та публічні дискусії сприяють підвищенню інформаційної грамотності громадян, що дозволяє їм критично аналізувати отриману інформацію та виявляти спроби маніпуляції [5, с. 135]. Розвиток таких програм, зокрема у вищих навчальних закладах, дозволяє підготувати кваліфікованих спеціалістів у галузі кібербезпеки, які здатні застосовувати сучасні технології для захисту інформаційного простору держави. Впровадження інноваційних технологій у сфері інформаційної безпеки сприяє модернізації систем управління кіберзахистом.

Сучасні дослідження свідчать про те, що застосування технологій машинного навчання та штучного інтелекту дозволяє автоматизувати процеси виявлення загроз, аналізувати великі обсяги даних та прогнозувати можливі кіберінциденти [4, с. 150]. Це забезпечує можливість своєчасного реагування на виникаючі загрози та значно знижує ризики масштабних кібернетичних атак, що можуть негативно вплинути на національну безпеку.

Підсумовуючи викладене, можна стверджувати, що інформаційна безпека є невід'ємною складовою системи національної безпеки України. Комплексний підхід до управління інформаційними ризиками, який об'єднує нормативно-правові акти [1, 2], сучасні технологічні рішення [3, с. 67; 4, с. 90] та організаційні заходи [5, с. 112], є запорукою ефективного захисту інформаційного простору.

Розвиток інноваційних технологій у поєднанні з підвищенням інформаційної культури населення дозволяє не лише протидіяти сучасним кіберзагрозам, але й створювати умови для стійкого розвитку держави у цифрову епоху.

Подальші дослідження та практичні розробки в галузі інформаційної безпеки повинні бути спрямовані на вдосконалення систем раннього попередження, оптимізацію моделей управління ризиками та розширення співпраці між державними, науковими та приватними структурами.

Лише інтеграція зусиль усіх суб'єктів інформаційних процесів дозволить забезпечити високий рівень кібербезпеки, що є ключовим фактором у забезпеченні національної безпеки України [4, с. 150]. З огляду на сучасні виклики, постійне вдосконалення нормативно-правової бази та активне впровадження інноваційних технологій, зокрема і у сфері забезпечення державної безпеки, мають стати пріоритетними завданнями державної політики.

Список використаних джерел:

1. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 21.01.2025).
2. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL:https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата вернення 01.02.2025).
3. Ліпкан В. А. Теоретичні основи та елементи національної безпеки України. Київ: 2003. 250 с.
4. Данільян О. Г., Дзьобань О. П., Панов М. І. Національна безпекаУкраїни: структура та напрямки реалізації: навчальний посібник. Харків: Фоліо, 2002. 322 с.
5. Домбровська С. М. Механізми забезпечення інформаційної безпеки як складової державної безпеки України. *Теорія та практика державного управління,* 2015. 280 с.
6. Про інформацію: Закон України 2 жовтня 1992 року № 2657-XII URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 21.01.2025).