Милосердна Ірина Михайлівна

Інформаційна безпека як елемент національної безпеки: теоретичний вимір та особливості впровадження

УДК 327:351.746.1]:007(477:061.1ЄС)
DOI https://doi.org/10.24195/2414-9616.2024-4.26

Милосердна Ірина Михайлівна
кандидат політичних наук, доцент,
доцент кафедри політології
Одеського національного університету
імені І. І. Мечникова
вул. Дворянська, 2, Одеса, Україна
ORCID: 0000-0003-2083-9500

Стаття присвячена аналізу уявлень щодо сутності феноменів «національної безпеки» та «інформаційної безпеки», а також визначення інформаційної безпеки як складової національної безпеки, яка в умовах швидкого розвитку інформаційно-комунікаційних технологій постає перед новим виміром ризиків та загроз.

В основі дослідження лежать системний і міждисциплінарний підходи, а також детермінований факторний аналіз, використання якого, дозволило виокремити ключові аспекти інформаційного виміру національної безпеки держави, а також основні загрози, перед якими вона опинилась в сучасних умовах.

Встановлено, що сучасна національна безпека держави постає перед новими викликами та загрозами, що обумовлено процесами цифровізації в усіх аспектах життя, впливом Інтернету, штучного інтелекту та соціальних мереж. В сучасних умовах держави для забезпечення національної безпеки спрямовують свою політику не тільки на посилення військового потенціалу, але й на засвоєння та контроль цифрових технологій в контексті транснаціональної транскордонної комп'ютерної злочинності та кібертероризму. У статті здійснено аналіз основних груп інформаційно-технічних небезпек: перша група пов'язана із зростанням пропаганди та дезінформації, підбурюванням до насильства, друга – новий клас соціальних злочинів, третя – використанням ІКТ у політичних цілях. Встановлено, що забезпечення та удосконалення інформаційної безпеки є значною складовою національної безпеки, яка сприяє розвитку стану захищеності інформаційної інфраструктури, демократичних процедур в державі.

У статті розглядається досвід країн ЄС щодо зміцнення інформаційної безпеки держави та становлення «цифрового суверенітету», як складової національної безпеки держави. Встановлено, що особливість європейського досвіду формування та посилення інформаційної безпеки полягає у комплексному характері, який супроводжується роботою в напрямках створення цілісної системи нормативних актів, планів, інститутів, діяльність яких спрямована на реалізацію планів та протидію новим загрозам. Також у статті відзначено роль взаємодії громадянського суспільства та держави у посиленні інформаційної безпеки, забезпеченню безпеки в кіберпросторі на національному рівні.

Ключові слова: *національна безпека держави, інформаційна безпека, кібербезпека, цифровізація, ЄС, Україна.*

Вступ. Останні десятиліття супроводжуються посиленням ролі інформації в житті як людини, так і держави загалом, що зумовлює інтенсивні зміни всіх сфер життєдіяльності. По суті інформація стала матеріальною цінністю для всіх форм організацій і залишається найважливішим елементом їхніх систем управління. Перед сучасними державами постають різні загрози їхній національній безпеці: від фізичної загрози громадянам держави, військових загроз, за умов посилення регіональних конфліктів, до нетрадиційних загроз, спричинених стрімкими темпами розвитку інформаційно-комунікаційних технологій, – інформаційна безпека та кібербезпека.

Мета статті полягає у дослідженні теоретичного виміру інформаційної безпеки як елементу національної безпеки та виявленні особливостей її впровадження в сучасних умовах.

Методи дослідження. Для аналізу сутності національної та інформаційної безпек, а також для визначення перспектив та викликів, які стоять перед сучасною національною безпекою використані системний і міждисциплінарний підходи, а також детермінований факторний аналіз, використання якого, дозволило виокремити ключові аспекти інформаційного виміру національної безпеки держави, а також основні загрози, перед якими вона опинилась в сучасних умовах.

Результати. Національна безпека – це складне багатогранне явище, тісно пов'язане з регіональною та міжнародною безпекою і визнане однією з ключових глобальних проблем людства. Вона відображає стан захищеності життєво важливих інтересів людини, суспільства та держави від внутрішніх і зовнішніх загроз через підтримку збройних сил і захист державних таємниць.

Однак сьогодні не існує стандартного визначення національної безпеки. Дослідники вивчали її через призму певного контексту й обстановки, що зумовлює наявність широкого діапазону розуміння та застосування. На думку В. Ліппмана, «нація має безпеку, коли їй не доводиться жертвувати своїми законними інтересами, щоб уникнути війни, і здатна, якщо їй кинуто виклик, зберегти їх за допомогою війни» [17].

А Г. Ласуелл зазначав, що «відмітне значення національної безпеки означає свободу від іноземного диктату» [16]. З точки зору С. Макінди

«національна безпека описується як здатність держави забезпечувати захист і оборону своїх громадян» [18].

Відповідно до Collins dictionary «Національна безпека країни – це її здатність захистити себе від загрози насильства або нападу» [7].

Аналіз цих визначень свідчить про те, що традиційна концепція національної безпеки зосереджена на виживанні держави: фізична безпека держави від зовнішніх загроз (здебільшого військового реагування), включно з національною обороною, національною цілісністю та національним суверенітетом. Проте еволюція національної безпеки держави відбувається відповідно до викликів, з якими вона стикається, і засобів, які вона може застосувати для боротьби з цими викликами. Нетрадиційні виклики безпеці та питання інформаційної безпеки посіли важливе місце в дискурсі національної безпеки країн та світу загалом.

Згідно з Cambridge Dictionary під інформаційною безпекою слід розуміти «методи, що використовуються для запобігання незаконному отриманню або використанню електронної інформації» [6].

Термін «інформаційна безпека» означає захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення з метою забезпечення: цілісності, що означає захист від неправомірної зміни або знищення інформації та включає забезпечення безвідмовності й достовірності інформації; конфіденційності, що означає збереження дозволених обмежень на доступ та розкриття, включно із засобами захисту особистого життя і службової інформації; і доступності, що означає забезпечення доступності та доступності. Також інформаційну безпеку можна визначити, як «захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення з метою забезпечення конфіденційності, цілісності та доступності» [20].

У «Insider threat job aid. A glossary of Basic Insider Threat Definitions» зазначається, що «інформаційна безпека пов'язана з упровадженням системи адміністративних політик і процедур для ідентифікації, контролю та захисту від несанкціонованого розкриття інформації, яку дозволено до захисту розпорядженням, статутом або регламентом. Інформаційна безпека включає в себе захист секретної, контрольованої несекретної та конфіденційної інформації» [15].

У рамках Резолюції Генеральної Асамблеї ООН A/RES/53/70 «Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки» ідея інформаційної безпеки набуває визнання та «відзначається значний прогрес у розробці й упровадженні новітніх інформаційних технологій та засобів телекомунікації, однак, висловлюючи заклопотаність тим, що ці технології та засоби потенційно можуть бути використані з метою, несумісною із завданнями забезпечення міжнародної стабільності, та можуть негативно впливати на безпеку держав, а також на безпеку суспільства. Таким чином, у Резолюції A/RES/53/70 підкреслюється ідея «запобігання неправомірному використанню або використанню інформаційних ресурсів або технологій у злочинних або терористичних цілях» [9].

При дослідженні сутності інформаційної безпеки, на думку М.О. Шевчука, доцільно виділити кілька підходів: статичний (розглядає безпеку як стан захищеності інформаційного середовища або інформації, а також систему гарантій), діяльнісний (визначає безпеку як процес її забезпечення, здатність держави ефективно захищати національні інтереси та цінності) і комплексний (поєднує безпеку як стан і процес). І на думку дослідника інформаційну безпеку слід розглядати як «безперервний процес діяльності компетентних органів, спрямований на запобігання та протидію загрозам інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов для цієї діяльності, які можуть бути реалізовані та контрольовані в довгостроковій перспективі» [5, с. 138].

Важливим наслідком поширення інформаційних та комунікаційних технологій і їх впровадження у всі сфери суспільного життя стало створення правових, організаційних та технологічних передумов для розвитку демократії, що забезпечує громадянам можливість вільного пошуку, отримання, передачі, створення та поширення інформації.

Однак із новими можливостями участі громадян у політиці, формування нового виміру реалізації національних інтересів, можна спостерігати й підвищення рівня появи нових загроз, джерела яких можуть мати як природній (помилки, стихійні лиха, випадкові події), так й умисний характер (умисне та цілеспрямоване використання ЗМІ, спеціальних програм для здійснення кібератак та ін.).

В умовах науково-технічного прогресу можна виокремити такі групи інформаційно-технічних загроз інформаційної безпеки та розвитку держави в цілому.

Перша група пов'язана з розвитком новітньої інформаційної зброї, здатної впливати як на психіку та свідомість людей, так і на інформаційно-технічну інфраструктуру суспільства. Йдеться про поширення пропаганди та дезінформації, які можуть призводити до маніпуляції даними або їх фальсифікації, що впливає на політичні процеси, сприяє дестабілізації режимів тощо.

Друга група загроз стосується нового класу соціальних злочинів, що базуються на використанні сучасних ІКТ, таких як махінації з електронними

коштами та комп'ютерне хуліганство. Особливо актуальним стає питання інформаційної безпеки в контексті зростання транснаціональної кіберзлочинності та кібертероризму. У цьому випадку під загрозою опиняється конфіденційність, оскільки кібератаки можуть бути спрямовані на різні джерела конфіденційної інформації з метою шпигунства, крадіжки персональних даних, шахрайства або «крадіжки особистості».

Третя група загроз пов'язана із використанням ІКТ у політичних цілях на національному та міжнародному рівнях, що обумовлено зростанням впливу ЗМІ на процес розроблення, прийняття та реалізацію політичних рішень, функціонування механізму політичної влади та розвитку політичного процесу.

Провідні країни світу спрямовують свою політику на розвиток, освоєння та контроль цифрових технологій, що призводить до формування технологічних сфер впливу та глобального цифрового порядку, під яким розуміють комплекс технічних, економічних, політичних і нормативних заходів, які регулюють світові інформаційні потоки. В умовах євроінтеграції України, доцільним є аналіз основних механізмів формування та забезпечення інформаційної безпеки, як елементу національної безпеки.

Слід зазначити, що на думку Деннісон С., У. Франке та П. Зерка «провідні країни-члени ЄС (такі як Данія, Бельгія, Франція, Німеччина, Іспанія, Швеція), схоже, найбільше занепокоєні кібератаками – або з погляду їхньої ймовірності, або з погляду впливу, або з погляду керованості. Така стурбованість має бути викликана усвідомленням того, що їхнє суспільство залежить від цифрових систем, оскільки ці країни вважаються «лідерами» з кіберпроблем у ЄС: Франція і Швеція домоглися значного прогресу в розробленні кіберстратегій; Данія стала першою країною-членом, яка призначила посла технологій» [8].

Сучасні загрози інформаційній безпеці як важливому елементу національної безпеки вимагають комплексного підходу до формування єдиного механізму забезпечення інформаційної безпеки та кібербезпеки в ЄС. Так, у 2004 році було створено Агентство Європейського союзу з мережевої та інформаційної безпеки (ENISA) [12]. Місія ENISA полягає в підвищенні «обізнаності про мережеву та інформаційну безпеку, а також у розвитку та просуванні культури мережевої та інформаційної безпеки в суспільстві на благо громадян, споживачів, підприємств та організацій державного сектору в Союзі» [21].

У 2013 році було висловлено ідею про Стратегію кібербезпеки Європейського союзу, а у 2016 році було ухвалено Директиву 2016/11481 про безпеку мережевих та інформаційних систем (далі NIS), що передбачає «заходи для досягнення високого загального рівня безпеки мережевих та інформаційних систем у рамках Союзу з метою поліпшення функціонування внутрішнього ринку» [11]. Кожна держава-член ЄС має ухвалити національні рамки, що включають у себе національну стратегію щодо забезпечення безпеки мережевих та інформаційних систем і призначення органів, для успішного виконання положень Директиви NIS. У 2019 році було ухвалено Закон про кібербезпеку, спрямований на досягнення високого рівня кібербезпеки, кіберстійкості та довіри в Європейському Союзі [22].

У 2020 році Європейська комісія презентувала нову стратегію ЄС у сфері безпеки на період 2020–2025 рр., зосередивши увагу на пріоритетних галузях, у яких ЄС може зробити свій внесок у підтримку держав-членів у зміцненні безпеки для всіх, хто живе в Європі. Від боротьби з тероризмом та організованою злочинністю, запобігання та виявлення гібридних загроз і підвищення стійкості нашої критичної інфраструктури до просування кібербезпеки та сприяння дослідженням та інноваціям – стратегія визначає інструменти й заходи, які необхідно розробити впродовж наступних 5 років для гарантування безпеки в нашому фізичному та цифровому середовищі [14]. Дана стратегія визначає 4 стратегічні пріоритети для дій на рівні ЄС:

– стійке до майбутнього середовище безпеки – люди покладаються на ключові інфраструктури, онлайн і офлайн і для їхнього забезпечення запропоновано нові правила ЄС щодо захисту та забезпечення стійкості критичної інфраструктури, фізичної та цифрової. Визначено необхідність створення Об'єднаного кіберпідрозділу як платформи для структурованого і скоординованого співробітництва, а також наголошено на необхідності міжнародні партнерства для подальшого запобігання, стримування і реагування на кібератаки, просування стандартів ЄС для підвищення рівня кібербезпеки країн-партнерів;

– боротьба із загрозами, що розвиваються, яка передбачає зміцнення потенціалу правоохоронних органів у сфері цифрових розслідувань;

– захист європейців від тероризму та організованої злочинності, що передбачає ініціювання кроків зі зміцнення законодавства про безпеку кордонів і більш ефективного використання наявних баз даних. Співпраця з країнами, що не входять до ЄС, і міжнародними організаціями також матиме ключове значення в боротьбі з тероризмом;

– сильна європейська екосистема безпеки, яка має формуватися на основі зміцнення мандату Європолу та подальший розвиток Євроюсту для тіснішого зв'язку між судовими та правоохоронними органами [13].

У 2022 році було ухвалено Директиву NIS 2, спрямовану на досягнення високого загального рівня кібербезпеки в країнах Європейського Союзу.

Держави-члени повинні забезпечити, щоб істотні та важливі організації вживали відповідних і пропорційних технічних, операційних та організаційних заходів для управління ризиками, пов'язаними з безпекою мережевих та інформаційних систем, а також для запобігання або мінімізації впливу інцидентів на одержувачів їхніх послуг і на інші служби. Ці заходи мають бути засновані на підході, що враховує всі небезпеки [10].

Для посилення інформаційної безпеки в ЄС також передбачається створення загальноєвропейських оперативних центрів безпеки (SOC), а також механізму надзвичайних ситуацій у кіберпросторі та механізму розгляду великих інцидентів кібербезпеки. На практиці обговорювані SOC являють собою великі національні або транскордонні платформи для збору інформації про загрози; мета – підвищити ефективність виявлення, запобігання та реагування на атаки. Очікується, що завдяки фінансуванню з боку ЄС у рамках програми «Цифрова Європа» (DEP) національні SOC будуть розширені до транскордонних SOC, що зрештою призведе до створення єдиного «європейського кіберзахисту». Інформація про великомасштабні інциденти кібербезпеки, отримана через транскордонні SOC, повинна передаватися в мережу CSIRT, EU-CyCLONe та Комісії. Механізм надзвичайних кіберситуацій, своєю чергою, призначений для дій із забезпечення готовності, відновлення після великомасштабних інцидентів і взаємодопомоги між країнами-членами [23].

Зміцнення інформаційної безпеки визначається як пріоритетний напрямок формування національної безпеки і в Україні. Можна погодитися із У. Ільницькою, що «національний інформаційний простір України зазнає суттєвих загроз, викликів, які становлять небезпеку функціонування держави, її політичного та економічного розвитку, інтеграції у європейські та євроатлантичні структури» [2, с. 29]. Щодо визначення інформаційної безпеки в нормативних актах України, то відповідно Закону України «Про національну безпеку України» від 21.06.2018 р., та Указом Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». Так в Законі України «Про національну безпеку України» зазначено, що «державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями» [1]. Таким чином, інформаційна безпека розглядається в контексті національної безпеки.

Як зазначає О.В. Олійник «головна мета державної політики інформаційної безпеки має полягати у захисті: конституційних прав і свобод людини і громадянина, забезпеченні єдності їх прав і обов'язків; духовних, морально-етичних, культурних, історичних, інтелектуальних та матеріальних цінностей суспільства, його інформаційного і природного середовища; конституційного ладу, суверенітету, територіальної цілісності, інформаційної безпеки в політичній, економічній, соціокультурній, науковотехнологічній, оборонній і державної безпеки, екологічній, власне інформаційній тощо складових національної безпеки» [3].

Продовжуючи думку О.В. Олійника можна виокремити основні принципи формування інформаційної безпеки: законність, баланс інтересів особи, суспільства та держави, комплексність, системність, економічна ефективність та інтеграція з міжнародними системами безпеки.

Результати. Таким чином, електронні послуги, нові технології, інформаційні системи та мережі міцно увійшли в наше повсякденне життя, а навмисні інциденти, що призводять до порушення роботи IT-сервісів і критично важливих інфраструктур, являють собою серйозну загрозу для їх функціонування.

У міру розвитку інформаційно-комунікаційних технологій поняття «інформаційна безпека» стало набувати дедалі виразнішого технічного змісту. Під нею розуміли захищеність інформаційного середовища, яке, своєю чергою, трактували як сукупність інформаційних ресурсів, систем розповсюдження, формування і використання інформації та інформаційної інфраструктури.

Проведений аналіз єдиного механізму забезпечення інформаційної безпеки та кібербезпеки в ЄС дав змогу встановити, що європейська модель інформаційної безпеки формується на основі концепції захисту інформаційних систем, що переважно охоплює сфери діяльності, які безпосередньо пов'язані з використанням технічних засобів збирання, оброблення, захисту, розповсюдження та використання інформації. Тому в межах цієї платформи оперують такими поняттями, як «кібербезпека», «кіберзагрози», «кібератаки». Однак необхідно звернути увагу й на інший бік інформаційної безпеки: деструктивний інформаційний вплив на свідомість населення та замовчування про сучасні інструменти кібервпливу (ботнети, спам, фішинг тощо).

Інформаційна безпека виступає інтегративною складовою національної безпеки та має формуватися на захищеності інтересів особистості, суспільства і держави. А найважливішим завданням системи забезпечення національної інформаційної безпеки є вдосконалення правового регулювання, включно з детальнішим врегулюванням захисту інформації; використання найефективніших сучасних методів і способів захисту інформації; удосконалення системи інформаційної безпеки; впровадження сучасних інформаційних технологій

в управлінську діяльність; пріоритетність розвитку інформаційних технологій (програмне забезпечення, інновації та застосування нанотехнологій в інформаційній безпеці, а також в інформаційній сфері).

ЛІТЕРАТУРА:

1. Закон України «Про національну безпеку України» від 21.06.2018 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

2. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Humanitarian vision.* 2016. Vol. 2. Num. 1. С. 27-32. URL : https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf

3. Олійник О.В. Принципи забезпечення інформаційної безпеки України. *Юридичний вісник.* 2016. Вип. 4(41). С. 72-78.

4. Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12

5. Шевчук М.О. До питання генези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2023. Т.2. №78. С. 134-139. URL : http://visnyk-pravo.uzhnu.edu.ua/article/view/285994/280058

6. Cambridge Dictionary. URL : https://dictionary.cambridge.org/dictionary/english/information-security?q=information+security+

7. Collins dictionary URL : https://www.collinsdictionary.com/dictionary/english/national-security#google_vignette

8. Dennison Susi, Franke Ulrike Esther, Zerka Paweł The nightmare of the dark: The security fears that keep Europeans awake at night. URL : https://ecfr.eu/special/the_nightmare_of_the_dark_the_security_fears_that_keep_europeans_awake_at_n/

9. Developments in the field of information and telecommunications in the context of international security : Resolution by the General Assembly A/RES/53/70 4 December 1998 URL : https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement

10. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) URL : https://eur-lex.europa.eu/eli/dir/2022/2555/oj

11. Directive 2016/1148 of the European Parliament and the Council concerning measures for a high common level of security of network and information systems across the Union. URL :https://eur-lex.europa.eu/eli/dir/2016/1148/oj

12. ENISA – The European Union Agency for Cybersecurity URL : https://www.ENISA.europa.eu/

13. EU Security Union Strategy: connecting the dots in a new security ecosystem. URL : https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379

14. European Commission: The EU's Cybersecurity Strategy for the Digital Decade (2020), Joint Communication to the European Parliament and the Council, JOIN(2020) 18 final. Available online in April 2024 URL : https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

15. Insider threat job aid. A glossary of Basic Insider Threat Definitions. CDSE : Center For Development of Security Excellence. 32 p. URL : https://www.cdse.edu/Portals/124/Documents/jobaids/insider/CDSE-Insider-Threat-Definitions.pdf

16. Lasswell Harold National Security and Individual Freedom, New York, Toronto, London. 1952. 259 p. URL : https://ia904709.us.archive.org/17/items/nationalsecurity00lass/nationalsecurity00lass.pdf

17. Lippmann Walter U.S. Foreign Policy: Shield of the Republic. Boston: Little, Brown and Company, 1943. URL : https://ia804705.us.archive.org/4/items/in.ernet.dli.2015.74564/2015.74564.U-S-Foreign-Policy-Shield-Of-The-Republic.pdf

18. Makinda Samuel M. Sovereignty and Global Security, Security Dialogue. *Sage Journals.* 1998. Volume 29 Issue 3. P. 281-292. URL : https://journals.sagepub.com/doi/abs/10.1177/0967010698029003003

19. Markopoulou Dimitra, Papakonstantinou Vagelis, Hert Paul The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review. 2019. Volume 35, Issue 6.* URL : :https://www.sciencedirect.com/science/article/pii/S0267364919300512)

20. Nieles Michael, Dempsey Kelley, Pillitteri Victoria Yan An Introduction to Information Security. NIST Special Publication 800-12 Revision 1. doi: https://doi.org/10.6028/NIST.SP.800-12r1

21. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EU. URL : https://eur-lex.europa.eu/eli/reg/2016/679/oj

22. Regulation (EU) 2019/881 on the European Union Agency for Cybersecurity and on information and communications technology cybersecurity certification (Cybersecurity Act) URL : https://eur-lex.europa.eu/EN/legal-content/summary/the-eu-cybersecurity-act.html

23. Ruohonen Jukka The Incoherency Risk in the EU's New Cyber Security Policies. *License: arXiv.org perpetual non-exclusive license.arXiv:2405.12043v1 [cs.CR]* 2024. URL : https://arxiv.org/html/2405.12043v1

REFERENCES:

1. Zakon Ukrayiny «Pro nacional`nu bezpeku Ukrayiny» vid 21.06.2018 r. *Ofitsiinyi sait Verkhovnoi Rady Ukrainy* [Official website of the Verkhovna Rada of Ukraine]. Retrieved from: https://zakon.rada.gov.ua/laws/show/2469-19#Text [in Ukrainian]

2. Ilnyczka, U. (2016) Informacijna bezpeka Ukrayiny: suchasni vyklyky, zagrozy ta mexanizmy protydiyi negatyvnym informacijno-psyxologichnym vplyvam. [Information security of Ukraine: modern challenges, threats and mechanisms of counteracting negative information-psychological influences]. *Humanitarian vision.* vol. 2, no. 1, pp. 27-32. Retrieved from: https://

science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf [in Ukrainian]

3. Olijnyk, O.V. (2016) Pryncypy zabezpechennya informacijnoyi bezpeky Ukrayiny. [Principles of maintenance of the informational security of Ukraine]. *Yurydychnyj visnyk.* no. 4(41), pp. 72-78. [in Ukrainian]

4. Ukaz Prezy`denta Ukrayiny Pro rishennya Rady nacionalnoyi bezpeky i oborony Ukrayiny vid 14 travnya 2021 roku «Pro Strategiyu kiberbezpeky Ukrayiny». *Ofitsiinyi sait Verkhovnoi Rady Ukrainy* [Official website of the Verkhovna Rada of Ukraine]. Retrieved from: https://zakon.rada.gov.ua/laws/show/447/2021#n12 [in Ukrainian]

5. Shevchuk, M.O. (2023) Do pytannya genezy ponyattya informacijnoyi bezpeky yak skladovoyi nacionalnoyi bezpeky. [On the question of the genesis of the concept of information security as a component of national security]. *Naukovyj visnyk Uzhgorodskogo nacionalnogo universytetu. Seriya: Pravo.* vol. 2, no. 78, pp. 134-139. Retrieved from: http://visnyk-pravo.uzhnu.edu.ua/article/view/285994/280058 [in Ukrainian]

6. Cambridge Dictionary. Retrieved from: https://dictionary.cambridge.org/dictionary/english/information-security?q=information+security+ [in English]

7. Collins dictionary. Retrieved from: https://www.collinsdictionary.com/dictionary/english/national-security#google_vignette [in English]

8. Dennison, Susi, Franke, Ulrike Esther, Zerka, Paweł The nightmare of the dark: The security fears that keep Europeans awake at night. Retrieved from: https://ecfr.eu/special/the_nightmare_of_the_dark_the_security_fears_that_keep_europeans_awake_at_n/ [in English]

9. Developments in the field of information and telecommunications in the context of international security : Resolution by the General Assembly A/RES/53/70 4 December 1998 Retrieved from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement [in English]

10. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Retrieved from: https://eur-lex.europa.eu/eli/dir/2022/2555/oj [in English]

11. Directive 2016/1148 of the European Parliament and the Council concerning measures for a high common level of security of network and information systems across the Union. Retrieved from: https://eur-lex.europa.eu/eli/dir/2016/1148/oj [in English]

12. ENISA – The European Union Agency for Cybersecurity. Retrieved from: https://www.ENISA.europa.eu/ [in English]

13. EU Security Union Strategy: connecting the dots in a new security ecosystem. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379 [in English]

14. European Commission: The EU's Cybersecurity Strategy for the Digital Decade (2020), Joint Communication to the European Parliament and the Council, JOIN 18 final. Available online in April 2024 Retrieved from: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 [in English]

15. Insider threat job aid. A glossary of Basic Insider Threat Definitions. CDSE : Center For Development of Security Excellence. 32 p. Retrieved from: https://www.cdse.edu/Portals/124/Documents/jobaids/insider/CDSE-Insider-Threat-Definitions.pdf [in English]

16. Lasswell, Harold (1952) National Security and Individual Freedom, New York, Toronto, London. 259 p. Retrieved from: https://ia904709.us.archive.org/17/items/nationalsecurity00lass/nationalsecurity00lass.pdf [in English]

17. Lippmann, Walter (1943) U.S. Foreign Policy: Shield of the Republic. Boston: Little, Brown and Company. Retrieved from:https://ia804705.us.archive.org/4/items/in.ernet.dli.2015.74564/2015.74564.U-S-Foreign-Policy-Shield-Of-The-Republic.pdf [in English]

18. Makinda, Samuel M. (1998) Sovereignty and Global Security, Security Dialogue. *Sage Journals.* vol. 29, is. 3, pp. 281-292. Retrieved from: https://journals.sagepub.com/doi/abs/10.1177/0967010698029003003 [in English]

19. Markopoulou, Dimitra, Papakonstantinou, Vagelis, Hert, Paul (2019) The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review.* vol. 35, is. 6. Retrieved from: :https://www.sciencedirect.com/science/article/pii/S0267364919300512. [in English]

20. Nieles, Michael, Dempsey, Kelley, Pillitteri, Victoria Yan An Introduction to Information Security. NIST Special Publication 800-12 Revision 1. Retrieved from: doi: https://doi.org/10.6028/NIST.SP.800-12r1 [in English]

21. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Retrieved from: https://eur-lex.europa.eu/eli/reg/2016/679/oj [in English]

22. Regulation (EU) 2019/881 on the European Union Agency for Cybersecurity and on information and communications technology cybersecurity certification (Cybersecurity Act). Retrieved from: https://eur-lex.europa.eu/EN/legal-content/summary/the-eu-cybersecurity-act.html [in English]

23. Ruohonen, Jukka (2024) The Incoherency Risk in the EU's New Cyber Security Policies. *License: arXiv.org perpetual non-exclusive license. arXiv:2405.12043v1 [cs.CR]*. Retrieved from: https://arxiv.org/html/2405.12043v1[in English]

Information security as an element of national security: theoretical dimension and implementation features

Myloserdna Iryna Mykhailivna

Candidate of Political Sciences,
Associate Professor,
Associate Professor at the Department
of Political Science
Odesa I. I. Mechnikov National University
Dvorianska str., 2, Odesa, Ukraine
ORCID: 0000-0003-2083-9500

The article is devoted to the analysis of ideas about the essence of the phenomena of «national security» and «information security», as well as to the definition of information security as a component of national security, which, in the context of rapid development of information and communication technologies, faces a new dimension of risks and threats. The study is based on systemic and interdisciplinary approaches, as well as deterministic factor analysis, which allowed to identify the key aspects of the information dimension of the national security of the State, as well as the main threats it faces in the current environment.

It is established that the modern national security of the State is facing new challenges and threats due to the processes of digitalisation in all aspects of life, the influence of the Internet, artificial intelligence and social networks. In today's environment, in order to ensure national security, states direct their policies not only to strengthen military capabilities, but also to master and control digital technologies in the context of transnational cross-border computer crime and cyberterrorism.

The article analyses the main groups of information and technical hazards: the first group is related to the growth of propaganda and disinformation, incitement to violence, the second is a new class of social crimes, and the third is the use of ICT for political purposes. The author establishes that ensuring and improving information security is a significant component of national security, which contributes to the development of the security of information infrastructure and democratic procedures in the State.

The article examines the experience of the EU countries in strengthening the information security of the State and establishing 'digital sovereignty' as a component of the national security of the State. It is established that the peculiarity of the European experience of forming and strengthening information security is its comprehensive nature, which is accompanied by work towards creating an integrated system of regulations, plans, and institutions whose activities are aimed at implementing plans and counteracting new threats. The article also notes the role of interaction between civil society and the State in strengthening information security and ensuring security in cyberspace at the national level.

Key words: *national security of the state, information security, cybersecurity, digitalisation, EU, Ukraine.*