Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»
Навчально-науковий інститут державного управління
Кафедра державного управління і місцевого самоврядування

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

Студента *Кравцова Олега Валентиновича*

академічної групи *281м-22з-2 ІДУ*

спеціальності *281 Публічне управління та адміністрування*

на тему: *«Забезпечення інформаційної безпеки органів публічного управління в умовах цифрової трансформації»*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	Чикаренко І.А.			
розділів:				

Рецензент:				

Нормоконтролер:	Вишневська О.В.			

Дніпро
2023

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи ступеня магістра на тему «Забезпечення інформаційної безпеки органів публічного управління в умовах цифрової трансформації».

82 стор., 5 рис., 65 джерел.

БЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНИЙ ПРОСТІР, ІНФОРМАЦІЙНА КУЛЬТУРА, ЗАГРОЗИ, ОРГАНИ ДЕРЖАВНОЇ ВЛАДИ, ЦИФРОВА ТРАНСФОРМАЦІЯ.

Об’єкт дослідження – система забезпечення інформаційної безпеки органів публічного управління в умова цифрової трансформації.

Предмет дослідження – процеси удосконалення системи інформаційної безпеки органів публічного управління.

Метою кваліфікаційної роботи є розроблення та обґрунтування пропозицій щодо підвищення рівня інформаційної безпеки органів публічного управління в умовах цифрової трансформації.

У першому розділі досліджуються теоретико-методологічні засади інформаційної безпеки в умовах цифрової трансформації. Другий розділ присвячено аналізу правового забезпечення інформаційної безпеки в умовах цифровізації інформаційного простору. У третьому розділі відображені шляхи удосконалення забезпечення інформаційної безпеки в умовах цифрової трансформації.

Сфера практичного застосування результатів роботи: підвищення ефективності практичної діяльності органів публічної адміністрації у сфері забезпечення інформаційної безпеки.

.

ABSTRACT

Explanatory note of the master's degree qualification thesis on the topic «Ensuring information security of public authorities in the context of digital transformation».

82 pages, 5 figures, 65 sources

SECURITY, INFORMATION SECURITY, INFORMATION SPACE, INFORMATION CULTURE, THREATS, PUBLIC AUTHORITIES, DIGITAL TRANSFORMATION.

The object of research is the system of ensuring the information security of public administration in the context of digital transformation.

The subject of research is the processes of improving the information security system of public administration.

The purpose of the qualification work is to develop and substantiate proposals for improving the level of information security of public administration in the context of digital transformation.

The first chapter examines the theoretical and methodological foundations of information security in the context of digital transformation. The second section is devoted to the analysis of legal support for information security in the context of digitalization of the information space. The third section reflects the ways to improve information security in the context of digital transformation.

Scope of practical application of the results of the work: improving the efficiency of practical activities of public administration bodies in the field of information security.

ЗМІСТ

ВСТУП

Розвиток інформаційного суспільства та процесів цифрової трансформації суттєво підвищило значущість інформаційної сфери. В інформаційному просторі відбувся стрибок у розвитку інформаційних загроз. Нові досягнення у сфері цифрових технологій, посилення ролі масової комунікації та розвиток когнітивних технологій збільшили можливості деструктивного інформаційного впливу на людину та суспільство. Поряд з унікальними можливостями для соціального прогресу цифрове середовище породило нові виклики та загрози, які потребують адекватного реагування. Це зумовило виділення інформаційної безпеки як однієї з підсистем національної безпеки, значимість якої у міру розвитку науково-технічного прогресу інформаційно-комунікаційних технологій продовжує зростати. Розвиток новітніх інформаційних технологій обумовлює збільшення технологічного розриву між вимогами, які постійно ускладнюються до показників захищеності інформаційних ресурсів у суб'єктів публічного управління і можливостей інформаційних технологій та програмно-апаратних засобів, що використовуються при забезпеченні інформаційної безпеки. Зростає потреба в науково обґрунтованих методах і технологічних рішеннях для поновлення і вдосконалення системи забезпечення інформаційної безпеки не тільки держави, а й суспільства й особистості зокрема. Істотною причиною цього, із одного боку, є недосконалі механізми державного управління цією сферою, а з іншого – це зумовлюється недостатністю науково обґрунтованих методів і технологічних рішень для поновлення і вдосконалення системи забезпечення інформаційної безпеки України в війни. Існуюча недосконалість діючої системи інформаційної безпеки призводить до колосальних збитків для держави, суспільства й особистості.

Повномасштабна збройна агресія росії поставила перед суб'єктами забезпечення інформаційної безпеки України невідкладні завдання, пов'язані

із захистом інформаційного суверенітету, зниженням руйнівного впливу наративів, активно використовуваних противником для деструктивного впливу на функціонування публічних адміністрацій і на морально-психологічний стан населення. Ці завдання нагальні, і відкладення їх вирішення на інший, більш сприятливий час, як засвідчив восьмирічний досвід протистояння збройній агресії рф, лише збільшує та ускладнює існуючі проблеми.

Анонімне цифрове середовище з кожним роком все активніше генерує ризики розповсюдження кримінальних та інших антисоціальних ідей, розпалювання ненависті та ворожнечі, поширення протиправного контенту, обману та маніпуляції свідомістю, залучення до терористичної та сепаратистської діяльності, споживання наркотиків та суспільно небезпечної поведінки. Агресія росії щодо України різко загострила проблему поширення недостовірної суспільнозначущої інформації у засобах масової інформації та інтернет-ресурсах. Технології штучного інтелекту, віртуальної та доповненої реальності здатні вивести інформаційні загрози на новий рівень небезпеки.

Реалізація поставлених у Стратегії національної безпеки України, Стратегії інформаційної безпеки України та інших документах стратегічного планування завдань щодо забезпечення надійного захисту особи, суспільства та держави від зростаючих інформаційних загроз детермінує необхідність розробки пропозицій щодо подальшого формування системи забезпечення інформаційної безпеки України, при цьому, одним з пріоритетних напрямів є забезпечення інформаційної та кібер безпеки в органах публічного управління в умовах цифрової трансформації суспільства та держави.

Питання, пов’язані із сутністю та складовими інформаційної безпеки, розглядали у своїх роботах такі вчені, як І. Арістова, О. Баранов, К. Бєляков, В. Глушков, О. Довгань, О. Золотар, Р. Калюжний, Б. Кормич, А. Марущак, Н. Новицька, О. Олійник, В. Петрик, В. Пилипчук, В. Полевий, Л. Радовецька, Є. Скулиш, О. Тихомиров, Т. Ткачук, В. Цимбалюк, В. Фурашев, О. Шевчук та інші.

Мета дослідження полягає у розробленні та обґрунтуванні пропозицій щодо підвищення рівня інформаційної безпеки органів публічного управління в умовах цифрової трансформації.

Об’єктом дослідження визначено систему забезпечення інформаційної безпеки органів публічного управління в умова цифрової трансформації.

Предметом дослідження є процеси удосконалення системи інформаційної безпеки органів публічного управління.

Дослідження поставленої наукової проблеми здійснювалося на основі вирішення таких завдань:

– дослідити понятійно-категоріальний апарат інформаційної безпеки;

– проаналізувати нормативно-правове забезпечення інформаційної безпеки в умовах цифрової трансформації;

– охарактеризувати основні загрози інформаційній безпеці України;

– дослідити засоби протидії загрозам інформаційній безпеці України;

– визначити пріоритетні напрями удосконалення законодавства у сфері забезпечення інформаційної безпеки в умовах цифрової трансформації;

– запропонувати шляхи формування культури інформаційної безпеки.

У процесі роботи використано методи теоретичного й емпіричного дослідження, основними з яких є методи системного аналізу та синтезу (історичний, індукція та дедукція, порівняння та аналогія, класифікація тощо). Методологічною основою дослідження є системний підхід, що використовується для вирішення більшості завдань роботи. За допомогою аналітичного методу здійснено відбір наукової та нормативно-правової інформації за темою дослідження.

Нормативно-правовою базою роботи є Конституція України, Закони України, Укази Президента України, Постанови Кабінету Міністрів України.

Теоретичну основу роботи складають наукові публікації вітчизняних та зарубіжних науковців, практичні узагальнення, що містяться в монографічній, спеціальній та періодичній літературі, інтернет-ресурси тощо.

Сфера практичного застосування результатів роботи: підвищення ефективності практичної діяльності органів публічної адміністрації у сфері забезпечення інформаційної безпеки.

РОЗДІЛ І
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

1.1. Понятійно-категоріальний апарат інформаційної безпеки

На сучасному етапі розвитку суспільства процес цифрової трансформації є глобальним, всеохопним, таким, що проникає у всі сфери життя. Він перетворюється на один з основних факторів суспільного розвитку та багато в чому характеризує сучасну соціальну динаміку.

Завдяки процесам цифровізації в суспільстві відбуваються системні зміни, відповідно до яких всі сегменти суспільства, кожна людина залучаються до глобального інформаційного простору, стаючи елементами глобальної інформаційної системи та відповідно тією чи іншою мірою залежними від неї.

Зазначена інформаційна залежність стосується всього світу, усіх держав і людей, які беруть участь у процесі виробництва, зберігання та використання інформації в ході інформаційного обміну та інформаційної взаємодії. Інформаційна взаємодія стала планетарним фактором, породивши цілу низку соціальних трансформацій та ввівши в систему соціальних відносин такі процеси та якості, як: інформаційні війни, інформаційна зброя, інформаційний тероризм, інформаційна злочинність та інформаційна безпека.

Відповідно до Стратегії національної безпеки України національна безпека є станом захищеності національних інтересів України від зовнішніх та внутрішніх загроз [1]. У документах стратегічного планування та законодавстві України спостерігаються різні підходи щодо визначення видів безпеки.

У Стратегії національної безпеки України виділено державну, громадську, інформаційну, екологічну та інші види безпеки. Також згадуються військова (оборона), економічна, транспортна, енергетична безпека, безпека

особистості. У Законі України «Про національну безпеку України» законодавець виділяє кібербезпеку, громадську безпеку, воєнну безпеку [2]. Подібне має місце і в науковій літературі, оскільки дослідники не завжди дбають про дотримання логічних правил класифікації.

Інформаційна складова наявна у всіх видах національної безпеки. А це дає підставу виділити інформаційну безпеку як основний елемент національної безпеки [3]. Об'єктами інформаційної безпеки є держава, суспільство та особа.

Основними елементами організаційної основи системи забезпечення інформаційної безпеки (СЗІБ) України є такі суб'єкти: Президент України, Верховна Рада України, Кабінет Міністрів України, Рада національної безпеки й оборони України, органи виконавчої влади України, міжвідомчі й державні комісії, створені Президентом України та Кабінетом Міністрів України, органи місцевого самоврядування, органи судової влади, громадські об'єднання, громадяни, що беруть участь відповідно до законодавства України у вирішенні завдань забезпечення інформаційної безпеки України (рис. 1.1).

Суб'єкти СЗІБ України мають тісно взаємодіяти між собою. Кожний суб'єкт, відповідно до своєї компетенції, спеціалізується на вирішенні конкретних завдань, використовуючи при цьому відповідні, визначені законом, адміністративно-правові форми та методи. І як результат такої взаємодії, ці суб'єкти доповнюють один одного, внаслідок чого утворюють єдину організаційно-функціональну систему, об'єднану системою владно-розпорядчих повноважень і функцією із забезпечення інформаційної безпеки.

Об'єктами системи забезпечення інформаційної безпеки України є:

– інтереси органів державного управління в інформаційній сфері;

– система органів державного управління, а також їхні компетентні особи і відносини між ними (суспільні відносини в інформаційній сфері);

– власне система забезпечення інформаційної безпеки України [4].

Рис. 1.1. Елементи організаційної основи системи забезпечення інформаційної безпеки України

Із певною долею умовності можна говорити про те, що в Україні в основному створено законодавчу основу забезпечення інформаційної безпеки, що включає сукупність основних нормативних правових актів, які містять юридичні принципи й норми, спрямовані на правове врегулювання суспільних відносин у сфері забезпечення інформаційної безпеки держави. Разом із тим, правова база регулювання відносин у цій сфері ще далека від досконалості, що пов'язано з формуванням нової структури економічних, політичних, соціальних і духовних реалій як усередині країни, так і на міжнародній арені. У законодавстві не відображені реальні й дієві правові механізми адекватної протидії новим ризикам інформаційної безпеки. Потребують уточнення й класифікації сфери діяльності держави щодо її забезпечення. Протиріччя, подвійне тлумачення та декларативність положень відповідних законів перешкоджають їхньому ефективному й цілеспрямованому виконанню.

Із огляду на викладене, випливає, що першочерговим завданням для законодавця є формування гнучкої правової системи інформаційної безпеки держави, яка б комплексно врегулювала дану сферу відносин і відобразила державну політику у сфері забезпечення інформаційної безпеки, заходи захисту інформації, види та джерела загроз у сфері інформаційної безпеки, першочергові заходи щодо забезпечення інформаційної безпеки.

На виконання Рішення Ради національної безпеки і оборони України від 21 березня 2008 року «Про невідкладні заходи щодо забезпечення інформаційної безпеки України» 08 липня 2009 року затверджено Доктрину інформаційної безпеки України [5]. Відповідно до вищезгаданого нормативно-правового документа, стан захищеності національних інтересів України в інформаційній сфері визначається сукупністю збалансованих інтересів особи, суспільства та держави. На підставі указу Президента України у 2014 році Доктрина інформаційної безпеки втратила актуальність та відповідно чинність у зв'язку зі збройною агресією Росії на сході України.

У 2017 році затверджено нову Доктрину інформаційної безпеки України (далі – Доктрину інформаційної безпеки України 2017), яка закріпила дефініцію інформаційної безпеки як стан захищеності особи, суспільства та держави від внутрішніх та зовнішніх інформаційних загроз [6].

Обидві викладені дефініції мають досить широкий характер і наповнюються конкретним змістом через визначення національних інтересів України в інформаційній сфері.

Вивчення їх переліку (Доктрини інформаційної безпеки 2009 та Доктрини інформаційної безпеки 2017) прямо не виявляє особистий психологічний компонент інформаційної безпеки. Однак його сутнісні ознаки проглядаються в положеннях, що стосуються збереження культурних, історичних та духовноморальних цінностей народу України, доведення до міжнародної громадськості достовірної інформації про державну політику України та її офіційної позиції щодо соціально значущих подій у країні та світі, застосування інформаційних технологій з метою забезпечення національної безпеки України в галузі культури, територіальної цілісності та суверенітету.

У Доктрині інформаційної безпеки України 2017 року серед напрямів забезпечення інформаційної безпеки в галузі оборони країни виділено нейтралізацію інформаційно-психологічного впливу, у тому числі спрямованого на підрив традицій, пов’язаних із захистом Вітчизни.

У науці серед дослідників інформаційної безпеки протягом тривалого часу домінував вузький підхід до розуміння захисту інформації та інформаційних систем. Таке зрізане бачення лягло в основу базового законодавчого акту для інформаційної сфери 1990-х років – Законів України «Про інформацію» (1992 рік) та «Про захист інформації в інформаційнокомунікаційних системах» (1994 рік) [7; 8].

Багато в чому підхід зберігся у Законі України «Про внесення змін до деяких законодавчих актів України у зв’язку з прийняттям Закону України

«Про інформацію» та Закону України «Про доступ до публічної інформації», що вніс певні зміни у вказані нормативно-правові акти [9].

У зв'язку з цим С. С. Єсімов обґрунтовано наголошував на тому, що проблема інформаційної безпеки штучно звужується до технічних аспектів захисту інформації, при цьому нехтуються соціально-гуманітарні аспекти [10].

Починаючи з кінця 1990-х років, багато дослідників розвивали альтернативний підхід. Серед них слід виділити одного із основоположників теорії правового забезпечення інформаційної безпеки Б. А. Кормича [11].

Надалі широкий підхід до трактування інформаційної безпеки, що передбачає включення до її змісту психологічних аспектів, знаходить усе більше прихильників.

Р. А. Калюжний та В. С. Цимбалюк вважають, що інформаційна безпека − це вид інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства й держави безпечних умов життєдіяльності, пов'язаних із створенням, розповсюдженням, зберіганням та використанням інформації. У практиці інформаційної безпеки виділяються два напрями: інформаційна безпека та захист інформації [12].

У навчальній літературі з інформаційної безпеки автори дотримуються розширеної парадигми розуміння. У спеціалізованому словнику основою інформаційної безпеки суспільства визначено безпеку індивідуальної, групової та масової свідомості громадян за наявності інформаційних загроз, до яких насамперед слід віднести інформаційні впливи [13].

Важливе значення для затвердження інформаційної безпеки як складової предмета правового регулювання в галузі інформаційної безпеки мало її відображення у двох знакових наукових правотворчих ініціативах.

По-перше, у виданій у 2012 році Концепції кодифікації інформаційного законодавства України, розробленій авторським колективом Інституту інформації, безпеки і права Національної академії правових наук України, серед основних державно-правових складових упорядкування інформаційних

відносин у галузі правового забезпечення інформаційної безпеки названо визначення сучасних викликів і загроз інформаційній безпеці людини, суспільства і держави, адекватне реагування на реальні й потенційні загрози правовими, організаційними, технічними та іншими засобами [14].

В. М. Брижко, О. А. Баранов і В. С. Цимбалюк пропонували та обґрунтовували необхідністю охоплення положень про захист інформації та захист від деструктивного впливу на свідомість та поведінку масового споживача поширених відомостей.

Розробка Інформаційного кодексу України була передбачена Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» та Стратегією розвитку інформаційного суспільства в Україні [15; 16].

Логічним, але революційним за своїм значенням кроком стало віднесення захисту суспільства від деструктивного інформаційного впливу до основних національних інтересів України у Стратегії державної безпеки України [17].

Інформаційна безпека – стан захищеності національних інтересів людини, суспільства і держави в інформаційній сфері, за якого унеможливлено завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується, негативний інформаційний вплив; витік державної таємниці та службової інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації, у тому числі шляхом проведення іноземними спецслужбами, окремими організаціями, групами, особами спеціальних інформаційних операцій та деструктивних інформаційних впливів, а також забезпечується своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національним інтересам та національній безпеці України. Інформаційна безпека є складовою національної безпеки України (пункт 7 ст. 3 Стратегії

державної безпеки України). У документі визначено низку завдань щодо забезпечення інформаційної безпеки.

Сьогодні можна впевнено зробити висновок про те, що інформаційна безпека людини, суспільства та держави входить до змісту інформаційної безпеки. З цього випливає, що інформаційна безпека має загальні ознаки, властиві такому виду безпеки, важливими з яких є інформаційний характер загроз безпеці та інформаційна сфера як галузь прояву цих загроз.

Основними принципами інформаційної безпеки є забезпечення конфіденційності, доступності, цілісності й автентичності інформаційних ресурсів та інфраструктури, що її підтримує (рис. 1.2).

Рис. 1.2. Основні принципи інформаційної безпеки

Доступність інформаційних ресурсів – це можливість за прийнятний час одержати необхідну інформаційну послугу, яка знаходиться у вільному доступі.

Інформація повинна надаватися повноправним користувачам ресурсів своєчасно й безперешкодно. Тому, не протиставляючи доступність решті аспектів, її можна виділити як найважливіший елемент інформаційної безпеки.

Цілісність інформаційних даних означає здатність інформації зберігати початковий вигляд і структуру як у процесі зберігання, так і після неодноразової передачі. Вносити зміни, видаляти або доповнювати інформацію має право тільки власник або користувач із легальним доступом до даних. Цілісність виявляється найважливішим аспектом інформаційної безпеки (ІБ) у тих випадках, коли інформація служить «керівництвом до дії».

Конфіденційність – це захист від несанкціонованого доступу до інформації. У процесі дій і операцій інформація стає доступною тільки користувачам, які включені до інформаційної системи й успішно пройшли ідентифікацію.

Достовірність указує на приналежність інформації довіреній особі або власнику, який одночасно виступає в ролі джерела інформації, це гарантія того, що джерелом інформації є саме та особа, яка заявлена як її автор. Достовірність інформації безпосередньо впливає на суспільну та індивідуальну свідомість, такою ж мірою й на громадську думку, і в силу цього стає одним із основних принципів забезпечення інформаційної безпеки.

Власне, у контексті інформаційного розвитку суспільства та забезпечення інформаційної безпеки існують об’єктивні та суб’єктивні фактори. Визначено 8 основних факторів інформаційної безпеки (рис. 1.3).

Перший із яких – це динамізм інформаційної сфери. Швидкість технічного прогресу інтенсивно примножує зміст інформаційного простору, що надає нові можливості використання інформаційного контенту, реалізації нових ідей і задумок.

Другий фактор – економічний, який створює підґрунтя інформаційного розвитку суспільства й держави та матеріально-технічні можливості впровадження інформаційно-комунікаційних технологій.

Третій фактор – інтелектуальний, шо включає як інтелект людини, так і штучний інтелект, який все більше входить в наше життя і може повноцінно застосовуватися у формуванні інформаційної безпеки. Зокрема, людський

інтелект посідає головуючу роль у цьому процесі, ні одна машина не зможе замінити людини.

Рис. 1.3. Основні фактори інформаційної безпеки

Четвертий – людський фактор. Людський фактор заслуговує особливої уваги на думку багатьох авторів, тому що саме люди формують режим інформаційної безпеки і вони ж виявляються головною загрозою, бо прийняття рішення людиною і його виконання не є константою, навіть при однакових умовах.

П’ятий фактор – технічний. Складові технічного фактору характеризують технічну досконаліть і сучасність засобів обробки інформації, що визначає рівень технічної готовності до розгортання інформаційних процесів.

Шостий фактор – підвищення соціального значення інформаційних процесів – пріоритетність організаційно-забезпечувальної діяльності держави в інформаційній сфері, як основу подальшого розвитку суспільства, що підтверджується такими чинниками: усепроникливість інформаційних

процесів; створення широких інформаційно-комунікативних можливостей; виникнення додаткових можливостей саморозвитку суб'єктів.

Сьомий фактор – політико-ідеологічний, визначає рівень усвідомленості соціально сильними групами індивідів необхідності вирішення соціальних проблем та проблем інформаційної сфери.

Восьмий, останній, фактор – це правове забезпечення. Даний фактор є основним, бо інформаційна безпека, як і будь яка інша галузь держави потребує обов'язкового нормативно-правового врегулювання. Інформаційна безпека виступає об'єктом правового захисту. Правові засоби забезпечення інформаційної безпеки є провідним фактором захисту національних інтересів у цій сфері, а їхнє застосування визначається оптимізацією балансу відносин між правом суб'єктів інформаційних відносин на отримання інформації та правом на встановлення обмежень таких відносин із боку інших осіб щодо відомостей, володарями яких вони є; розробкою та реалізацією правових заходів захисту інформації, доступ до якої повинен обмежуватися правовими підставами в процесі захисту інформаційних ресурсів. Правове забезпечення ліквідації загроз і ризиків у сфері інформаційної безпеки є основним фактором структурування, формування, розглядається як законотворча діяльність, що спрямована на запобігання шкоди інтересам особи, суспільства та держави в інформаційній сфері.

Поряд із вище зазначеним, слід відмітити, той факт, що кожний фактор, який несе позитивну складову для побудови інформаційної безпеки, може мати певні ризики щодо сприяння розвитку останнього, а тому одним із пріоритетних завдань держави на етапі розвитку є визначення цих ризиків і розуміння напрямків правового регулювання та створення правових гарантій, необхідних для самореалізації суб'єктів в інформаційній сфері. Більшість із перелічених факторів є загальними чинниками (джерелами) процесу утворення національного права і тому дозволяють розглядати процеси

розвитку інформаційного права України в контексті проблем становлення правової системи держави в цілому.

У чинному законодавстві України сформувалися такі правові інститути у структурі підгалузі правового забезпечення інформаційної безпеки: захист інформації, охоплюючи захист окремих видів інформації обмеженого доступу; захист критично важливих об'єктів інформаційної інфраструктури; захист дітей від негативного впливу продукції сексуального чи еротичного характеру. У важливому для досліджуваної галузі Законі України «Про захист суспільної моралі» щодо дітей (ст. 7) термін «інформаційна безпека» не використовується.

У Законі України «Про захист суспільної моралі» є необхідність запровадження поняття «інформаційна безпека» з таких причин: потреба в позначенні психологічної складової інформаційної безпеки; наявність специфіки в системі інформаційної безпеки; наявність чіткої межі між захистом інформації та інформаційно-психологічною безпекою за критеріями об'єкта та методів впливу; існування комплексу специфічних загроз; спільність правового інструментарію, використовуваного захисту від різних форм деструктивного інформаційного впливу.

Принципова відмінність інформаційної безпеки традиційного блоку від інформаційної безпеки щодо суспільної моралі в тому, що її змістом є не захист інформації, а захист від інформації самої людини та суспільства, у тому числі дітей. З огляду на це, інформаційну безпеку можна визначити як захист особи та суспільства від негативного інформаційного впливу.

Теоретично під безпекою розуміють реальні явища, процеси та відносини, попередження чи усунення загроз, що становить мету та зміст політики безпеки [18]. Щодо сфери інформаційної безпеки йдеться про об'єкти деструктивного інформаційного впливу.

У проєкті Закону України «Про інформаційну безпеку» як об'єкти інформаційної безпеки виділялися:

– щодо людини та громадянина: забезпечення конституційних прав і свобод людини і громадянина на збирання, зберігання, використання та поширення інформації; право на спілкування мовою походження; недопущення несанкціонованого втручання у зміст, процеси обробки, передачі та використання персональних даних; захищеність від негативного впливу інформаційних технологій та інформаційно-психологічного впливу;

– щодо суспільства: збереження та примноження духовних, культурних і моральних цінностей українського народу та громадян України всіх національностей; інформаційне забезпечення суспільно-політичної стабільності, міжетнічної і міжконфесійної злагоди та розвитку громадянського суспільства;

– щодо держави: забезпечення інформаційного суверенітету, запобігання інформаційній агресії, експансії та інформаційній блокаді України з боку іноземних держав, організацій, груп та осіб; формування та реалізація органами державної влади та інститутами громадянського суспільства ефективної державної політики в інформаційній сфері; інформаційно-інфраструктурне забезпечення суспільно-економічного й науково-технічного розвитку та формування позитивного іміджу України; становлення та розвиток інформаційного суспільства в Україні; інтеграція України у європейський та світовий інформаційний простір [19].

У Стратегії інформаційної безпеки України об’єктом захисту від деструктивного інформаційно-психологічного впливу названо суспільство. У таких випадках спостерігається двоїстість об’єктів інформаційної безпеки: до них відносять людину, групу людей, суспільство, державу, психологічні складові – індивідуальну психіку та суспільну свідомість. У цьому випадку немає суперечності. Зазначене зумовлено різним рівнем деталізації при характеристиці об’єктів інформаційної безпеки.

У плані правового регулювання вибір необхідного рівня деталізації залежатиме від характеру та предмета правового акта. Для базового закону або

документа стратегічного планування доцільніше використовувати усі рівні. Для вузького предмета правового регулювання доцільно брати перший рівень деталізації.

У Стратегії інформаційної безпеки України йдеться про нейтралізацію інформаційної агресії, зокрема спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством [20]; у розділі XII Кримінального кодексу України (далі – КК України) як видовий об'єкт злочинів виділено суспільну мораль [21]; безпосереднім об'єктом адміністративного правопорушення у сфері інформаційної безпеки, передбаченим Кодексом України про адміністративні правопорушення, визначено інформацію [22].

Об'єкт інформаційної безпеки на трьох рівнях деталізації має різні особливості з позиції загальної та соціальної психології та соціології.

На першому рівні об'єктами інформаційної безпеки є особа, великі та малі соціальні групи. Первинним об'єктом інформаційної безпеки є особа, на яку направлено інформаційно-психологічний вплив. Як зазначає О. О. Золотар, людина як особистість і соціальний суб'єкт, її психіка схильні до дії інформаційних факторів, які, трансформуючись через поведінку, мають несприятливий вплив на соціальні суб'єкти [23].

Наступним об'єктом інформаційної безпеки є соціальні групи – групи людей, у якій спільність суспільно значущих рис виявляється у колективній ідентичності та контактах, що їх супроводжують, взаємодіях та соціальних відносинах.

Соціальні групи в науці розглядаються як психологічні спільності людей, котрі мають спільну ідентичність і групову психологію. У суспільних науках існує низка класифікацій соціальних груп, відповідно до яких поділяються на

великі, малі, первинні, вторинні, формальні, неформальні, стійкі, нестійкі, відкриті та закриті.

Щодо особистості об'єктом інформаційної безпеки є психіка. Психіка людини визначається як системна властивість високоорганізованої матерії, що полягає в активному відображенні суб'єктом об'єктивного світу, у побудові суб'єктом невідчужуваної від нього картини світу та регуляції на цій основі поведінки та діяльності. Впливаючи на картину світу людини, можемо впливати на поведінку.

Науковці О. Д. Довгань та Т. Ю. Ткачук під негативним інформаційно-психологічним впливом розуміють такий вплив на особу чи групу осіб, який здійснюється на їх психіку, зокрема й усупереч їхній волі, із застосуванням спеціальних засобів і методів, що призводить до шкідливих для людини, суспільства та держави наслідків [24].

На основі вищевикладеного визначаємо інформаційну безпеку як складову частину системи національної безпеки, що становить стан захищеності особи, соціальних груп, суспільства від деструктивного інформаційного впливу.

Щодо інформаційної безпеки держави, то вчені зазначають, що чинниками забезпечення інформаційної безпеки держави є гарантування:

– безпеки інформації загального доступу, мереж зв'язку, інформаційнотелекомунікаційних систем, технічних та програмних засобів виконання маніпуляцій з інформацією, доступу до інформації;

– конфіденційності інформації з обмеженим доступом;

– захищеності особи, суспільства й держави від шкідливого впливу певних видів інформації (у цьому разі йдеться не про інформацію, віднесену до категорій з обмеженим доступом, а про такі види, котрі здатні зашкодити вказаним суб'єктам інформаційних відносин).

Науковці П. В. Квіткін, І. В. Дятлова та Л. О. Петрова зазначають, що проблема інформаційної безпеки особистості набуває актуальності для

українського суспільства, яке є об’єктом інформаційно-пропагандистських та інформаційно-психологічних операцій противника. Реаліями сьогодення є проблеми в соціально-економічному розвитку країни, процесів політичної і духовної сфер суспільної життєдіяльності, які використовуються для дискредитації внутрішньої та зовнішньої політики держави, національно-історичних цінностей і євроатлантичних прагнень українського народу.

1.2. Нормативно-правове забезпечення інформаційної безпеки в умовах цифрової трансформації

Стимульовані інформаційними технологіями економічні та соціальні перетворення, загальна інформатизація, використання інформації як одного з ефективних засобів впливу на суспільну свідомість та технологічний прогрес, поява нових форм відносин в умовах активного інформаційного обміну призводять до необхідності перегляду принципів взаємодії в системі держава-суспільство-особа.

Настання інформаційного суспільства трансформує звичні моделі економічної, соціальної, політичної діяльності, що тягне перебудову державноправової діяльності з урахуванням нових умов інформаційної відкритості та необхідності вирішення проблем забезпечення інформаційної безпеки.

Розвиток інформаційно-комунікаційних технологій та процесів цифрової трансформації ставить завдання реформування системи правового регулювання суспільних відносин у різних сферах. Це особливо актуально стосовно нових викликів цифрового середовища, кількість та небезпека яких стрімко зростають.

З початку нового тисячоліття процес нормативного регулювання інформаційної безпеки значно активізувався, особливо у зв’язку з ухваленням Окінавської хартії глобального інформаційного суспільства та Доктрини

інформаційної безпеки України (2009 рік) [25; 26]. Загалом, за останні двадцять років було проведено значну роботу, спрямовану на розвиток правового забезпечення інформаційної безпеки.

Останнім десятиліттям ця сфера законодавства стала однією з динамічних. Фрагментарні зміни, що вносяться в інформаційне та інше галузеве законодавство, викликані поточними проблемами, позбавлено системності та опори на наукову основу.

А. Ю. Нашинець-Наумова у монографії «Інформаційна безпека: питання правового регулювання» зазначає, що сьогодні проблематика інформаційної безпеки держави досліджується в роботах багатьох українських учених. Проте зазначені дослідження та наукові праці стосувалися лише національної безпеки в інформаційній сфері. Залишаються недостатньо вивченими концептуальні засади системи забезпечення інформаційної безпеки держави [27].

Аналізуючи систему правового забезпечення інформаційної безпеки, беремо за основу запропонований І. М. Шопіною концептуальний підхід до вирішення правових проблем забезпечення інформаційної безпеки [28].

Цей підхід передбачає вивчення правових засобів забезпечення інформаційної безпеки у нерозривному зв’язку з цілями, завданнями та механізмами реалізації державної політики щодо забезпечення інформаційної безпеки.

Спроба детальної правової регламентації базових аспектів забезпечення інформаційної безпеки здійснювалася у законопроєкті «Про засади інформаційної безпеки України» [57]. У проєкті закону було визначено принципи забезпечення інформаційної безпеки, основні завдання державної політики у сфері забезпечення інформаційної безпеки, функції державної системи забезпечення інформаційної безпеки.

Поняття «забезпечення безпеки» належить до базових категорій у теорії безпеки. Термін «забезпечення», що лежить в основі, орієнтує на активну діяльність певних суб’єктів, спрямовану на досягнення стану захищеності

об’єктів безпеки [29]. Змістом діяльності є реалізація уповноваженими суб’єктами політичних, правових, військових, соціально-економічних, інформаційних, організаційних та інших заходів, спрямованих на протидію загрозам національній безпеці.

У Стратегії інформаційної безпеки України забезпечення інформаційної безпеки визначається як здійснення комплексу взаємопов’язаних організаційних, правових та інших заходів щодо прогнозування, виявлення, стримування, запобігання, відображення інформаційних загроз та ліквідації їх негативних наслідків.

У Законі України «Про основи національної безпеки України», так само як і в законі, що прийшов йому на зміну – «Про національну безпеку України», у забезпеченні безпеки виділено два рівні: державна політика у сфері забезпечення безпеки; діяльність із забезпечення безпеки [30; 2].

Такий підхід підтримується в науковій літературі. Суть такого розмежування зводиться до того, що на першому рівні здійснюється стратегічне планування забезпечення безпеки (постановка цілей, завдань, напрямів, визначення суб’єктів, форм і методів реалізації), на другому – безпосередня реалізація системи заходів забезпечення безпеки відповідно до виробленого плану.

Під забезпеченням інформаційної безпеки розуміємо діяльність державних інститутів, інститутів громадянського суспільства щодо вироблення та реалізації системи правових, організаційних, інформаційних і інших заходів, спрямованих на забезпечення захищеності особи, соціальних груп та суспільства від деструктивного інформаційного впливу.

Поряд із протидією інформаційним загрозам до змісту забезпечення інформаційної безпеки додано заходи щодо підвищення стійкості людини, соціальних груп та суспільства до впливу загроз.

Останній напрям має важливе значення через неможливість повного захисту соціальних суб'єктів від негативного психологічного впливу та недостатню ефективність систем фільтрації інформації.

Третій змістовий блок забезпечення інформаційної безпеки становлять заходи щодо впливу на інформаційне середовище, у якому здійснюється деструктивний інформаційний вплив на особистість та соціальні групи. Активізуючи позитивні чинники та нейтралізуючи негативні елементи цифрового середовища, можна підвищувати рівень захищеності об'єктів. Цей напрям укладається в концепцію «інформаційної екології», що передбачає створення певного стану інформаційного середовища, безпечного для фізичного та психічного здоров'я людини, індивідуальної, групової та суспільної психології. Інформаційна екосистема – це система, що складається з людини, інформації, інформаційного середовища та інформаційних технологій.

Діяльність із забезпечення інформаційної безпеки охоплює чотири основні елементи: протидія джерелам загроз інформаційної безпеки; нівелювання чи зменшення деструктивного впливу загроз на об'єкти інформаційної безпеки; збільшення стійкості об'єктів щодо деструктивного інформаційного впливу; надання впливу на елементи цифрового середовища.

Заходи забезпечення інформаційної безпеки охоплюють: регулювання, зокрема обмеження інформаційних потоків; організація інформаційних потоків, зокрема ініціювання поширення певної інформації; поширення способів й засобів обробки та оцінки інформації; формування групового і індивідуального психологічного захисту.

У Стратегії національної безпеки України вони визначені як об'єктивно значущі потреби особистості, суспільства та держави у безпечному та сталому розвитку. Щодо інформаційної сфери національні інтереси визначаються тією роллю, яку відіграє інформація, інформаційна інфраструктура в забезпеченні сталого розвитку нації в конкретних історичних умовах.

Стратегія державної безпеки України закріплює національні інтереси України на сучасному етапі як захист конституційного ладу, суверенітету, незалежності, державної та територіальної цілісності України, зміцнення оборони країни; підтримання громадянського миру та згоди в країні; розвиток безпечного інформаційного простору; захист суспільства від деструктивного інформаційного впливу; зміцнення традиційних духовно-моральних цінностей, збереження культурної та історичної спадщини народу України.

Захист від деструктивного інформаційного впливу вперше виділено як один із національних інтересів у базовому документі стратегічного планування. У цьому плані необхідне внесення низки змін та доповнень до чинної Стратегії інформаційної безпеки України, у якій захист від деструктивного інформаційного впливу безпосередньо не відображено.

У Стратегії національної безпеки України безпосередньо мета забезпечення інформаційної безпеки не визначена. Узагальнення інформаційних положень та зміцнення суверенітету в інформаційному просторі і є метою забезпечення інформаційної безпеки [1].

У Стратегії інформаційної безпеки України загальну стратегічну мету забезпечення інформаційної безпеки визначено як посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина [20].

Стратегічною метою забезпечення інформаційної безпеки є підтримка стану захищеності особистості, соціальних груп та суспільства від деструктивного інформаційного впливу, що забезпечує гарантовану реалізацію національних інтересів України.

На наступному рівні визначення цілі необхідно дати характеристику завдань та функцій забезпечення інформаційної безпеки. Щодо завдань і

функцій забезпечення інформаційної безпеки, то загальноприйнятого уявлення про завдання та функції забезпечення безпеки немає.

Аналіз Закону України «Про національну безпеку України» та документів стратегічного планування в галузі забезпечення національної безпеки показує відмінності в переліку завдань та функцій.

У ч. 2 ст. 36 Закону України «Про національну безпеку України» зазначено, що Стратегія національної безпеки України визначає: напрями та завдання реформування й розвитку сектору безпеки й оборони (пункт 4). У Стратегії національної безпеки України вказано, що держава повинна виконувати лише необхідні функції, насамперед безпекову, зовнішньополітичну, соціальну, регуляторну (пункт 50), а завдання не вказані.

У Стратегії інформаційної безпеки України завдання забезпечення інформаційної безпеки не виділено, а його основні напрями визначено стосовно окремих сфер державного управління: інформаційний вплив Російської Федерації як держави-агресора на населення України; інформаційне домінування Російської Федерації як держави-агресора на тимчасово окупованих територіях України; обмежені можливості реагування на дезінформаційні кампанії; несформованість системи стратегічних комунікацій; недосконалість регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів; спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України; доступ до інформації на місцевому рівні; недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам [20].

Позитивно вирізняється в цьому плані Стратегія державної безпеки України, де чітко окреслено основні завдання забезпечення інформаційної безпеки. Так, до сфери інформаційної безпеки належать:

– формування безпечного середовища обороту достовірної інформації в цифровому середовищі;

– розвиток системи прогнозування, виявлення та попередження загроз інформаційній безпеці України, визначення їх джерел, оперативної ліквідації наслідків реалізації таких загроз;

– створення умов для ефективного попередження, виявлення та припинення правопорушень, скоєних з використанням інформаційно-комунікаційних технологій;

– протидія використанню інформаційної інфраструктури терористичними організаціями, спеціальними службами та пропагандистськими структурами іноземних держав для здійснення деструктивного інформаційного впливу на громадян та суспільство.

Аналіз Стратегії державної безпеки України дозволяє виділити додаткові завдання забезпечення інформаційної безпеки: підтримання морально-політичного та психологічного стану особового складу Збройних сил України та інших військових формувань, військово-патріотичне виховання; недопущення втручання у внутрішні справи України, припинення розвідувальної та іншої діяльності іноземних держав та окремих осіб проти національних інтересів України; попередження та нейтралізація соціальних, міжконфесійних та міжнаціональних конфліктів, деструктивних релігійних течій; реалізація державної інформаційної політики щодо зміцнення сприйняття суспільством євроатлантичних пріоритетів та європейських культурно-історичних цінностей, неприйняття громадянами деструктивних ідей, стереотипів; зміцнення культурного суверенітету України та збереження єдиного культурного простору, захист суспільства від зовнішнього деструктивного інформаційного впливу.

Стратегія національної безпеки України та Стратегія державної безпеки України детально визначає завдання щодо забезпечення інформаційної безпеки. Більша частина завдань закріплена в межах забезпечення неінформаційної безпеки та інших стратегічних національних пріоритетів.

Узагальнюючи вищевикладене, до завдань забезпечення інформаційної безпеки слід зарахувати: прогнозування, виявлення, аналіз та оцінку загроз інформаційній безпеці, у тому числі щодо Законів України «Про боротьбу з тероризмом», «Про запобігання корупції» [31; 32]; аналіз та оцінку вразливості особи, соціальних груп і суспільства від деструктивного інформаційного впливу; стратегічне планування у сфері забезпечення інформаційної безпеки; правове регулювання у сфері забезпечення інформаційної безпеки; застосування комплексу оперативних та довготривалих заходів щодо превенції, припинення та усунення загроз інформаційній безпеці, мінімізації та ліквідації наслідків впливу; застосування комплексу оперативних і довготривалих заходів щодо підвищення здатності особи, соціальних груп та суспільства протистояти деструктивному інформаційному впливу; організацію діяльності системи забезпечення інформаційної безпеки; кадрове, інформаційне, матеріально-технічне та фінансове забезпечення діяльності суб'єктів забезпечення інформаційної безпеки; співробітництво у сфері забезпечення інформаційної безпеки з країнами Європейського Союзу та Організації Північноатлантичного Союзу.

Цифрова грамотність («цифрова» компетентність) визнана Європейським Союзом однією з 8 ключових компетенцій для повноцінного життя та діяльності. У 2016 році Європейський Союз презентував оновлений фреймворк Digital Competence (DigComp 2.0), що складається з п'яти основних блоків компетенцій: інформаційна грамотність та грамотність щодо роботи з даними; комунікація та взаємодія; цифровий контент; інформаційна безпека; вирішення проблем [33]. У Стратегії інформаційної безпеки України закріплено, що забезпечення інформаційної безпеки здійснюється на основі поєднання законодавчої, правозастосовної, правоохоронної, судової, контрольної та інших форм діяльності державних органів у взаємодії з органами місцевого самоврядування, фізичними та юридичними особами.

До базових принципів забезпечення безпеки згідно Закону України «Про національну безпеку України» входить системність та комплексність застосування органами публічної влади політичних, організаційних, соціальноекономічних, інформаційних, правових та інших заходів забезпечення безпеки. Реалізація цього принципу у сфері державного управління передбачає наявність системи забезпечення національної безпеки в Україні та відповідних підсистем забезпечення окремих видів безпеки. У чинному Законі України «Про національну безпеку України» поняття системи забезпечення безпеки не використовується.

Законодавці виділяли в системі забезпечення безпеки два основні елементи: інституційний (суб'єкти забезпечення безпеки) та нормативний (законодавство у сфері забезпечення безпеки) (рис. 1.4).

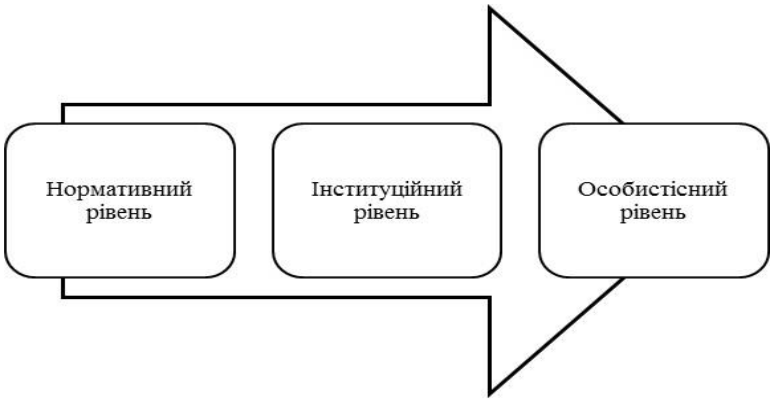

Рис. 1.4. Рівні забезпечення інформаційної безпеки суспільства та особистості

У документах стратегічного планування став застосовуватися дещо інший підхід до визначення системи забезпечення безпеки. Виділено такі елементи, як сили та засоби забезпечення безпеки.

Цей підхід знайшов відображення у Стратегії національної безпеки України та Стратегії інформаційної безпеки України [1; 20]. Під силами забезпечення інформаційної безпеки розуміються державні органи, підрозділи та посадові особи державних органів, органів місцевого самоврядування, уповноважені на рішення відповідно до законодавства завдань забезпечення

інформаційної безпеки, а під засобами – правові, організаційні, технічні та інші засоби, які використовуються силами забезпечення інформаційної безпеки. У Стратегії національної безпеки України складовими частинами системи забезпечення національної безпеки визначено сукупність органів публічної влади та нормативно-правових актів. Забезпечення інформаційної безпеки охоплює сили, засоби та методи, правове регулювання.

У Стратегії інформаційної безпеки України йдеться про те, що система забезпечення інформаційної безпеки України є частиною системи забезпечення національної безпеки країни та охоплює особу, суспільство та державу.

Фундаментом правової основи забезпечення інформаційної безпеки стали Закони України «Про інформацію», «Про захист інформації в інформаційнокомунікаційних системах», «Про захист суспільної моралі», «Про електронні комунікації» [7; 8; 34; 35].

Безпосередньо інформаційна безпека у Законі України «Про електронні комунікації» не вказується. Але зазначено у ч. 7 ст. 2, що безпека мереж і послуг – здатність електронних комунікаційних мереж і послуг протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж і послуг, а також даних, що зберігаються, передаються чи обробляються, та пов’язаних із ними послуг, що надаються або доступ до яких здійснюється через електронні комунікаційні мережі чи послуги [35]. Воєнний стан вимагає переосмислення ієрархії суспільних відносин, що охороняються кримінальним законом, серед яких окреме місце виділено інформаційній безпеці, що відображено у Законі України «Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції». Водночас в умовах воєнного стану, поєднаного з цифровою трансформацією, з метою прискореного розвитку економіки України, що позначено у Законі України «Про стимулювання розвитку цифрової економіки в Україні», забезпечення

інформаційної безпеки охоплює усі напрями: інформаційну безпеку особи, інформаційну безпеку суспільства, інформаційну безпеку держави.

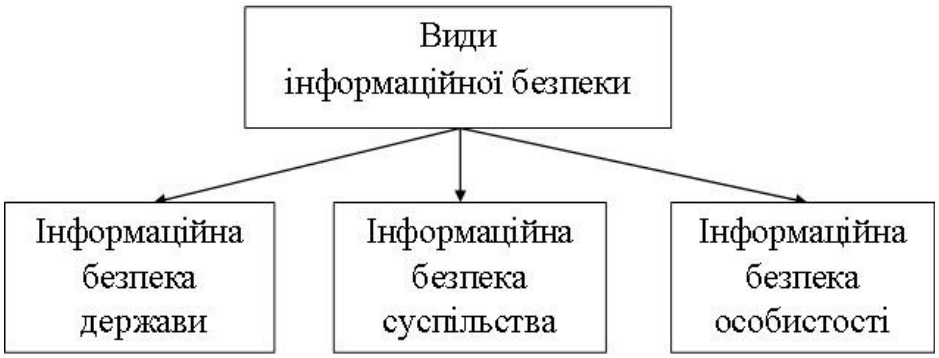

Рис. 1.5. Види інформаційної безпеки

Інформаційна безпека як об’єкт забезпечення є відкритою динамічною системою суспільних відносин, що забезпечують реалізацію інтересів особи, суспільства та держави в інформаційній сфері; охоплює суспільні відносини, що забезпечують реалізацію права на інформацію та охорону інформації від неправомірного доступу; суспільні відносини, які забезпечують безпеку інформаційних ресурсів; суспільні відносини, що забезпечують безпеку використання інформаційно-комунікаційних технологій.

Таки чином, системи правового забезпечення інформаційної безпеки подана як сукупність наукових знань, що становлять зміст теорії систем права та теорії інформаційного права, що розвиваються. Зазначена система представлена як цілісне складне утворення, що розвивається, охоплює основні взаємопов’язані підгалузі, що регулюють предметні інформаційні відносини. Характеризується цілісністю, зв’язком між елементами просторовим і функціональним, структурою і організацією, рівнями системи та їх ієрархію, специфічним способом регулювання, самоорганізацію системи, її функціонуванням та розвитком.

Певний вплив формування системи правового забезпечення інформаційної безпеки щодо деструктивного інформаційного впливу надають суміжні наукові теорії, розвиток яких істотно впливає на науковий рівень теорії

та систему інформаційного права: правова теорія організації правових систем, правова кібернетика, теоретико-інформаційні основи ухвалення управлінських організаційно-правових рішень, факторний аналіз.

Система правового забезпечення інформаційної безпеки розвивається на методологічній базі адекватного проблемно орієнтованого варіанта системного інформаційно-кібернетичного підходу на основі синергетики з розподілом на кібербезпеку та інформаційну безпеку особи, суспільства та держави.

Для переходу до цифрової економіки державі необхідно створити інформаційну інфраструктуру, у якій відкритість та прозорість даних поєднуються з рівністю можливостей окремих осіб в економіці (інклюзивна економіка) та ефективною системою інформаційної безпеки, яка захистить інтереси особи, суспільства і держави.

РОЗДІЛ 2
ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ ІНФОРМАЦІЙНОГО ПРОСТОРУ

2.1. Класифікація загроз інформаційній безпеці України

Інтенсивна інформатизація усіх сфер життєдіяльності суспільства є сьогодні одним із визначальних глобальних чинників подальшого соціально-економічного, інтелектуального та духовного розвитку людства. Водночас, світова спільнота вступає в новий етап своєї історії, котрий має всі підстави охарактеризувати його як еру інформаційних воєн. Так, інформаційна складова є ключовим елементом гібридної війни Російської Федерації проти нашої держави. Відтак, в умовах швидкого формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору, широкого використання інформаційнокомунікаційних технологій у всіх сферах життя особливого значення набувають проблеми інформаційної безпеки [6]. При цьому одним із стратегічних пріоритетів забезпечення інформаційної безпеки державою визначено створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них [36].

Спираючись на положення Закону України «Про національну безпеку України» [2], можна стверджувати, що система загроз слугує базою для стратифікації національної безпеки (з урахуванням джерела, характеру і специфіки загроз) на зовнішньополітичну, внутрішньополітичну, державну, воєнну, економічну, соціальну, гуманітарну, екологічну та інформаційну безпеку, а також безпеку державного кордону. Втім, виходячи з визначення національної безпеки, наведеного в цьому ж законі, перелік сфер, у яких можуть проявлятися загрози національній безпеці, не є вичерпним. Зокрема, залежно від середовища формування і масштабів загроз національним інтересам, традиційним став поділ національної безпеки відповідно до джерел

загроз на зовнішню та внутрішню [37]. Але за сучасних умов такий поділ стає вельми умовним, адже зовнішні загрози можуть випливати із внутрішніх джерел, а також інтегруватися із загрозами внутрішніми.

Відповідно, національна безпека перебуває у взаємозв'язку із чинниками, які щодо неї можуть розглядатися як загрози, адже національна безпека є системою оптимізації взаємовідносин між усвідомленими загрозами та ресурсами, що має суспільство для протидії цим загрозам. Загрози для суспільства є завжди, а рівень захищеності від них ніколи не буває максимальним. Тому національна безпека є динамічним засобом досягнення й підтримки балансу між реальними та потенційними загрозами, з одного боку, та здатністю суб'єкта протидіяти їм, з іншого.

Що стосується загроз безпеці, то їх у загальному вигляді визначають як сукупність чинників і умов, які створюють небезпеку певному об'єкту. Загрози можна розглядати як найвищий ступінь небезпеки (безпосередню небезпеку), а небезпеку – як потенційну загрозу. Своєю чергою, небезпека розглядається як завдання шкоди тим чи іншим інтересам, для реалізації чого необхідне створення відповідних умов (можливостей і намірів). Тож небезпека передбачає наявність або намірів, або можливості завдання шкоди, тоді як загроза містить і те, й інше. Небезпеки можуть виходити з багатьох джерел і стосуватися багатьох об'єктів, маючи безадресний характер. Натомість загроза, маючи конкретні джерело й об'єкт, завжди носить персоніфікований характер.

Загроза за своєю суттю не тотожна небезпеці, оскільки поняття «небезпека» є ширшим за спектром свого прояву. Загроза може становити небезпеку й виражатися через небезпеки, якщо йдеться про природне середовище, однак у соціальному, де йде протиборство суб'єктів безпеки, вона становить сукупність намірів і можливостей одного суб'єкта завдати шкоди інтересам іншого. Тому поняття загрози науковець пропонує формулювати не тільки через категорію «небезпека», а й через категорії «намір» і «можливість»:

«загроза безпеці – це сукупність умов і чинників, намірів і можливостей, здатних становити небезпеку життєво важливим інтересам особистості, суспільства й держави».

В. Горбулін та А. Качинський розглядають загрозу як родову ознаку безпеки (можливість чи неминучість виникнення соціальних, природних або техногенних явищ із прогнозованими, але неконтрольованими небажаними подіями, що можуть статись у певний момент часу в межах даної території, спричинити смерть людей чи завдати шкоди їхньому здоров'ю, призвести до матеріальних і фінансових збитків, погіршити стан довкілля тощо) [37]. Небезпеку ж науковці вважають якісним станом – безпекою на її нульовому рівні.

Загрози національній безпеці можна класифікувати за різними підставами, що свідчить про їх складну та багатошарову систему. Зокрема, у політології загрози національній безпеці класифікують таким чином:

– за місцем знаходження джерела – зовнішні та внутрішні;

– за масштабами можливих наслідків – загальнонаціональні, регіональні, локальні, поодинокі;

– за ступенем сформованості – потенційні, реальні;

– за ступенем суб'єктивного сприйняття – завищені, занижені, мінімальні, умовні, адекватні;

– за характером виникнення – загрози природного, техногенного й соціального характеру;

– за сферами життєдіяльності – загрози в економічній, політичній, оборонній, міжнародній, соціальній, інформаційній, науково-технічній, екологічній, культурній та духовній сферах тощо.

Аналіз найбільш актуальних в умовах сьогодення загроз національній безпеці дозволяє дійти висновку щодо взаємозв'язку джерел виникнення і способів прояву більшості внутрішніх і зовнішніх загроз. Відповідно, на доктринальному рівні з'являються пропозиції щодо розширення типології

зовнішніх та внутрішніх загроз національній безпеці шляхом виокремлення нового типу загроз – транскордонних, що мають глобальний характер та об'єднують одночасно ознаки внутрішніх та зовнішніх загроз: за формою прояву є переважно внутрішніми, а за своєю сутністю (за джерелами виникнення та стимуляції, складом можливих учасників тощо) можуть бути й зовнішніми. До цього типу загроз слід передусім відносити загрози інформаційній безпеці держави, що стимулюють розвиток нефізичної концепції безпеки.

Чинна Стратегія національної безпеки серед основних загроз національній безпеці, які мають безпосередній стосунок до інформаційної сфери, визначає агресивні дії росії, спрямовані на виснаження української економіки й підрив суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території. Це, зокрема, інформаційнопсихологічна війна, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації викривленої інформаційної картини світу, а також ведення інформаційної війни проти України. Водночас це також відсутність власної цілісної комунікативної політики нашої держави, недостатній рівень медіа-культури українського суспільства, уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, фізична й моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом. Слід зауважити, що у Стратегії відмежовуються прояви інформаційнопсихологічної війни (п. 3.1), загрози кібербезпеці й безпеці інформаційних ресурсів (п. 3.7) від загроз суто інформаційній безпеці (п. 3.6).

Підсистема інформаційної безпеки посідає особливе місце в системі національної безпеки. Інформаційні відносини і процеси пронизують усі інші, які мають місце в суспільстві, тож інформаційна сфера існує одночасно на двох рівнях: самостійно й у взаємозв'язку з іншими сферами життєдіяльності

суспільства шляхом їх інформаційного обслуговування та забезпечення взаємодії за допомогою інформації. Інформація завжди втілює певне змістовне навантаження, а отже, інформаційна сфера має своїм змістом знання (інформацію) про інші сфери життєдіяльності суспільства. Це забезпечується формуванням інформаційних моделей інших сфер життєдіяльності суспільства, їх інфраструктури, суб'єктів та взаємодії останніх. Відтак, інформаційна сфера та її окремі елементи дають змогу чинити опосередкований вплив на соціальну, економічну, політичну, духовну та інші сфери життєдіяльності людського суспільства. Тому забезпечення інформаційної безпеки є запорукою забезпечення інших складових державної безпеки та національної безпеки в цілому.

Отже, хоча всі складові у структурі національної безпеки пов'язані між собою, треба зважати, що окремі види безпеки є не лише самостійними, але й такими, що мають відповідні виміри в інших сферах життєдіяльності суспільства, закладаючи фундамент забезпечення їх безпеки. З-поміж таких видів, які отримали назву «інтегративні» [38], слід передусім назвати інформаційну безпеку. Таким чином, загрози інформаційного характеру можуть спрямовуватися до будь-яких складових державної безпеки, проте їхній негативний вплив завжди опосередковуватиметься завданням шкоди інформаційній безпеці держави. Приміром, економічна безпека в сучасних умовах інформаційно-мережевої економіки безпосередньо залежить від безпеки інформаційної, адже головним ресурсом розвитку виробництва наразі стає інформаційний продукт [39]. Не випадково виняткову небезпечність загроз інформаційній безпеці підкреслює у своїй роботі Г. Сащук: «…Враховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися світогляд та мораль як окремих осіб, так і суспільства в цілому, нав'язуються чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності та форм проявів сучасних методів прихованого агресивного впливу, вияву дій, що мають цілеспрямований

агресивний характер і які протирічать інтересам національної безпеки, та вироблення механізмів протидії їм у всіх напрямах» [40].

Тож, система загроз інформаційній безпеці має комплексний характер і в загальному вигляді містить такі їх типи: загрози безпеці інформації та інформаційної інфраструктури; загрози безпеці суб'єктів інформаційної сфери та соціальних зв'язків між ними від інформаційних впливів; загрози належному порядку реалізації прав та інтересів суб'єктів інформаційної сфери. Тому варто погодитись із визначенням загроз інформаційній безпеці держави як сукупності умов та чинників, які становлять небезпеку життєво важливим інтересам держави суспільства й особи у зв'язку з можливістю негативного інформаційного впливу на свідомість та поведінку громадян, а також інформаційні ресурси та інформаційно-технічну інфраструктуру [41].

До найбільш важливих властивостей загроз інформаційній безпеці держави слід віднести вибірковість, передбачуваність та шкідливість.

Вибірковість характеризує націленість загрози на заподіяння шкоди тим чи іншим конкретним властивостям об'єкта безпеки.

Передбачуваність – це наявність ознак виникнення загрози, що дозволяють заздалегідь прогнозувати можливість виникнення загрози та визначати конкретні об'єкти, на які вона буде спрямована.

Шкідливість – можливість завдати об'єкту безпеки шкоди різної тяжкості [42].

До основних загроз національній безпеці України в інформаційній сфері пропонують відносити: поширення ідей, що провокують конфлікти на національному, релігійному і соціальному ґрунті та масові заворушення, а також розпалення серед українського населення ідей сепаратизму; заклики з боку окремих груп та осіб щодо посягання на державний суверенітет, територіальну цілісність, економічний, науковотехнічний і оборонний потенціал нашої держави; проведення на шкоду інтересам України спеціальних інформаційних операцій та актів зовнішньої інформаційної

агресії; комп'ютерна злочинність; інформаційний тероризм; розвідувально-підривна діяльність іноземних спеціальних служб; розголошення інформації, яка становить державну та іншу, передбачену законом таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства й держави; намагання маніпулювати громадською думкою, зокрема шляхом поширення недостовірної, неповної або упередженої інформації; дискредитація політики нашої держави та авторитету окремих державних діячів; прояви обмеження свободи слова й доступу громадян до інформації та інших їхніх прав і свобод; поширення засобами масової інформації культу насильства, жорстокості, порнографії та інших проявів аморальності; поширення ідеологій та впливу деструктивних неокультів; значний обсяг іноземної присутності в інформаційному просторі України; небезпечне для економічної незалежності України зростання частки іноземного капіталу у стратегічних галузях економіки, пов'язаних з інформаційною сферою; науковотехнологічне відставання України від розвинутих країн; низька конкурентоспроможність продукції з обслуговування інформаційної сфери; нерозвиненість внутрішнього ринку високотехнологічної продукції та відсутність його ефективного захисту від іноземної технічної та технологічної експансії; зниження внутрішнього попиту на підготовку науково-технічних кадрів для наукових, конструкторських, технологічних установ та високотехнологічних підприємств, незадовільний рівень оплати науково-технічної праці, падіння її престижу, недосконалість механізмів захисту прав інтелектуальної власності; відтік учених, фахівців, кваліфікованої робочої сили за межі України; інспірування інших деструктивних процесів в інформаційній сфері нашої держави [41]. Утім, слід враховувати, що й такі розгорнуті переліки загроз не можуть вважатися вичерпними та константними. Джерелами загроз при цьому можуть виступати: людина, технічні пристрої, моделі, алгоритми, програми, технологічні схеми обробки, зовнішнє середовище тощо [43].

Найбільш небезпечні загрози інформаційній безпеці держави, передусім транскордонні та такі, що мають політичне забарвлення, вже тривалий час вивчаються в рамках проблеми інформаційної війни, поняттям якої вони охоплюються. Інформаційну війну, з урахуванням існуючих поглядів на її природу, можна визначити як сукупність цілеспрямованих інформаційних впливів, що здійснюються з використанням інформаційної зброї (алгоритму цілеспрямованого впливу на інформаційну систему шляхом передачі їй інформації або здійснення з інформацією інших запланованих дій), а також дій, не опосередкованих її використанням, спрямованих на заволодіння інформацією, що не є загальнодоступною, її несанкціоноване поширення, модифікацію або знищення, здійснювані задля досягнення запланованої мети.

Інформаційна війна – це найвищий ступінь інформаційного протиборства, спрямований на розв'язання суспільно-політичних, ідеологічних, національних, територіальних конфліктів між державами, народами, націями та соціальними групами шляхом широкомасштабної реалізації засобів і методів інформаційної зброї. На думку В. Горбуліна, О. Додонова, Д. Ланде [44] та І. Сопілко [45], інформаційні війни, котрі є лише елементами реальних багатоаспектних протистоянь військово-політичного характеру, прийнято називати інформаційними операціями. При цьому основними методами інформаційної війни слугують блокування або перекручування інформаційних потоків і процесів прийняття противником рішень.

До проявів інформаційної війни можна віднести і так звану інформаційну злочинність [46], левова частка якої припадає на кіберзлочини. Відомі факти правоохоронної практики свідчать про те, що прояви інформаційної злочинності – це переважно організована злочинність у своїй найбільш небезпечній частині. У рамках сучасних тенденцій до розширення мережевої архітектури організованої злочинності в теперішній час створюються неформальні групи хакерів у навчальних закладах та

безпосередньо у віртуальному просторі. Є також відомості про залучення організованими злочинними групами хакерів до підготовки злочинів у кредитно-банківській сфері, на фондовому ринку, до протиправного заволодіння інформацією, що накопичується в інформаційно-довідкових і облікових комп'ютерних системах правоохоронних органів. Не виключена й розробка організованими злочинними співтовариствами планів інформаційних операцій, в тому числі інформаційних диверсій [47].

За оцінками фахівців тенденціями у сфері загроз інформаційній безпеці є: неконтрольовані ризики, пов'язані з так званим «Інтернетом речей» та поширенням мережевих з'єднань; стрімке зростання «кіберзлочинів як сервісу» – надання цифрових послуг кримінальними синдикатами; зростання правових ризиків у сфері регулювання мережевих комунікацій; хакерські атаки, спрямовані на підрив репутації брендів та політичних сил.

Одним із джерел загроз інтересам суспільства в інформаційній сфері є також безперервне ускладнення інформаційних систем, тому особливою групою актуальних для України загроз інформаційній безпеці є загрози, зумовлені віртуалізацією [48] – соціальним відчуженням людини, зануренням її в особистісний віртуальний світ. Змінені стани свідомості – транс, одержимість, сп'яніння, депривація сну тощо є ознаками віртуальної інтенції в людині і при цьому атрибутивно виступають знаковосимвольною структурою віртуальності [49]. За прискорених темпів інформаційного прогресу, особливо з розвитком «Інтернету речей», людина взагалі ризикує перетворитися на придаток до інформаційних технологій та інформаційних ресурсів [45].

Утім, технічний аспект не є головним у структурі інформаційної безпеки. Необхідно забезпечити не лише безпеку інформації від знищення, перекручення, блокування, несанкціонованого витоку або порушення встановленого порядку маршрутизації, але й інформаційну безпеку суспільства. Власне ж суспільство є носієм такої глобальної загрози

інформаційній безпеці людини, як інформаційна дискримінація, котра проявляється в розподілі людей на тих, що мають доступ до інформації, і тих, котрі його позбавлені. Принципове значення для сучасного суспільства при цьому має факт існування інформаційної картини світу. Відповідно, одним із найпоширеніших видів інформаційних загроз стає розповсюдження так званих патогенних текстів, які суперечать чинній ідеологічній системі, спрямовані, зокрема, на підрив національних та державних інтересів, загрожують суспільній моралі, чинять шкідливий психологічний вплив, призводять до нехтування основними правами і свободами, втручаються в особисте життя тощо. Як слушно зазначає З. Живко, закрити національний інформаційний простір від такого інформаційного впливу, передусім зовнішнього, за допомогою адміністративних заходів неможливо, тож слід оберігати його від загроз безпеці так само, як наземний, повітряний і морський [50].

2.2. Протидія загрозам інформаційній безпеці України

Основними принципами державного регулювання у сфері, що розглядається, є орієнтація на державно-правовий механізм забезпечення інформаційної безпеки та реалізація національних інтересів і цілей. Ефективність механізму забезпечення інформаційної безпеки визначається передусім його здатністю сприяти збереженню єдності нації, стабільності суспільних відносин, відтворенню національно-культурних цінностей, подоланню політичних, військових, економічних, соціальних криз, створенню передумов стабільного розвитку, а також здатністю ефективно протидіяти загрозам інформаційній безпеці. Останнє, у свою чергу, викликає до життя власне механізми протидії інформаційним загрозам, які на сучасному етапі характеризуються підвищеною небезпечністю, адже інформаційне протиборство нарощує свої можливості в результаті стрімкого зростання обсягу та значення інформації в сучасному світі.

Відтак, безпека сучасної держави безпосередньо залежить від стану її інформаційного простору. Комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації [6].

У теорії національної безпеки механізм протидії загрозам національній безпеці зазвичай розглядають у широкому або у вузькому сенсі. У вузькому сенсі він виступає як складова частина державного механізму і становить систему державних організацій, органів, установ, а також недержавних інституцій, спеціально створюваних для забезпечення національної безпеки або таких, що наділяються окремими функціями щодо забезпечення національної безпеки, у їхній взаємодії та практичному функціонуванні (сили забезпечення національної безпеки). У широкому сенсі механізм протидії загрозам національній безпеці включає не лише сили, але й систему засобів, за допомогою яких здійснюється протидія відповідним загрозам з метою захисту життєво важливих інтересів суспільства й держави. Такими засобами виступають технології, а також технічні, програмні, лінгвістичні, правові, організаційні засоби, включаючи телекомунікаційні канали, що використовуються з метою збирання, формування, обробки, передачі або приймання інформації щодо стану національної безпеки та стосовно заходів, спрямованих на її зміцнення, а також власне методи, способи і прийоми, використовувані суб’єктами забезпечення національної безпеки для вирішення завдань щодо протидії загрозам національній безпеці.

Механізм забезпечення національної безпеки – це динамічна система, у межах якої можна виділити такі стадії: формулювання інтересів, захист яких забезпечуватиметься; виявлення та прогнозування внутрішніх і зовнішніх загроз життєво важливим інтересам; вироблення системи заходів щодо протидії загрозам; нейтралізація загроз; здійснення заходів щодо відновлення нормального функціонування об’єктів безпеки. Численність засобів протидії

інформаційним загрозам та варіативність їх комбінацій залежно від специфіки загроз дають змогу вести мову у множині – про механізми протидії інформаційним загрозам національній безпеці.

Залежно від місцезнаходження джерела можливої загрози всі загрози національній безпеці, в тому числі інформаційні, традиційно поділяються на дві групи – зовнішні та внутрішні. Для інформаційної безпеки того чи іншого об'єкта внутрішніми вважаються ті загрози, які «виникають безпосередньо на об'єкті та зумовлюють взаємодію між його елементами або суб'єктами», тоді як зовнішніми – ті, що «виникають внаслідок його взаємодії із зовнішніми об'єктами» [51].

До зовнішніх загроз інформаційній безпеці при цьому відносять:

– діяльність іноземних розвідувальних і спеціальних служб;

– діяльність іноземних політичних і економічних структур, злочинних груп і формувань, а також окремих осіб чи їх об'єднань, спрямована проти інтересів громадян, суспільства й держави;

– діяльність політичних та економічних структур, злочинних груп і формувань, а також окремих осіб чи їх об'єднань усередині країни, спрямована проти інтересів громадян, держави й суспільства (у випадках, коли джерело загрози може бути розцінене як зовнішнє для конкретної інформаційної системи, котрій може бути завдана шкода внаслідок реалізації інформаційної загрози);

– стихійні лиха й катастрофи.

Інформаційні загрози прицільно спрямовуються на інформаційну інфраструктуру (інформаційні ресурси) і на саму інформацію та її потоки, як-от: бази і банки даних, архіви, масиви документів, бібліотеки, музейні фонди тощо, де на різних носіях зберігається той чи інший тип інформації. Інформаційна інфраструктура є сукупністю інформаційних систем, що включає:

– інформаційно-телекомунікаційні структури – державні й корпоративні комп'ютерні мережі, телекомунікаційні мережі та системи спеціального й загального користування, мережі й канали передачі даних, засоби управління інформаційними потоками;

– інформаційні, комп'ютерні й телекомунікаційні технології, що формують кібернетичний простір;

– засоби масової інформації;

– організаційні структури, які забезпечують функціонування та розвиток єдиного інформаційного простору, зокрема, збір, обробку, зберігання, розповсюдження, пошук і передачу інформації.

Чинна Стратегія національної безпеки України з-поміж основних загроз національній безпеці, які мають безпосередній стосунок до інформаційної сфери, визначає агресивні дії росії, що здійснюються для виснаження української економіки й підриву суспільно-політичної стабільності з метою знищення держави Україна й захоплення її території. Це, зокрема, – інформаційно-психологічна війна, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної реальній викривленої інформаційної картини світу. Крім того, це – відсутність власної цілісної комунікативної політики держави, недостатній рівень медіа-культури українського суспільства, уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, фізична й моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом [1]. Слід зауважити, що у Стратегії розмежовуються прояви: інформаційно-психологічної війни (п. 3.1); загрози кібербезпеці і безпеці інформаційних ресурсів (п. 3.7); загрози інформаційній безпеці (п. 3.6), що, на наш погляд, не є доцільним.

Доктрина інформаційної безпеки України (п. 4) містить перелік актуальних загроз національним інтересам та національній безпеці України в інформаційній сфері, а саме:

– 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 й дестабілізація 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;

– інформаційне домінування держави-агресора на тимчасово окупованих територіях;

– 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 медіакультури суспільства;

– поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

Стратегія кібербезпеки України передбачає також, що сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об'єктах критичної інфраструктури. Більшого поширення набуває політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні веб-сайти в мережі Інтернет. Дедалі частіше об'єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які забезпечують безпеку, оборону, захист від надзвичайних ситуацій. Новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але і для вчинення принципово нових їх видів, притаманних суспільству з високим рівнем інформатизації [36].

Глобальна мережа Інтернет є в теперішній час основною ареною протистояння різних сил і засобів, що вимагає нового рівня забезпечення національної безпеки від різнопланових загроз інформаційного опосередкування. Сьогодні інформаційна агресивність віртуального простору суттєво впливає на трансформацію діяльності всіх національних, а також міжнародних антитерористичних і антиекстремістських структур. Крім того, терористичні, екстремістські утворення, організовані злочинні угруповання вдаються до маскування проявів екстремізму й тероризму в інформаційному просторі позитивними гаслами й риторикою «добра та миру». Тому профілактичні заходи в інформаційній сфері компетентних органів державної влади мають спрямовуватися насамперед на формування імунітету суспільної свідомості до впливу деструктивних ідей. Задля цього важливо виробити систему заходів щодо запобігання й, за необхідності, зміни характеру та вектора інформаційного впливу в соціальних мережах, себто, розробити механізм протидії відповідним загрозам.

Реалізація зовнішніх загроз передбачає пошук уразливості в інформаційній структурі для доступу до основних вузлів інформаційної інфраструктури, сховищ інформації, організаційної мережі, осіб-секретоносіїв тощо. Інструментами реалізації зовнішніх інформаційних загроз виступають різнопланові види так званої інформаційної зброї (не лише віруси, «хробаки», «трояни» та інші форми шкідливого програмного забезпечення, але й інші знаряддя інформаційного впливу).

Протидія зовнішнім загрозам інформаційній безпеці України відбувається в умовах прогресування тенденції до переформатування сфер впливу у світовому просторі на тлі глобалізації політичних, соціальноекономічних, культурних відносин. Виявлення та аналіз відповідних загроз ускладнюється низкою чинників:

– наявність у частини населення відчуття відсутності зовнішніх загроз країні;

– достеменно не визначені потенційні зовнішні загрози країні, що призводить до відсутності чіткої класифікації й ранжування загроз за ступенем важливості й порівняльною динамікою їх наростання;

– відсутність ясного розуміння причин і джерел виникнення цих загроз тощо.

Забезпечення безпеки в умовах внутрішніх і зовнішніх динамічних змін потребує наявності дієвого механізму забезпечення безпеки, зокрема механізмів протидії загрозам. Механізм протидії інформаційним загрозам від зовнішніх джерел можна визначити як інтегровану цілісну сукупність необхідних і достатніх функціональних і правових елементів, за допомогою яких суб’єкт формує раціональну систему впливу на загрози інформаційній безпеці та зумовлені ними ризики, забезпечуючи в такий спосіб результативне виконання завдань і функцій, покладених на систему забезпечення інформаційної безпеки та національної безпеки в цілому.

Механізми протидії інформаційним загрозам від зовнішніх джерел як частина загального механізму забезпечення інформаційної безпеки держави та національної безпеки в цілому мають передбачати:

– мету забезпечення безпеки, що полягає у збереженні цілісності й захищеності інформаційної сфери у процесі її функціонування й розвитку;

– рівень безпеки, що диференціює структурні складові системи, які можуть стикатися з потенційними й реальними небезпеками;

– сфери безпеки, що визначають можливості функціонування й розвитку інформаційної сфери;

– параметри безпеки, що встановлюють припустимі межі відхилень у потенціалі системи інформаційної безпеки, кількості її елементів, їх якості, властивостях, зв’язках;

– перелік загроз, наслідки їх реалізації й механізм запобігання, зумовлені: внутрішніми закономірностями функціонування системи інформаційної безпеки та впливом на неї зовнішнього середовища, що веде до небажаних і необоротних порушень у її відтворенні й розвиткові; змінами, що настають у разі реалізації загроз (такі, що компенсуються або не компенсуються; оборотні та необоротні; такі, що зачіпають або не зачіпають життєздатність системи); організаційно оформленою сукупністю стратегічних і тактичних дій, що забезпечують підтримку функціонування системи інформаційної безпеки та її здатність до самовідтворення.

З-поміж інформаційних загроз від зовнішніх джерел наразі найбільшу небезпеку для національної безпеки України становлять:

– спроби несанкціонованого доступу до інформації та впливу на інформаційні ресурси, інформаційну інфраструктуру органів виконавчої влади, що реалізують зовнішню та внутрішню політику України, українських представництв і організацій за кордоном, представництв України при міжнародних організаціях.

– недостатня поінформованість населення зарубіжних країн (передусім тих, що межують з Україною) про зовнішньо- та внутрішньополітичну діяльність України;

– поширення за кордоном дезінформації про зовнішню та внутрішню політику України;

– інформаційний вплив іноземних політичних, економічних, військових і інформаційних структур на розробку й реалізацію стратегії зовнішньої та внутрішньої політики України;

– порушення прав українських громадян і юридичних осіб в інформаційній сфері за кордоном.

Механізми протидії інформаційним загрозам зовнішніх джерел передбачають необхідність організації багаторівневої й різноспрямованої системи заходів з урахуванням передусім специфіки зовнішніх чинників – геополітичної конфігурації, регіональної кон'юнктури і структурнофункціональної ролі країни, а також впливу транснаціональної організованої злочинності.

Отже, своєчасний моніторинг характеру, особливостей, масштабів загроз та їх наступне прогнозування мають особливе значення. Прогнозування є важливим і самостійним елементом профілактики інформаційних загроз від зовнішніх джерел, та, відповідно, забезпечення національної безпеки. Основним методом прогнозування є моделювання, головними принципами якого є: встановлення мети моделі; виділення обмеженої кількості ключових чинників, які привносять істотні зміни в досліджувану систему; з'ясування характеру взаємозв'язків між виділеними чинниками; встановлення принципу множинності зв'язків між чинниками й виявлення сутнісних зв'язків, які й визначають характер розвитку та зміни системи.

Стратегічні знання, отримані за результатами прогнозування, дозволяють ілюструвати модель розвитку досліджуваного середовища, а також обґрунтовувати змістовні особливості її структурних елементів. При цьому для

моніторингу, прогнозування і профілактики загроз придатне будь-яке середовище, котре характеризується наявністю зовнішніх джерел, з яких можуть продукуватися та відтворюватися загрози інформаційній безпеці особистості, суспільства й держави.

Слід враховувати, що в умовах стрімкого розвитку інформаційного суспільства, який також зумовлює вдосконалення методів ведення інформаційних воєн, звичні технології та механізми протидії зовнішнім загрозам національній безпеці застаріли, і на передній план виходять нові способи стримування розгортання загроз та мінімізації зумовлених ними ризиків. Методи протидії інформаційним загрозам від зовнішніх джерел можна умовно поділити на дві групи:

– профілактичні, або превентивні, які застосовуються для недопущення розгортання відповідних загроз або для запобігання подальшим ризикам на початковому етапі розгортання таких загроз;

– оперативні методи, які використовуються безпосередньо у відповідь на агресивні кроки, що виходять від зовнішніх джерел інформаційних загроз та пов’язані з їх розгортанням та реалізацією.

З-поміж заходів превентивної протидії інформаційним загрозам від зовнішніх джерел вирізняють чотири основні групи: нормативно-правові, адміністративні, інформаційні й економічні.

Оперативна протидія має здійснюватися тільки після виявлення достовірної інформації щодо структур, груп або осіб, котрі є рушійними силами, а також оцінки ступеня загрози й наявних ресурсів для її нейтралізації. Лише після ефективної роботи з інформацією можна обрати оптимальний оперативний метод протидії, який відповідає наявним ресурсам і є достатнім для нейтралізації загрози відповідного ступеня. Серед оперативних заходів протидії інформаційним загрозам зовнішніх джерел виділяють, зокрема, такі:

– персоніфікація дій джерела загрози, в тому числі інформаційних впливів;

– делегітимізація дій джерела загрози;

– спростування чуток і розвінчування дезінформації з боку джерела загрози;

– формування потрібного інформаційного емоційного фону й політичних настанов щодо реагування на дії джерела загрози; робота зі ЗМІ; зовнішній тиск на джерело загрози;

– зміна моделі комунікації, нав'язуваної джерелом загрози.

Механізм протидії інформаційним загрозам зовнішніх джерел, розгортання яких відбувається в ході гібридної війни, має включати:

– постійний контроль інформаційного простору (преса, телебачення, радіо, Інтернет); обмеження розмірів простору, об'єктів інформаційної інфраструктури та соціальних груп, що піддаються ураженню інформаційною дією;

– посилення авторитету своєї влади, уряду, армії серед населення країни, аби перешкодити переходу на бік ворога та підтримці дій, які він нав'язує;

– ефективна інформаційна політика: стратегічна спрямованість та зворотний зв'язок із суспільством.

Окрім того, можна виокремити політичні, економічні та інші механізми протидії інформаційним загрозам зовнішніх джерел. Так, ураховуючи політичні цілі, що випливають із єдиної стратегічної мети забезпечення національної безпеки України, можна виділити окремі політичні механізми протидії інформаційним загрозам від зовнішніх джерел:

– механізми розробки та прийняття рішень у Раді безпеки ООН, взаємодія в рамках ОБСЄ, механізми зміцнення й розвитку в межах інших міждержавних утворень, які є засобом політичної, економічної та військової євроінтеграції України;

– механізми державного й військового управління, впливу політичних партій, уведення адміністративно-правових режимів тощо,

пов’язані з управлінням внутрішньополітичними процесами, що прямо впливають на забезпечення інформаційної безпеки країни;

– механізми просування інтересів держави в міжнародній інформаційній сфері, інформаційне забезпечення державної політики України, пов’язане з доведенням до вітчизняної й міжнародної громадськості достовірної інформації про державну політику країни, розвиток сучасних інформаційних технологій, захист інформаційних ресурсів тощо;

– механізми протидії зовнішнім загрозам політичній, економічній та іншій безпеці України тощо.

Зрозуміло, що механізми протидії інформаційним загрозам від зовнішніх джерел можуть видозмінюватися, позаяк конкретний механізм створюється відразу із з’ясуванням наявності певної загрози й формулюванням стратегічної мети щодо її нейтралізації. Слід також враховувати, що за сучасних умов розподіл інформаційних загроз на внутрішні й зовнішні є вельми умовним. Оскільки інформаційні загрози завжди мають комплексний характер, замахи на зовнішню безпеку країни формують загрози внутрішній безпеці, а внутрішня дестабілізація веде і до зовнішньої уразливості держави. Крім того, інформаційні загрози національній безпеці України видозмінюються, розробляються й зосереджують як за кордоном, так і усередині нашої держави (і джерелом зовнішньої загрози, скажімо, для безпеки інформаційних ресурсів певного державного органу України, може будь-яка група або особа, навіть така, що перебуває в Україні, якщо вона не може бути включена до архітектури безпеки цього державного органу), або можуть виходити з віртуального простору, що взагалі ускладнює можливість чіткого визначення локації їх джерела. Вони взаємно впливають одне на одне, набувають комплексного характеру і тому для їхньої локалізації й нейтралізації потрібен системний підхід. Зокрема, для протидії інформаційним загрозам, що походять з віртуального простору, потрібне налагодження механізму, який включає:

– розвиток українського сегмента Інтернету;

– створення й контролювання українських аналогів соціальних мереж;

– розвиток нормативно-правової й законодавчої бази забезпечення інформаційної безпеки в мережі Інтернет;

– виявлення джерел інформаційних кампаній у соціальних мережах;

– зсув акценту від технократичного до гуманітарних аспектів забезпечення інформаційної безпеки;

– розвиток державної підтримки науково-практичних досліджень гуманітарних аспектів інформаційної безпеки;

– урахування можливих негативних наслідків використання новітніх інформаційних технологій тощо.

Слід також враховувати, що загрози, передусім зовнішні, належать до сторонніх щодо системи забезпечення безпеки чинників, а відтак, неможливо не лише досягти стану їх абсолютної відсутності, але і скласти вичерпний перелік, адже вони трансформуються в умовах мінливого середовища. Тож, у сучасному світі відбувається зміщення акцентів із загроз на ризики, оскільки такий підхід дозволяє відходити від розуміння загроз як констант та застосовувати різнопланові підходи для унеможливлення їх розгортання, особливо за умов невизначеності. Тобто, механізми протидії інформаційним загрозам від зовнішніх джерел, які базуються на принципах управління ризиками і передбачають процес прийняття та виконання управлінських рішень, спрямованих на зниження імовірності виникнення несприятливих наслідків та мінімізацію можливої шкоди, викликаної реалізацією загроз, за сучасних умов є найбільш перспективними й результативними. Відповідні механізми дають змогу впливати передусім на керовані елементи (ризики), досягаючи вагомих для забезпечення її прийнятного стану результатів за рахунок застосування відносно незначних зусиль, а також успішно поєднувати профілактичні й оперативні методи протидії інформаційним загрозам від зовнішніх джерел.

РОЗДІЛ 3
ШЛЯХИ УДОСКОНАЛЕННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

3.1. Пріоритетні напрями удосконалення законодавства у сфері забезпечення інформаційної безпеки в умовах цифрової трансформації

Формування принципово нового технологічного середовища з урахуванням цифрових технологій істотно впливає на економіку, політику та соціальні процеси сучасного світу. Вплив цифрової революції поширився на систему права на національному та на міжнародному рівні. Передові цифрові технології, що застосовуються в різноманітних галузях діяльності, які охоплюють Інтернет речей (Internet of things), штучний інтелект і машинне навчання (Artificial intelligence & Deep learning), технології на принципах розподіленого реєстру (Blockchain), хмарні комп'ютерні сервіси та обчислення (Cloud mputing), розумні комплекси та пристрої (Smart everything), великі дані (Big Data), віртуальна та доповнена реальність (Augmented & additive reality), сучасні біоінженерні технології (Biotech), системи кібербезпеки (Cybersecurity), соціальні мережі (Facebook, Instagram, Twitter), цифрові двійники (Digital twins), цифрові технологічні платформи (агрегатори) та пов'язані з ними інші технології, створили технологічний базис для формування принципово нового середовища адміністративно-правового та інформаційно-правового регулювання.

Застосування цифрових технологій у зв'язку зі стратегічною спрямованістю європейського та національного розвитку цифрової економіки, цифровізації різноманітних сфер діяльності зумовили зростаючий науковий інтерес до теоретичних та науково-практичних досліджень, у тому числі в галузі правового регулювання забезпечення інформаційної безпеки. Перспективи розвитку інформаційного права багато в чому пов'язані з

використанням цифрових технологій у сфері забезпечення інформаційної безпеки.

Питання про значення інформаційної безпеки в житті суспільства та кожного з нас не потребує додаткового обґрунтування, але, безсумнівно, потребує пильної уваги. В інформаційному суспільстві, заснованому на знаннях, роль інформаційної безпеки визначається потребою реалізації права людини на інформацію, позбавлення деструктивного інформаційного впливу, необхідністю забезпечення системи стратегічного планування та розвитку національного інформаційного середовища.

Розробка методологічних, організаційних і нормативно-правових засад побудови системи інформаційної безпеки розпочалася у 90-ті роки минулого століття, але не втратила актуальності сьогодні для забезпечення інтересів особи, суспільства та держави.

Сукупність національних документів стратегічного планування, охоплюючи ухвалені стратегії та доктрини, сьогодні значною мірою характеризує основні цілі, завдання та напрями розвитку інформаційної безпеки. Серед інших важливих завдань Стратегія інформаційної безпеки України передбачає розвиток механізмів електронної взаємодії між органами державного управління України, місцевими органами державної влади з державними позабюджетними фондами, фізичними та юридичними особами в межах концепції електронного уряду.

Доцільно відзначити, що в умовах збройної агресії росії набуває суттєвого значення виконання вимоги Стратегії воєнної безпеки України щодо інформаційної безпеки, відображеної у Законах України: «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах

воєнного або надзвичайного стану»; «Про внесення змін до статті 114-2 Кримінального кодексу України щодо удосконалення відповідальності за несанкціоноване розповсюдження інформації про засоби протидії збройній агресії Російської Федерації» та інших [52; 53].

В умовах динаміки інформаційного суспільства інформаційна безпека набуває характеру стратегічного ресурсу в системі цифровізації управління, оскільки цифрові технології, перебуваючи у постійному розвитку та розширюючи доступ до інформації на основі електронної взаємодії різних суб'єктів, створюють умови для переходу державного управління на новий рівень та підвищення якості життя населення, що потребує наукового осмислення з позиції інформаційного права та подальшого вдосконалення правового регулювання відносин в інформаційній сфері.

Велику роль в умовах цифровізації мають питання реалізації конституційного права на інформацію, забезпечення права на достовірну інформацію, що охоплює інформаційна безпеки.

Юридичні ознаки забезпечення інформаційної безпеки вказують на первинну публічно-правову природу та самостійність, що дозволило визначити зазначений інститут у двох аспектах: вузькому та широкому. У широкому аспекті забезпечення інформаційної безпеки – правовий елемент інформаційної діяльності держави, спрямований на реалізацію державної політики у соціально-інформаційній та економічній сфері шляхом створення умов захисту інформації, інформаційних систем і ресурсів та захисту від деструктивного інформаційного впливу. У вузькому аспекті забезпечення інформаційної безпеки є самостійним елементом в структурі інформаційного права, створеним та регульованим спеціальними нормативно-правовими актами.

У документальному аспекті інформаційна безпека охоплює сукупність нормативно-правових актів та ненормативно-правових актів, довідкові, нормативно-технічні документи, документи стратегічного планування,

програмно-цільові документи, ненормативні правові акти, правові знання, правова статистика, акти правозастосовної практики, акти тлумачення законодавства, правові коментарі тощо.

Нормативно-правові документи, інформаційні ресурси є складовою інформаційної системи і належать до інформаційної інфраструктури, входять до системи забезпечення інформаційної безпеки України.

Право на достовірну інформацію багато в чому пов'язане з тим, що Стратегія інформаційної безпеки Україні закріплює поступовий перехід від інформаційного суспільства до суспільства знань, у якому переважне значення з урахуванням національних пріоритетів мають отримання, збереження, виробництво та розповсюдження достовірної інформації, що забезпечується заходами та засобами інформаційної безпеки [20].

Під нормативною базою інформаційної безпеки у широкому сенсі слід розуміти всю сукупність правових знань, що охоплюють не лише нормативно-правові акти, а й документи стратегічного планування, програмно-цільові документи, акти правозастосовної практики, акти тлумачення законодавства, коментарі до законів.

У вузькому значенні під нормативною базою інформаційної безпеки слід розуміти масив нормативно-правових актів та тісно пов'язаних з ними актів та документів правового змісту – акти тлумачення, довідкові матеріали, нормативно-технічні документи тощо.

Важливими властивостями інформаційної безпеки є її актуальність, що забезпечується системною єдністю її цінності та корисності, що набуло достатнього наукового обґрунтування у працях учених [54; 55].

Оскільки у формуванні системи нормативно-правових актів беруть участь місцеві органи влади та органи місцевого самоврядування, необхідно на основі досягнень цифровізації та системного підходу виявити однорідні та суттєво взаємопов'язані компоненти наявної нормативної бази інформаційної

безпеки для об’єднання їх у систему нормативного забезпечення інформаційної безпеки.

Зазначена система є впорядкованою багаторівневою сукупністю інформаційних ресурсів нормативно-правового характеру на базі сучасних інформаційних технологій, єдиного програмно-апаратного середовища, що надає функціонально повний набір інформаційно-технологічних сервісів, які забезпечують збирання, обробку, зберігання, надання та передачу інформації з метою підвищення інформаційної безпеки та безпеки критичної інформаційної інфраструктури.

Охоплення інформаційних технологій системою інформаційної безпеки, формування, розвиток та подальше вдосконалення державної системи інформаційної безпеки є важливими складовими національної безпеки держави що має суттєве значення в умовах збройної агресії Російської Федерації щодо України.

Управління процесами забезпечення інформаційної безпеки має перебувати у підпорядкуванні держави, яка згідно з Конституцією України зобов’язана забезпечити права, свободи та законні інтереси фізичних і юридичних осіб на основі достовірної та актуальної інформації, захисту від інформаційного деструктивного впливу. Для цього потрібний науковотехнічний потенціал та використання цифрових технологій для забезпечення інформаційної безпеки, що відповідає всім необхідним сучасним параметрам безпеки.

На основі розвитку правової культури інформаційного суспільства та правосвідомості вимагають уваги такі визнані інститути правового регулювання у сфері забезпечення інформаційної безпеки, як юридична техніка, експертиза нормативно-правових актів, застосування цифрових технологій у юридичній діяльності, правового моніторингу, використання різноманітних форм контролю та оцінки якості законодавства та ефективності застосування права.

Аналіз чинного законодавства показав наявність розвиненої системи правового забезпечення інформаційної безпеки. Водночас є прогалини у правовому регулюванні. У зв'язку з надзвичайно високою динамічністю розвитку інформаційної сфери в умовах цифрової трансформації необхідно виробляти правові рішення, що дозволяють успішно підготуватися до появи нових інформаційних загроз.

Одна з прогалин у чинному інформаційному законодавстві полягає в тому, що за наявності широкого переліку правових механізмів забезпечення інформаційної безпеки у базових джерелах інформаційного права є брак основоположних положень та засад інформаційної безпеки.

Для іншого ключового елемента інформаційної безпеки – захисту інформації такі основні норми закріплені у Законі України «Про захист інформації у інформаційно-комунікаційних системах».

Стаття 1 «Визначення термінів» і стаття 9 «Забезпечення захисту інформації в системі» закону закріплює правову дефініцію захисту інформації, визначає методи та зміст державного регулювання відносин у цій сфері, встановлює низку правових обов'язків та вимог щодо захисту інформації [38].

Причина очевидна – назва цього закону адекватно відображає його предмет регулювання, але блок інформаційної безпеки виходить за межі захисту інформації.

Має місце, коли передові вітчизняні розробки у сфері правового регулювання отримують підтримку, але не знаходять втілення у законодавстві. Закріплення блоку норм про поняття, правові принципи та засоби забезпечення інформаційної безпеки дуже важливе.

Надання інформаційній безпеці статусу стратегічного національного пріоритету у Стратегії інформаційної безпеки України вимагає зміни ситуації, що склалася, та повноцінної правової регламентації основ забезпечення інформаційної безпеки на рівні закону.

Тому доцільною є пропозиції про доповнення змісту Закону України «Про інформацію» нормами щодо забезпечення інформаційної безпеки. Пропозиція полягає у внесенні до закону окремої статті щодо забезпечення інформаційної безпеки.

Таке рішення забезпечить побудову логічної та цілісної системи правового регулювання інформаційної безпеки, що охоплює спочатку базові відправні засади забезпечення, а потім правові норми щодо двох фундаментальних напрямів забезпечення – захисту інформації та інформаційної безпеки.

У 2014 році такий законопроєкт розроблявся групою вчених та депутатів Верховної Ради України, проте не був ухвалений парламентом. Аналіз положень цього законопроєкту показав, що він переважно регламентує цілі, завдання, принципи та напрями забезпечення інформаційної безпеки, організацію державної системи забезпечення інформаційної безпеки та міжнародного співробітництва.

Однак таке широке коло питань забезпечення інформаційної безпеки доцільно нормативно закріпити в документі стратегічного планування. Механізм практичного використання може бути різним – як використання основи для розробки офіційного документа стратегічного планування з такою назвою, так і застосування під час оновлення Стратегії інформаційної безпеки України. Кожне з рішень має переваги та недоліки.

Наприклад, основним аргументом на користь варіанта єдиного документа є тісний взаємозв’язок інформаційно-психологічних та інформаційно-технічних загроз, так само як діяльність державних органів щодо протидії. Щодо законодавства у сфері забезпечення інформаційної безпеки, то оптимальною стратегією розвитку є закріплення правових засад забезпечення інформаційної безпеки у Законі України «Про інформацію» у поєднанні з регламентацією окремих напрямів та аспектів забезпечення інформаційної безпеки у самостійних законодавчих актах.

У цифровій сфері важливе значення мають інформаційні системи та офіційні сайти органів публічного управління, надання адміністративних послуг органами публічного управління, що здійснюється на основі інформаційних систем.

А. Є. Краковська та М. К. Бабик вказують, що цифровізація адміністративних послуг повинна у повному обсязі забезпечити користувачів безпечними сервісами, метою яких буде надання доступу до детальної інформації про послугу, можливість заповнювати та завантажувати необхідні для отримання послуги зразки та форми документів, механізмом інформування користувача про стан розгляду, а також здатністю онлайн оплати послуги. Нині такий механізм в Україні працює недосконало, що викликає певні труднощі під час отримання адміністративних послуг за допомогою сучасних технологій [56]. Учені в загальному аспекті пропонують внесення змін до нормативних актів, але не конкретизують вимоги.

Інформаційні системи, що містять правову інформацію, яка застосовується у сфері публічного управління та судової системи, є базою інформаційно-правового забезпечення організаційно-управлінської діяльності органів публічної влади, судової діяльності у сфері інформаційної безпеки, що дозволяє розвивати державні інформаційні системи у різних галузях діяльності із забезпеченням вимог інформаційної безпеки.

У базовому нормативному акті щодо державних інформаційних ресурсів Закон України «Про публічні електронні реєстри» безпосередньо не згадується інформаційна безпека. Водночас зазначений закон доцільно доповнити словами: «Вимоги про захист інформації, які містяться в реєстрах, встановлюються центральним органом виконавчої влади зі спеціальним статусом у сферах електронних комунікацій, радіочастотного спектру та надання послуг поштового зв’язку» [57].

Аналіз європейського досвіду свідчить про успішність переведення органів публічної влади на сервісні моделі споживання хмарних сервісів,

центрів обробки даних з метою підвищення стабільності роботи інформаційнокомунікаційних систем, підвищення безпеки інформації, що міститься в інформаційних ресурсах, зменшення витрат на розвиток інформаційнокомунікаційної інфраструктури, охоплюючи хмарні сервіси.

12 березня поточного року Кабінет Міністрів України дозволив українським державним установам у воєнний час користуватися хмарними технологіями з розміщенням даних у закордонних дата-центрах [58]. Реалізація розміщення даних у закордонних дата-центрах вимагає внесення доповнень до закону України, що регулює надання хмарних послуг.

З метою підвищення ефективності інфраструктури електронного уряду в Україні впроваджена єдина платформа цифрової взаємодії, що охоплює єдине програмно-апаратне середовище та методологію, яке підтримує взаємовідносини громадян, державних органів та юридичних осіб на базі сучасних інформаційних технологій. Модель єдиної платформи цифрової взаємодії передбачає поетапний перехід державних інформаційних систем на вказану платформу та впровадження сервісної моделі надання інформаційних послуг в електронній формі, що посилить інформаційну безпеку у певному секторі інформаційного простору країни.

В опрацюванні правових актів у сфері інформаційної безпеки беруть участь державні органи та органи місцевого самоврядування. В умовах інформаційного суспільства та цифровізації ключове значення набуває трансформація зазначеної системи в загальнонаціональну систему інформаційної безпеки відповідно до принципів державно-приватного партнерства, що дозволить перейти на наступний рівень правової інформатизації на основі цифрових технологій з метою формування єдиного цифрового інформаційно-правового простору України.

Запровадження нових цифрових технологій, цифрової взаємодії потребує пошуку нових концептуальних підходів і правових методів,

механізмів публічного управління за обов’язкового дотримання вимог забезпечення інформаційної безпеки.

Цифрова трансформація впливає на механізми інформаційно-правової та електронної взаємодії між державою та суспільством, іншими суб’єктами інформаційного обміну, що відповідно вимагає адекватного забезпечення інформаційної безпеки.

Запит на розвиток інформаційної інфраструктури національної системи забезпечення інформаційної безпеки виходить із підвищення правової поінформованості та культури фізичних і юридичних осіб, а також необхідності забезпечення інформаційних потоків різних рівнів лінгвістичними, інформаційними засобами та інструментами, що забезпечують взаємодію громадян із державними інформаційними ресурсами.

Створення єдиного цифрового простору на платформній основі є перспективним, і в рамках реалізації зазначеного підходу можливий розвиток національної системи інформаційної безпеки на основі платформних рішень.

Водночас потрібні відповідні зміни у законодавстві та інтеграція сукупності публічних інформаційних ресурсів та сучасних цифрових технологій, спрямованих на забезпечення взаємодії всіх суб’єктів інформаційного обміну, інтеграція нормативного масиву інформаційної безпеки, що забезпечить її актуальний стан.

У сучасних умовах інформаційна безпека в інформаційному суспільстві набуває характеру стратегічного ресурсу; трансформуючись у систему цифровізації та публічного управління, вона дозволить публічним інформаційним системам перейти на платформне забезпечення та запровадити сучасні сервісні моделі інформаційних послуг на підставі нових правових і технологічних рішень у сфері забезпечення інформаційної безпеки.

Національна система інформаційної безпеки має розвиватися та набути офіційного статусу, бути інтегрованою, багаторівневою та відкритою для взаємодії з іншими інформаційними системами, а її інформаційно-правове

забезпечення будуватися на базі конвергентних інформаційних технологій та платформних рішень.

У зазначеному контексті важливо виділити необхідність забезпечення інформаційної безпеки особи та суспільства від деструктивного інформаційного впливу. Провідну роль у структурі цього інституту мають норми інформаційного права. Водночас усталені правові механізми безпеки вимагають подальшого розвитку та адаптації до нових загроз та викликів в умовах цифрової трансформації.

Аналіз інформаційного та іншого галузевого законодавства дозволив виділити такі основні правові механізми забезпечення інформаційної безпеки від деструктивного інформаційного впливу:

– встановлення правових заборон та інших обмежень на поширення певних видів негативної інформації;

– встановлення спеціальних правил обороту інформаційної продукції певних видів;

– закріплення обов'язків суб'єктів інформаційних правовідносин щодо забезпечення інформаційно-психологічної безпеки;

– вікова класифікація та маркування інформаційної продукції;

– експертиза інформаційної продукції;

– ідентифікація особи абонентів, користувачів мережі Інтернет та цифрових сервісів;

– видалення чи обмеження доступу до протиправного контенту;

– встановлення юридичної відповідальності за правопорушення, що посягають на інформаційно-психологічну безпеку;

– правове закріплення заходів контрпропаганди;

– правове стимулювання розвитку цифрової грамотності та формування культури інформаційної безпеки.

Важливу роль у механізмі правового забезпечення інформаційної безпеки відіграють заходи юридичної відповідальності за скоєння

правопорушень у цій галузі, які закріплені кримінальним, адміністративно-деліктним і цивільним законодавством. Водночас розширено практику нормативного закріплення санкцій за правопорушення у сфері захисту від деструктивного інформаційного впливу безпосередньо інформаційним законодавством.

Зазначені правові механізми демонструють доцільність розробки та прийняття окремого Закону України «Про захист від деструктивного інформаційного впливу на населення України».

3.2. Формування культури інформаційної безпеки

З кожним роком зростає потреба у забезпеченні інформаційної безпеки особи, держави та суспільства. Збільшення обсягів використання мережі Інтернет розширює масштаби інформаційних загроз, пов'язаних із діяльністю представників кіберзлочинності, розв'язуванням інформаційних воєн, комп'ютерними атаками хакерів на державні та приватні інформаційні ресурси, які є критично важливими для існування держави та суспільства.

Інша важлива небезпека використання мережі Інтернет у тому, що потужність формованого інформаційного потоку значно перевищує можливості освоєння та застосування інформації людьми. У сприйнятті світу зміщується акцент із наукового, освітнього та культурного на розважально-довідковий. Це формує кліпове мислення, що характеризується поверхневим сприйняттям інформації, падінням здібностей до аналізу, спрощенням поглядів та переваг людей, що сприяє формуванню нав'язаних моделей поведінки [59].

Необхідно брати до уваги, що при сучасних темпах розвитку інформаційних технологій та інформаційного простору жоден управлінський апарат не в силах вчасно встановлювати необхідні механізми та адаптувати державне регулювання зазначеної сфери до обставин, що постійно змінюються.

Цей факт призводить до необхідності забезпечення інформаційної безпеки.

При розгляді основних напрямів забезпечення інформаційної безпеки у різних галузях переважає необхідність забезпечення безпеки держави та суспільства. Інтереси особи та забезпечення інформаційної безпеки окремих громадян розглядаються локально, причому як напрям забезпечення інформаційної безпеки в галузі науки, технологій та освіти, фігурує забезпечення захищеності громадян від інформаційних загроз, у тому числі шляхом формування культури особистої інформаційної безпеки.

В умовах посилення цифрової трансформації зростає значення адаптації громадян до нових реалій в умовах цифрового середовища, підвищення поінформованості та набуття навичок протистояння інформаційним загрозам та ризикам. Водночас в умовах інформаційної війни, яку проводить Російська Федерація, основна увага в державній політиці надається боротьбі з загрозами інформаційної безпеки. Це правильно, оскільки завдання держави полягає в тому, щоб максимально захистити особу та соціум від деструктивного впливу інформаційних ризиків.

Однак донині в експертній спільноті склалося розуміння того, що в інформаційному середовищі не можна уникнути будь-яких факторів, що утворюють загрози. Це зумовлено багатьма причинами: складністю виявлення загроз інформаційній безпеці, латентним характером дії, чисельністю джерел загроз інформаційній безпеці, обмеженою ефективністю методів припинення поширення деструктивної інформації.

Не можна забувати про те, що в правовій демократичній державі ступінь втручання в суспільне життя, у тому числі в духовну сферу, має бути лімітованим.

Спроби державного директивного нав’язування поглядів та цінностей, припинення будь-якого інакомислення несумісні з принципами демократичного устрою. Ці ідеї знайшли відображення в Конституції України,

що закріплює принципи ідеологічного та політичного плюралізму, свободу думки, слова та інформації, гарантованість свободи масової інформації та допускає суворо лімітоване обмеження прав та свобод.

Слід наголосити, що поняття «культура особистої інформаційної безпеки» може мати широке тлумачення, яке не несе певної конкретики, оскільки його розшифрування в нормативних документах не відображено.

Культура особистої інформаційної безпеки – одна із складових загальної культури людини та її інформаційної культури. Культура охоплює сукупність інформаційного світогляду та системи спеціальних знань, що забезпечують самостійну діяльність із задоволення індивідуальних інформаційних потреб з використанням інформаційно-комунікаційних технологій та автоматизованих систем на принципах захищеності особистої інформації та підтримувальної інфраструктури від випадкових чи навмисних впливів природного чи штучного характеру, які можуть завдати збитків особі.

А. Ю. Геворкян зазначає, що спеціальні знання, вміння та навички – це здатність чітко усвідомлювати інформаційні потреби, з'ясовувати та проводити оцінку джерел інформації (мається на увазі процес виявлення найбільш достовірних, повних та оперативних джерел інформації), знаходити, аналізувати, організовувати, інтерпретувати, синтезувати інформацію, контролювати ефективність процесу задоволення інформаційних потреб [60].

Для того, щоб сформувати культуру особистої інформаційної безпеки, необхідно коригувати систему формування світогляду, знань та умінь, пов'язаних із виробництвом, перетворенням, використанням та зберіганням інформації. Для формування культури особистої інформаційної безпеки доцільно:

– проводити заходи у галузі духовно-морального виховання громадян;

– формувати та розвивати правосвідомість громадян та відповідальне ставлення до використання інформаційних технологій, у тому числі споживчу та користувальницьку культуру;

– забезпечити створення та розвиток систем нормативно-правової, інформаційно-консультативної, технологічної та технічної допомоги у виявленні, попередженні, запобіганні та відображенні загроз інформаційній безпеці громадян та ліквідації наслідків прояву;

– удосконалювати механізми обмеження доступу до інформації, поширення якої в Україні заборонено законом, та її видалення;

– удосконалювати механізми законодавчого регулювання діяльності традиційних і нових засобів масової інформації (Інтернет, телебачення, соціальні мережі, вебсайти в мережі Інтернет, месенджери);

– забезпечити використання сучасних інформаційних платформ для поширення достовірної та якісної інформації, наповнення національного інформаційного простору доступними, якісними та легальними медіапродуктами та сервісами.

Зазначені заходи, які проводяться за допомогою апарату публічного управління, можуть допомогти сформувати культуру особистої інформаційної безпеки. Робота з її формування має вестися на всіх рівнях.

У зв’язку з цим потрібне посилення іншого магістрального спрямування забезпечення інформаційної безпеки – підвищення життєстійкості об’єктів інформаційної безпеки, їх здатність самостійно блокувати або знижувати до прийнятних значень деструктивний вплив загроз інформаційної безпеки. Це завдання можна позначити як формування інформаційного імунітету особистості та суспільства.

А. Ю. Геворкян запропонував комплексний проєкт формування сталої культури інформаційної безпеки українського суспільства, у якому зібрані всі основні аспекти та елементи системи інформаційної безпеки та наведено їх взаємозв’язок із головним завданням держави – зміцненням національної

безпеки. Це три взаємопов'язані блоки для досягнення максимального ефекту від запровадження та реалізації:

– теоретико-правові основи формування культури інформаційної безпеки суспільства;

– визначення основних викликів і загроз інформаційній безпеці;

– визначення короткострокових і стратегічних завдань державної політики в галузі формування культури інформаційної безпеки суспільства [60].

У правових актах та науковій літературі цей напрям забезпечення безпеки зазвичай позначається як формування інформаційної грамотності та цифрової компетентності, культури інформаційної безпеки.

Відповідні положення закріплені в документах стратегічного планування. У Стратегії інформаційної безпеки України та Національній економічній стратегії на період до 2030 року окреслено завдання формування культури особистої інформаційної безпеки.

Національна економічна стратегія на період до 2030 року закріплює, що для створення інформаційного простору знань потрібні розвиток правосвідомості громадян та відповідальне використання інформаційнокомунікаційних технологій.

У 2002 році Генеральна асамблея ООН ухвалила резолюцію, присвячену створенню глобальної культури кібербезпеки «Утворення глобальної культури кібербезпеки». У преамбулі зазначається, що забезпечення кібербезпеки залежить не тільки від роботи правоохоронних структур, а й від превентивних заходів, обізнаності та відповідальності власників та користувачів інформаційно-комунікаційних технологій. Останні два аспекти закріплені серед елементів глобальної культури кібербезпеки у додатку до резолюції.

Аналіз правових актів Європейського Союзу у сфері забезпечення кібербезпеки, зокрема програми «Безпечний Інтернет», показав, що

підвищення поінформованості дітей, батьків і педагогів щодо правил безпечного використання мережі виділялося як один із пріоритетних напрямів.

Ще до активного розвитку Інтернету, у європейських країнах за активної підтримки ЮНЕСКО сформувався специфічний напрям «медіа освіта» (media education), покликаний допомогти школярам та студентам краще адаптуватися у світі медіакультури та спрямований на досягнення медіаграмотності (media literacy).

Медіаграмотність – це комплекс знань, навичок і вмінь, що дозволяють розуміти, аналізувати та критично оцінювати медіа та їхні сюжети та статті, визначається як грамотне використання інструментів, що забезпечують доступ до інформації, розвиток критичного аналізу змісту інформації та прищеплення комунікативних навичок.

З появою та зростанням популярності Інтернету дослідники почали говорити про «цифрову грамотність» як здатність критично розуміти та використовувати інформацію, одержувану за допомогою комп'ютера в різних форматах із широкого діапазону джерел. Цифрова грамотність – це наявність навичок, необхідних для життя, навчання і роботи в суспільстві, де спілкування і доступ до інформації здійснюється за допомогою цифрових технологій (інтернет-платформи, соціальні мережі, мобільні пристрої тощо) [61].

Істотне зростання можливостей Інтернету та входження у повсякденне життя людини привели дослідників до акцентування уваги на понятті цифрової компетентності. Цифрова компетентність – здатність впевнено, ефективно, критично та безпечно обирати та застосовувати інформаційно-комунікаційні технології у різних сферах життєдіяльності (інформаційне середовище, комунікації, споживання, технічна сфера), готовність до такої діяльності. За останні десятиліття в країні підготовлено комплекс наукових та методичних праць, присвячених формуванню інформаційної (медійної, цифрової) грамотності та культури інформаційної безпеки.

Виділяють чотири різновиди цифрової компетентності: інформаційна та медіакомпетентність, комунікативна, технічна та споживча компетентність. Методологічним підходом до формування культури інформаційної безпеки є цифрова (кібер) гігієна.

Як зазначається на вебсайті Міністерства та Комітету цифрової трансформації , цифрова гігієна – це грамотне споживання інформації, а також дотримання базових правил кібербезпеки: не використовувати один і той самий пароль на всіх акаунтах, застосовувати двохфакторну ідентифікацію, регулярно здійснювати резервне копіювання та оновлення [62]. Експерти сформулювали правила кібергігієни, що охоплює безпечне зберігання паролів, використання багатофакторної автентифікації.

Для інформаційної безпеки більше значення мають правила цифрової гігієни: не видавати особистої інформації; не вірити та не довіряти незнайомцям; не викладати нічого важливого у хмару; бути уважним та усвідомленим; пам’ятати та дбати про майбутнє; розпізнавати маніпуляцію та маніпуляторів; дотримуватися розумної помірності; бути джерелом знань.

Аналізуючи зв’язок цифрової компетентності та зіткнення з онлайн ризиками, дослідники дійшли висновку про наявність прямої кореляції між ними. Чим частіше користувач зіштовхувався з онлайнризиками, тим вищий у нього рівень цифрової компетентності. Однак такий спосіб формування цифрової компетентності є небезпечним, оскільки може спричинити неприйнятну шкоду. Головне завдання полягає в навчанні дітей, батьків, вчителів та інших категорій громадян навичок та вмінь, які складають зміст цифрової грамотності (компетентності).

У цьому напрямі в Україні за останнє десятиліття виконано певну роботу. Проводяться виміри рівня цифрової обізнаності, запущено портал цифрової грамотності, у закладах освіти проводяться уроки кібербезпеки.

Міністерством цифрової трансформації України відповідно до Концепції розвитку цифрових компетентностей та плану заходів щодо її реалізації

розроблені Рамки цифрової компетенції для громадян України [63]. Це інструмент щодо покращення цифрової компетенції українців, спрямованих на підвищення цифрової грамотності та практичного використання сервісів ІТ технологій конкретними групами населення.

Якщо говорити безпосередньо про Україну, то 53% громадян володіли цифровою грамотністю нижче за базовий рівень, за даними дослідження 2019 року. У 28% громадян вище за базовий рівень. Лише 11% українців можуть розпізнати неправдиву інформацію в Інтернеті.

В. Є. Іонан, заступник Міністра цифрової трансформації України з питань євроінтеграції, вказує, що багато хто, як і раніше, має недостатні знання та навички у сфері цифрових технологій. Цифрова грамотність населення у першій половині 2021 року оцінюється: ситуація з комунікацією та взаємодією у цифровому суспільстві: 27% на високому рівні, 69% на середньому рівні; з розв'язанням проблем у цифровій середовищі та навчанням протягом життя: 20% на високому рівні, 77% на середньому рівні. Навички безпеки у цифровій середовищі: лише 14% на високому рівні, 82% на середньому рівні. Ще гірша ситуація зі створенням цифрового контенту: лише 10% на високому рівні, 83% на середньому рівні [64].

Важливим напрямом роботи з формування культури інформаційної безпеки є стимулювання проєктів підвищення медійної та цифрової грамотності громадян. Робота в цій галузі ведеться різними громадськими організаціями національного та місцевого рівнів, причому нерідко з власної ініціативи. Потрібне подальше посилення державної підтримки цього напряму громадської активності.

Наказом Міністерства освіти і науки України затверджено Типову програму підвищення кваліфікації педагогічних працівників із розвитку цифрової компетентності, яка розроблена відповідно до сучасних вимог суспільства [65].

У 2019 році було запущено тематичний інтернет-портал «Цифрова грамотність». На місцевому рівні діють численні проєкти підвищення медійної та цифрової грамотності.

Крім освіти як основної форми підвищення цифрової грамотності та культури інформаційної безпеки, важливе значення має інформаційнопросвітницька робота. Вона спрямована на розвиток критичного мислення, підвищення поінформованості про загрози інформаційній безпеці (хибні новини, маніпуляцію свідомістю, шахрайство та ін.) та правила реагування на них. Формами ведення інформаційно-просвітницької роботи є створення та поширення тематичних інформаційних матеріалів (плакатів, пам'яток, роликів), інтернет-ресурсів, проведення навчальних занять та інших профілактичних заходів.

Запит на здобуття знань про правила безпеки в цифровому середовищі є в суспільстві. Дослідження аналітичного центру Разумкова показало, що громадяни переймаються власною інформаційною безпекою. Більше половини опитаних хотіли б дізнатися про те, як краще захиститися від цифрових загроз та розвинути навички безпечного використання цифрових пристроїв та технологій, про інструменти особистої цифрової безпеки, люди відчувають інформаційний дефіцит. Потрібна подальша активізація інформаційно просвітницької роботи інститутів громадянського суспільства в розглянутій сфері за державної підтримки.

На сучасному етапі розвитку України немає можливості повністю позбавити людину інформаційних загроз або зменшити потік новин. Отже, необхідно вживати заходів забезпечення інформаційної безпеки. Використовувати варто не лише технічні методи, а й соціальні технології. Особливу увагу слід звернути на необхідність удосконалення освітньої системи, яка сьогодні не повною мірою відповідає вимогам інформаційного суспільства та захисту від деструктивного інформаційного впливу російського медіасередовища.

Виховання критичного мислення шляхом вивчення питань інформаційної безпеки дозволить уникнути руйнівних психологічних наслідків інформаційних воєн для особистості та дозволить уникнути маніпулятивних технологій російських політичних шахраїв, які активно ведуть діяльність у мережі Інтернет. Грамотний підхід до освіти дітей і молоді з питань інформаційної безпеки дозволить сформувати правильне ставлення до необхідності збереження цілісності, достовірності та доступності інформації, зробить внесок у формування культури особистої інформаційної безпеки, що дозволить успішно посісти своє місце в інформаційному суспільстві.

ВИСНОВКИ

Одним з аспектів захисту територіальної цілісності, суверенітету та національної економіки в умовах цифрової трансформації є забезпечення інформаційної безпеки. Діяльність щодо забезпечення інформаційної безпеки громадян, суспільства та держави, будучи формально спрямованою на реалізацію відповідного права осіб, є необхідною складовою механізму державного управління в умовах воєнного стану, бо сприяє збору, аналізу та узагальненню інформації про деструктивний інформаційний вплив агресора та заходи щодо протидії цьому впливу. Це вкрай важливо для ухвалення державних рішень у цій галузі та підготовки відповідних нормативно-правових актів.

1. В інституційному вимірі забезпечення інформаційної безпеки в умовах цифрової трансформації означає створення певного механізму, що складається з сукупності національних і міжнародних інституцій, які здатні захистити особу та суспільство від деструктивного інформаційного впливу, забезпечити належний захист інформації. Основними проблемами інституціоналізації забезпечення інформаційної безпеки в Україні є: відсутність належної конкретизації на рівні спеціальних законів, наприклад, щодо інформаційного забезпечення діяльності збройних сил, правоохоронних і інших державних органів; недостатність адміністративно-правового забезпечення інформаційної безпеки у частині блокування та видалення протиправного контенту відомчими нормативними актами; незабезпеченість матеріально-правових норм належним рівнем процесуального законодавства; відсутність нормативно-правового захисту дітей від деструктивного інформаційного впливу. Закладені в законодавстві правові механізми забезпечення інформаційної безпеки потребують подальшого розвитку та адаптації до нових викликів та загроз в умовах цифрової трансформації та інформаційного протиборства в умовах правового режиму воєнного стану.

2. Вдосконалення інституту правового забезпечення інформаційної безпеки в Україні має спиратися на чітку правову основу й новітні доктринально-правові напрацювання; передбачати процесуальне закріплення відповідних матеріальних норм, доповнення їх належними гарантіями та санкціями юридичної відповідальності за порушення; забезпечувати поєднання загальнодержавних, суспільних та індивідуальних інтересів. Належне унормування відповідного кола суспільних відносин покликане сприяти усуненню поширення інформації, яка потенційно може загрожувати державі, суспільству, правам і свободам людини.

Зволікання з вирішенням проблеми належного адміністративно-правового унормування забезпечення інформаційної безпеки не сприятиме оптимальному й ефективному виконанню органами публічної адміністрації зобов'язань із захисту громадян від деструктивного інформаційного впливу.

Важливими напрямами вдосконалення законодавства України щодо адміністративно-правового забезпечення інформаційної безпеки в Україні доцільно вважати: внесення змін до законів України, які регулюють суспільні відносини щодо забезпечення інформаційної безпеки у контексті рішень Європейського Суду з прав людини; законодавчу деталізацію й розмежування порядку виконання рішень щодо блокування або видалення відповідного контенту; запровадження спеціальних процедур ефективного контролю за виконанням рішень уповноважених органів щодо блокування або видалення протиправного контенту.

3. Загрози інформаційній безпеці здебільшого супроводжують виникнення та реалізацію загроз в економічний та політичній сферах, у сфері виконання функцій держави тощо, і заподіяння шкоди в інформаційні сфері виступає передусім засобом досягнення інших цілей. Поряд із суто корисливою метою (наприклад, отримання коштів із банківських установ унаслідок вчинення корупційних злочинів), у сучасних умовах інформаційні загрози пов'язані з розпалюванням міжнаціональної, міжконфесійної та іншої

ворожнечі, дискредитацією правоохоронної системи та органів державної влади в цілому, заподіянням шкоди честі, гідності та діловій репутації фізичних осіб, у тому числі публічних, формуванням «образу ворога», «зомбуванням» населення задля створення умов для управління масовою свідомістю. При цьому потенціал інформаційної сфери через її інтегруючий характер та здатність проникнення до інших сфер життєдіяльності суспільства поки що недостатньо усвідомлюється політиками та правоохоронцями (за винятком проявів кіберзлочинності), однак успішно використовується представниками організованих злочинних співтовариств та політичними противниками нашої держави.

Головною загрозою інформаційній безпеці України наразі лишається загроза впливу зовнішнього ворога на інформаційну інфраструктуру, інформаційні ресурси, на суспільство, свідомість та підсвідомість людей з метою нав’язати власну систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони руслі. Стратегічне інформаційне протистояння являє собою як самостійний феномен, здатний вирішувати конфлікт без застосування традиційних збройних сил, так і небезпечний компонент гібридної війни, розгорнутої росією проти України.

4. Механізми протидії інформаційним загрозам від зовнішніх джерел – це сукупність різноманітних видів діяльності органів державного й військового управління, громадських організацій і політичних інститутів та інших суб’єктів, а також способів їх взаємин, які дозволяють оперативно впливати на зовнішні загрози інформаційній безпеці або управляти зумовленими ними ризиками з метою їх локалізації й нейтралізації. Конкретні механізми протидії інформаційним загрозам від зовнішніх джерел вибудовуються на підставі системи потенційних і реальних небезпек, імовірності їх настання, з урахуванням циклу розвитку системи (зародження, становлення, зрілість, трансформація) та її конкретного стану (криза, депресія,

піднесення), виходячи з наявних фінансових, матеріальних, кадрових можливостей країни, на основі балансу інтересів суспільства, держави, груп, окремих осіб. Оцінка відповідних механізмів базується на:

– інформаційній політиці держави, її впливі на параметри безпеки;

– виявленні ступеня ризику відхилень параметрів для стійкості системи інформаційної безпеки;

– визначенні зовнішніх обставин, у яких відбуваються відхилення: збільшення (за несприятливого зовнішнього середовища) або зниження (за сприятливого зовнішнього середовища) ризиків.

Таким чином, механізми протидії інформаційним загрозам від зовнішніх джерел є передусім такими, що базуються на принципах управління ризиками, дозволяють блокувати деструктивні елементи, властивості, процеси, що руйнують систему інформаційної безпеки та національної безпеки в цілому, і стимулювати конструктивні елементи, властивості, процеси, що сприяють її функціонуванню й розвитку.

5. Щодо цифрових технологій інформаційна безпека набуває особливого значення, є обов’язковою умовою забезпечення стану захищеності в цифровому середовищі, функціонуванням системи органів публічної влади на різних цифрових платформах, наданням на їх основі адміністративних послуг. Можна виділити низку напрямів розвитку законодавства у сфері забезпечення інформаційної безпеки: закріплення базових положень про інформаційну безпеку, у тому числі принципів інформаційної безпеки, прав та обов’язків, пов’язаних із забезпеченням інформаційної безпеки та інституту юридичної відповідальності; регулювання питань у сфері поширення відомостей, заборонених законодавством, регулювання забезпечення інформаційної безпеки у масових комунікаціях; забезпечення інформаційної безпеки в державних інформаційних системах та реєстрах; регулювання протидії поширенню фейкової інформації та дезінформації.

6. Важливою складовою правового забезпечення інформаційної безпеки особи та суспільства, які значною мірою визначають інформаційну безпеку держави, є необхідність формування культури інформаційної безпеки.

Культура інформаційної безпеки – це сукупність певних знань, умінь, навичок та високий рівень правосвідомості особистості в інформаційній сфері. До знань, умінь та навичок у сфері інформаційної безпеки належать: здатність забезпечувати безпечну реалізацію інтересів в інформаційній сфері, усвідомлення національних інформаційних пріоритетів та інтересів, сформоване вміння визначати загрози інформаційній безпеці, оцінювати ризики, сформовані вміння та навички протистояння можливим загрозам в інформаційній сфері.

З метою формування культури інформаційної безпеки особистості та суспільства за умов цифрової трансформації необхідно розробити документи планування; правове просвітництво, охоплюючи питання відповідальності за правопорушення в інформаційній сфері; визначення викликів і загроз інформаційній безпеці; постановку короткострокових та довгострокових завдань, що охоплюють активне залучення до цього процесу установ освіти та культури, інститутів громадянського суспільства; розвиток механізмів саморегулювання користувачів засобів масової комунікації, соціальних мереж та інших можливостей інформаційних технологій та систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 р. «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text.

2. Про національну безпеку України: Закон України від 21.06.2018 р. № 2496-VIII. URL: https://zakon.rada.gov.ua/laws/card/2469-19.

3. Богуцький П. П. Концептуальні засади права національної безпеки України. Київ; Одеса: Фенікс, 2020. 374 с.

4. Про схвалення Рекомендацій щодо вікової класифікації інформаційної продукції: Рішення Національної експертної комісії України з питань захисту суспільної моралі від 05.09.2013 р. № 60. URL: https://zakon.rada.gov.ua/rada/show/vr060623-13#Text.

5. Про рішення Ради національної безпеки і оборони України від 21 березня 2008 р. «Про невідкладні заходи щодо забезпечення інформаційної безпеки України»: Указ Президента України від 23.04.2008 р. № 377/2008. URL: https://zakon.rada.gov.ua/laws/card/377/2008.

6. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 р. № 47/2017. URL: https://zakon.rada.gov.ua/laws/card/47/2017.

7. Про інформацію: Закон України від 02.10.1992 р. № 2657. URL: https://zakon.rada.gov.ua/laws/card/2657-12.

8. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. № 80/94. URL: https://zakon.rada.gov.ua/laws/card/80/94-вр.

9. Про внесення змін до деяких законодавчих актів України у зв’язку з прийняттям Закону України «Про інформацію» та Закону України «Про

доступ до публічної інформації»: Закон України від 27.03.2014 р. № 1174-VII. URL: 209 https://zakon.rada.gov.ua/laws/card/1170-18.

10. Єсімов С. С. Шляхи удосконалення нормативно-правового регулювання в сфері інформаційної безпеки. *Науковий вісник Львівського державного університету внутрішніх справ.* Серія юридична. 2013. № 4. С. 144–150.

11. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України: дис. … д-ра юрид. наук: спец. 12.00.07. Одеса, 2004. 427 с.

12. Калюжний Р. А., Цимбалюк В. С. Координація діяльності органів влади у боротьбі з організованою кіберзлочинністю. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2002. № 6. С. 105–111.

13. Інформаційна безпека. IT-словник. URL: http://xn--r1a3b.xn--b1amgblet.xn-j1amh/index.php.

14. Розробка проєкту Концепції кодифікації інформаційного законодавства України. *Інформація і право*. 2012. № 1. URL: http://ippi.org.ua/vid-redaktsiinoi-kolegii-rozrobka-proektu-kontseptsii-kodifikatsii informatsiinogo-zakonodavstva-ukr.

15. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 р. № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text.

16. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386-р. URL: https://www.kmu.gov.ua/npas/246420577.

17. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII. URL: https://zakon.rada.gov.ua/laws/card/3855-12.

18. Корж І. Безпека: медотологічні підходи до поняття. *National law journal: theory and practice*. 2019. August. P. 68-72.

19. 57. Проєкт Закону України «Про засади інформаційної безпеки України». URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=51123.

20. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 р. «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

21. Бойченко В. П. Кримінально-правова охорона суспільної моралі в Україні: антропологічний вимір: дис. … канд. юрид. наук: спец.: 12.00.08. Одеса, 2021. 230 с.

22. Кодекс України про адміністративні правопорушення: Закон України від 07.12.1984 р. № 8073-X. URL: https://zakon.rada.gov.ua/laws/card/80731-10.

23. Золотар О. О. Інформаційна безпека людини: теорія і практика: Монографія. Київ: ТОВ Видавничий дім АртЕк, 2018. 446.

24. 10. Довгань О. Д., Ткачук Т. Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. *Інформація і право*. 2018. № 2 (25). С. 73–85.

25. Окінавська хартія глобального інформаційного суспільства. URL: https://zakon.rada.gov.ua/laws/show/998_163#Text.

26. Про Доктрину інформаційної безпеки України: Указ Президента України від 08.07.2009 р. № 514/2009. URL: https://zakon.rada.gov.ua/laws/card/514/2009.

27. 71. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Гельветика, 2017. 168 с.

28. Шопіна І. М. Поняття інформаційної безпеки: концептуальні підходи до визначення. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія Право*. 2022. № 13 (25). С. 133–140.

29. Баран М. В. Суб’єкти забезпечення інформаційної безпеки в

Україні. *Юридичний науковий електронний журнал*. 2022. № 6. С. 220–223.

30. Про основи національної безпеки: Закон України від 19.06.2003 р. № 964-IV. URL: https://zakon.rada.gov.ua/laws/card/964-15.

31. Про боротьбу з тероризмом: Закон України від 20.03.2003 р. № 638-IV. URL: https://zakon.rada.gov.ua/laws/card/638-15.

32. Про запобігання корупції: Закон України від 14.10.2014 р. № 1700-VII. URL: https://zakon.rada.gov.ua/laws/card/1700-18.

33. Петренко Л. В., Петренко А. В. Психологічні умови формування «цифрових» компетенцій майбутніх фахівців. Цифрова економіка. Київ: КНЕУ, 215 2018. С. 290–293.

34. Про захист суспільної моралі: Закон України від 20.11.2003 р. № 1296- IV. URL: https://zakon.rada.gov.ua/laws/card/1296-15.

35. Про електронні комунікації: Закон України від 16.12.2020 р. № 1089- IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.

36. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» від 15 березня 2016 року № 96/2016: URL: www.president.gov.ua/documents/962016-19836.

37. Горбулін В. П., Качинський А. П. Засади національної безпеки України: [підручник]. Київ: Інтертехнологія, 2009. 272 с.

38. Прокоф'єва-Янчиленко Д. М. Кримінологічна безпека як інтегративна складова національної безпеки. *Наукові праці Національного університету «Одеська юридична академія»*. 2014. № 14: URL: naukovipraci.nuoua.od.ua/tom-xiv.

39. Цивілізаційний вибір України: парадигма осмислення і стратегія дії: [національна доповідь] / ред.кол.: С. Пирожков, О. Майборода, Ю. Шайгородський та ін.; Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України. Київ: НАН України, 2016. 284 с.

40. Сащук Г. Інформаційна безпека в системі забезпечення

національної безпеки. URL: http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php.

41. Інформаційна безпека (соціально-правові аспекти): [підручник]. В. Остроухов, В. Петрик, М. Присяжнюк та ін.; за ред. Є. Д. Скулиша. Київ : КНТ, 2010. 776 с.

42. Дереко В. Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави*. 2015. № 2 (18). С. 16–22.

43. Хмелевський Р. М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності. *Сучасний захист інформації*. 2016. № 4. С. 65–70.

44. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: [монография]. Київ: Інтертехнологія, 2009. 164 с.

45. Сопілко І. М. Інформаційні загрози та безпека сучасного українського суспільства. *Юридичний вісник*. 2015. № 1 (34). С.75–80.

46. Григор'єв В. І. Технології сучасної інформаційно-психологічної війни. *Інформаційна безпека людини, суспільства, держави*. 2015. № 3 (19). С. 48–52.

47. Прозоров А. Ю. Ціннісні основи інформаційної безпеки особи, суспільства та держави. *Інформаційна безпека людини, суспільства, держави.* 2016. № 1 (20). С. 29–37.

48. Домбровська С. М. Механізми забезпечення інформаційної безпеки як складової державної безпеки України. *Теорія та практика державного управління*. 2015. Вип. 1 (48). С. 2–4.

49. Пилипчук В. Г., Дзьобань О. П. Проблема агресії і насильства: світоглядно-інформаційний вимір. URL: social-science.com.ua/article/806.

50. Живко З. Б., Живко М. О. Інформаційні загрози: суть і проблеми. *Тези доповідей II міжнародної НПК «Безпека та захист інформації в*

інформаційних системах». С. 116–118.

51. Дереко В. Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави*. 2015. № 2 (18). С. 16-22.

52. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану»: Закон України від 24.03.2022 р. № 2160-IX. URL: https://zakon.rada.gov.ua/laws/show/2160-20#Text.

53. Про внесення змін до статті 114-2 Кримінального кодексу України щодо удосконалення відповідальності за несанкціоноване розповсюдження інформації про засоби протидії збройній агресії Російської Федерації: Закон України від 01.04.2022 р. № 2178-IX. URL: https://zakon.rada.gov.ua/laws/show/2178-20#Text.

54. Батиргареєва В. С. Правова платформа для забезпечення в Україні ефективного захисту цифрових трансформацій суспільства. *Інформація і право*. 2022. № 1 (40). С. 21–34.

55. Сопільник Л., Ковалів М., Єсімов С. і інші. Розвиток цифрової економіки в контексті забезпечення інформаційної безпеки в Україні. *Traektoriâ Nauki = Path of Science*. 2020. Vol. 6. № 5. S. 2023–2032.

56. Краковська А. Є., Бабик М. К. Цифровізація адміністративних послуг в Україні: проблеми та перспективи розвитку. *Науковий вісник Ужгородського Національного Університету. Серія право.* 2022. Випуск 70. С. 329–334.

57. Про публічні електронні реєстри: Закон України від 18.11.2021 р. № 1907-IX. URL: https://zakon.rada.gov.ua/laws/show/1907-20/conv#n472.

58. Деякі питання забезпечення функціонування інформаційнокомунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова Кабінету Міністрів України від 12.03.2022 р. № 263. URL: https://zakon.rada.gov.ua/laws/show/263- 2022-%D0%BF#Text.

59. Ведмедев М. М. Феномен кліпового мислення в дискусійному просторі сучасної науки. *Sciences of Europe*. 2021. № 70. С. 41–49.

60. Геворкян А. Ю. Формування основ культури інформаційної безпеки суспільства як фактор зміцнення національної безпеки. *Вісник Національного університету цивільного захисту України. Серія «Державне управління».* 2021. № 1 (14). С. 168–177.

61. Тілікіна Н. В. Медіа, інформаційна і комп'ютерна грамотність як компоненти цифрової грамотності. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична*. 2021. Випуск 29. С. 46–56.

62. Цифрова гігієна: яких правил варто дотримуватися в Інтернеті? 24 березня 2020. URL: https://thedigital.gov.ua/news/tsifrova-gigiena-yakikh-pravil-varto-dotrimuvatisya-v-interneti.

63. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації: Розпорядження Кабінету Міністрів України від 03.03.2021 р. № 167-р. URL: https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80.

64. Іонан В. Цифрограм 2.0. Цифрова грамотність українців у режимі реального часу. 26.05.2021. URL: https://ua.interfax.com.ua/news/blog/746434.html.

65. Ухвалено типову програму підвищення кваліфікації педагогічних працівників із розвитку цифрової компетентності. 13 грудня 2021 року. URL: ttps://mon.gov.ua/ua/news/uhvaleno-tipovu-programu-pidvishennya-kvalifikaciyi-pedagogichnih-pracivnikiv-iz-rozvitku-cifrovoyi-kompetentnosti.