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 *Сидоренко Інни Василівни*

академічної групи *281м-21з-4 ІДУ*

спеціальності *281 Публічне управління та адміністрування*

на тему: *«Особливості забезпечення інформаційної безпеки в органах публічного управління»*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	Кравцов О.В.			
розділів:				

Рецензент:				

Нормоконтролер:	Вишневська О.В.			

Дніпро
2022

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи магістра на тему «Особливості забезпечення інформаційної безпеки в органах публічного управління»

75 сторінок, 2 рис., 67 джерел.

ДЕРЖАВНА БЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНІ ЗАГРОЗИ, ЗАХИСТ ІНФОРМАЦІЇ, КІБЕРБЕЗПЕКА, ОРГАНИ ПУБЛІЧНОГО УПРАВЛІННЯ

Об’єкт дослідження – державна політика у сфері інформаційної безпеки.

Предмет дослідження – забезпечення інформаційної безпеки в органах публічного управління.

Мета дослідження – розробка пропозицій щодо покращення забезпечення інформаційної безпеки в органах публічного управління.

У першому розділі досліджуються теоретичні та нормативно правові засади забезпечення інформаційної безпеки.

Другий розділ присвячено аналізу тенденцій і підходів до забезпечення кібербезпеки у публічному управлінні в Україні та в інших країнах.

У третьому розділі наведено напрями удосконалення забезпечення інформаційної безпеки в органах публічного управління

Результати дослідження можуть бути застосовані в діяльності органів публічної влади для організації якісного надання адміністративних послуг в умовах цифровізації.

ABSTRACT

Explanatory note of the master's degree qualification thesis on the topic «Peculiarities of ensuring information security in public administration bodies ».

73 pages, 2 figure, 67 sources.

ADMINISTRATIVE SERVICES, ADMINISTRATIVE SERVICES CENTER, DIIA, DIGITALIZATION, PUBLIC SERVICES, PUBLIC ADMINISTRATION.

Object of research – state policy in the field of information security.

Subject of research – ensuring information security in public administration bodies.

The purpose of research – development of proposals for improving information security in public administration bodies.

The first section examines the theoretical and normative legal foundations of ensuring information security.

The second section is devoted to the analysis of trends and approaches to ensuring cyber security in public administration in Ukraine and other countries.

In the third section, directions for improving information security in public administration bodies are given.

The results of the study can be applied in the activities of public authorities for the organization of high-quality provision of administrative services in conditions of digitalization

ЗМІСТ

ВСТУП

Інформаційна безпека виступає інтегрованим компонентом національної безпеки і є пріоритетною функцією держави. З одного боку, інформаційна безпека спрямована на забезпечення якісного всебічного інформування громадян та їх необмеженого доступу до різних інформаційних джерел. З іншого боку, вона передбачає контроль за непоширенням дезінформації, сприяння суспільній цілісності, охорону інформаційного суверенітету, протидію негативним інформаційним впливам пропагандистського та психологічного характеру, захисту державного інформаційного простору від різних маніпуляційних дій та інформаційних впливів.

На сьогодні, в умовах російської агресії, Україна здійснює низку складних демократичних та соціально-економічних трансформацій, перебуваючи в зоні ризику забезпечення своєї інформаційної безпеки. При цьому органи публічного управління знаходяться в зоні підвищеного ризику. Проблем додає те, що тривалий час сфері інформаційної безпеки не приділялась належна увага. Відповідно загострювалися протиріччя та конфліктні ситуації як внутрішнього, так і зовнішнього характеру. При цьому основним засобом здійснення негативного впливу на нашу країну були й залишаються цифрові технології. Існуюча недосконаліть діючої системи інформаційної безпеки призводить до колосальних збитків для держави, суспільства й особистості. З метою ефективного забезпечення її інформаційної безпеки та кібербезпеки розробляється відповідна державна політика та здійснюється державне управління розвитком даного напряму, але за декілька, навіть років неможливо все виправити. Імплементація Європейського законодавства, безумовно, дозволить швидко закрити більшість прогалин в сфері забезпечення інформаційної безпеки. Також, потрібно врахувати, що і Європа знаходиться в умовах безпрецедентної інформаційної і кібервійни яка поставила необхідність модернізації відповідних нормативно-правових актів та розробки та впровадженню заходів протидії.

Таким чином, бурхливість розвитку цифрових технологій супроводжується підвищенням рівня традиційних і появою загроз принципово нового характеру для громадян, суспільства та держави, що актуалізує тематику дослідження.

Вивченню питань забезпечення інформаційної безпеки приділяли увагу багато науковців та дослідників. Зокрема, різні аспекти забезпечення інформаційної безпеки розглядали такі науковці, як: В. Абакумов, В. Антонюк, В. Богуш, І. Боднар, В. Брижко, М. Волошина, О. Горбатюк, Н. Грицяк, С. Гуцу, О. Дзьобань, К. Захарченко, Р. Калюжний, О. Литвиненко, В. Ліпкан, Л. Наливайко, В. Петрик, О. Рижук, О. Юдін.

Незважаючи на це розвиток механізмів забезпечення інформаційної безпеки потребує подальшої розробки та наукового обґрунтування шляхів їх модернізації, що зумовило вибір теми, мету та завдання наукового дослідження.

Об’єкт дослідження – державна політика у сфері інформаційної безпеки.

Предмет дослідження – забезпечення інформаційної безпеки в органах публічного управління.

Метою роботи є розробка пропозицій щодо покращення забезпечення інформаційної безпеки в органах публічного управління.

Досягнення мети включає вирішення таких завдань:

- дослідити поняття «інформаційна безпека»;
- охарактеризувати нормативно-правові основи державної політики із забезпечення інформаційної безпеки;
- проаналізувати основні напрямки політики інформаційної безпеки;
- розглянути міжнародний досвід забезпечення інформаційної безпеки;
- розглянути основні технології виявлення загроз інформаційній безпеці;
- розробити шляхи удосконалення державної політики в сфері інформаційної безпеки;
- запропонувати шляхи покращення забезпечення інформаційної безпеки в органах місцевого самоврядування.

У магістерській роботі використано загальнонаукові та спеціальні методи: аналізу та синтезу – для деталізації об’єкта дослідження; узагальнення – для розкриття основних засад механізмів забезпечення інформаційної безпеки; порівняльний метод та узагальнення – для вивчення нормативно-правового забезпечення та особливостей інформаційної безпеки; системний метод – для розкриття концептуальних основ забезпечення інформаційної безпеки; порівняння та узагальнення – при дослідженні особливостей забезпечення інформаційної безпеки; метод моделювання – для розроблення перспективних напрямів застосування механізмів реалізації державної політики інформаційної безпеки та можливих шляхів удосконалення системи інформаційної безпеки України.

Методологічною базою дослідження є наукові праці вітчизняних і зарубіжних учених.

Практичне значення отриманих результатів полягає в тому, що викладені у роботі положення можуть бути використані для підвищення рівня забезпечення інформаційної безпеки.

РОЗДІЛ 1.
ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Інформаційна безпека як невід'ємна складова національної безпеки

Проблема інформаційної безпеки має давнє походження і стала особливо актуальною в наш час, коли безпосередньо використання інформаційних технологій відбувається практично у всіх сферах нашого життя. Інформаційна безпека являє собою одне з важливіших понять у науці та різних сферах людської діяльності. Визначення наукового поняття «інформаційна безпека» в теоретичному і практичному плані є принциповим, оскільки воно повинно окреслити його сутність, а також виокремити його визначальні елементи, необхідні в процесі розробки засад державної політики із забезпечення інформаційної безпеки. Тому важливим завданнями наукового аналізу є саме вияснення змісту поняття «інформаційна безпека». Слід зазначити, що будь-яке вчення лише тоді досягає зрілості та досконалості, коли розкриває сутність досліджуваних явищ, має можливість передбачати майбутні зміни не лише в сфері явищ, а й у сфері їх сутностей. Тому пізнання сутності інформаційної безпеки можливо лише на основі теорії досліджуваного предмета, вияснення його внутрішнього змісту, виявлення властивих йому характерних ознак.

Інформаційна безпека України є органічною складовою національної безпеки, відтак її розгляд є необхідним для формування базових знань та уявлень про нашу національну безпеку. Актуальність розгляду сутності інформаційної безпеки обумовлена цілою низкою чинників:

- вона сьогодні є головним стратегічним напрямом державної політики, основою забезпечення ефективної економічної та оборонної могутності держави;
- інформаційна безпека у сучасному світі є таким атрибутом, від якого у визначальному плані залежить і ефективність життєдіяльності сучасного суспільства;

– інформаційна безпека принципово вимагає необхідність змінити обсяг і важливість інформації, яка обертається в технічних засобах її збереження, обробки та передачі;

– інформаційна безпека визначається станом комп'ютеризації основних сфер діяльності, який вимагає врахування широкого спектру внутрішніх і зовнішніх загроз, які характеризуються функціонуванням нетрадиційних каналів, що ведуть до втрати інформації і несанкціонованого доступу до неї;

– інформаційна безпека передбачає масове оснащення всіх державних установ, підприємств, організацій і приватних осіб засобами обчислювальної з метою для виявлення і послаблення і можливо ліквідації реальної загрози створення розгалужених систем регулярного несанкціонованого контролю за інформаційними процесами і ресурсами, країни;

– інформаційна безпека має враховувати реальність сьогодення, пов'язаною із застосування інформаційної зброї її ведення інформаційних війн;

– вона потребує належного правового регулювання суспільних відносин у сфері інформаційної безпеки, які не повинні призвести до серйозних негативних наслідків, що могли б ускладнювати підтримання необхідного балансу інтересів особи, суспільства та держави;

– недобросовісне виконання завдань інформаційної безпеки може призвести до зниження рівня внутрішньої інформаційної безпеки

України, прямим наслідком чого може стати дестабілізація соціально-політичної обстановки, проведення акцій опору щодо прийнятих тих чи інших державних рішень;

– ігнорування інформаційної безпеки веде до погіршення ситуації із забезпеченням збереження державної таємниці, недостатньо розвиненого механізму забезпечення службової таємниці;

– відсутність інформаційної безпеки може свідчити про відставання вітчизняних інформаційних технологій, що буде змушувати при створенні інформаційних систем закуповувати імпортну техніку І залучати іноземні фірми, через що значно підвищиться імовірність несанкціонованого доступу до

інформації, зросте залежність від іноземних виробників комп'ютерної і телекомунікаційної техніки, програмного забезпечення.

Спроби визначити зміст категорії «інформаційна безпека» були зроблені ще в часи функціонування радянського режиму. Поняття «інформаційна безпека» з'явилося наприкінці 80-х років у праці німецького вченого Г.Одермана, в якій йшлося про важливий інформаційний компонент у міжнародній безпеці та робилась спроба розглянути проблеми безпеки, які пов'язані з інформаційними загрозами комплексно.

В. Ліпкан поняття інформаційної безпеки визначає як складову національної безпеки, яка визначає певний вид соціальної діяльності, основним змістом якої є створення сприятливих (необхідних і достатніх) умов для розвитку та реалізації національних інтересів [14]. Тому на його думку сутність поняття «інформаційна безпека» полягає в створенні державними і недержавними інституціями сприятливих умов для розвитку і реалізації національних інтересів в інформаційній сфері.

Цікавий погляд на поняття «інформаційна безпека» має відомий український дослідник Р. Калюжний, який вважає, що інформаційна безпека − це вид суспільних інформаційних правовідносин стосовно створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності, спеціальних правовідносин, які пов'язані з створенням, зберіганням, поширенням і використанням інформації [15].

Аналіз наукової літератури свідчить, що переважно науковці визначення поняття інформаційної безпеки розглядають як:

− по-перше, це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання та розвиток в інтересах громадян, організацій, держави. Під інформаційним середовищем вони розуміють сферу діяльності суб'єктів, пов'язану із створенням, обробленням й споживанням інформації;

− по-друге, інформаційна безпека − це стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє

існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. На їх думку стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і як наслідок − обґрунтованість рішень і дій, що приймаються;

− по-третє, інформаційна безпека – складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується необхідний інформаційний суверенітет України;

− по-четверте, інформаційна безпека − це процес вдосконалення державного регулювання розвитку інформаційної сфери, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

− по-п'яте, вони вважають, що інформаційна безпека − це насамперед неухильне дотримання конституційного права громадян на свободу слова, їх вільного доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації;

− по-шосте, на їх думку, інформаційна безпека – це вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України [16; 17].

Залежно від виду загроз інформаційній безпеці інформаційну безпеку можна також розглядати наступним чином (рис. 1.1):

Рис. 1.1. Елементи системи інформаційної безпеки

– як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації;

– інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб;

– інформаційних прав і свобод людини і громадянина.

Загалом, у багатьох українських, а також і зарубіжних дослідників інформаційна безпека розглядається сьогодні як невід'ємна складова безпеки національної. Крім того, інформаційна безпека в такому аспекті розглядається не просто як окремий елемент національної безпеки, але як її інтегральна і наскрізна, якісна характеристика та показник захищеності всіх громадян, суспільства і держави [18].

Аналіз різних підходів до визначення змісту поняття «інформаційна безпека» надає нам можливість зауважити про недоцільність суворого обрання тієї чи іншої позиції. Наведені вище погляди до визначення поняття інформаційної безпеки дають змогу розглядати дану проблему більш комплексно і системно, додаючи знання про цей багатогранний феномен. Найбільш прийнятним є інтегральний підхід, за якого інформаційна безпека

визначатиметься за допомогою окреслення найбільш важливих її сутнісних ознак з урахуванням постійної динаміки розвитку інформаційної політики.

Існує два аспекти вивчення інформаційної безпеки в контексті національної безпеки. З одного боку, це самостійний елемент національної безпеки будь-якої країни, а з іншого – інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної і тощо. Слід зазначити, що структуру поняття інформаційної безпеки складають основні її елементи, які відображають життєво важливі інтереси держави, суспільства і громадськості. Вони перебувають у взаємодії з інтересами елементів, які складають дане утворення. Законом України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 року. зазначено, що інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки. Отже, інформаційна безпека є одним із видів національної безпеки, важлива функція держави. Інформаційна безпека України означає:

- законодавче формування державної інформаційної політики;
- створення відповідно до законів України можливостей досягнення інформаційної достатності для ухвалення рішень органами державної влади, громадянами та об'єднаннями громадян, іншими суб'єктами права в Україні;
- гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України;
- всебічний розвиток інформаційної структури;
- підтримка розвитку національних інформаційних ресурсів України з урахуванням досягнень науки та техніки й особливостей духовно-культурного життя народу України;
- створення і впровадження безпечних інформаційних технологій;
- захист права власності держави на стратегічні об'єкти інформаційної інфраструктури України;
- охорону державної таємниці, а також інформації з обмеженим доступом, що є об'єктом права власності або об'єктом лише володіння, користування чи розпорядження державою;

− створення загальної системи охорони інформації, зокрема охорони державної таємниці, а також іншої інформації з обмеженим доступом;

− захист національного інформаційного простору України від розповсюдження спотвореної або забороненої для поширення законодавством України інформаційної продукції;

− встановлення законодавством режиму доступу іноземних держав або їх представників до національних інформаційних ресурсів на основі договорів з іноземними державами; законодавче визначення порядку поширення інформаційної продукції зарубіжного виробництва на території України [19].

Об’єктами інформаційної безпеки є інформаційні ресурси. Сутність інформаційних ресурсів деякі науковці проблем інформаційної політики частіше за все визначають поняттям «інформаційний простір» [20; 21]. Таке визначення є занадто вузьким, його слід доповнити уточненням, що це не просто механічна сума ресурсів, а ще і певна конфігурація відносин різних суб’єктів політики до ресурсів, які сприяють забезпеченню інформаційної безпеки.

Зазначимо, що національні інформаційні ресурси України складають окремі документи і масиви документів, результати інтелектуальної, творчої та інформаційної діяльності, бази й банки даних, всі види архівів, бібліотеки, музейні фонди та інші, що містять дані, відомості й знання, які зафіксовані на відповідних носіях інформації,

Становлення і розвиток української держави потребує докорінної зміни ставлення не лише до формування її інформаційної політики, а і в її межах забезпечення інформаційної безпеки, що містить вивчення та опанування теоретичних підвалин даних процесів. Інформаційна безпека, як складова національної безпеки держави, сьогодні є необхідною умовою всіх реальних сфер діяльності суспільства і в значній мірі визначає та ефективно впливає на стан інших складових національної безпеки, в той самий час є її самостійною складовою, роль і значення якої з кожним роком невпинно зростає

Аналіз інформаційної безпеки передбачає розгляд сукупності таких об’єктивних чинників: потреб громадян, суспільства і держави і світового

співтовариства; уразливість суспільства і держави від небезпечних загроз зовнішніх інформаційних технологій; наявність широкого кола небезпек, якими має управляти існуюча система забезпечення інформаційної безпеки. Інформаційна безпека, як складовий компонент загальної проблеми інформаційного забезпечення людини, держави і суспільства, має бути орієнтованою на захист всіх їх законних інтересів.

Основними видами інформаційної безпеки є інформаційна безпека особистості, яка являє собою захищеність психіки й свідомості людини від небезпечних інформаційних впливів, зокрема маніпулюванням її свідомості, дезінформуванням, спонуканням до неправової діяльності тощо. А також це інформаційна безпека держави, яка характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) відносно небезпечних (дестабілізуючих) інформаційних впливів, причому як запровадження, так і добування інформації [22].

Інформаційна безпека виступає як характеристика стабільного, стійкого стану системи, яка при впливі внутрішніх та зовнішніх загроз та небезпек зберігає суттєво важливі характеристики для власного існування. Основними характеристиками інформаційної безпеки є:

− доступність, що являє собою можливість за прийнятний час отримати шукану інформаційну послугу будь-яким суб’єктом виконавчої влади;

− цілісність, як актуальність і несуперечливість інформації, її захищеність від руйнування і несанкціонованої зміни;

− конфіденційність, спрямована на захист від несанкціонованого ознайомлення з інформаційними носіями.

В інформаційному праві інформаційна безпека – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позиції захисту життєво важливих інтересів особистості, суспільства, держави і акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами [23].

Рівнями інформаційної безпеки є:

− нормативно-правовий − закони, нормативно-правові акти тощо;

− адміністративний − дії загального характеру, які вживаються органами державного управління;

− процедурний − конкретні процедури забезпечення інформаційної безпеки;

− програмно-технічний − конкретні технічні заходи забезпечення інформаційної безпеки.

Отже, інформаційна безпека являє собою одне з найважливіших понять у науці і різних сферах людської діяльності. Сутність і комплексність цього поняття виявляється характером сучасної інформаційної політики. Інформаційна безпека визначає стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через неповноту, невчасність та невірогідність інформації, яка безпосередньо використовується; а також негативний зовнішній інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. Знання в цій сфері дозволять зрозуміти природу інформації та її властивостей, усвідомити сутність інформаційної небезпеки і шляхів її запобігання та усунення.

При дослідженні поняття інформаційної безпеки, встановлена важливість різних підходів стосовно визначення сутності даного феномену, а саме розуміння інформаційної безпеки виявляється як стан захищеності інформаційного простору держави та національних інтересів України в інформаційному середовищі; прийняття певних превентивних заходів стосовно забезпечення життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі. З’ясовано, що інформаційний вимір національної безпеки держави – це не тільки захист комп’ютерних систем і телекомунікаційних мереж держави як частини системи

національної безпеки, але й цілий комплекс проблем, які пов’язані з інформаційною уразливістю як окремого індивіда, так і суспільства в цілому.

Таким чином, інформаційна безпека представляє собою одне з найважливіших понять у науці і різних сферах людської діяльності. Сутність і комплексність цього поняття виявляється характером сучасного інформаційного суспільства. Інформаційна безпека як одна з характеристик стійкого розвитку виступає в якості базової цінності держави. Водночас, ціннісні орієнтації, що ґрунтуються на уявленнях про інформаційну безпеку у різних суспільних груп і окремих осіб, часто не збігаються. Саме тому роль інформаційної безпеки має розглядатися за допомогою системи методів, які виражають загальні цінності у сфері інформаційних відносин суспільства.

Проблема ефективного забезпечення інформаційної безпеки має передбачати вирішення таких головних і масштабних задач, як: розроблення теоретичних основ забезпечення безпеки інформації; створення системи органів, які мають відповідати за безпеку інформації; вирішення проблеми керування захистом інформації та її автоматизації; створення належної нормативно-правової бази, яка повинна регламентувати рішення всіх задач забезпечення безпеки інформації; налагодження виробництва засобів захисту інформації; організацію підготовки відповідних фахівців та ін.

1.2. Правові основи державної політики із забезпечення інформаційної безпеки

Фундаментальною основою здійснення державної політики із забезпечення інформаційної безпеки виступають норми права, які покликані регулювати та впорядкувати відповідні її напрямки, забезпечити їх цілеспрямованість, системність, стабільність і збалансованість. На думку О. Тихомирова саме розуміння правового аспекту політики інформаційної безпеки надає цьому процесу розуміння системності в її реалізації (поєднання під правовим кутом зору спеціальних юридичних важелів її забезпечення), що

об’єктивно зумовлено міждисциплінарним характером інформаційної безпеки та правовим характером діяльності сучасної держави [24].

Досліджуючи правове забезпечення інформаційної політики важливо звернути увагу на те, що її становлення і розвиток нерозривно пов’язане із правовим регулюванням інформаційних відносин, яке містить значну кількість норм що безпосередньо чи опосередковано стосуються процесу її реалізації. На думку В. Остроухова – нормативна база інформаційної безпеки повинна виконувати в першу чергу три основні функції: перша – регулювати взаємовідносини між суб’єктами інформаційної безпеки, визначати їх права, обов’язки та відповідальність; друга − нормативно забезпечувати дії суб’єктів інформаційної безпеки на всіх рівнях, а саме − людини, суспільства, держави; третя − встановлювати порядок застосування різних сил і засобів забезпечення інформаційної безпеки [25].

Інформаційна безпека України передбачала правове визначення інформації як стратегічно важливого для держави ресурсу, створення взаємопов’язаної системи інформаційних масивів держави різного рівня й призначення, а також державних органів, що мали відповідати за формування, зберігання, використання і захист цих масивів, визначення прав, обов’язків, гарантій забезпечення прав і відповідальності суб’єктів інформаційних відносин у різних прикладних сферах, раціональне поєднання монопольного і немонопольного в інформаційній сфері, ліцензування і сертифікація деяких видів інформаційної діяльності та продукції, чітке законодавче визначення виду, типу обсягу інформації з обмеженим доступом, процедур віднесення до такої інформації і зняття обмежень, прав, обов’язків та відповідальності суб’єктів інформаційних відносин щодо поділу та класифікації такої інформації, її використання, створення загальної системи забезпечення інформаційної безпеки [23].

О. Баранов, говорячи про початки створення нормативно-правового забезпечення інформаційної безпеки України, зауважив: «Закони покликані не тільки юридично фіксувати суспільні відносини, що вже склалися або достатньою мірою сформувалися, але й активно формувати перспективні відносини, які

визначатимуть вектор розвитку суспільства в майбутньому» [26]. З огляду на відсутність світового досвіду докорінної зміни державного устрою у тих масштабах, котрі пізнавала молода українська держава, до речі як і всі держави колишнього СРСР, нова законодавча база створювалася з позиції «чистого аркуша». Наголосимо, що вже за кілька тижнів після проведення референдуму 1 грудня 1991 р., яким було затверджено Акт проголошення незалежності, Верховною радою незалежної України було прийнято Закон України «Про основи державної політики у сфері науки і науково-технічної діяльності» (1991 р.) Цей закон мав на меті створення правових основ державної політики у сфері науки і науково-технічної діяльності, а також визначав правові, організаційні та фінансові засади її функціонування і розвитку, створення умови для забезпечення потреб суспільства і держави у технологічному розвитку. Фактично в ньому було закладено підвалини для розвитку інформаційного суспільства, про яке на момент початку розбудови держави особливо ніхто не замислювався. Закон виглядав як передвісник становлення і розбудови інформаційного суспільства, з врахуванням системних вимог забезпечення його інформаційної безпеки [27].

В українському національному праві системоутворюючим фактором і поштовхом до виникнення і формування інформаційного права як інституції публічного (державного) права можна вважати прийнятий у 1992 р. Закон України «Про інформацію»[28]. Не можна недооцінювати значення цього акту на той час. Після довготривалої інформаційної ізоляції за часів УРСР, українська держава і суспільство опинились посеред бурхливих інформаційних процесів, які вимагали від України формування власних пріоритетів і напрямів розвитку інформаційної сфери та захисту її інформаційної безпеки. Прийняття цього Закону стало знаковою подією в організації безпечного інформаційного простору держави. Фактично, вперше на вищому законодавчому рівні ним були визначені:

- принципи інформаційних відносин; пріоритетні напрями державної інформаційної політики;
- гарантії права на інформацію;
- основні види інформаційної діяльності;

- режими доступу до інформації;
- процедура інформаційного запиту;
- коло учасників інформаційних правовідносин, їхні права та обов'язки;
- питання охорони інформації;
- підстави відповідальності за делікти в інформаційній сфері; правові форми міжнародного співробітництва в галузі інформації; гарантії інформаційної безпеки України [29].

Але слід зазначити, що первинна редакція Закону про інформацію мала низку недоліків і прогалин, а саме – недосконалість понятійнокатегоріального апарату, полишення без уваги окремих видів інформаційної діяльності, суттєві вади мали місце щодо регулювання відносин з приводу обробки та захисту персональних даних та доступу до публічної інформації. Закон «Про інформацію» зазнавши суттєвих змін, які були спрямовані на створення належної правової бази для формування та реалізації державної інформаційної політики, зміцнення інформаційної безпеки, вдосконалення механізмів контролю за дотриманням законності, залишався системо утворюючим для галузі інформаційного права. На основі положень цього закону було прийнято цілу низку законів, що стосувались безпосередньо інформаційної безпеки, зокрема це Закони України: про друковані засоби масової інформації (пресу) в Україні [30], про науково-технічну інформацію [9], про телебачення і радіомовлення [32], про захист інформації в інформаційно-телекомунікаційних системах [33], про захист інформації в автоматизованих системах [34], про Національну програму інформатизації [35], про Концепцію Національної програми інформатизації [36], про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію [37], про основи національної безпеки України [38], в якому йшлося «про основні сфери національної безпеки», серед яких виокремлювалась й інформаційна, про телекомунікації [39], про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки [40], про Доктрину інформаційної безпеки України [41], а також інші закони та інформативно-правові акти, зокрема ратифіковані або

парафовані Україною Договір про безпеку і співробітництво в Європі, Договір «Відкрите небо», Угода про партнерство і співробітництво між європейським співтовариством і Україною, Додатковий протокол до Європейської конвенції про інформацію щодо іноземного законодавства, які зобов'язували здійснювати багатосторонній обмін інформацією, потребували створення загальнодержавних механізмів зберігання та споживання отриманої інформації в національних інтересах [42].

Зокрема Закон «Про Національну програму інформатизації» [35], визначив загальні засади формування, виконання та коригування Національної програми інформатизації як комплексу взаємопов`язаних окремих завдань (проектів) інформатизації, спрямованих на реалізацію державної політики та пріоритетних напрямів створення сучасної інформаційної інфраструктури України шляхом концентрації та раціонального використання фінансових, матеріально-технічних та інших ресурсів, виробничого й науково-технічного потенціалу держави, а також координації діяльності органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій усіх форм власності й громадян у сфері інформатизації та захисту інформаційної безпеки.

Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [40] було встановлено завдання створити цілісну систему законодавства, гармонізовану з нормами міжнародного права з питань розвитку інформаційного суспільства (р. Ш, п. 2 акта). Передбачалось за визначений період зробити суттєві кроки, спрямовані на вдосконалення регулювання суспільних інформаційних відносин загалом та окремих інститутів зокрема, захисту персональних даних, доступу до публічної інформації тощо.

Основні положення правового забезпечення захищеності інформації та відповідальності за її порушення знайшли своє відображення і відповідне обґрунтування, зокрема, в Кримінальному, Кримінального процесуальному, Цивільному, Господарському кодексі України та Кодексу України про адміністративні правопорушення.

Слід наголосити, що Головним законодавчим документом є Конституція України. В ст. 17 якої наголошено, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [43]. Крім того, саме Основний Закон України закріпив цілий комплекс прав і свобод людини і громадянина, що визначають її правовий статус у сфері інформаційних відносин.

Згодом відбулись значні зміни у вітчизняному інформаційному законодавстві з метою надання законодавчим реформам певного системного характеру [44]. Це стосувалось прийняття Законів України: «Про захист персональних даних» від 1 червня 2010 р. (із подальшими змінами) [45]; «Про доступ до публічної інформації» від 13 січня 2011 р [46]; «Про внесення змін до Закону України «Про інформацію» від 13 січня 2011 р. [47], яким було введено в дію нову редакцію базового інформаційного закону.

У контексті правонаступництва нова редакція Закону України «Про інформацію» [47] поряд із відкритістю, доступністю, достовірністю і повнотою інформації, свободою її обміну, свободою вираження поглядів і переконань, правомірністю одержання, використання, поширення, зберігання, захисту інформації та захищеністю особи від втручання в її особисте та сімейне життя основним принципом інформаційних відносин визначає також гарантованість права на інформацію (ст. 2 Закону). Окремо закріплене право кожного на інформацію із значно вже розширеним, у тому числі і порівняно із конституційним формулюванням, гарантії цього права (відповідно статті 5, 6 Закону). У світлі існуючої нагальної доцільності уточнення, доповнення, систематизації конституційних встановлень щодо гарантій цього права, закріплення узагальнених умов його реалізації на рівні закону має важливе значення.

У новій редакції Закону України «Про інформацію» визначено серед основних напрямів державної інформаційної політики, зокрема, забезпечення інформаційної безпеки України (ст. 3 закону). Судячи з тексту статті 3 нової редакції Закону, її розробники вирішили замінити «інформаційний суверенітет»

на «інформаційну безпеку». У нормах вказаного акта зазнав корекції перелік видів інформації з обмеженим доступом: нарівні з таємною інформацією такою визначається і службова інформація (ст. 21 закону). Нове законодавство містить, у порівнянні з закріпленим раніше у ч. 2 ст. 30 Закону України «Про інформацію» від 2 жовтня 1992 р., визначення ще одного виду інформації, а саме – конфіденційної інформації. Такою є інформація доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень (ч. 2 ст. 21 Закону). У зв'язку з цим, одним із найбільш принципових для нової редакції Закону є оновлене поняття інформації про персональні дані. Важливою позитивною новелою є те, що серед напрямів державної інформаційної політики з'явилося «забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони і захисту інформації».

Важливим етапом законодавчого врегулювання правовідносин стало також прийняття нової редакції Закону України «Про доступ до публічної інформації» [46]. Важливість цього законодавчого акта, в порівнянні із Законом України «Про інформацію», зумовлена сферою його дії: цей акт визначив порядок здійснення та забезпечення права на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, які в свою чергу є основними суб'єктами публічного адміністрування інформації з обмеженим доступом, і встановив необхідні й достатні умови для обмеження доступу до публічної інформації з метою забезпечення належної інформаційної безпеки. Певною мірою позитивним кроком є також закріплення переліку вимог щодо встановлення обмеження доступу до публічної інформації (ч. 2 ст. 6 Закону), що з деякою модифікацією відтворюють, зокрема, положення частини 3 ст. 34 Конституції України, яка встановила подібні конституційні обмеження щодо права кожного на свободу думки і слова, на вільне вираження своїх поглядів і переконань та права на інформацію.

Заслуговує на увагу проект Закону України «Про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю». У законопроекті

пропонувалось внести зміни до низки законодавчих актів, зокрема, до Кодексу України про адміністративні правопорушення, законів України «Про основи національної безпеки України», «Про телекомунікації» з метою формування засад державної політики у сфері забезпечення кібернетичної безпеки України, основних напрямів державної політики та основних функцій суб'єктів забезпечення національної безпеки в цій сфері, а також запровадження у законодавство нових термінів, зокрема «кібернетична безпека (кібербезпека)» та «кібернетичний простір (кіберпростір)». Цей законопроект знайшов своє втілення у Законі України «Про національну безпеку України» [48]. Зокрема у Статті 31. «Стратегія кібербезпеки України» визначено, що стратегія кібербезпеки України є документом довгострокового планування, в якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, підвищення ефективності основних суб'єктів забезпечення кібербезпеки, щодо виконання ними завдань у кіберпросторі.

Таким чином основна спрямованість національного законодавства у сфері забезпечення інформаційної безпеки свідчить, що більшість правових норм відповідають міжнародним стандартам, принципам і нормам її забезпечення Водночас чинна нормативно-правова база в інформаційній сфері потребує вдосконалення з метою усунення суперечностей і заповнення прогалин у законодавстві стосовно інформаційної безпеки держави, суспільства і громадян.

РОЗДІЛ 2
ТЕНДЕНЦІЇ І ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У ПУБЛІЧНОМУ УПРАВЛІННІ

2.1. Основні напрямки політики інформаційної безпеки

Для України сьогодні логічним кроком на шляху до забезпечення національного суверенітету є розробка цілісної гнучкої динамічної державної політики інформаційної безпеки, яка має враховувати багатоаспектність явищ інформаційної безпеки, перспективні тенденції змін інформаційного простору, особливості геополітичного становища, соціально-економічного стану країни та необхідні рівні ефективного і зручного (систематизованого) інформаційного законодавства. У ст.17. Конституції України зазначено: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» [43].

Державна політика забезпечення інформаційної безпеки України є невід'ємною складовою державної політики національної безпеки України і являє собою офіційно прийняту систему поглядів та практичну діяльність органів державної влади і управління, спрямовану на забезпечення такого стану соціальних суб'єктів, при якому дія будь-якої інформаційної загрози не призводить до зниження рівня їх інформаційної безпеки нижче припустимого, небезпечного з високою ймовірністю реалізації негативних інформаційних впливів.

Здійснення державної політики інформаційної безпеки має важливе значення для життєздатності держави, яка тоді є вищою, коли краще опрацьовані базові напрями цієї політики і шляхи їх реалізації у цій сфері. Виважений, науково-обґрунтований підхід до формування і реалізації сучасної політики інформаційної безпеки стає сьогодні найважливішим завданням у комплексі цілей державної політики.

Слід зазначити, що збалансована державна інформаційна політика України формується, виходячи з пріоритетності національних інтересів та загроз національній безпеці країни. Вона ґрунтується на засадах правової демократичної держави і впроваджується шляхом розробки та реалізації відповідних національних доктрин, стратегій, концепцій та програм згідно із чинним законодавством.

Захист інформаційної безпеки має здійснюватися, насамперед, шляхом проведення виваженої та збалансованої політики держави в інформаційній сфері, яка має три основні вектори: захист інформаційних прав і свобод людини, захист державної безпеки в інформаційній сфері та захист національного інформаційного ринку, економічних інтересів держави в інформаційній сфері та національних виробників інформаційної продукції [49,с. 146].

В цілому політика забезпечення інформаційної безпеки має будуватися на таких засадах:

− обмеження доступу до інформаційного ресурсу є винятком із загального принципу відкритості інформації й реалізуватися має тільки відповідно до чинного законодавства;

− створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

− підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;

− вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності;

− суб'єкти, які збирають, накопичують і обробляють персональні дані й конфіденційну інформацію, несуть відповідальність перед законом за збереження і використання;

− держава реалізує контроль за створенням і використанням засобів захисту інформації шляхом їхньої обов'язкової сертифікації та ліцензування діяльності в галузі захисту інформації;

− держава сприяє всебічному розвитку української мови як основного інструменту перетворення накопичених людством знань в інформаційний ресурс України [22].

− Основними цілями інформаційної політики України є *забезпечення*:

− захисту інформаційного суверенітету держави, особливо захисту національного інформаційного простору з інформаційним;

− рівня інформаційної достатності для прийняття рішень державними органами і громадянами;

− реалізації конституційних прав і свобод громадян, суспільства і держави [50].

З метою обґрунтування цілей інформаційної політики 4 лютого 1998 р. був прийнятий Законі України «Про Національну програму інформатизації» спрямований на їх реалізацію згідно з указами Президента України «Про рішення Ради національної безпеки і оборони України від 17 червня 1997 р. «Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин» від 21 липня 1997 р. № 663/97, 14 липня 2000 р. було прийнято рішення «Про вдосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади», а 6 грудня 2001 р. «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України», 27 січня 2016 р. була затверджена «Стратегія кібербезпеки України» [51], 25 лютого 2017 р. «Доктрина інформаційної безпеки України» [52].

Основні функції державної політики щодо інформаційної безпеки України полягали у:

– створенні елементів системи забезпечення інформаційної безпеки, що включає створення необхідних правових засад для побудови, розвитку та її функціонування;

– формуванні організаційної структури системи та її окремих елементів;

– визначенні та раціональному розподілі їх функцій;

– комплексному забезпеченні діяльності елементів системи (кадрове, фінансове, матеріальне, технічне, інформаційне та інші);

– підготовці елементів системи до виконання покладених на них функцій згідно з призначенням;

– управлінні діяльністю системи забезпечення інформаційної безпеки, яка включає вироблення стратегії і планування конкретних заходів щодо забезпечення інформаційної безпеки;

– організації і безпосереднім керівництві системою та її структурними елементами;

– оцінці результативності дій та витрат на проведення заходів щодо забезпечення інформаційної безпеки та їх наслідків;

– здійсненні планової та оперативної діяльності щодо забезпечення інформаційної безпеки, що включає визначення національних інтересів та їх пріоритетів в інформаційній сфері;

– прогнозуванні, виявленні та оцінці можливих загроз, дестабілізуючих чинників та конфліктів в інформаційній сфері, причин їх виникнення, а також наслідків їх прояву;

– запобіганні та усуненні впливу загроз та дестабілізуючих чинників на національні інтереси в інформаційній сфері;

– локалізації, деескалації та розв’язання інформаційних конфліктів;

– ліквідації наслідків інформаційних конфліктів або впливу дестабілізуючих чинників;

– міжнародному співробітництві в сфері інформаційної безпеки, яка включає розроблення нормативно-правової бази, що регулює інформаційні відносини між державами та їх взаємодію в галузі інформаційної безпеки;

– входженні в існуючі та утворенні нових двосторонніх і багатосторонніх структур (організацій), діяльність яких спрямована на спільне вирішення проблем інформаційної безпеки;

– участі у роботі керівних, виконавчих та забезпечувальних підрозділів цих структур (організацій), спільному проведенні планових та оперативних заходів [53].

Виконання повного переліку цих функцій були необхідною умовою ефективної реалізації державної політики із забезпечення інформаційної політики. Основними принципами державної політики щодо забезпечення інформаційної безпеки України, згідно з Концепцією інформаційної безпеки України, є: верховенство права; пріоритетність захисту прав і свобод людини і громадянина в інформаційній сфері; своєчасність і адекватність заходів захисту життєво важливих національних інтересів України від реальних і потенційних загроз інформаційній безпеці; захист інформаційного суверенітету України; свобода думки і слова та вільне вираження своїх поглядів і переконань; свобода збирати, зберігати, використовувати та поширювати інформацію; захищеність особи від втручання в її особисте та сімейне життя; обмеження доступу до інформації виключно на підставі закону; гармонізація особистих, суспільних і державних інтересів, відповідальність всього Українського народу за забезпечення інформаційної безпеки; розмежування повноважень, взаємодія та відповідальність державних і недержавних суб’єктів забезпечення інформаційної безпеки; пріоритетність розвитку та поширення національних інформаційних технологій, ресурсів, продукції та послуг, а також політика постійного поліпшення кількості та технічної якості каналів передачі інформації; можливість залучення в інтересах забезпечення інформаційної безпеки України систем і механізмів міжнародної та колективної безпеки; гармонізація інформаційного законодавства з нормами міжнародного права і правовими актами Європейського Союзу. сприяння розвитку в національному інформаційному просторі контенту, який підтримує збереження і захист

загальнолюдських цінностей, інтелектуальний, духовний і культурний розвиток Українського народу [54].

Щодо головних напрямів державної політики з питань національної безпеки України в інформаційній сфері, то вони полягають у:

− забезпеченні інформаційного суверенітету України;

− удосконаленні державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів;

− впровадженні новітніх технологій у цій сфері, наповнення внутрішнього, а також світового інформаційного простору достовірною інформацією про Україну;

− вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України та інші [38].

Виключне значення набувало затвердження національної стратегії державної політики із забезпечення інформаційної безпеки та реалізація положень плану її здійснення, а також завдань поетапного інституційного забезпечення інформаційної безпеки в Україні, що є ключовими напрямками державної політики на шляху переходу українського суспільства до життєдіяльності в сучасних умовах, а також особливостей використання інформаційно-комунікаційних технологій у всіх сферах його функціонування [55; 56; 57].

Стратегія реалізації політики інформаційної безпеки вибудовується на засадах впровадження проблемно-цільового методу в інформаційній діяльності органів державного управління. Сутність такого підходу полягає в тому, що виходячи із законодавчо встановлених меж компетенції, а також державних пріоритетів та аналізу обставин, що склалися, вибудовується дерево цілей, яких необхідно досягти за певний період [58].

З метою ефективного здійснення державної політики у сфері забезпечення інформаційної безпеки 8 лютого 2002 р. була створена Міжвідомча комісія з

питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України як консультативно-дорадчий орган, що мала своїми завданнями:

− аналіз стану і можливих загроз національній безпеці України в інформаційній сфері та узагальнення міжнародного досвіду з формування та реалізації інформаційної політики;

− аналіз здійснення галузевих програм і виконання заходів, пов'язаних з реалізацією міністерствами та іншими центральними органами виконавчої влади державної політики в інформаційній сфері;

− розроблення та внесення Президентові України та Раді національної безпеки і оборони України пропозицій щодо визначення національних інтересів України в інформаційній сфері, концептуальних підходів до формування державної інформаційної політики та забезпечення інформаційної безпеки України;

− здійснення системних заходів, спрямованих на вдосконалення інформаційної політики України, реалізацію державної стратегії розвитку і захисту національного інформаційного простору та входження України у світовий інформаційний простір;

− удосконалення системи правового та наукового забезпечення інформаційної безпеки України;

− розвиток інформаційної інфраструктури держави, з питань модернізації її матеріально-технічної бази та належного фінансового забезпечення;

− організація та порядок міжвідомчої взаємодії міністерств, інших центральних органів виконавчої влади у сфері забезпечення інформаційної безпеки;

− удосконалення системи оперативного інформаційно-аналітичного забезпечення Президента України (в тому числі альтернативною інформацією) у сфері національної безпеки і оборони [50].

Необхідність посилення інформаційної безпеки зумовили появу Міністерства інформаційної політики, яке було створено 2 грудня 2014 року і покликане забезпечувати інформаційний суверенітет всередині країни та за її межами, ефективне використання державних інформаційних ресурсів, здійснювати реформування засобів масової інформації щодо поширення суспільно важливої інформації [59]. Були визначені основні функції міністерства, серед яких:

− формування державної політики щодо діяльності засобів масової комунікації;

− розробка стратегії інформаційної політики держави та забезпечення її реалізації;

− формування державної політики у сферах поширення інформації, просвітницької діяльності та використання національних інформаційних ресурсів;

− створення умов для розвитку інформаційного суспільства, державний контроль за діяльністю ЗМК незалежно від їх підпорядкування і форми власності [60,с.66].

Важливе значення для здійснення державної політики із реалізації інформаційної безпеки мала розробка програми її забезпечення, яка передбачала розподіл функцій між суб’єктами, відповідальними за неї, та передбачала їх відповідальність за її керування у контексті необхідної реалізації загального плану безперервності функціонування системи забезпечення інформаційної безпеки держави. Якщо наносилась шкода в результаті недосконалості інформаційних відносин, використанні неякісної інформації тощо, то це свідчило про зниження інформаційної безпеки. Це давало змогу розглядати цей процес як не вирішення проблеми гарантування інформаційної безпеки в Україні:

− недосконаліть інформаційної політики та політики інформаційної безпеки держави;

− недосконаліть нормативно-правової бази в сфері інформаційних відносин та інформаційної безпеки;

– недостатню розвиненість інформаційної інфраструктури держави;

– введення іноземними державами обмежень стосовно України щодо розповсюдження інформації та отримання нових інформаційних технологій;

– протиправна діяльність посадових осіб, різних формувань та груп у сфері інформаційних інтересів громадян та держави;

– недосконаліть державної системи забезпечення інформаційної безпеки;

– можливість виникнення непередбачених ситуацій у системах та процесах, що базуються на використані інформаційних технологій [61].

Програма державної політики щодо забезпечення інформаційної безпеки спрямовувалась на вирішення таких основних завдань:

– формування правових, організаційних, науково-технічних, економічних, фінансових, методичних і гуманітарних передумов розвитку інформатизації;

– застосування та розвиток сучасних інформаційних технологій у різних сферах суспільного життя України;

– формування системи національних інформаційних ресурсів;

– створення загальнодержавної мережі інформаційного забезпечення науки, освіти, культури, охорони здоров`я тощо;

– створення загальнодержавних систем інформаційно-аналітичної підтримки діяльності органів державної влади та органів місцевого самоврядування;

– підвищення ефективності вітчизняного виробництва на основі широкого використання інформаційних технологій;

– формування та підтримка ринку інформаційних продуктів і послуг; інтеграція України у світовий інформаційний простір [62].

В питаннях інформаційно безпеки Україна активно співпрацювала зі світовими організаціями безпеки та охорони інформації. Зокрема, Державна служба спеціального зв’язку та захисту інформації України й компанія Microsoft 22 грудня 2014 року уклали Угоду про співробітництво з питань безпеки

(Government Security Program). У рамках цієї програми держава отримала доступ до інформації, яка збирається в центрі Безпекового реагування Microsoft, про нові кіберзагрози, джерела мережевих атак. Національна інформаційна політика в контексті євроінтеграційної стратегії України сприяла наближенню до європейських стандартів у сфері інформації та комунікації, зумовлювала динаміку змін в інформаційній сфері держави, що стимулювало позитивні зрушення у використанні нових комунікаційних послуг, а також значною мірою впливала на вдосконалення інформаційного законодавства, та належне забезпечення інформаційної безпеки [63]. Це свідчило про значення поглиблення співпраці з країнами ЄС у вирішенні завдань національної політики із забезпечення інформаційної безпеки держави, суспільства і населення.

Загалом, державна політика забезпечення інформаційної безпеки України (рис. 2.1) полягає у:

− забезпеченні конституційних прав людини на доступ до інформації, використанні інформації в інтересах здійснення не забороненої чинним законодавством діяльності, фізичного, інтелектуального й духовного розвитку, а також; у захисті інформації, яка стосується особистої безпеки громадянина;

− створенні умов для гармонійного розвитку інформаційної структури, для реалізації конституційних прав і свобод людини й громадянина у сфері отримання інформації та використання її з метою забезпечення непорушності конституційного ладу, культурного й наукового потенціалу;

− здійснення інформаційного забезпечення державної політики України, пов'язане з доведенням до української та міжнародної громадськості достовірної інформації про державну політику України, її офіційної позиції стосовно соціальне значущих подій українського та міжнародного життя, з забезпеченням доступу громадян до відкритих інформаційних ресурсів;

− розвиток сучасних інформаційних технологій, вітчизняної індустрії інформації, в тому числі індустрії засобів інформатизації, телекомунікації і зв'язку, забезпечення потреби внутрішнього ринку її продукцією і вихід цієї

продукції на світовий ринок, а також; забезпечення накопичення, зберігання та ефективного використання вітчизняних ресурсів;

– захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки інформаційних і телекомунікаційних систем, як наявних, так і тих, що створюються на території України.

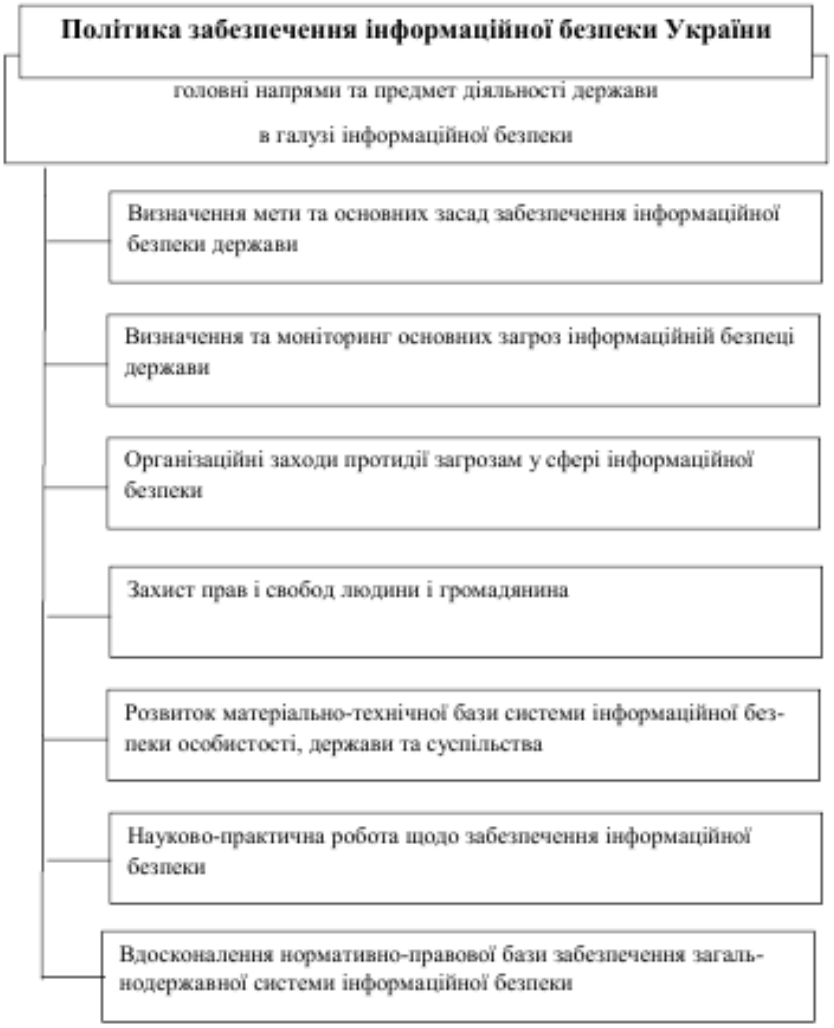

Рис. 2.1. Напрями державної політики із забезпечення інформаційної безпеки України

Отже, як показано вище, за роки незалежності в Україні створено основні елементи державної політики щодо забезпечення інформаційної безпеки, напрацьовано нормативно-правову базу їх діяльності, визначено основні функції й повноваження державних органів в інформаційній сфері. Головними напрямами політики інформаційної безпеки в країні визначено: формування та

впровадження правових, організаційних, науковотехнічних, економічних, фінансових, технологічних, методичних умов її реалізації з урахуванням світових тенденцій.

2.2. Міжнародні норми та практика забезпечення інформаційної безпеки

Сьогодні основні для розуміння забезпечення міжнародної інформаційної безпеки міжнародно-правові норми закріплені у Статуті ООН, а також інших міжнародних нормативно-правових актах, що формують правовий базис для розв'язання збройних конфліктів, визначають засади міжнародного гуманітарного права, а також регулюють процес упередження та боротьби з міжнародним тероризмом. Таким чином, серед основних правових принципів, що пов'язані з міжнародними інформаційними відносинами в частині гарантування інформаційної безпеки називають такі: «принцип суверенної рівності держав у сфері використання інформаційних ресурсів, забезпечення інформаційного суверенітету держави та рівноправної участі в переговорних процесах щодо встановлення і кодифікації міжнародно-правових документів у сфері інформаційної безпеки»; «принцип невтручання у внутрішні справи інших держав, неприпустимість інформаційної інтервенції з метою проведення спеціальних інформаційних кампаній, ворожої пропаганди та поширення деструктивної чи спеціально спрямованої інформації» [29]; «принцип заборони застосування сили або загрози силою, який забороняє використання інструментів інформаційного впливу проти територіальної цілісності чи політичної незалежності будь-якої держави»; «принцип мирного врегулювання міжнародних спорів, який зобов'язує держави до превентивної дипломатії або переведення збройного конфлікту на переговорний рівень за допомогою інструментів інформаційного впливу»; «принцип територіальної цілісності та непорушності кордонів, який стосується визначення меж національного інформаційного простору та заходів захисту від несанкціонованого втручання ззовні»; «принцип

дотримання фундаментальних прав і свобод людини, який визначає конституційні та спеціальні норми, а також норми міжнародних договорів щодо свободи слова та вільного обігу інформації, незалежності і плюралізму міжнародних мас-медіа, свободи вираження, заборони цензури та захисту конфіденційності інформаційних ресурсів»; «принцип самовизначення народів і націй, який встановлює права національних меншин на культурну самобутність та інформаційну діяльність; принцип міжнародного співробітництва, який зобов'язує держави співпрацювати задля зміцнення миру та міжнародного взаєморозуміння, розвитку глобальної інфраструктури з метою досягнення інтересів людства». Отже, це комплекс політичних, економічних і соціокультурних принципів, важливих для міжнародного порозуміння.

Відповідна тенденція закріпилася і у резолюціях Генеральної асамблеї ООН, а саме Резолюція ГА ООН 53/576 (1998 р.) «Роль науки і техніки в контексті міжнародної безпеки, роззброєння та інших, пов'язаних з цим сфер»; Резолюція ГА ООН 54/49 (1999 р.) «Досягнення у сфері інформатизації і телекомунікації в контексті міжнародної безпеки»; Резолюція ГА ООН 55/28 (2000 р.) «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки»; Резолюція ГА ООН 60/45 (2005 р.) «Досягнення у сфері інформатизації і телекомунікацій у контексті міжнародної безпеки» та багато інших.

В резолюції 1989 р. № 44/21 Генеральна Асамблея ООН звернулась до всіх держав із закликом сприяти міжнародній співпраці «в усіх напрямах забезпечення міжнародної безпеки, підтвердила дієвість і значення Статуту ООН, необхідність дотримання основних його принципів, висловилась за співробітництво в рамках Організації та її основних структур» з метою знайти різноманітні «підходи до зміцнення принципів і систем міжнародної безпеки на основі нормативних документів ООН».

У 1999 році на 54-ій сесії ГА ООН було прийнято оновлений проект резолюції (A/RES/54/49) «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки», який вперше вказав на загрози міжнародної інформаційної безпеки відносно не тільки до цивільної, але і до військової сфер.

Поряд із зазначеним, за результатами роботи сесії було опубліковано проект «Принципів, що стосуються міжнародної інформаційної безпеки» (A/55/140У). Принципи є свого роду робочим варіантом кодексу поведінки держав в інформаційному просторі, створюючи для них відповідні моральні зобов'язання, що також закладають основу для широких міжнародних переговорів під егідою ООН і інших міжнародних організацій з проблем міжнародної інформаційної безпеки (МІБ). У них міститься необхідна понятійна база з предмету МІБ, наводяться основні визначення: міжнародної інформаційної безпеки, погроз інформаційній безпеці, інформаційної зброї, інформаційної війни, міжнародного інформаційного тероризму та злочинності [28].

Фактично на рівні цих резолюцій йдеться про незастосування сили, але одночасно й небезпеки нового покоління інформаційної зброї, коли вкрай необхідна якісна система міжнародного контролю за інформаційними озброєннями. Передбачалося узгодити позиції світового співтовариства щодо проблеми потенційного воєнного використання інформаційно-комунікаційних технологій, вдосконалення існуючих і нових систем озброєнь. У таких резолюціях помітно, як міжнародна спільнота шукає і нових методів для гарантій невтручання у внутрішні справи держав, що ускладнюється з розвитком власне інформаційних впливів. Тому розглядаються усі доступні можливості для створення міжнародної системи моніторингу інформаційних загроз, для забезпечення фундаментальних прав і свобод в інформаційній сфері, але й попередження випадків використання високих технологій з протиправною метою. Цей специфічний міжнародно-правовий режим інформаційної безпеки відтак мусить передбачити оновлене міжнародно-правове регулювання інформаційної безпеки. Безпосередньо на рівні ООН це також кодифікація спеціальних принципів і норм, які склалися на основі Статуту ООН, а також оновлення існуючих і укладання нових угод у сфері інформаційної безпеки.

Упорядкування і стабілізація міжнародного співробітництва держав в інформаційній сфері – складне та багатогранне питання, що потребує окремого дослідження. Сучасні технології мають транскордонний характер, відтак і

злочини стосуються міжнародної безпеки та стабільності в цілому, а не лише окремих систем права. І. Забара, наприклад, констатує функціонування двох провідних напрямів міжнародно-правового регулювання використання інформаційно-комунікаційних технологій: інформаційний («змістовний») та комунікаційний («технічний»). У міжнародно-правовій проблематиці інформаційної безпеки вони розглядаються з позицій протидії використанню ІКТ, що спрямовані на шкоду 1) основним правам і свободам людини та 2) критично важливим структурам держав [47].

Інформаційний напрям передбачає протидію транскордонному поширенню за допомогою інформаційно-комунікаційних технологій матеріалів, що суперечить принципам і нормам міжнародного права, розпалюють міжнаціональну, міжрасову, міжконфесійну ворожнечу, поширюють расистські, ксенофобські ідеї. Це письмові матеріали чи зображення або будьяка демонстрація положень, які підбурюють до ненависті, дискримінації, насилля проти будь-якої особи або групи осіб. Такі дії, як слушно зауважують фахівці, можуть відбуватися і через використання інформаційної інфраструктури для пропаганди насильства, залякування, пригнічення, нав’язування певних моделей поведінки; для екстремістських та терористичних актів; повалення державного ладу тощо. Комунікаційний напрям передусім орієнтований на боротьбу зі зловмисним використанням комунікаційних систем та інформаційних ресурсів, що має негативний вплив на політичну, фінансову, соціально-економічну та інші сфери життя сучасного людства.

Відтак вчені і практики нині звертають увагу на охоронні та забезпечувальні норми як частину міжнародного інформаційного права, що розвиваю сучасну кібер-стабільність і кібер-мир (зокрема, окремі норми в Резолюціях ГА ООН «Створення глобальної культури кібербезпеки і захист найважливіших інформаційних структур» №57/239 (2002), № 58/199 (2003), № 64/211 (2009), Декларації Еріче про принципи кібер-стабільності та кібер-миру (2009), Глобальній програмі кібербезпеки Міжнародного союзу електрозв’язку (2007) тощо.

Відтак, усвідомлюючи ті зміни суспільно-політичного життя, що спричиняє сучасне цифрове середовище, високі технології у сукупності з глобалізаційними процесами, Радою Європи підготовлено Конвенцію про кіберзлочинність. Вона відкрита до підписання у листопаді 2001 року, набула чинності 1 липня 2004 року, підписана Україною у квітні 2005 року та ратифікована у грудні 2006 року. Через цей документ міжнародна спільнота наголошує, що держави мають вжити усіх заходів, «для встановлення кримінальної відповідальності відповідно до їх внутрішнього законодавства за навмисний доступ до цілої комп'ютерної системи або її частини без права на це» (ст. 2). Зокрема йдеться про кримінальну відповідальність за правопорушення, пов'язані з незаконним доступом, нелегальним перехопленням і втручанням у комп'ютерні дані чи систему; також кіберзлочинами названо зловживання пристроями, підробку та шахрайство, пов'язані з комп'ютерами, дитяча порнографія, порушення авторських прав та деякі інші.

Відзначимо, що зрештою сьогодні співзвучна цим проблемам і нормотворчість в Україні. Вітчизняним законодавством визнано і достатньо точно визначено сутність таких небезпек як кіберзлочин (суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України); кібератака (навмисні дії, які здійснюються за допомогою засобів електронних комунікацій та спрямовані на порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки і режиму функціонування комунікаційних і технологічних систем тощо); кібершпигунство (шпигунство, що здійснюється у кіберпросторі або з його використанням); кібертероризм; кіберзагроза та багато інших пов'язаних явищ.

У міжнародній площині, не лише ООН та Рада Європи займаються питаннями правового забезпечення інформаційної безпеки. До проблематики активно долучається все більше число міжнародних організацій. Наприклад, з

ініціативи так званої «Великої вісімки» (на той час G8) у 2000 р. ухвалено «Окінавську хартію глобального інформаційного суспільства» [204]. У документі передусім сформульовано прагнення солідарними зусиллями (в державному і приватному секторах) ліквідувати міжнародний розрив в галузі інформації і знань, наблизити прогрес, «раціональний розвиток інформаційного суспільства» через політичне співробітництво. Хартія містить змістовні розділи щодо 1) використання можливостей цифрових технологій; 2) подолання електронно-цифрового розриву; 3) сприяння загальній участі у використанні сучасних технологій для досягнення взаємодоповнюючих цілей зі стійкого економічного зростання, підвищення суспільного добробуту, стимулювання соціальної злагоди, зміцнення демократії, транспарентного і відповідального управління, прав людини, розвитку культурного різноманіття, зміцнення міжнародного миру; 4) подальшому розвитку зі створення безпечного і вільного від злочинності кіберпростору.

Глави держав і урядів 56 держав-учасниць ОБСЄ на саміті 2010 р. також приділили певну увагу проблемам інформаційного суспільства. Зокрема заради розвитку вільного, демократичного, загального і неподільного євроатлантичного і євразійського співтовариства безпеки, вони вкотре задекларували актуальність низи транснаціональних загроз. Відтак серед таких проблем як – тероризм, організована злочинність, нелегальна міграція, поширення зброї масового ураження, незаконний оборот легкої і стрілецької зброї, наркотиків і торгівля людьми – на рівні виокремлено і кіберзагрози. Для протистояння їм, так само як і іншим небезпекам в військово-політичній, економіко-екологічній сферах, у галузі прав людини і основних свобод, необхідна все більша міжнародна єдність цілей і дій.

Водночас багато держав у розбудові власної систем інформаційної безпеки враховують не лише спільні орієнтири глобального розвитку, але також (а іноді й передусім): національні інтереси; накопичений досвід інформаційних протистоянь і захисту інформаційного суверенітету; реальні та потенційні загрози для конкретного суспільства, національної безпеки та безпеки держави;

національні культурні й духовні цінності, традиції тощо. Не варто забувати й про об’єктивні фактори, які також унеможливлюють однакові підходи до проблеми у всіх країнах світу. Такими зокрема є рівень інформаційного розвитку країни, її технологічні потужності, підготовка до інформаційних викликів широких верств, суспільства, державних службовців, комунікаційні можливості тощо. Попередні застереження, висловленні світовими лідерами галузі про цифрову нерівність тут як ніколи доречні.

Демократичні держави володіють ширшими можливостями, розвинутішими правовими механізмами реалізації національних інтересів, в тому числі й в інформаційній сфері. На думку вчених, такі країни вигідно відрізняє: 1) чітке визначення пріоритетів національних інтересів в інформаційній сфері, 2) гарантування інформаційного суверенітету держави, 3) регламентація порядку використання національних інформаційних ресурсів, 4) створення загальної системи охорони та захисту інформації з обмеженим доступом, 5) поширення духовних та культурних цінностей на населення інших країн, 6) обмеження спроб зовнішньої інформаційної та духовної експансії [11].

Стратегії та тактики інформаційної політики та інформаційної безпеки держав у політико-правовому полі можуть відрізнятися. Часто науковці, як приклад у цьому зв’язку, наводять сучасний досвід Великій Британії.

Продумана, деталізована система забезпечення інформаційної безпеки цієї держави реалізується через дієві механізми захисту прав та свобод громадян у інформаційній сфері, гарантії діяльності медіа, громадських організацій. Водночас пріоритет національної безпеки тут також дуже виразний, тому в національних інтересах згадані вище суб’єкти за законом мають і чітко окреслені межі діяльності. Законодавчо регулюються питання захисту інформації, збереження державної таємниці, мереж і телекомунікацій, окремий Кодекс визначає практики доступу до урядової інформації.

Спільний європейський простір також зобов’язує держави-члени ЄС адаптовувати нормативно-правові положення до спільних вимог, які встановлені і в інформаційній сфері, а також готовність співпрацювати над розробкою

спільних, в тому числі й ширших міжнародних стратегій (документів, інституцій, механізмів), які б зміцнювали довіру, прозорість й безпечність глобального інформаційного простору, узгоджували діяльність держав у спільному кіберпросторі. Україна також орієнтується на ці високі стандарти інформаційної безпеки.

Прикладом для наслідування в окремих аспектах інформаційної політики може слугувати й досвід ФРН. Тут ще у 2011 р. прийнята Стратегія кібербезпеки, створено Центр кіберреагування, узгоджена інформаційнобезпекова політика уряду та державного секретаріату, а також інших органів влади, активно розвиваються механізми захисту інфраструктури стратегічного значення, налагоджується двостороння співпраця державного сектору з приватним у боротьбі проти кіберзлочинності. Комплексний підхід, на думку фахівців, дозволяє федеративному уряду ФРН забезпечити оперативне виявлення, реагування та локалізацію інформаційних атак, системно захищати суспільство від деструктивних кібервпливів та небезпечних інцидентів, запроваджувати кращі інформаційні технології у всіх сферах суспільного життя, зокрема й розвивати електронну демократію тощо.

Нерідко у контексті осмислення різних досвідів становлення політикоправових відносин в інформаційній сфері вчені з пострадянського простору наводять і приклад Франції. У цій країні велика відповідальність щодо регулювання відповідних проблем покладається на узгоджену діяльність Міністерства внутрішніх справ та Міністерства оборони, тобто є комплексна візія внутрішніх та зовнішніх інформаційних загроз, розуміння їх взаємозв’язаності. Політико правові механізми закладені в основу достатньо дієвої системи безпеки інформації та попередження комп’ютерних злочинів. Законодавчо окремо врегульовано питання про електронні комунікації, зокрема нормами забезпечується контроль за передачею інформації в радіочастотному просторі. Вчені загалом вирізняють два головні акценти у правовому забезпеченні інформаційної безпеки Франції: 1) захист національного інформаційного простору, в тому числі й обмеження іноземної присутності в інформаційній сфері;

2) культурна дипломатія інформаційними засобами, зокрема поширення національних інтересів у франкомовних країнах Африки, Азії та Латинської Америки.

Сполучені Штати Америки спрямовують свою інформаційну політику на впорядкування інформаційних потоків у політичній, економічній та військовій галузях задля забезпечення збалансованості між державним контролем і свободою інформаційної діяльності. Сформовано законодавчу базу забезпечення інформаційної безпеки. Зокрема, йдеться про регламентацію основ такого забезпечення (закони «Про удосконалення інформаційної безпеки», «Про комп'ютерну безпеку», «Про комп'ютерне шахрайство і зловживання»); регулювання інформаційних відносин та порядок доступу до закритої інформації (закони «Про свободу інформації», «Про таємницю», «Про право на фінансову таємницю», «Про охорону особистих таємниць» «Про висвітлення діяльності уряду»). Наведені вище закони формують правову основу для прийняття підзаконних нормативно-правових актів, націлених на реалізацію єдиної державної політики у сфері інформаційної безпеки.

Важливим інститутом забезпечення спільного стратегічного бачення у цій сфері є Департамент внутрішньої безпеки США (Department of Homeland Security), що в цілому реалізує координацію діяльності державних органів, громадських і всіх приватних структур, які покликані до захисту інформаційного простору федерації та поширення цінностей інформаційної політики цієї наддержави за її межами. Особливо слід наголосити на позиції Сполучених Штатів стосовно ворожих дій в кіберсередовищі. Це – право використовувати будь-які засоби: дипломатичні, політичні, воєнні та економічні, які є адекватними і не суперечать міжнародному законодавству для захисту країни, союзників, партнерів та інтересів США.

Отже, говорячи про формування правових основ і гарантій міжнародної інформаційної безпеки, слід визнати, що наразі можна засвідчити різні позиції провідних держав сучасності щодо розуміння потенційних загроз в інформаційних озброєннях та їх використанні проти критично важливих сфер

життєдіяльності суспільства. Зважаючи на це, на 54-й сесії Генеральної Асамблеї ООН було ухвалено оновлену резолюцію 54/49 «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки», на підставі якої концепція світової інформаційної безпеки набула визнання як глобальна проблема сучасності. Мотивацією для прийняття резолюції стало усвідомлення принципово нових потенційних загроз для міжнародного миру під впливом науково-технологічного прогресу та глобальної взаємозалежності усіх сфер життєдіяльності міжнародного співтовариства. У цій резолюції державам-членам було запропоновано висловитися щодо проблем інформаційної безпеки, дослідити технології загроз у цій сфері, у тому числі протиправне застосування інформаційних і комунікаційних систем та ресурсів, розробити загальноприйнятні принципи, спрямовані на зміцнення безпеки та посилення боротьби з інформаційним тероризмом і злочинністю.

Втім питання на цьому вочевидь не було вичерпаним, а в нових інформаційних реаліях ще гостріше постало перед світовою спільнотою. Уніфіковані норми щодо правового регулювання міжнародної інформаційної безпеки стають необхідністю нашого часу, що характеризується всеохоплюючою глобалізацією і потужними антиглобалізаційними рухами, зростанням гострих протистоянь між ними, в тому числі й в інформаційному просторі; порушенням територіальної цілісності і інформаційного суверенітету держав, поєднанням конвенційних і не конвенційних засобів сучасної війни; зрештою дрібними кіберзлочинами та масштабними хакерськими атаками, масованим інтелектуальним піратством тощо Тому вже 69-а сесія Генеральної Асамблеї ООН 2014 р. «вітає початок роботи» Групи урядових експертів з досягнень в сфері інформатизації і телекомунікацій в контексті міжнародної безпеки, але також закликає усі держави-члени приймати до уваги її оцінки і рекомендації; вчасно інформувати про загальну ситуацію у сфері інформаційної безпеки, національні зусилля для її зміцнення, усіляко сприяти збереженню вільного потоку інформації, відповідально ставитися до використання інформаційно-комунікаційних технологій в конфліктах, політичних взаємодіях тощо.

РОЗДІЛ 3
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОРГАНАХ ПУБЛІЧНОГО УПРАВЛІННЯ

3.1. Технологія виявлення загроз інформаційній безпеці та механізми їх попередження й усунення

Виявлення, попередження та нівелювання інформаційних загроз інформаційного характеру сьогодні перетворюється в першочергове завдання кожної держави. Цьому безперечно має сприяти технологія з'ясування загроз інформаційної безпеки, яка являє собою належний комплекс взаємозалежних технологічних, а також інженерних дисциплін, що визначають методи їх ефективного виявлення. Сучасні технології виявлення наявних загроз інформаційній безпеці, без сумніву, сприяють розв'язанню добре структурованих задач забезпечення інформаційної безпеки країни.

За умови швидкого формування, а також й розвитку інформаційного суспільства в країні особливого значення набувають проблеми інформаційної безпеки, передусім протидія інформаційним загрозам. З'ясування сучасних загроз інформаційній безпеці української держави ґрунтується на наукових здобутках таких відомих дослідників як зокрема: О. Бандурка, В. Горбулін, Є. Скулиш, І. Івченко, Р. Калюжний, А. Качинський, В. Ліпкан, В. Пилипчик та інших, які присвятили свої праці питанням забезпечення національної безпеки. Організація протидії загрозам інформаційній безпеці також стала предметом досліджень таких учених, як В. Бут, В. Домарєв, М. Живко, М. Танцюра, В. Цимбалюк [66].

Інформаційні загрози являють собою сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам держави, суспільства і особистості в інформаційній сфері. Враховуючи те, що інформаційна безпека є невід'ємною складовою національної безпеки, вона потребує застосування відповідного механізму щодо виявлення інформаційних загроз, взагалі, та

з’ясування їх сутності зокрема [67]. Відповідно ці загрози потребують відповідної класифікація за характером їх виникнення.

Зокрема В. Ліпкан пропонує класифікувати загрози інформаційній безпеці відповідно до загальної класифікації загроз національній безпеці за структурою впливу: системні, структурні та елементні; за характером реалізації: реальні, потенційні, здійснені, уявні; за ставленням до них: об’єктивні та суб’єктивні; за об’єктом впливу – держава, суспільство і особа.

Л. Євдоченко, формуючи свій власний підхід до класифікації інформаційних загроз, визначає і класифікує їх за кількома критеріями: за способом впливу на об’єкти інформаційної безпеки (інформаційні, фізичні й програмно-математичні, організаційно правові); за джерелами надходження (внутрішні та зовнішні); за характером вияву (політичні, економічні, організаційно-технічні).

Загрози інформаційній безпеці, за визначенням В. Горбуліна, можуть бути класифіковані за різними підставами, що висвітлює їх складну та багатошарову систему. Зокрема ці загрози класифікуються: за місцем знаходження джерела, як зовнішні та внутрішні;

− за масштабами можливих наслідків: загальнонаціональні, регіональні, локальні, поодинокі;

− за ступенем сформованості (потенційні, реальні);

− за ступенем суб’єктивного сприйняття, це завищені, занижені, мінімальні, умовні, адекватні;

− за характером виникнення (загрози природного, техногенного й соціального характеру);

− за сферами життєдіяльності, це загрози в економічній, політичній, оборонній, міжнародній, соціальній, інформаційній, науковотехнічній, екологічній, культурній і духовній сферах.

О. Золотар запропоновано класифікацію інформаційної безпеки за територіальною ознакою: інформаційна безпека громадян України, що проживають АР Крим та на тимчасово окупованих територіях; інформаційна

безпека військовослужбовців та інших осіб, що безпосередньо беруть участь у бойових діях, членів їх сімей, а також мирного населення в зоні бойових дій і на територіях, до них прилеглих та інформаційна безпека населення України, що проживає на «мирних: територіях.

Загрози національній безпеці України в інформаційній сфері це – сукупність умов та чинників, які становлять небезпеку життєво важливим інтересам держави, суспільства і особи через можливість негативного інформаційного впливу на свідомість та поведінку громадян, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру. Їх можна трактувати як сукупність внутрішніх та зовнішніх умов, які можуть нанести шкоду інтересам особистості та суспільства через небажані інформаційні атаки на відповідні об’єкти інформаційної інфраструктури держави. Поділу на внутрішні й зовнішні підлягають передусім джерела загроз. Їх науковці поділяють на три групи:

− перша група – це джерела загроз інформаційній безпеці особистості через розширення можливості маніпулювання свідомістю людини шляхом формування навкруг неї індивідуального «віртуального інформаційного простору», а також можливість використання технологій впливу на її психічну діяльність;

− друга група − джерела загроз інформаційній безпеці суспільства, які виявляються шляхом ускладнення інформаційних систем і мереж зв’язку, критично важливих інфраструктур забезпечення життя суспільства. Це зокрема, навмисні і ненавмисні помилки, збої і відмови техніки і програмного забезпечення, шкідливий вплив зі сторони злочинних структур і кримінальних елементів; розширення масштабів вітчизняної і міжнародної комп’ютерної злочинності;

− третя група − це джерела, які становлять загрозу інформаційній безпеці держави з допомогою отримання протиправного доступу до відомостей, що складають державну таємницю та іншу конфіденційну інформацію, розкриття яких може завдати їй значних збитків.

Оптимальним видається розглядати класифікацію інформаційних загроз за ознакою характеру джерела виникнення та стимулювання небезпеки, тобто класифікувати об'єктивні та суб'єктивні типи джерел інформаційних загроз. До них, насамперед слід віднести, як головну інформаційну загрозу національній безпеці, це загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості, з метою нав'язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони напрямку. Власне, це є загроза суверенітету України в життєво важливих сферах суспільної й державної діяльності, що реалізовується на інформаційному рівні.

В Указі Президента України «Про Доктрину інформаційної безпеки України» серед інших виокремлено такі загрози інформаційній безпеці України:

- поширення викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;
- зовнішні деструктивні інформаційні впливи на суспільну свідомість;
- деструктивні інформаційні впливи, які спрямовані на власне підрив конституційного ладу, суверенітету, а також територіальної цілісності й недоторканності України;
- прояви сепаратизму в ЗМІ, мережі інтернет за етнічною, мовною, релігійною та іншими ознаками.

Чинна Стратегія національної безпеки України серед основних загроз національній безпеці, які мають безпосередній стосунок до інформаційної сфери, визначає агресивні дії Росії, що підривають суспільно-політичну стабільність з метою знищення держави Україна й захоплення її території, в тому числі інформаційно-психологічну війну, приниження української мови й культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу, а також ведення інформаційної війни проти України, відсутність цілісної

комунікативної політики держави, недостатній рівень медіакультури 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.

Загальна мета російських центрів, у яких розробляються концепції та плани інформаційної війни – створити в Україні плацдарми впливу на українську політику, шляхом просування політиків, які виконуватимуть російське замовлення, або хоч би не протистоятимуть Росії у разі конфлікту економічних, політичних чи дипломатичних інтересів. Для цього центрами розробляються загальні концепції, які пізніше деталізуються, допасовуються до обставин поточного моменту та доводяться до виконавців на місцях.

В. Гусаров виокремлює такі напрями інформаційних атак Росії проти України:

− нав’язування думок про неспроможність української влади керувати державою та приймати раціональні рішення;

− формування негативних суджень про воєнно-політичне керівництво України та про те, що їх хаотичні бойові дії призводять до невиправданих жертв серед сил АТО;

− поширення поглядів про те, що українська армія на Сході України деморалізована та неспроможна вести бойові дії, а також про недовіру особового складу до керівництва;

− нав’язування думки про те, що Україна не обійдеться без російського газу та що сторонам необхідно повернутися до перегляду газових контрактів.

Саме свідоме нагнітання російськими ЗМІ антиукраїнської істерії під час Євромайдану призвело до втрати Криму через те, що там не знайшлося критичної маси осіб, які чинили б опір «ввічливій окупації» натомість зросла кількість тих, хто схвалював анексію. Усі повідомлення, що і нині транслюються у східних областях України російськими телеканалами, є відвертим намаганням далі дестабілізувати ситуацію в цих регіонах. Їхніх жителів переконують, що «нелегітимна» влада Києва, силові структури та українська армія є їхніми

ворогами. Свідченням небезпечного характеру цих технологій стало фактичне захоплення Росією інформаційного простору Сходу України, що створило передумови для проголошення ДНР і ЛНР і організацію збройного конфлікту з Україною. Нині цілеспрямована діяльність Росії дає змогу провокувати напруженість і в інших регіонах, підтримувати антиукраїнські настрої серед власного населення, дискредитувати Україну та виправдовувати свою політику в державах–членах ЄС.

До потенційних загроз інформаційній безпеці держави належить також наявність інформаційної зброї, яка за визначенням вітчизняних науковців А. Чічановського та О. Старіша, включає спеціальні засоби, технології та дані, що допомагають впливати на інформаційний простір суспільства і завдавати збитків життєво важливим інтересам держави. Така зброя визначається комплексом засобів, призначених для:

- впливу на інформаційні системи супротивної сторони;
- упровадження в діючі комп'ютерні мережі систем управління, а також телекомунікацій відповідних елементів і програмного забезпечення, які спотворюють дані;
- управління поведінкою людей шляхом впливу на їхню свідомість з допомогою системи засобів масової комунікації.

Небезпечною загрозою є наявність дезінформації. Фахівці розрізняють близько 10 видів дезінформації. Як дезінформацію розглядають не тільки цілеспрямовано сформовану хибну інформацію, але і, наприклад, інформацію, що однобічно висвітлює деякі події тощо. Виявити у великому обсязі інформаційних потоків дезінформацію – вкрай складне завдання. Цьому має сприяти автоматизація їх виявлення на основі знання-орієнтованого підходу, що є складовим функціонування інформаційних систем і технологій.

Особливу загрозу для інформаційної безпеки країни представляють хакери − комп'ютерні зламники, що практикуються на проникненні в чужі комп'ютерні системи. Серйозною загрозою можуть бути запущені ними програмні віруси. Тому для вирішення завдань протидії таким загрозам створюються відповідні

органи управління. Зокрема наявність у їх штаті відповідних фахівців з даних питань зможе значно полегшити розв’язання зазначених проблем.

Власне, виділені нами види інформаційних загроз визначає предметне поле діяльності, в якому повинні працювати спеціальні державні служби/інституції, що вповноважені державою на виявлення та нівелювання цих загроз. Важливим елементом технології реагування на ці загрози є створення загальнодержавної системи інформаційної безпеки України, її наступальної спрямованості, як важливої умови захисту національного суверенітету, яка передбачає:

− розробку й удосконалення нормативно-правової бази в сфері інформаційної безпеки, яка нині є фрагментарною та не повною мірою відповідає нагальним потребам;

− створення (визначення) керівного та координаційного органу системи інформаційної безпеки України в структурі органів виконавчої влади;

− визначення (уточнення) переліку суб’єктів, які відповідають за стан інформаційної безпеки;

− проведення досліджень та визначення потреб у технічному, фінансовому й кадровому забезпеченні функціонування системи;

− активізація заходів у Міністерстві оборони та Генеральному штабі Збройних Сил України зі створення власної системи інформаційної безпеки як складової національної системи інформбезпеки.

На сьогодні розглядати будь-які загрози в інформаційній сфері необхідно з урахуванням того контексту, в якому вони виникають і знаходять свій вияв. Зміст і специфіка технології виявлення і усунення інформаційних загроз, ризиків та викликів залежать від розвиненості й цивілізованості суспільства, його міжнародних зв’язків. При цьому рівень інформаційної безпеки має визначатися здатністю технології до реальної оцінки й оптимальної протидії цим загрозам.

Тому основним пріоритетними напрямами технології із виявлення й усунення інформаційних загроз та важливими кроками її здійснення з боку владних органів України мають бути:

– створення власної національної моделі інформаційного простору та забезпечення необхідних заходів щодо запобігання інформаційним загрозам;

– модернізації усієї системи інформаційної безпеки держави та формування й реалізація ефективної інформаційної політики;

– удосконалення законодавства з питань інформаційної безпеки, узгодження національного законодавства з міжнародними стандартами та дієве правове регулювання інформаційних процесів;

– розвиток сучасної інформаційної інфраструктури;

– впровадження новітніх інформаційно-комунікативних технологій у процеси державного управління;

– ефективна взаємодія органів державної влади з усіма інститутами громадянського суспільства під час формування, реалізації та коригуванні необхідної технології, яка має спрямовуватися на виявлення та ліквідацію інформаційних загроз, недопущення інформаційної експансії.

Така технологія має здійснюватись за такими напрямами:

– реалізація упереджувальної стратегії та тактики (превентивні заходи);

– здійснення реагувальної стратегії (оперативне реагування на інформаційні атаки супротивника та активний наступ);

– захист національного інформаційного простору. Головна ціль полягає в розробці технології забезпечення домінування та переваги в запобіганні інформаційних загроз.

Підсумовуючи запропоновані підходи, щодо технології виявлення, а згодом і усунення загроз інформаційній безпеці держави, варто зазначити, що вона має забезпечувати надійний захист від неправомірного зовнішнього і внутрішнього втручання, які негативно впливають на інформаційну систему як самої держави, так і інших країн. Таким чином, ця технологія має включати конкретні дії держави щодо забезпечення безпечних умов існуючих інформаційних процесів та забезпечення безпечного розвитку таких процесів у майбутньому. Це охоплює регулювання питань захисту інформаційної інфраструктури держави, захисту інформаційного ринку та створення безпечних

умов розвитку інформаційних процесів. В контексті зазначеного, проведення необхідної технології, як складової державної політики інформаційної безпеки, передбачає створення в першу чергу необхідних організаційних та правових засад, які мають ув’язуватися з існуючими загрозами в інформаційній сфері.

3.2. Сучасні критерії державної політики в процесі реалізації інформаційної безпеки та шляхи її удосконалення

Критерії сучасного рівня державної політики із забезпечення інформаційної безпеки є досить складним завданням, що вимагає аналізу широкого кола проблем, напрямків та їх інтерпретації в організаційно-правовому полі, як основи побудови всієї системи національної безпеки. В її основі повинна бути методологія щодо оцінки діяльності органів державного управління з надання гарантій інформаційної безпеки особі, соціальним групам та суспільству в цілому.

Критеріями оцінки стану інформаційної безпеки може виступати «інформаційний статус» суб’єктів, що її реалізовують (можливості індивідів у використанні інформаційного простору, забезпеченість всіма необхідними засобами, рівень інформаційної освіти та ін.); розвиненість, доступність та надійність інформаційно-комунікаційних мереж; розвиненість, надійність, систематизованість і зручність інформаційних ресурсів тощо [64].

Для характеристики критеріїв інформаційної безпеки рекомендовано застосовувати модель тріади CIA (англ. − CIATriad), яка передбачає три основні характеристики інформаційної безпеки: конфіденційність, цілісність та доступність. В цілому до основних критеріїв інформаційної варто віднести такі міжнародні критерії інформаційної безпеки:

захист інформаційних ресурсів від несанкціонованого доступу з метою забезпечення конфіденційності;

− забезпечення цілісності інформаційних ресурсів шляхом їх захисту від несанкціонованої модифікації або знищення;

– забезпечення працездатності систем за допомогою технології протидії загрозам [65].

Комплексний характер актуальних загроз національній безпеці в інформаційній сфері насамперед потребує визначення ефективних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації. Для цього потрібна ефективна управлінська діяльність, яку доцільно розглядати в двох аспектах: управління технічними системами та вплив на соціальні процеси з метою досягнення поставлених цілей.

Шляхами вдосконалення організаційних засад державної політики у сфері інформаційної безпеки України передбачається адаптація в Україні світового досвіду (зокрема, США) щодо створення єдиної державної інформаційно-комунікаційної інфраструктури. Вона, з одного боку, сприятиме формуванню стійкої організаційноінформаційної мережі, а з другого покликана забезпечити захист інформаційних і комунікаційних засобів від потенційних загроз. При цьому важливе значення набуває модель міжсекторної взаємодії щодо забезпечення інформаційної безпеки.

В умовах нових інформаційних викликів Україна має бути готова до забезпечення своєї інформаційної безпеки, при цьому нашій державі необхідно розробити всеосяжну і чітку стратегію інформаційного захисту, що має сприяти досягненню поставлених цілей, а не перешкоджати їх досягненню. А в майбутньому цю систему необхідно розвивати, враховуючи правові, технологічні, матеріально-фінансові та інші аспекти. Адже сьогодні, коли ресурсні можливості держави обмежені, необхідний пошук нових шляхів і напрямів забезпечення інформаційної безпеки України в умовах зростання інформаційних викликів та загроз. Вирішення та розв’язання даної проблеми полягає в:

– чіткій державній інформаційній політиці України, тому що інформаційні ресурси держави значною мірою перебувають під зовнішнім впливом;

− інформаційному забезпеченні внутрішньої і зовнішньої політики держави, що створює передумови для її підтримки громадянами, сприяє формуванню об’єктивного іміджу України в світі;

− наявності цілісної ідеології щодо ефективного функціонування інформаційної владної вертикалі, що виходить з історичного досвіду розвитку України, свого географічного простору і населення, традиційних національних інтересів, сучасних глобальних викликів та загроз;

− узгодженні та координуванні діяльності різних силових відомств під час здійснення як розслідування злочинів у інформаційному просторі так і створенні ефективної системи захисту вітчизняного інформаційного простору України;

− контролі і використанні інформаційного простору України, захисті при цьому своїх інформаційних функцій від ворожих дій супротивника тощо.

Серед напрямів, за якими доцільно характеризувати означені питання, можна визначити щонайменше три. Перший напрям (прикладний) – розробка та впровадження стандартів і алгоритмів ведення мережевих інформаційних війн, які допомагатимуть швидко реагувати на певні виклики та компенсувати в певних обставинах брак досвіду та власних інструментів. Другий напрям (кадровий) − налагодження системної роботи з підготовки відповідних фахівців, яка базуватиметься на чіткій методологічній базі та практичних методиках навчання. Третій напрям (науковий) – створення мережі незалежних наукових центрів та стимулювання роботи окремих науковців, котрі зможуть досліджувати проблематику інформаційних загроз і шляхів їх виявлення та усунення [67].

Як засвідчили події останніх років − Євромайдан, анексія Росією Автономної республіки Крим та її гібридна агресія на Сході України, вітчизняна інформаційна сфера, в її безпековому аспекті, потребує суттєвих структурних змін. Зазначені зміни мають спрямовуватися на:

− удосконалення систем моніторингу й контролю інформаційних потоків, як у межах країни, так і в міжнародному масштабі;

– уніфікацію та модернізацію засобів і методів управління інформаційними потоками, що мають базуватися на гнучких схемах роботи;

– розробку та практичне впровадження національної стратегії інформаційно-комунікаційної безпеки, що відповідає сучасним викликам гібридної й інформаційно-психологічної війн другого покоління;

– формування профільної нормативно-правової бази, що дозволятиме оперативно реагувати на сучасні виклики та загрози в контексті інформаційно-психологічних війн у соціальних онлайн-мережах;

– створення та широке застосування ефективної системи підготовки фахівців у галузі інформаційно-психологічних війн із відповідними знаннями та рівнем практичної підготовки;

– активне залучення широких верств громадськості до питань національної безпеки на волонтерських засадах;

– формування ефективного ментального бар'єру свідомості громадськості проти іноземних впливів;

– створення національного конкурентоспроможного середовища медіа-проектів;

– вивчення іноземного досвіду, стратегій, тактики ведення інформаційно-психологічних війн [92].

Цілі реалізації державної політики забезпечення інформаційної безпеки можуть бути досягнуті лише шляхом послідовного та випереджаючого розвитку вітчизняного законодавства, за умов обов'язкового дотримання європейських конституційних принципів. Оскільки нормативноправова база не охоплює всі основні елементи, необхідні для ефективної протидії реальним інформаційним загрозам, певною мірою застаріла, це потребує удосконалення системи нормативно-правового регулювання державної політики у сфері розвитку інформаційної безпеки в сучасних умовах. З метою визначення правового та організаційного механізмів реалізації єдиної політики щодо формування та розвитку системи забезпечення інформаційної безпеки, необхідно прийняти Закон «Про інформаційну безпеку». Крім цього одним із

шляхів комплексного вирішення проблем у сфері забезпечення інформаційної безпеки України може стати кодифікація інформаційного законодавства, яка підтримується багатьма науковцями-юристами та дослідниками національного інформаційного простору.

Важливим є створення сучасної правової бази на основі безпосереднього поєднання основоположних ідей правового регулювання інформаційної сфери та принципів забезпечення національної безпеки. Оскільки нормами вітчизняного законодавства не визначені стандарти та вимоги, способи та заходи щодо створення цілісної системи національної інформаційної безпеки, то ця проблема є головною у питаннях забезпечення інформаційної безпеки країни. Система правових стандартів має стати системноутворюючим чинником для системної та ефективної реалізації державної інформаційної політики, а також надійної протидії деструктивному іноземному інформаційному впливу та інформаційним загрозам у цілому [94]. Доцільно розглянути питання встановлення кримінальної відповідальності за умисне публічне розповсюдження завідомо неправдивої інформації вчиненої з метою поширення тривоги, паніки та страху в суспільстві, підбурювання до насильства, ненависті чи дискримінації, закликів до підриву та невиконання законних вимог службових осіб органів державної влади.

Подальша розробка національної правової бази, її гармонізація з міжнародними інституціями, тобто приведення необхідних відносин у сфері інформації у відповідність до міжнародних стандартів, без сумніву, сприятиме зміцненню інформаційної безпеки України та зростанню її міжнародного авторитету як демократичної і правової держави.

Інформаційний суверенітет України передбачає вдосконалення державного регулювання розвитку інформаційної сфери, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до боротьби з іншими явищами, які загрожують національній безпеці України; недопущення неправомірного

втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Основними організаційними напрямками розвитку технології щодо виявлення загроз інформаційній безпеці держави на перспективу і в порядку важливості є:

− по-перше, − це створення і впровадження спеціальних інформаційних технологій, які орієнтовані на діючу інфраструктуру країни, досягнення вітчизняної науки і техніки, менталітет й технічну культуру персоналу, який відповідає за її організацію;

− по-друге, створення спеціальних інформаційних і технологічних сил та засобів, які призначені для успішного ведення інформаційного протистояння з агресивними інформаційними ворожими системами інших держав;

− по-третє, здійснення міжнародної політики в галузі інформаційної безпеки, яка належно спрямована на створення взаємобезпечних загальних інформаційних технологій та єдиних інформаційних засобів (типу мегамережі «Інтернет»), які гарантують можливість інформаційної співпраці на основі дотримання норм міжнародного права усіма суб’єктами інформаційної співпраці.

Все це потребує цілеспрямованої скоординованої діяльності органів державного управління, які мають характеризуватися: планомірністю, конкретністю, активністю; надійністю, універсальністю, комплексністю. Зарубіжний досвід забезпечення інформаційної безпеки, свідчить, що значна кількість держав світу приділяє особливу увагу інформаційній безпеці, шляхом створення спеціальних органів і підрозділів для боротьби з інформаційними загрозами. На жаль в Україні поки що немає можливості протиставити достатню кількість кваліфікованих фахівців, які б могли на належному рівні протидіяти зростаючим інформаційним загрозам іноземних держав щодо українського інформаційного простору. Саме тому Україна має

використовувати досвід розвинутих країн, що певною мірою мають напрацювання у сфері забезпечення інформаційної безпеки, зокрема досвід Європейського Союзу.

Крім цього, слід визначити основні завдання, виконання яких сприятиме ефективній реалізації політики інформаційної безпеки. Зокрема це:

− формулювання чітких, зрозумілих стратегічних цілей інформаційної політики, заснованих на обґрунтованій програмі державного управління, які має ґрунтуватися на реальних програмах і є частиною необхідної, виваженої інформаційної політики;

− діяльність інформаційних служб повинна здійснюватися в рамках виробленої інформаційної політики держави, мета й завдання якої має узгоджуватися з державним політичним й економічним управлінням;

− важливо безпосередньо здійснювати ефективний моніторинг інформаційного простору, ретельний контроль змісту, вірогідності отриманої інформації;

− державним інформаційним службам у своїй діяльності необхідно використовувати новітні інформаційні технології, методи й спеціальні інструменти виявлення загроз інформаційній безпеці країни [96].

Постала також необхідність розробити нові інструменти, передусім аналітично оцінного спрямування, що можуть на ранніх етапах прогнозувати та запобігати негативним наслідкам загроз інформаційній безпеці і відповідно можливим збиткам для суспільства й держави. Таку функцію має виконувати державна система моніторингу стану національної безпеки як комплекс заходів щодо спостережень, збирання, опрацювання, передавання, збереження та аналізу інформації про стан національної безпеки, прогнозування його змін і розроблення науково обґрунтованих рекомендацій для прийняття рішень про запобігання можливим негативним наслідкам.

Вкрай важливим є підвищення рівня інформаційної культури всіх суб’єктів інформаційних відносин та налагодження їх якісної взаємодії, що створить підґрунтя для забезпечення високого рівня інформаційної безпеки.

Тому потрібно, щоб у концепції подальшого розвитку держави, викладеної в стратегічних документах, робився акцент на тому, яким чином її кадровий інформаційний потенціал може бути використаний для розв'язання пріоритетних завдань забезпечення інформаційної безпеки.

В процесі визначення критеріїв ефективності політики держави щодо забезпечення інформаційної безпеки слід брати до уваги наступні показники:

− концептуальні засади інформаційної безпеки, її принципів, стандартів та правил, погоджених із чинним законодавством й принципами забезпечення інформаційної безпеки держави, суспільства і особистості;

− визначення об’єктів та цілей;

− визначення прийнятних з погляду забезпечення інтересів усіх суб’єктів структур інформаційної безпеки, встановлення контролю над об’єктами інформаційної безпеки, а також оцінки загроз інформаційній безпеці та управлінням їх усунення;

− визначення статусно-функціональних ролей, очікувань та міри відповідальності задіяних суб’єктів інформаційної безпеки, включно з їх звітністю про події, які несуть потенційні загрози.

Таким чином, проблема гарантування інформаційної безпеки держави, суспільства та особистості має комплексний характер і для її розв’язання потрібна ефективна державна політика, спрямована на системне об’єднання на державному рівні законодавчих, організаційних та програмно-технічних засобів. Створення потужної та ефективної системи інформаційної безпеки України, а також розроблення дієвих стратегій і тактик протидії різним інформаційним загрозам повинні стати пріоритетними завданнями органів державної влади та недержавних інститутів.

3.3. Особливості забезпечення інформаційної безпеки в органах місцевого самоврядування

Незважаючи на активну децентралізацію влади, інформаційна безпека органів місцевого самоврядування (на відміну від інших видів безпек) не є самостійно-відірваним об'єктом від усього національного інформаційного простору. Вона не залежить від факторів та чинників, які зумовлені кліматичними показниками чи демографічним станом. Як правило, інформаційні небезпеки на місцях – це відлуння загальних проблем цифровізації, що існують в державі, а тому для їх вирішення у першу чергу необхідно удосконалювати підходи до загальнодержавного інформаційного захисту.

Основу нормативно-правового регулювання питання інформаційної безпеки становлять загальнодержавні нормативні акти, а відтак правове забезпечення місцевої політики інформаційної безпеки та протидії загрозам інформаційного середовища має чітко узгоджуватися з ними. Таким чином, підтримується єдність національного інформаційного простору.

На теренах ЄС є чимало нормативних актів, які встановлюють стандарти інформаційної безпеки в органах місцевого самоврядування. Новий підхід у розумінні сутності інформаційної безпеки та захисту інформації у мережі в умовах глобалізації було запропоновано у Резолюції Ради Європи 2002/С 43/02. Ідея документа спрямована на вироблення загальних підходів та конкретних дій у сфері мережевої та інформаційної безпеки. До речі, складові елементи категорії «інформаційна безпека» (забезпечення доступності послуг та даних; запобігання порушенням та несанкціонованим перехопленням комунікаційних технологій; верифікація повноти та незмінності відправлених, отриманих або збережених даних; забезпечення конфіденційності даних, захист інформаційних систем від несанкціонованого доступу; захист інформаційних систем від атак із застосуванням шкідливого програмного забезпечення; забезпечення надійної автентифікації суб'єктів інформаційної взаємодії [8]), що запропоновані в

Резолюції, можна використовувати і у вітчизняному інформаційному законодавстві.

Основи інформаційної безпекової діяльності в Україні закладено в Конституції України. Так, у ст. 17 Основного Закону зазначається, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [1]. Забезпечення інформаційної безпеки України – це, відповідно до ч. 1 ст. 3 Закону України «Про інформацію», основний напрямок державної інформаційної політики [4]. Згідно зі ст. 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», комплексна система захисту інформації, у тому числі, в органах місцевого самоврядування, є взаємопов'язаною сукупністю організаційних та інженерно-технічних заходів, засобів і методів захисту інформації, що являє собою діяльність, спрямовану на протидію несанкціонованим діям щодо інформації в системі [3].

Інший документ, на який необхідно звернути увагу з огляду на дослідження питання забезпечення інформаційної безпеки на місцях, є Стратегія кібербезпеки України, що затверджена Указом Президента України № 96/2016 від 15.03.2016 [7]. Беззаперечно, кіберпростір є сучасною площиною забезпечення реалізації інформаційних процесів у електронній формі, а тому його захищеність, зокрема у контексті діяльності органів місцевого самоврядування, є елементом стратегії місцевої інформаційної безпеки. У зазначеній вище Стратегії органи місцевого самоврядування визначені як обов'язковий елемент системи кібербезпеки, що покликані взаємодіяти з державними органами, військовими формуваннями, правоохоронними органами, науковими установами, навчальними закладами, громадськими об'єднаннями, а також підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури [7]. У згаданій Стратегії доцільним було б розкриття механізму взаємодії органів місцевого самоврядування з іншими

суб'єктами забезпечення кібербезпеки, що суттєво підвищить ефективність акту загалом та створить підґрунтя для розробки нормативного забезпечення місцевого значення.

Одним із найважливіших атрибутів інформаційних правовідносин є їх захищеність. У Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» закріплено правовий статус таких видів захисту як криптографічний та технічний [3]. Але зазначені переліки не охоплюють весь обсяг методів, способів захисту інформації від загроз та небезпек, що циркулюють та можуть виникати на обмеженій території. Незважаючи на те, що формальної згадки про участь органів місцевого самоврядування у питаннях організації захисту інформаційних потоків у Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» немає, відповідно до ст. 30 Закону України «Про місцеве самоврядування» до відання виконавчих органів сільських, селищних, міських рад віднесено сприяння діяльності Державної служби спеціального зв'язку та захисту інформації України [5]. Таке положення потребує більш детального роз'яснення, зокрема, щодо механізму взаємодії. Тому є необхідність розробки спільних меморандумів взаємодії органів місцевого самоврядування та підрозділів Державної служби спеціального зв'язку та захисту інформації України у питаннях захисту інформації.

Більш детально необхідно зупинитися на загальній стратегії інформаційної безпеки, система якої формально проголошена в Національній програмі інформатизації. Згідно зі ст. 5 Закону України «Про Національну програму інформатизації», головною метою процесів інформатизації є створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави [6]. Зазначений вище Закон є досить важливим елементом системи інформаційної безпеки навіть незважаючи на те, що приписної конструкції про роль та участь органів місцевого самоврядування у ньому немає. Справа в тому, що ст. 17–19

Закону створюють правові підстави та закріплюють за суб'єктами інформаційних відносин у державі (центральними органами виконавчої влади, органами місцевого самоврядування, підприємствами, установами, організаціями) обов'язок розробки та прийняття програм інформатизації, що за великим рахунком, є сукупністю стратегій та правових інструментів для формування політики інформаційної діяльності відповідно до власних потреб кожного суб'єкта. Питання інформаційної безпеки не є виключенням.

Згідно зі ст. 2 означеного Закону, Національна програма інформатизації, серед іншого, включає в себе програми та проекти інформатизації органів місцевого самоврядування, які ними ж розробляються і після погодження з Генеральним державним замовником Національної програми інформатизації [6] підлягають виконанню.

Беручи до уваги положення ст. 6 Закону України «Про Національну програму інформатизації», у якій стверджується, що функцією саме органів державної влади є забезпечення інформаційної безпеки, вважаємо, що зазначене формулювання назви статті не охоплює загалом органів місцевого самоврядування як невід'ємних суб'єктів забезпечення інформаційної безпеки. А тому пропонується відкорегувати назву ст. 6 Закону України «Про Національну програму інформатизації» та запропонувати її наступну редакцію: «Стаття 6. Функції державних органів та органів місцевого самоврядування у реалізації Національної програми інформатизації».

Важливо також звернути уваги на підзаконне нормативно-правове регулювання у сфері інформатизаційних процесів на місцях. Так, типові проекти інформатизації в областях, районах, (містах) розробляються та приймаються на основі Постанови Кабінету Міністрів України № 644 від 12 квітня 2000 р. «Про затвердження Порядку формування та виконання регіональної програми і проекту інформатизації». На підставі аналізу деяких місцевих Програм інформатизації приходимо до висновку про наявність у них недоліків, що мають бути усунені шляхом внесення змін до Порядку формування та виконання регіональної програми і проекту інформатизації.

По-перше, констатується відсутність системного правового уявлення про інформаційну безпеку та суб'єктів її забезпечення, а також не прослідковується зв'язок положень програми із приписами загальних стратегічних актів-документів загальнодержавного характеру в розрізі аналізу питань програми інформатизації. У зв'язку з цим, пропонується в обов'язковому порядку розробляти питання інформаційної безпеки, яке необхідно формалізувати в конкретних завданнях з інформатизації. Для цього в Додатку 1 до Порядку формування та виконання регіональної програми і проекту інформатизації у примітках (Завдання повинні охоплювати такі питання) необхідно доповнити наступне питання: «Заходи забезпечення інформаційної безпеки».

По-друге, слід зауважити про необхідність перегляду строків стратегії реалізації програм інформатизації, які згідно з п. 3 досліджуваного Порядку становлять 3 роки. З урахуванням швидкої динаміки розвитку інформаційно-телекомунікаційних процесів та стандартів інформаційної безпеки, строк 3 роки рекомендується скоротити до 2-х. У ході аналізу деяких програм інформатизації на місцях (наприклад, програми інформатизації Дніпровської міської ради на 2016–2020 р. [2]) було також встановлено недотримання строків при розробці та прийняті програм. А тому необхідно забезпечити організацію контролю за реалізацією приписів Програми формування та виконання регіональної програми і проекту інформатизації спеціально створеною комісією при органах місцевої влади, яка включала б фахівців у сфері інформаційного захисту, громадськість, уповноважених осіб органів влади, представників місцевих правоохоронних органів тощо.

Незважаючи на те, що з позиції інформаційно-телекомунікаційного простору муніципальна безпека є складовим елементом національної загальнодержавної інформаційної безпеки, тим не менш, вона має свої специфічні ознаки, які суттєвим чином можуть впливати на стан інформаційної захищеності в

органах місцевого самоврядування. До загальних чинників, що можуть у тій чи іншій мірі впливати на стан місцевої інформаційної безпеки, слід віднести:

1) наближеність до кордону (у цьому випадку особливо яскравим прикладом слугує стан неоголошеної інформаційної війни на прилеглих до зони бойових дій територіях Донецької та Луганської областей, де транслюються недостовірні відомості та інформація про події в Україні та прилеглих територіях, що направлені на дискредитацію влади); 2) рівень розвитку інформаційно-телекомунікаційних систем органів місцевого самоврядування, їх інтегрованість в загальнонаціональний інформаційний простір; 3) переважання обсягу паперового документообігу над електронним; 4) забезпеченість персональними робочими станціями, законність використання програмного забезпечення (його ліцензованість та сертифікованість), наявність корпоративної захищеної мережі обміну, збереження та накопичення інформаційних ресурсів); 5) наявність спеціалізованого програмного забезпечення для адміністрування власних баз даних; 6) напружена політична ситуація, яка може провокуватись виборчим процесом або самими діями представників місцевих органів влади; 7) використання (або невикористання) в постійному режимі місцевої PR інформаційної політики; 8) загальні показники інформатизованості місцевого населення, їх активність у муніципальному житті; 9) наявність прозорих та автономних місцевих засобів масової інформації, їх пов'язаність із представниками місцевої влади; 10) наявність фактів втручань та переслідування громадських активістів, журналістів, місцевого населення за їх інформаційно-поширюючу діяльність, відсутність притягнень до відповідальності за протиправну діяльність; 11) низький рівень правового регулювання основ інформаційних відносин та процесів в приватному секторі, що комунікує із представниками місцевої влади, правоохоронними органами та іншими суб'єктами забезпечення безпеки.

До вищезазначеного слід додати, що для кожного муніципального учасника характерні свої загрози та ризики у сфері нормального функціонування інформаційної інфраструктури, які існують як в середині, так і ззовні інформаційного поля. Проте всі інформаційні небезпеки, що можуть виникати в ході інформаційної діяльності суб'єктів муніципальних відносин, мають певну

схожість. З метою групування за природою ризиків необхідно вдатися до виокремлення інформаційної ролі (статусу) таких суб'єктів, тобто «виробників» (тих, які створюють відомості та інформацію в якості продукту) та «користувачів» як споживачів такої інформації. Особливою інформаційною роллю наділені органи місцевого самоврядування як «координатори» інформаційної взаємодії, тобто пов'язуюча ланка комунікації між усіма учасниками інформаційної системи. Саме для них буде характерна потрійна інформаційна роль як виробника, користувача, так і посередника. Звичайно, що така класифікація є умовною і за певних обставин роль одного суб'єкта може трансформуватись до іншого і навпаки. Наприклад, «виробник» інформаційного продукту – місцеве населення, а правоохоронний орган, якому надійшла конфіденційна інформація – споживач, який зобов'язаний вжити заходів зі збереження, нерозголошення такої інформації та використання її виключно на благо особи та суспільства. З іншого боку, правоохоронний орган може виступати виробником відомостей, наприклад, про результати здійснення контролю за дотриманням місцевого громадського порядку та безпеки. У цьому випадку його завдання полягає у наданні достовірної, правдивої, неупередженої та повної інформації. З-поміж іншого, для органів місцевого самоврядування можуть бути характерні такі інформаційні загрози: несанкціоноване поширення відомостей, які перебувають в обігу органів місцевої влади; відсутність єдиного захищеного каналу зв'язку із комунальними підприємствами, правоохоронними органами тощо; факти дискредитації роботи місцевих органів в мережі Інтернет на соціальних порталах та форумах; незабезпеченість (низький рівень забезпеченості) персональними робочими станціями, безперебійним та надійним доступом до мережі Інтернет; поширення недостовірних відомостей про діяльність посадових осіб місцевих органів та інформаційний тиск.

І насамкінець, окрім інформаційних загроз, які повинні бути враховані суб'єктами інформаційних відносин на місцях при розробці програм інформатизації, необхідно з'ясувати об'єкти інформаційного захисту. Загалом всі елементи, через які проходять потоки інформації, будь-які елементи, де

інформація накопичується та поширюється далі, можна однозначно віднести до об’єктів, що потребують захисту або хоча б уваги. З теоретико-методологічного підходу розроблено не один критерій щодо класифікації потенційних інформаційних об’єктів захисту. Але фокусуючись на обмеженій території та з урахуванням сучасного вітчизняного стану розвитку інформаційних, технологічних систем і нерівномірних особливостей розвитку регіонів, пропонується при розробці концепції інформаційної безпеки на місцях акцентувати увагу на наступних об’єктах системи загалом: програмне забезпечення; соціальні медіа; системи накопичення та збереження даних; системи обробки, кодування та поширення інформації; бази даних; апаратна інфраструктура; корпоративні внутрішні мережі; місце збереження та обігу паперової інформації тощо.

Отже, інформаційна безпека в органах місцевого самоврядування – це складний механізм забезпечення технологічного функціонування інформаційної системи в органах місцевого самоврядування, а також протидія її небезпекам, загрозам та ризикам.

З урахуванням високої динаміки процесів цифрової трансформації, що здатні суттєво порушувати інформаційно-телекомунікаційне муніципальне середовище та несистемності положень підзаконних нормативних актів, рекомендується розробити концепцію інформаційної безпеки в органах місцевого самоврядування.

ВИСНОВКИ

1. Інформаційна безпека представляє собою одне з найважливіших понять у науці і різних сферах людської діяльності. Сутність і комплексність цього поняття виявляється характером сучасного інформаційного суспільства. Інформаційна безпека, як одна з характеристик стійкого розвитку, виступає в якості базової цінності держави. Водночас, ціннісні орієнтації, що ґрунтуються на уявленнях про інформаційну безпеку у різних суспільних груп і окремих осіб, часто не збігаються. Саме тому роль інформаційної безпеки має розглядатися за допомогою системи методів, які виражають загальні цінності у сфері інформаційних відносин суспільства. Проблема ефективного забезпечення інформаційної безпеки має передбачати вирішення таких головних і масштабних задач, як: розроблення теоретичних основ забезпечення безпеки інформації; створення системи органів, які мають відповідати за безпеку інформації; вирішення проблеми керування захистом інформації та її автоматизації; створення належної нормативно-правової бази, яка повинна регламентувати рішення всіх задач забезпечення безпеки інформації; налагодження виробництва засобів захисту інформації; організацію підготовки відповідних фахівців та ін.

2. Основна спрямованість національного законодавства у сфері забезпечення інформаційної безпеки свідчить, що більшість правових норм відповідають міжнародним стандартам, принципам і нормам її забезпечення. Водночас чинна нормативно-правова база в інформаційній сфері потребує вдосконалення з метою усунення суперечностей і заповнення прогалин у законодавстві стосовно інформаційної безпеки держави, суспільства і громадян.

3. Державна політика забезпечення інформаційної безпеки України полягає у:

− забезпеченні конституційних прав людини на доступ до інформації, використанні інформації в інтересах здійснення не забороненої чинним законодавством діяльності, фізичного, інтелектуального й духовного розвитку, а також; у захисті інформації, яка стосується особистої безпеки громадянина;

– створенні умов для гармонійного розвитку інформаційної структури, для реалізації конституційних прав і свобод людини й громадянина у сфері отримання інформації та використання її з метою забезпечення непорушності конституційного ладу, культурного й наукового потенціалу;

– здійснення інформаційного забезпечення державної політики України, пов'язане з доведенням до української та міжнародної громадськості достовірної інформації про державну політику України, її офіційної позиції стосовно соціально значущих подій українського та міжнародного життя, з забезпеченням доступу громадян до відкритих інформаційних ресурсів;

– розвиток сучасних інформаційних технологій, вітчизняної індустрії інформації, в тому числі індустрії засобів інформатизації, телекомунікації і зв'язку, забезпечення потреби внутрішнього ринку її продукцією і вихід цієї продукції на світовий ринок, а також; забезпечення накопичення, зберігання та ефективного використання вітчизняних ресурсів;

– захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки інформаційних і телекомунікаційних систем, як наявних, так і тих, що створюються на території України.

4. За роки незалежності в Україні створено основні елементи державної політики щодо забезпечення інформаційної безпеки, напрацьовано нормативно-правову базу їх діяльності, визначено основні функції й повноваження державних органів в інформаційній сфері. Головними напрямами політики інформаційної безпеки в країні визначено: формування та впровадження правових, організаційних, науковотехнічних, економічних, фінансових, технологічних, методичних умов її реалізації з урахуванням світових тенденцій.

5. Розглядаючи формування правових основ і гарантій міжнародної інформаційної безпеки, слід визнати, що наразі можна засвідчити різні позиції провідних держав сучасності щодо розуміння потенційних загроз в інформаційних озброєннях та їх використанні проти критично важливих сфер життєдіяльності суспільства. Уніфіковані норми щодо правового регулювання міжнародної інформаційної безпеки стають необхідністю нашого часу, що

характеризується всеохоплюючою глобалізацією і потужними антиглобалізаційними рухами, зростанням гострих протистоянь між ними, в тому числі й в інформаційному просторі; порушенням територіальної цілісності і інформаційного суверенітету держав, поєднанням конвенційних і не конвенційних засобів сучасної війни; зрештою дрібними кіберзлочинами та масштабними хакерськими атаками, масованим інтелектуальним піратством тощо.

6. Основними пріоритетними напрямами технології із виявлення й усунення інформаційних загроз та важливими кроками її здійснення з боку владних органів України мають бути:

− створення власної національної моделі інформаційного простору та забезпечення необхідних заходів щодо запобігання інформаційним загрозам;

− модернізація усієї системи інформаційної безпеки держави та формування й реалізація ефективної інформаційної політики;

− удосконалення законодавства з питань інформаційної безпеки, узгодження національного законодавства з міжнародними стандартами та дієве правове регулювання інформаційних процесів;

− розвиток сучасної інформаційної інфраструктури;

− впровадження новітніх цифрових технологій у процеси державного управління;

− ефективна взаємодія органів державної влади з усіма інститутами громадянського суспільства під час формування, реалізації та коригуванні необхідної технології, яка має спрямовуватися на виявлення та ліквідацію інформаційних загроз, недопущення інформаційної експансії.

Така технологія має здійснюватись за такими напрямами:

− реалізація упереджувальної стратегії та тактики (превентивні заходи);

− здійснення реагувальної стратегії (оперативне реагування на інформаційні атаки супротивника та активний наступ);

− захист національного інформаційного простору.

Технологія виявлення, а згодом і усунення загроз інформаційній безпеці держави, мають забезпечувати надійний захист від неправомірного зовнішнього і внутрішнього втручання, які негативно впливають на інформаційну систему як самої держави, так і інших країн. Таким чином, ця технологія має включати конкретні дії держави щодо забезпечення безпечних умов існуючих інформаційних процесів та забезпечення безпечного розвитку таких процесів у майбутньому. Це охоплює регулювання питань захисту інформаційної інфраструктури держави, захисту інформаційного ринку та створення безпечних умов розвитку інформаційних процесів. В контексті зазначеного, проведення необхідної технології, як складової державної політики інформаційної безпеки, передбачає створення, в першу чергу, необхідних організаційних та правових засад, які мають ув’язуватися з існуючими загрозами в інформаційній сфері.

7. Фокусуючись на обмеженій території та з урахуванням сучасного вітчизняного стану розвитку інформаційних, технологічних систем і нерівномірних особливостей розвитку регіонів, пропонується при розробці концепції інформаційної безпеки на місцях акцентувати увагу на наступних об’єктах системи загалом: програмне забезпечення; соціальні медіа; системи накопичення та збереження даних; системи обробки, кодування та поширення інформації; бази даних; апаратна інфраструктура; корпоративні внутрішні мережі; місце збереження та обігу паперової інформації тощо. Отже, інформаційна безпека в органах місцевого самоврядування – це складний механізм забезпечення технологічного функціонування інформаційної системи в органах місцевого самоврядування, а також протидія її небезпекам, загрозам та ризикам. З урахуванням високої динаміки процесів цифрової трансформації, що здатні суттєво порушувати інформаційно-телекомунікаційне муніципальне середовище та несистемність положень підзаконних нормативних актів, рекомендується розробити сучасну концепцію інформаційної безпеки в органах місцевого самоврядування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Венгеров А.Б. Категория «информация» в понятийном аппарате юридической науки / А. Б. Венгеров. Советское государство и право. 1977. № 10. С. 28-32.

2. Основи інформаційної безпеки держави: навч. посіб. / Андрєєва О.М, Гондюл В.П., Рижков М. М. та ін. К.: ІМВ, 2008. 254 с.

3. Богуш В.М. Інформаційна безпека держави / В.М. Богуш. К.: «МК-Прес», 2005. 431 с.

4. Довгань О.Д. Теоретико-правові основи забезпечення інформаційної безпеки України: автореф. дис. д-ра юрид. наук: 12.00.07 / Довгань О. Д.; Ін-т законодавства Верхов. Ради України. Київ, 2016. 44 с.

5. Живко М.О. Інформаційна безпека України через призму національної безпеки / М. О. Живко // Психологічні аспекти національної безпеки: зб. тез міжнар. наук.-практ. конф., 22-23 берез. 2007 р. / МВС України, Львів. держ. ун-т внутріш. справ; [відп. за вип. М. Й. Варій]. Львів, 2007. С. 86-88.

6. Класифікація інформаційної безпеки / Золотар О.О. // Інформація і право. 2011. № 2(2). С. 109-113.

7. Литвиненко О. Інформаційна безпека – складова національного суверенітету/ О. Литвиненко // Політика і час. 1997. № 4. С. 32-35.

8. Марущак М. Інформаційна безпека держави / М. Марущак. Вид-во КНТ. 2008. 136 с.

9. Мосенко Ю.О. Деякі питання вдосконалення основних складових категоріального апарату державної інформаційної політики України / Ю. О. Мосенко // Вісн. господар. судочинства. 2009. № 1. С. 103-109.

10. Набруско В. І. Інформаційний суверенітет країни – запорука національної безпеки України. Виклики і загрози / В. І. Набруско // Актуальні проблеми міжнародних відносин: [зб. наук. пр.] / Київ. нац. ун-т ім. Т.

Шевченка, Ін-т міжнар. відносин; [редкол.: Копійка В. В. та ін.]. К., 2011. Вип. 102, ч. 1. С. 63-65

11. Нашинець-Наумова А. Інформаційна безпека як складова частина національної безпеки України / А. Нашинець-Наумова // Підприємництво, госп-во і право. 2013. № 8. С. 63-66.

12. Шайтан О. Понятійно-категоріальний апарат інформаційної безпеки держави у гуманітарній сфері / О. Шайтан // Юрид. журн. 2012. № 4. С. 74-76.

13. Про поняття «інформаційна безпека» / Фурашев В.М. // Правова інформатика. 2011. № 1(29). С. 47-53.

14. Калюжний Р. Питання концепції реформування інформаційного законодавства України / Калюжний Р., Говловський В., Цимбалюк В., Гузалюк М. // Збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». К.: НТУУ «КПІ», Міністерство освіти і науки України, СБУ. 2000. С. 17-21.

15. Ліпкан ВА. Національна і міжнародна безпека у визначеннях та поняттях / В.А. Ліпкан, О.С. Ліпкан, О.О. Яковенко. К.: Текст, 2006. С. 146-147.

16. Золотар О. Класифікація інформаційної безпеки /О. Золотар // Інформація і право. 2011. № 2. С. 109-113.

17. Захаренко К.В. Категорія інформаційної безпеки у вітчизняному філософсько-політологічному дискурсі / К.В. Захаренко // Гуманітарний вісник ЗДІА. 2018. Вип. 72. С.44-52.

18. Інформаційна безпека України в умовах євроінтеграції: навч. посібник / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський**.** К.: КНТ, 2006. 280 с.

19. Молодцов О.В. Сутність інформаційного простору як парадигми суспільного розвитку / О. В. Молодцов. Статистика України. 2004. № 3. С. 50-54.

20. Морозов А. Організаційні та правові засади створення національного інформаційного простору / А. Морозов, В. Косолапов, В. Ковтун. – Наука та наукознавство. 2000. № 3. С. 32-35.

21. Юдін О.К. Інформаційна безпека держави: навч. посіб. / О.К. Юдін, В.М. Богуш. Харків: Консум, 2005. 576 с.

22. Законодавчі основи забезпечення інформаційної безпеки України: наукова доповідь / Пилипчук В.Г., Корж І.Ф., Петришин О.В., Савінова Н.А., Фурашев В.М. (За заг. ред. Пилипчука В.Г.) К: НДІІП НАПрН України, 2014. 60 с.

23. Тихомиров О. Забезпечення інформаційної безпеки: теоретико-правовий аспект / О. Тихомиров // Право України. 2011. № 4. С. 252-259.

24. Інформаційна безпека (соціально-правові аспекти): підручник / Остроухов В.В., Петрик В.М. та ін.; за ред. Є.Д. Скулиша. К.: КНТ, 2010. 776 с.

25. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи / О.А. Баранов. К.: СофтПрес, 2005. 316 с.

26. Тарнавська Т.В. Генеза поняття «система»: історичний огляд / Т.В. Тарнавська // Духовність особистості: методологія, теорія і практика. 2011. № 6 (47). С.130-139.

27. Закон України про інформацію // Відомості Верховної Ради України. 1992. № 48. Ст. 650.

28. Петрицький А. Інформаційне законодавство України: актуальні проблеми та шляхи їх вирішення / А. Петрицький // Вісник Маріупольського державного університету. Серія: право. 2013. Вип. 5. С. 64-68.

29. Закон України про друковані засоби масової інформації (пресу) в Україні // Відомості Верховної Ради України. 1993. № 1. С. 1.

30. Закон України про науково-технічну інформацію // Відомості Верховної Ради України. 1993. № 33. С. 345.

31. Про телебачення і радіомовлення: Закон України від 21.12.1993 р. // Відомості Верховної Ради України. 1994. № 10. С. 43.

32. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07/1994 р. №80/94-ВР // Відомості Верховної Ради України. 1994. № 31. С. 286.

33. Закон України про захист інформації в автоматизованих системах // Відомості Верховної Ради України. 1994. № 31. С. 286.

34. Закон України про Національну програму інформатизації // Відомості Верховної Ради України. 1998. № 27-28. С. 181.

35. Про Концепцію Національної програми інформатизації: Закон України від 4 лютого 1998 р. // Відомості Верховної Ради. 1998. № 27-28. С. 182.

36. Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію: Постанова Кабінету Міністрів України від 27.11.1998 р. № 1893 // Офіційний вісник України. 1998. № 48. С. 31

37. Закон України про основи національної безпеки від 19 червня 2003 р. // Офіційний Вісник України. 2003. № 29. С. 1433.

38. Про телекомунікації: Закон України від 18.11.2003 р. № 1280-IV // Відомості Верховної Ради України. 2004. № 12. С. 155.

39. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 9 січня 2007 року № 537-V // Відомості Верховної Ради України. 2007. №12. С. 102.

40.Про Доктрину інформаційної безпеки України: Указ Президента України від 08.07.2009 р. № 514/2009 // Офіційний вісник Президента України. 2009. № 20. С. 18. С. 677.

41. Малик Я.Й. Інформаційна безпека України: стан та перспективи розвитку / Я.Й. Малик // Ефективність державного управління: Зб. наук. праць. 2015. Вип. 44. С. 13-20.

42. Конституція України від 28 червня 1996 року // Відомості Верховної Ради України. 1996. №30. С. 141.

43. Чорна М.Ф. Інформаційна безпека України: політико-правові засади генези і становлення / М.Ф. Чорна, В.Д. Доносо, В.С. Доносо // Правове життя: сучасний стан та перспективи розвитку: зб. тез наук. доп. X Міжнар. наук.практ. конф. молодих учених (21-22 берез. 2014 р.) / М-во освіти і науки України [та ін.]; [редкол.: І.Я. Коцан, О.В. Лаба]. Луцьк, 2014. С. 102-104.

44. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. 2010. № 34. С. 481.

45. Про доступ до публічної інформації: Закон України від 13.01.2011 р. // Відомості Верховної Ради України. 2011. № 32. С. 314.

46. Про внесення змін до Закону України «Про інформацію»: Закон України від 13.01.2011 № 2938-VI // Відомості Верховної Ради України. 2011. № 32. – С. 313.

47. Закон України «Про національну безпеку України» // Відомості Верховної Ради. 2018. № 31. С. 241.

48. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: монографія / Б.А. Кормич. Одеса: Юридична література, 2003. 472 с.

49. Данільян О.Г. Національна безпека України: сутність, структура та напрями реалізації: навчальний посібник / О.Г. Даняльян. Х: Фоліо, 2002. 285 с.

50. Про рішення Ради національної безпеки і оборони України від року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 № 96/2016. URL: www.president.gov.ua / documents/962016-19836.

51. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 № 47/2017. URL: ww.president.gov.ua / documents/472017-21374.

52. Інформаційна безпека особистості, суспільства, держави: підручник. К.: Видавничо-поліграфічний центр «Київський університет», 2008. 274 с. 53. Концепція інформаційної безпеки України. URL: www.mip.gov.ua.

54. Бортко. Г.Н. Национальные стратегии информационного общества: преимущества и условия реализации в Украине / Г.Н. Бортко. – Информационное общество. 2004. № 2. С. 25-29.

55. Додонов О.Г. Державна інформаційна політика і становлення інформаційного суспільства в Україні / О.Г. Додонов, О.С. Горбачик // Стратегічна панорама. 2002. № 1. С. 166-170.

56. Проценко П.П Проблематика переходу до інформаційного суспільства / П.П. Проценко. Політичний менеджмент. 2004. № 6. С. 129-137.

57. Шаповал О.В. Розробка національних стратегій інформаційного розвитку – пріоритет сучасності / О.В. Шаповал. Нова парадигма. Випуск 38. К., 2004. С. 166-172.

58. Постанова КМ України від 14 січня 2015 р. №2 «Питання діяльності Міністерства інформаційної політики України». URL: www. zakon 4.rada.gov.ua /laws/show/2–2015–n.

59. Зушко М. Інформаційна політика в зміцненні безпеки України / М. Зушко, Л. Швайка // Економічна безпека держави та суб'єктів підприємницької діяльності в Україні: проблеми та шляхи їх вирішення: Мат. IV Всеукраїн. наук.практ. конф. (18–20 травня 2017 р., м. Львів) / упоряд. А. М. Штангрет; редкол.: О. І. Копилюк, Є. М. Палига та ін. Львів: Укр. акад. Друкарства. 2017. С. 65-67.

60. Боднар І.Р. Роль держави у формуванні інформаційної політики/ І.Р. Боднар. Вісник ЛКА. Львів: Видавництво ЛКА. Випуск 34. Серія економічна. 2011. С. 291-296.

61. Інформаційна безпека суспільства // Віче. 2015. квітень.

62. Інформаційна політика України: європейський контекст: моногр / Л. Губерський, Є.. Макаренко, Є. Камінський та ін. К.: Либідь, 2007. 360 с.

63. Громико І. Державна домінантність визначення інформаційної безпеки України в умовах протидії загрозам / І. Громико, Т. Саханчук // Право України. 2008. № 8. С.130-134.

64. Ковтун С.В. Інформаційна безпека: підручник / С.В. Ковтун. – Харків. Вид. ХНЕУ, 2009. 368 с.

65. Нестеряк Ю.В. Міжнародні критерії інформаційної безпеки держави: теоретикометодологічний аналіз / Ю.В. Нестеряк // Вісник НАДУ. 2013. № 3. С.40-46.

66. Конах В.К. Національний інформаційний простір України: проблеми формування та державного регулювання: аналітична доповідь / В.К. Конах. К.: НІСД, 2014. 76 с.

67. Курбан О.В. Основи сучасної національної інформаційної безпеки України / О.В. Курбан // Вісник ХДАК. 2017. Вип. 50. С. 55-66.