Міністерство освіти і науки України
Національний університет «Острозька академія»
Навчально-науковий інститут міжнародних відносин та національної безпеки
Кафедра національної безпеки та політології

Кваліфікаційна робота
на здобуття освітнього ступеня магістра на тему:

«Державна політика забезпечення інформаційної безпеки України: основні напрямки та особливості здійснення»

Виконав студент ІІ курсу, групи ЗМНб-21
Спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності)
Леснік Роман Миколайович

Керівник – кандидат політичних наук, доцент
Жовтенко Тарас Григорович

Рецензент – кандидат політичних наук, доцент кафедри політології та соціології Рівненського державного гуманітарного університету
Крет Роман Михайлович

Острог, 2022

ЗМІСТ

ВСТУП

Постановка проблеми дослідження. Феномен «інформаційної безпеки» передбачає якісне інформування людей і вільний доступ до різноманітних інформаційних баз, але також мають бути контрольні дії щодо нерозповсюдження секретної інформації, підтримання суспільства в цілісному стані, захисту від будь-якої негативної інформації. вплив тощо. Вирішення такого складного проблемного питання дасть можливість захистити суспільні та державні інтереси, а також сприятиме утвердженню прав громадян на повну та якісну інформацію. Для ефективного забезпечення інформаційної безпеки в державі необхідно вирішити наступні масштабні завдання: розробити теоретичні основи забезпечення захисту інформації; створити систему структур, які б відповідали за збереження інформаційної безпеки; вирішити питання захисту інформації та налагодити її автоматизацію; створити законодавчу базу, яка б регулювала вирішення всіх завдань із забезпечення захисту інформації; розпочати виробництво засобів захисту інформації; організовують підготовку фахівців відповідного профілю тощо Комплекс питань інформаційної безпеки держави включає такі напрями діяльності держави, як: захист та обмеження обігу інформації; захист інформаційної інфраструктури держави; безпека розвитку інформаційної сфери держави; захист національного інформаційного ринку; запобігання інформаційному тероризму та інформаційній війні.

Необхідність прискорення визначення декларативних стратегічних засад забезпечення інформаційної безпеки в сучасних реаліях викликана такими викликами, як: складна ситуація в національній інформаційній сфері, яка пов’язана як зі значним інформаційним впливом, так і з втручанням російських ЗМІ; масштабне поширення російськими ЗМІ дезінформації про Україну; виконання Російською Федерацією спеціального інформаційного завдання з метою дискредитації та створення негативного міжнародного іміджу України у

світі; існують технічні проблеми з трансляцією українських електронних ЗМІ в окремих регіонах нашої країни та світу. Невипадково в положеннях Стратегії інформаційної безпеки України, оприлюдненій у грудні 2021 року, проголошено тезу про те, що інформаційна політика Російської Федерації є загрозою не лише для України, а й для інших провідних демократичних держав світу. За таких умов актуальним і своєчасним є висвітлення основних положень Стратегії інформаційної безпеки України в контексті визначення ролі та завдань вітчизняної спецслужби у запобіганні загрозам і викликам у вітчизняному інформаційному просторі, забезпеченні безпеки держави у інформаційна сфера. Можна переконливо стверджувати, що для відновлення свого геополітичного впливу в Україні Російська Федерація, продовжуючи гібридну війну, системно використовує для цього політичні, соціально-економічні та інформаційно-психологічні важелі та засоби. Деструктивна пропаганда як ззовні, так і всередині України, використовуючи соціальні протиріччя, розпалює соціальну ворожнечу, провокує конфлікти, підриває суспільну єдність. Відбувається посилення інформаційного впливу з боку Російської Федерації, що межує з відвертим ігноруванням вимог міжнародного та внутрішнього законодавства, зокрема щодо нагнітання сепаратистських та автономістичних настроїв.

Характеристика стану дослідження проблеми. Основним теоретичним підґрунтям роботи стали праці в таких галузях та таких вчених: філософії: О. Довгань, Б. Кормич, В. Петрик, Р. Шаповал та ін. інших галузей права: вітчизняні вчені – Ю. Бисага, Ю. Білак, В. Білоус, О. Дзьобань, А. Качинський, Я. Малик, Н. Нижник, Л. Шиманський та ін.

Накопичений теоретичний і практичний досвід формування системи забезпечення інформаційної безпеки України демонструє значні суперечності у правовому регулюванні відносин, що виникають у національному інформаційному просторі, що й зумовлює актуальність дослідження даної тематики.

Метою дослідження є основні напрямки та особливості здійснення державної політики забезпечення інформаційної безпеки України.

Поставлена мета зумовлює необхідність вирішення наступних **завдань:**

– розглянути поняття та складові інформаційної безпеки країни;

– розглянути основні загрози інформаційній безпеці країни;

– розглянути зміст політики забезпечення інформаційної безпеки держави;

– розглянути основні засади державної політики забезпечення інформаційної безпеки України;

– дослідити основні показники державної політики забезпечення інформаційної безпеки України;

– з’ясувати головні тренди та напрямки реалізації державної політики з інформаційної безпеки України;

– розглянути основні проблеми реалізації державної політики з інформаційної безпеки України;

– визначити напрямки реформування державної політики з інформаційної безпеки України.

Об’єктом дослідження є відносини у сфері забезпечення інформаційної безпеки країни.

Предметом дослідження є оцінка здійснення та результативності державної політики забезпечення інформаційної безпеки України

Методи дослідження були обрані з урахуванням поставленої мети і завдань дослідження, його об’єкта і предмета. У роботі застосовувалися діалектичний метод пізнання, загальнонаукові (системний, функціональний та ін.) і спеціальні методи правових досліджень (формально-догматичний та ін).

Так, системно-структурний метод був використаний в роботі для дослідження системи загроз національній безпеці.

За допомогою формально-догматичного методу досліджено поняття «безпека», «загроза», а також інші поняття, пов’язані з системою забезпечення інформаційної безпеки країни.

З метою поглибленого дослідження, пізнання і вивчення питання «Державна політика забезпечення інформаційної безпеки України: основні напрямки та особливості здійснення» було використано зазначені методи у сукупності. При викладі результатів дослідження застосовувалися проблемний підхід.

Характеристика джерельної бази. Основою роботи є нормативно-правові акти, наукові статті, монографії, дисертаційні дослідження та інформаційні інтернет-ресурси.

Хронологічні рамки дослідження охоплюють період 2014-2022 року на території України в умовах збройної агресії РФ

Структура роботи. Робота складається зі вступу, трьох розділів, восьми підрозділів, висновків, списку використаних джерел та літератури.

РОЗДІЛ І
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КРАЇНИ

1.1. Поняття та складові інформаційної безпеки країни

Відповідно до Закону України «Про Концепцію Національної програми інформатизації» інформаційна безпека є невід'ємною складовою оборонної, економічної, політичної, а також інших складових національної безпеки [1], це стан захищеності життєво важливі інтереси особи, суспільства і держави від внутрішніх і зовнішніх загроз. Отже, національна безпека залежить від змісту національно-державних інтересів і характеризує такий стан країни, при якому їй не загрожує небезпека війни чи інші посягання на суверенний розвиток.

У загальному розумінні безпека – це стан захищеності від будь-чого і може стосуватися як окремої людини, так і суспільства і держави в цілому. При цьому безпека як поняття різниться залежно від сфери застосування: політологія, соціологія економіки та ін. У теорії національної безпеки широко використовуються такі формулювання: «національна безпека», «особиста безпека», державна безпека», «міжнародна безпека», «інформаційна безпека», «політична безпека», «соціальна безпека», «військова безпека» тощо [2]. Щодо визначення поняття «інформаційна безпека», то на сьогодні немає цілісного підходу, немає єдиної думки дослідників щодо його визначення. З одного боку, термін «інформаційна безпека» широко використовується в наукових публікаціях, навчальній літературі та законодавчих документах різного рівня, з іншого боку, це поняття досі не має чіткого розуміння, а його зміст у різних джерелах має кардинальний характер. відмінності [3-5].

Інформаційна безпека – це складне, системне, багаторівневе явище, на стан і перспективи розвитку якого безпосередньо впливають зовнішні та внутрішні фактори, найважливішими з яких є: 1) політична ситуація у світі; 2) наявність потенційних зовнішніх і внутрішніх загроз; 3) стан і рівень інформаційно-комунікаційного розвитку країни; 4) внутрішньополітична ситуація в державі. Водночас інформаційна безпека є складною, динамічною, цілісною соціальною системою, складовими якої є підсистеми безпеки особистості, держави, суспільства. Саме взаємообумовлена, системна інформаційна єдність останніх становить якісну детермінацію, покликану захистити життєво важливі інтереси людини, суспільства і держави, забезпечити їх конкурентоспроможний, поступальний розвиток [6, с. 154–155].

Забезпечення інформаційної безпеки за рахунок послідовної реалізації чітко сформульованої національної інформаційної стратегії може суттєво сприяти забезпеченню успіху у вирішенні завдань у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах діяльності держави. Таким чином, реалізація успішної інформаційної політики може суттєво вплинути на вирішення внутрішніх, зовнішніх, військових конфліктів. Чітке розуміння та ідентифікація факторів, що призводять до загострення загроз інформаційній безпеці, мають системний характер, а тому охоплюють усі без винятку сфери життя людини, суспільства та держави. На практиці аналіз викликів завжди є суб'єктивним процесом сприйняття суб'єктом певних факторів через призму власних інтересів і професіоналізму. Важливою складовою гібридної війни експерти називають вторгнення в інформаційно-комунікаційний простір певної країни з метою придушення опору та формування глобального політичного стандарту, який відповідає інтересам агресора. Для цього використовуються найрізноманітніші інструменти маніпулювання громадською думкою: втручання у функціонування інформаційно-телекомунікаційних систем і мереж; розвиток кіберзлочинності; вплив на засоби масової комунікації та

маніпулювання громадською думкою [7, с. 18].

Як слушно зауважує М. Дмитренко: «Характер і особливості ведення російсько-української війни свідчать про те, що її метою є зміна самоідентифікації населення та перетворення східного регіону нашої країни на «сіру зону», а також перетворення східного регіону нашої країни на «сіру зону». яка залишить РФ важелі впливу через постійну загрозу поширення нестабільності на всю Україну. Це війна не за території, а за світогляд, думки та душі людей. А оскільки контроль над інформаційною інфраструктурою передбачає підстави для формування громадської думки, яка завжди спочатку проявляється в певних переконаннях, а вже потім у конкретних діях, потім в умовах конкурентної боротьби контроль над інформаційною сферою перетворюється на один із основних ресурсів влади» [8, с. 40–41].

Основними визначальними чинниками, які негативно впливають на інформаційний простір в Україні, слід вважати: 1) постійні втрати серед особового складу (убиті, полонені, поранені), що призводять до формування недовіри до українського військово-політичного керівництва, яке нібито не в змозі контролювати ситуацію, що склалася в Україні; 2) недосконала національна система інформаційної безпеки сприяє зниженню рівня патріотизму; 3) активність зовнішньої інформаційної діяльності з боку Російської Федерації впливає на формування твердження про прийнятність для України федеративного устрою держави та припинення бойових дій на Сході України в умовах кремлівського режиму [9, с. 39].

Серед основних складових інформаційної безпеки держави виділяють: обсяг виробленого в державі та державою інформаційного продукту; здатність мереж витримувати зростаюче інформаційне навантаження; здатність держави управляти розвитком виробництва та розповсюдження інформації; можливість доступу населення до всіх можливих джерел інформації, а також відкритість

більшості з них [11].

Необхідність забезпечення інформаційної безпеки визначається багатьма чинниками: необхідністю підтримки національної безпеки Української держави в цілому; наявність небезпек, що загрожують інформаційному середовищу держави та можуть завдати шкоди загальнодержавним інтересам; можливість частково керувати свідомістю та поведінкою громадян шляхом інформаційного впливу. Інформаційна безпека України ставить перед собою головне стратегічне завдання: створити потужний національний інформаційний простір як головний аспект, що засвідчує присутність країни на світовій інформаційній арені. Також така мета передбачає необхідність створення системи протидії будь-якій інформаційній загрозі та захисту власних інформаційних ресурсів, середовища та інфраструктурної складової країни. Враховуючи те, що на сьогодні національному інформаційному ресурсу відводиться роль одного з головних чинників, на яких ґрунтується економічна могутність країни та її суб'єктів, необхідно сформулювати державні інтереси, фактори та загрози інформаційній сфері, проаналізувати ефективність існуючої системи захисту та можливості її вдосконалення. Державна інформаційна політика створює умови для дискусії не лише про права громадян, юридичних осіб та країни в інформаційному полі, а й про необхідність захисту інтелектуальної власності, державних інформаційних ресурсів та конфіденційної інформації. Крім того, можна виділити низку основних положень державної політики забезпечення інформаційної безпеки: зменшення доступності інформації є винятком із загальних принципів відкритості джерел інформації та реалізується лише на законодавчій основі; необхідність персоніфікації відповідальності за те, що інформація була збережена, засекречена чи розсекречена; надання та припинення доступу до інформаційних ресурсів здійснюється на підставі встановленого законом права власності на цю інформацію; держава формує правову базу, яка регулюватиме права, обов'язки та відповідальність усіх суб'єктів інформаційного простору;

наявність юридичної відповідальності юридичних і фізичних осіб, які здійснюють збір, накопичення та обробку персональних даних і конфіденційної інформації, за її збереження та використання; держава законодавчо захищає суспільство від неправдивої, спотвореної та недостовірної інформації, що надходить через ЗМІ; органи влади контролюють створення та використання будь-яких засобів захисту інформації, обов'язкову сертифікацію та ліцензування діяльності у сфері захисту інформації; протекціоністська політика з боку держави, що означає підтримку вітчизняного виробника, який виробляє засоби інформатизації та захисту інформації, та вжиття заходів щодо захисту внутрішнього ринку від появи на ньому неякісного інформаційного продукту; держава робить світові інформаційні ресурси, глобальні інформаційні мережі більш доступними для громадян; країна намагається відмовитися від використання іноземних інформаційних технологій для інформатизації державних владних і управлінських структур і надати перевагу конкурентним вітчизняним аналогам; в державі формується програма інформаційної безпеки, в якій державні організації та комерційні структури консолідують свої сили для створення єдиної системи інформаційної безпеки; країна активно протидіє інформаційному вторгненню решти держав, сприяє інтернаціоналізації глобальних інформаційних мереж і систем [12].

Відповідно до вищезазначених принципів і положень, забезпечити інформаційну безпеку країни можливо, здійснивши низку важливих кроків: розробити науково-практичні основи інформаційної безпеки відповідно до сучасної геополітичної ситуації та умов, що диктуються політичними та соціальним -економічний розвиток; сформувати законодавчу та нормативно-правову базу для забезпечення інформаційної безпеки, зокрема розробити реєстр інформаційних ресурсів, врегулювати обмін інформацією між органами державної влади та підприємствами, унормувати відповідальність посадових осіб та пересічних українців за дотримання критеріїв інформаційної безпеки;

розробити механізми реалізації права громадянина на інформацію; сформувати систему захисту інформації, яка є складовою загального механізму національної безпеки України; розробити сучасні методи та технічні засоби, які б забезпечували комплексний підхід до вирішення завдань захисту інформації; розробити критерії та методи, за якими здійснюватиметься оцінка систем та засобів захисту інформації з точки зору ефективності та їх сертифікація; дослідити форми та можливості держави цивілізовано впливати на суспільну свідомість; всебічно дослідити діяльність персоналу в інформаційних системах, зокрема методи мотивації, зміцнити морально-психологічну стійкість і соціальну захищеність спеціалістів, які працюють з секретними та конфіденційними даними. Інформаційна безпека країни в національному масштабі визначається як система заходів, спрямованих на запобігання несанкціонованому доступу до інформаційних ресурсів, їх модифікації та знищенню. Він передбачає реалізацію таких цілей: захист політичних, державних і громадських інтересів; захищати моральні цінності; заборонити інформацію, що пропагує агресивну війну, насильство, дискримінацію та порушення прав громадян.

Національні інтереси Української держави мають певні пріоритети, визначені в Законі України «Про основи національної безпеки України». Серед них ті, що стосуються інформаційної сфери: гарантувати конституційні права і свободи людини і громадянина; збереження та зміцнення науково-технічного потенціалу, утвердження інноваційної моделі розвитку; забезпечувати розвиток і здійснення функцій, які покликана виконувати українська мова як державна в усіх сферах життя суспільства на всій території України, гарантувати вільний розвиток, використання та захист усіх мов національних меншин в Україні; розвивати духовність, моральні засади, інтелектуальний потенціал української нації. Важливою проблемою безпеки в інформаційній сфері, як уже зазначалося, є забезпечення захисту та моніторингу національної інформаційної бази та поширення інформації про стан у глобальному інформаційному просторі. Під

інформаційним простором слід розуміти середовище, в межах якого відбувається створення, збір, зберігання, обробка та розповсюдження інформаційних даних, що підпадає під юрисдикцію держави.

Слід підкреслити, що будь-які інформаційні технології складаються з: формування інформаційних даних, їх обробки, зберігання та передачі (засвоєння). В цілях безпеки слід подбати про надійну роботу всіх компонентів такої системи. Розглядаючи проблему з цього боку, можна виділити головну мету діяльності в інформаційній сфері – створення повноцінної відкритої інформаційної бази. Відсутня інформація, їх повністю або переважно негативний характер по відношенню до сучасного світу впливає на рівень зовнішньополітичної та економічної діяльності як на державному рівні в цілому, так і на окремих представниках населення та їх об'єднаннях. Це зумовлює національну важливість цієї проблеми, і якщо нею нехтувати, то вона стає загрозою національній безпеці. Саме завдяки цьому створюються належні умови для розширення інформаційної присутності у глобальному інформаційному просторі, що є найважливішим завданням державної політики у такій сфері, як інформаційна безпека. Одним із основних елементів реалізації державної політики в інформаційній сфері є інформаційна інфраструктура, яка є складовою частиною стратегічних інформаційних ресурсів і має важливе значення для обороноздатності держави та її інформаційного ринку.

Відповідно до Закону України «Про Концепцію Національної програми інформатизації» інформаційна інфраструктура включає: міжнародні та міжміські телекомунікаційні та комп’ютерні мережі; системи інформаційно-аналітичних центрів; інформаційні ресурси; Інформаційні технології; системи науково-дослідних установ з проблем інформатизації; виробництво та обслуговування технічних засобів інформації; система підготовки кваліфікованих спеціалістів у галузі інформатизації [1].

Інформаційна інфраструктура – це єдність таких компонентів, як: система виробництва продуктів інформаційної сфери, їх доставки споживачам, система виробництва інформаційних продуктів та їх доставки, система виробництва інформаційних технологічних засобів, система накопичення інформаційних засобів. і зберігання інформаційних продуктів або інформаційних ресурсів, тобто системи сервісних послуг, які надаються об'єктам інфраструктури, і системи підготовки фахівців.

1.2. Основні загрози інформаційній безпеці країни

В умовах стрімкого становлення та розвитку інформаційного суспільства в Україні та світовому інформаційному просторі, широкого використання інформаційно-комунікаційних технологій в усіх сферах життя проблеми інформаційної безпеки набувають особливого значення [13]. При цьому одним із стратегічних пріоритетів забезпечення державою інформаційної безпеки є створення цілісної системи оцінки інформаційних загроз та оперативного реагування на них [14]. Виходячи з положень Закону України «Про національну безпеку України» [15], можна стверджувати, що система загроз є основою для стратифікації національної безпеки (з урахуванням джерела, характеру та специфіки). загроз) у зовнішньополітичну, внутрішню політику, державну, військову, економічну, соціальну, гуманітарну, екологічну та інформаційну безпеку, а також безпеку державного кордону. Однак, виходячи з визначення національної безпеки, наведеного в цьому ж законі, перелік сфер, у яких можуть проявлятися загрози національній безпеці, не є вичерпним. Зокрема, залежно від середовища формування та масштабу загроз національним інтересам традиційним став поділ національної безпеки за джерелами загроз на зовнішню та внутрішню [16].

Але в сучасних умовах такий поділ стає дуже умовним, оскільки зовнішні загрози можуть виникати з внутрішніх джерел, а також інтегруватися з внутрішніми загрозами. Саме необхідність протидії загрозам визначає можливість і необхідність дослідження національної безпеки з точки зору функціонального підходу, згідно з яким національна безпека розглядається як динамічне явище, що постійно змінюється та розвивається. Цей підхід орієнтований на аналіз національної безпеки як процесу збереження та підтримання її стабільного стану як єдиного цілого, оптимального розвитку всіх рівнів і видів безпеки в цілому, що забезпечує реалізацію національних інтересів в умовах можливого розгортання загроз. Це також дає змогу оцінити здатність суспільства належним чином забезпечувати «гомеостатичний стан» об'єктів національної безпеки як стабільність певного набору характеристик за умови збереження життєздатності зазначених об'єктів, а також здатність протистояти спробам зовнішніми факторами змінювати стійкі внутрішні характеристики [17, с. 66].

Відповідно, національна безпека взаємопов'язана з чинниками, які можна вважати загрозами для неї, тому що «національна безпека — це система оптимізації співвідношення між передбачуваними загрозами та ресурсами, які суспільство має для протидії цим загрозам. Загрози суспільству є завжди, і рівень захисту від них ніколи не буває максимальним. Тому національна безпека є динамічним засобом досягнення та підтримки балансу між реальними та потенційними загрозами, з одного боку, та здатністю суб'єкта їм протидіяти, з іншого». Незважаючи на те, що поняття загрози неодноразово згадувалося в різних доктринальних та нормативно-правових джерелах, єдиного підходу до визначення його змісту та ролі в теорії науки про безпеку досі немає. Зокрема, А. Антонов і В. Балашов під загрозою розуміють процес таких змін у стані особи, суспільства, держави, які вони оцінюють як здатні створити перешкоди реалізації їхніх інтересів або унеможливити її [17].

Водночас слово «загроза», наприклад, у словнику С. Ожегова [18, с. 673], означає можливу небезпеку, тобто ще не усвідомлену.

Тобто під поняттям «загроза» мається на увазі не тільки процес зміни, а й можливість її виникнення. Під загрозою розуміють також «можливість або неминучість настання чогось небезпечного, неприємного, важкого для когось, чогось», «те, що може завдати якогось зла, якоїсь біди» [19, с. 95].

Що стосується загроз безпеці, то вони зазвичай визначаються як сукупність факторів і умов, які створюють небезпеку для певного об'єкта. О. Гацко звертає увагу на неоднозначність термінів «загроза», «небезпека», «виклик» і «ризик», які в теорії науки про безпеку вживаються як самостійно, так і взаємовизначальні, і навіть як синоніми [20, с. 111-113]. Дослідник пропонує розглядати загрозу як найвищий ступінь небезпеки (безпосередню небезпеку), а небезпеку – як потенційну загрозу. У свою чергу, небезпека розглядається як завдання заподіяння шкоди певним інтересам, для реалізації якої необхідно створити відповідні умови (можливості та наміри). Таким чином, небезпека передбачає або намір, або можливість заподіяння шкоди, тоді як загроза передбачає і те, і інше. Загрози можуть надходити з багатьох джерел і впливати на багато об’єктів, будучи неадресними. Натомість загроза, маючи конкретне джерело та об’єкт, завжди має персоніфікований характер. За такого підходу загроза розглядається як «сукупність умов і факторів, що створюють реальну та потенційну небезпеку (виклик, ризик) для об’єктів... безпеки» [20, с. 113].

У теорії забезпечення національної безпеки категорія «загроза» є не менш важливою за категорію «життєві інтереси» і тісно пов’язана з останньою, оскільки джерела загроз полягають насамперед у багатоаспектності та розбіжності інтересів. Погрозу також пропонується розглядати як «порушення інтересів», що, однак, вважається сумнівним з точки зору досягнення мети чіткого визначення змісту цієї категорії. Адже інтерес — це усвідомлена потреба,

а посягання на потребу, як і захист потреби, не впливають ні на її існування, ні на усвідомлення. У цьому контексті представляє інтерес типологія загроз національним інтересам США, яка включає три категорії: 1) регіональні (збройні конфлікти); 2) транснаціональні (наркобізнес, незаконна торгівля зброєю, міжнародна злочинність, піратство, екологічні загрози тощо); 3) асиметричні загрози.

Основною причиною виділення такої категорії загроз як асиметричних є ситуації, коли військова, економічна, науково-технічна та інша міць США та їх союзників значно перевищує міць реальних і потенційних супротивників, що, однак, не гарантує національна безпека. При цьому виділяють асиметричні загрози тактичного, оперативного та стратегічного рівня, короткострокові та довгострокові. Основою існування асиметричних загроз є різне сприйняття інтересів сторін. Наприклад, загроза з боку США та їх союзників сприймається противниками як загроза виживанню, тоді як США визначають обмежені цілі, які зазвичай не стосуються життєво важливих інтересів держави-супротивника. Наявність асиметричної загрози нанесення неприйнятної для США шкоди може стримати їх від рішучих дій і заходів проти значно слабшої за них ворожої держави. Крім того, використання такою державою тероризму, спеціальних інформаційних операцій дає змогу замаскувати джерело загрози, зробити неефективними контрзаходи США [21, с. 24].

О. Брега розглядає загрозу національній безпеці як одну з «елементарних частин теорії та практики забезпечення національної безпеки», яка характеризується об’єктивно-суб’єктивним змістом [22]. Загрози національній безпеці можна класифікувати за різними ознаками, що свідчить про їх складну та багатошарову систему.

Зокрема, у політології загрози національній безпеці класифікують:

– за місцем виникнення джерела — зовнішні та внутрішні; за

масштабом можливих наслідків – національні, регіональні, локальні, індивідуальні;

– за ступенем сформованості - потенційні, реальні; за ступенем суб'єктивного сприйняття - завищені, занижені, мінімальні, умовні, адекватні;

– за характером виникнення - загрози природного, техногенного та соціального характеру;

– за сферами життєдіяльності – загрози в економічній, політичній, оборонній, міжнародній, соціальній, інформаційній, науково-технічній, екологічній, культурній та духовній сферах [23] тощо.

1.3. Зміст політики забезпечення інформаційної безпеки держави

При цьому основною метою державної політики у сфері інформаційної безпеки є управління реальними та потенційними загрозами з метою створення необхідних умов для задоволення інформаційних потреб людей і громадян, а також реалізації національних інтересів. Як зазначають Р. Шаповал та В. Клочко, державна політика у сфері забезпечення інформаційної безпеки України – це діяльність державно-правових інституцій щодо управління реальними та потенційними загрозами та небезпеками з метою задоволення інформаційних потреб людей та громадян, а також реалізації національних інтересів, тому державна інформаційна політика та державна політика у сфері забезпечення інформаційної безпеки співвідносяться як ціле та частина [24, с. 6].

Отже, інформаційна безпека забезпечується реалізацією єдиної державної політики в інформаційній сфері, системи заходів економічного, політичного та організаційного характеру, адекватних загрозам національній безпеці, а також можливостей держави управляти відповідними ризиками. Система

інформаційної безпеки є інструментом реалізації державної політики у сфері інформаційної безпеки. Основною метою цієї системи є досягнення цілей національної безпеки в інформаційній сфері, а отже, її основною функцією є забезпечення збалансованого існування інтересів особи, суспільства та держави в інформаційній сфері. Державна політика у сфері забезпечення інформаційної безпеки має три основні вектори: захист інформаційних прав і свобод людини, захист державної безпеки в інформаційній сфері та захист національного інформаційного ринку, економічні інтереси держави в інформаційній сфері, національний товаровиробник інформаційних продуктів [25, с. 146].

Враховуючи національні інтереси та загрози в інформаційній сфері, Закон України «Про національну безпеку України» визначає основні напрями державної політики у сфері забезпечення інформаційної безпеки [15].

Єдність та взаємозв'язок напрямів державної політики у сфері забезпечення інформаційної безпеки має забезпечуватися правовими механізмами, визначеними на законодавчому рівні, серед яких: чіткі цілі та завдання державної політики; взаємодія державних і громадських інституцій у реалізації міжвідомчих напрямів державної політики; організація системи інформування суб'єктів, що здійснюють діяльність у сфері інформаційної безпеки, про поточні проблеми, виявлення потенційних і реальних загроз та їх джерел, а також відповідних заходів і засобів щодо їх запобігання, нейтралізації та ліквідації можливих наслідків; скоординованих і цілеспрямованих дій суб'єктів, що діють у різних сферах життєдіяльності суспільства і держави, з питань адекватного реагування на виявлені потенційні та реальні загрози; національне керівництво, координація та контроль у сфері забезпечення інформаційної безпеки [26, с. 170].

Враховуючи необхідність удосконалення нормативно-правового забезпечення та запобігання та нейтралізації потенційних і реальних загроз

національній безпеці в інформаційній сфері, з початком гібридної війни проти України виникла необхідність кардинальних змін у системі інформаційної безпеки України. Основний план заходів реалізовано в рішенні РНБО від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України», затвердженому Указом Президента України № 449/2014 від 1 травня 2014 р [14].

Згідно з рішенням РНБО, Кабінету Міністрів України доручено розробити та внести на розгляд парламенту проекти законів про внесення змін до законів України щодо протидії інформаційній агресії іноземних держав, передбачивши, зокрема, визначення механізм протидії негативному інформаційно-психологічному впливу, зокрема шляхом заборони ретрансляції телеканалів. а також щодо запровадження для іноземних ЗМІ системи інформування та захисту журналістів, які працюють у місцях збройних конфліктів, вчинення терористичних актів, ліквідації небезпечних злочинних угруповань. Крім того, необхідно було розробити проект стратегії розвитку інформаційного простору України, розробити та реалізувати комплекс заходів організаційного, інформаційно-роз'яснювального характеру щодо комплексного охоплення заходів щодо реалізації державної політики у сфері забезпечення інформаційної безпеки, а також посилити контроль за дотриманням законодавства з питань інформаційно-психологічної та кібербезпеки. Відповідно до зазначеного плану заходів розроблено Стратегію кібербезпеки України, зокрема, згідно з якою розвиток та безпека кіберпростору, запровадження електронного урядування, гарантування безпеки та стабільного функціонування електронних комунікацій та державних електронних інформаційних ресурсів мають бути складовими державної політики у сфері розвитку інформаційного простору та формування інформаційного суспільства в Україні [14], а також Доктрини інформаційної безпеки України [27].

В умовах гібридної війни держава, яка стала об'єктом агресії, неминуче

наражається на широкий спектр інформаційних загроз, нейтралізація яких, з одного боку, потребує неординарних правових та адміністративних заходів, а з іншого – , може супроводжуватися суттєвим обмеженням демократичних прав і свобод. Знаходження балансу між інтересами національної безпеки та ідеями правової держави є стратегічно важливим завданням держави.

ЗМІ – чи не найефективніша зброя сучасної гібридної війни. Зважаючи на це, державна політика у сфері інформаційного права повинна бути зосереджена на вибірковому застосуванні обмежень щодо окремих ЗМІ, які виявилися недружніми, заангажованими та маніпулятивними. Такий підхід вимагає максимальної правової визначеності обмежувальних критеріїв, оскільки за їх відсутності існує ризик потрапляння під заборону неангажованих та політично нейтральних ЗМІ (наприклад, у разі нецілеспрямованого поширення недостовірної інформації). При цьому низка громадських діячів та організацій наголошує, що встановлені заборони позбавлені фактичного підґрунтя, не мають правового підґрунтя, суперечать Конституції та пригнічують демократичні права і свободи. Тому будь-які обмеження в інформаційному середовищі мають бути точковими і стосуватися лише тих ресурсів, які скомпрометовані конкретними діями або є джерелом загроз для держави та суспільства [28, с. 21–22].

Нормативно-правове регулювання формування єдиного інформаційного простору України має сприяти гармонійному розвитку інформаційних ресурсів, інформаційних послуг та інформаційних продуктів в країні. Важливість проблеми розвитку законодавства у сфері інформації та інформаційної безпеки, формування інформаційного суспільства визначається тим, що норми законів у цій сфері суттєво впливають на законодавче регулювання відносин між суб’єктами в усіх сферах. державного життя. В умовах деструктивного інформаційного впливу на цільову аудиторію України та інших країн світу з боку країни-агресора Російської Федерації визначено такі основні напрями вжиття заходів щодо захисту національного інформаційного простору та забезпечення

національної системи інформаційної безпеки України. можна виділити: по-перше, удосконалити нормативно-правову базу у сфері інформаційної державної політики, яка б визначала взаємодію владних структур України з органами місцевого самоврядування, державними органами та громадськими інституціями; по-друге, створити єдиний міжвідомчий координаційний орган, який би здійснював керівництво, координацію та контроль заходів з інформаційної безпеки (його можна, наприклад, створити у формі міжвідомчої комісії при РНБО); по-третє, створити систему комплексного моніторингу популярних аудіовізуальних та друкованих ЗМІ, а також популярних Інтернет-ресурсів; по-четверте, сприяти подальшим комплексним науковим дослідженням у сфері інформаційної безпеки. На основі Стратегії національної безпеки України Указом Президента України затверджено Доктрину інформаційної безпеки України, яка лягла в основу національної політики інформаційної безпеки. Метою доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії деструктивному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни. Доктрина визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями та пріоритети державної політики в цій сфері. Державна інформаційна політика в умовах глобалізації буде ефективною лише за умови, що вона матиме комплексний, системний характер і, безперечно, буде відкритою, спрямованою на підвищення інтересів громадян, суспільства та держави. Загалом політика інформаційної безпеки як суспільне явище має комплексний характер, що включає внутрішньо- та зовнішньополітичні, економічні, технологічні, військові та інші елементи, тому потребує комплексного підходу. Діяльність органів державної влади має бути спрямована на реалізацію конкретних завдань у цій сфері та об'єднана єдиною метою – забезпечення належних умов для реалізації забезпечення інформаційної безпеки України. Система інформаційної безпеки держави є

складовою частиною загальної системи національної безпеки країни і являє собою сукупність органів державної влади, недержавних структур і громадян, які повинні координувати діяльність із забезпечення інформаційної безпеки на основі єдиних правових норм, ефективно протистояти інформаційним загрозам у сучасних умовах [13].

Так, сучасна інформаційна інфраструктура в нашій державі перебуває на стадії становлення. Нормативно-правова база відносин у сфері масової інформації розроблена не до кінця. Відсутня конкретна державна політика у сфері формування національного інформаційного простору, розвитку системи масової інформації, організації міжнародного інформаційного обміну. На цьому фоні також відзначається погіршення ситуації із забезпечення безпеки відомостей, що становлять державну таємницю. Органи державної влади та місцевого самоврядування змушені закуповувати імпортне обладнання із залученням іноземних фірм через недостатню державну підтримку розвитку вітчизняної індустрії інформаційних технологій, що підвищує ймовірність несанкціонованого доступу до інформації. Особливо небезпечним у цьому контексті є придбання програмно-технічного забезпечення виробництва країни-агресора. На жаль, при забезпеченні безпеки в інформаційно-психологічній сфері розглядається лише технічна сторона, а психологічна здебільшого залишається поза увагою. Це призводить до посилення інформаційної агресії з боку Російської Федерації, яка для просування своїх інтересів використовує суспільно-політичну ситуацію в нашій державі, в тому числі і за участю українців. Події, що відбуваються в Україні, свідчать про використання іноземними акторами зарубіжних та вітчизняних ЗМІ та соціальних мереж для зміни стану інформаційного простору з метою впливу на хід подій, що завдає значних політичних та економічних збитків нашій державі [29].

РОЗДІЛ ІІ
ОЦІНКА ЗДІЙСНЕННЯ ТА РЕЗУЛЬТАТИВНОСТІ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Основні засади державної політики забезпечення інформаційної безпеки України

Наразі у вітчизняному інформаційному просторі спостерігається високий рівень зовнішніх загроз, зумовлений активною інформаційно-пропагандистською експансією з боку Російської Федерації. Зокрема, через інформаційну сферу здійснюються спроби вплинути на політичні та соціально-економічні процеси в нашій державі, підірвати авторитет легітимної української влади з метою деморалізації суспільства та посилення невдоволення та протестних настроїв. Також російська сторона активно впроваджує технології розміщення актуальної інформації в мережі Інтернет та ЗМІ, розповсюдження якої спрямоване на місцеве населення окупованих територій, громадян Російської Федерації та міжнародне співтовариство. Антиукраїнська інформаційна кампанія функціонально реалізується російською стороною за низкою напрямків, які спрямовані на: популяризацію ідей федеративного державного устрою України як альтернативи розпаду держави; забезпечення постійного потоку маніпулятивної дезінформації про події в Україні та на її окупованих територіях; внесення розколу в середовище українських правлячих кіл, у тому числі шляхом публікації провокаційних та деструктивних матеріалів, критики центральної влади, яка «ігнорує інтереси регіонів», компрометації громадсько-політичних діячів, інспірації масових протестів; створення в Україні під виглядом представництв європейських організацій, підконтрольних російській стороні, громадських структур для проведення активної роботи в

інформаційній, аналітичній та гуманітарній сферах в геополітичних інтересах Російської Федерації тощо. За таких умов при розгляді особливого значення набуває проблема організації забезпечення інформаційної безпеки, її структурна класифікація, яка є відносно умовною і побудована відповідно до певних цілей і завдань. У цьому аспекті інформаційну безпеку в залежності від джерел виникнення загрози доцільно розділити на два види – безпеку технічного характеру, зумовлену технологіями інформаційно-комунікаційних процесів, і безпеку, спричинену соціальними факторами. Отже, на сьогодні загрози інформаційній безпеці мають соціальний характер і зосереджені у внутрішньополітичній, економічній, соціальній, екологічній, інформаційній та духовній сферах нашого суспільства [30, с. 51-52].

З метою адекватного реагування на поширення гібридних загроз в Україні наприкінці 2021 року на державному рівні було затверджено Стратегію інформаційної безпеки як основоположний документ, що визначає завдання та напрями діяльності держави з метою запобігання кризовим явищам у вітчизняному інформаційному просторі, посилення інформаційної безпеки та її складових. Очікується, що практична реалізація цієї Стратегії має посилити спроможність держави щодо забезпечення власної інформаційної безпеки та захисту інформаційного простору. Цей документ визначає Росію та її інформаційну політику як головну загрозу безпеці України. Стратегію планується реалізувати до 2025 року. Метою цієї Стратегії є зміцнення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, забезпечення інформаційними засобами та заходами соціально-політичної стабільності, захисту держави, захисту державний суверенітет, територіальну цілісність України, демократичний конституційний лад, забезпечення прав і свобод кожного громадянина. Досягнення мети здійснюватиметься шляхом здійснення заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії,

у тому числі спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету та територіальної цілісності України, забезпечення інформаційної стабільності. суспільства і держави, створення ефективної системи взаємодії органів державної влади, органів місцевого самоврядування з суспільством, а також розвиток міжнародного співробітництва у сфері інформаційної безпеки на засадах партнерства та взаємопідтримки. Цей декларативний документ (Стратегія інформаційної безпеки) визначає 7 важливих довгострокових цілей. Перший передбачає боротьбу з дезінформацією та інформаційними операціями, насамперед держави-агресора, спрямованими проти України. Друге – забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності. Третє – підвищення рівня медіакультури та медіаграмотності суспільства. Четвертий – забезпечення дотримання прав особи на збір, зберігання, використання та поширення інформації, свободу вираження своїх поглядів і переконань, захист приватного життя, доступ до об'єктивної та достовірної інформації, а також забезпечення захисту журналістів. прав. П'яте – інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та прилеглих до них територіях України, у всеукраїнський інформаційний простір. Шосте – розвиток інформаційного суспільства та підвищення рівня культури діалогу. Сьома мета – створення ефективної системи стратегічних комунікацій. Тобто зазначені цілі формують сфери, які потребують посилення контролю з боку держави, є визначальними в контексті забезпечення інформаційної безпеки [31].

Отже, до переліку загроз і викликів, які постають перед нашою державою, входять: повноформатна експансивна інформаційна політика Російської Федерації; досить низький рівень медіаграмотності громадян; динамічне зростання кількості глобальних кампаній дезінформації; інформаційне домінування Російської Федерації на тимчасово окупованих територіях;

використання технологій для маніпулювання свідомістю пересічних громадян щодо наслідків вступу України до НАТО та ЄС тощо. Зокрема, планується, що успішна реалізація Стратегії інформаційної безпеки матиме такі позитивні наслідки, як: сконструйована захищена інформація простір, що гарантує інформаційну безпеку держави та її суб'єктів; ефективне функціонування системи стратегічних комунікацій; запровадження ефективних заходів протидії поширенню нелегального контенту тощо

Цілеспрямоване маніпулювання громадською думкою із застосуванням технологій інформаційно-психологічного впливу є одним із найнебезпечніших проявів гібридної війни, яку держава-агресор веде проти України. Інформаційна безпека – це характеристика стійкого, стійкого стану загальної системи державного управління, яка зберігає свої важливі складові під впливом внутрішніх і зовнішніх загроз. Іншими словами, інформаційна безпека відповідає за захист інтересів громадянина і держави в інформаційній сфері від різних загроз, як реальних, так і віртуальних. Концепція інформаційної безпеки України розкривається через стратегію її існування як суверенної та стабільної держави, а також через розробку та реалізацію цілеспрямованої системної та виваженої політики захисту національних інтересів від зовнішніх та внутрішніх інформаційних загроз. Важливим і актуальним нормативно-правовим актом, який узагальнює нагальні та декларує актуальні питання забезпечення безпеки у вітчизняному інформаційному просторі, є Стратегія інформаційної безпеки держави, яка розрахована на найближчі п’ять років (2022 – 2025 роки). Положення цієї Стратегії концептуально розкривають такі важливі для нашої країни аспекти, як: глобальні та національні загрози та виклики вітчизняній інформаційній безпеці; завдання та напрями реалізації основних положень Стратегії; принципи стратегічного планування в цій сфері; методику досягнення ефективності реалізації її основних положень; механізми успішної реалізації його положень у практичній площині в контексті побудови основ державної

інформаційної політики. Водночас важливим завданням держави є прискорення затвердження плану заходів щодо реалізації Стратегії інформаційної безпеки та забезпечення контролю за її виконанням. Актуальним завданням державного стратегічного планування залишається раціональний розподіл державою потенційних можливостей і наявних ресурсів (людських, інформаційних, фінансових, телекомунікаційних, технічних, технологічних), завдяки чому держава гарантує забезпечення національної безпеки та стабільної соціально-економічної ситуації. та цифровий розвиток громадянського суспільства в цілому.

Для досягнення цієї мети необхідний достатньо високий рівень культури управління державним апаратом і використання методів системного аналізу та прогнозування, спеціальних методів забезпечення інформаційної безпеки тощо. Саме стратегічне планування у сфері забезпечення інформаційної безпеки дає змогу суттєво підвищити ефективність та якість державного управління у цій сфері. Стратегічне планування має розглядатися всіма органами державної влади та управління як універсальний інструмент, завдяки якому можна забезпечити виконання поточних державних завдань у сфері забезпечення інформаційної безпеки, в тому числі з використанням механізму державно-приватного партнерства. У сучасних умовах суспільство в цілому та державно-громадський сектор ІТ-сфери, зокрема, відчувають на собі наслідки триваючої агресії Російської Федерації, яка має гібридний характер, проникаючи в інформаційний простір, водночас завдаючи значної шкоди державні інтереси та приватний бізнес. Російська Федерація намагається маніпулювати свідомістю пересічних громадян, нагнітати соціальну напругу, поширювати заборонену законом інформацію за допомогою новітніх технологій, зокрема соціальних мереж та систем мікроблогів тощо [32].

Найближчим часом прогнозується збільшення кількості подальших спеціальних інформаційних операцій Російської Федерації проти України з

метою створення умов для соціальної напруги, формування загальної недовіри до чинної влади, шляхом розповсюдження фейків або спотворень. інформація про діяльність центральних органів влади, військового командування, правоохоронних органів, а також стимулювання населення до участі в акціях непокори, насамперед з використанням соціально-економічних та соціально-політичних питань. Кінцевою метою цієї діяльності є формування проросійської суспільно-політичної платформи та прихід до влади проросійських політиків для кардинальної зміни зовнішньополітичного курсу України.

У сучасних реаліях гібридна війна стає все більш інтенсивною та набуває нових форм. Тому реформа СБУ має врахувати інноваційні гібридні загрози з боку Російської Федерації та надати спецслужбі додаткові механізми протидії таким загрозам. Запобігання та недопущення такого сценарію «керованого хаосу» з боку Російської Федерації вимагає посилення можливостей вітчизняних спецслужб у здійсненні контррозвідувальних та оперативно-розшукових заходів, спрямованих, насамперед, на попередження та локалізація такої деструктивної діяльності на шкоду державним інтересам в інформаційній сфері. Важливими завданнями, які повинні залишатися в компетенції СБУ, є: здійснення заходів, спрямованих на виявлення, попередження та припинення використання іноземними організаціями та їх посадовими особами, радикально налаштованими представниками вітчизняних ЗМІ на шкоду безпеці України; вжиття на системній основі додаткових заходів, спрямованих на блокування поширення у засобах масової інформації та мережі Інтернет матеріалів, що містять заклики до посягання на державний суверенітет, територіальну цілісність України, розпалювання міжнаціональних, міжконфесійних конфліктів, пропаганду війни тощо.

2.2. Основні показники державної політики забезпечення інформаційної безпеки України

Органи державної влади, до компетенції яких належить регулювання суспільно-політичних відносин в інформаційній сфері, а також недержавні суб'єкти цієї діяльності, які залучаються до вирішення завдань державного управління, виступають суб'єктами державної інформаційної політики та забезпечують рух її правових та організаційних механізмів [33].

Власне, суб'єктами забезпечення інформаційної безпеки є органи, організації та особи, уповноважені законом здійснювати відповідну діяльність. Умовно їх можна поділити на три основні види залежно від інтересів у здійсненні даної діяльності: 1) особи як особистості; 2) громадські організації та громадськість; 3) органи державної влади. Суб'єкти державної політики у сфері інформаційної безпеки також можна поділити на дві основні категорії: а) державні установи, що реалізують інформаційну політику; б) суб'єкти масової інформації та комунікації. У системі суб'єктів державної інформаційної політики державні установи поділяються на групи залежно від: 1) рівня влади та управління (центральні, регіональні, місцеві); 2) гілки державної влади (законодавча, виконавча, судова); 3) скерування діяльності органів державної влади (органів цивільного та господарського управління, «силового блоку», зовнішньополітичних відомств тощо) [33]. У системі державної інформаційної політики суб'єкти масової інформації та комунікації поділяються на групи за такими категоріями: 1) за формою власності (державні ЗМІ та ЗМІ; недержавні ЗМІ та ЗМІ, у тому числі підконтрольні іноземні фізичні та юридичні особи); 2) за способом поширення інформації (електронні ЗМІ та ЗМІ, друковані ЗМІ та ЗМІ, Інтернет-ЗМІ) [34].

Держава посідає особливе місце як серед суб'єктів державної

інформаційної політики, так і серед суб'єктів інформаційної безпеки, оскільки володіє унікальними засобами та силами протидії загрозам у цій сфері [35].

Загальна структура державної системи забезпечення інформаційної безпеки включає чотири основні владні підсистеми, що утворюють гілки влади, що відрізняються функціями у сфері забезпечення інформаційної безпеки відповідно до своєї компетенції: глава держави, законодавча влада, виконавча влада, і судова влада. Цілі діяльності, повноваження та суб'єкти кожної з підсистем детально проаналізовано в [36]. Комплексність реалізації державної політики у цій сфері покладена на центральний орган виконавчої влади (ЦОВВ) – Міністерство інформаційної політики України, яке з 2015 року є головним органом із забезпечення інформаційної безпеки держави [37].

Особливістю реалізації даної функції дата-центром є те, що він повинен здійснювати свою діяльність на основі використання інформаційної інфраструктури, виробляти та споживати інформаційні ресурси, а також як представник власника державних інформаційних ресурсів здійснювати певні дії щодо забезпечити збереження цих ресурсів і безпеку функціонування інформаційно-телекомунікаційних систем, мереж зв'язку, систем автоматизації управління [37]. Діяльність зазначеного Міністерства у сфері інформаційної безпеки ґрунтується на таких принципах: 1) дотримання Конституції та законодавства України, а також загальновизнаних принципів і норм міжнародного права; 2) відкритість у здійсненні функцій державної влади та управління з урахуванням обмежень, встановлених законодавством України; 3) правова рівність усіх учасників процесу інформаційної взаємодії незалежно від їх політичного, соціального та економічного статусу; 4) пріоритетний розвиток вітчизняних сучасних інформаційно-телекомунікаційних технологій тощо.

Відповідно до Положення про Міністерство інформаційної політики його завданнями (у систематизованому вигляді) є [37]:

– реалізація конституційних прав і свобод громадян Української держави у сфері інформаційної діяльності;

– вдосконалення та захист вітчизняного інформаційного простору, інтеграція України у світовий інформаційний простір;

– протидія загрозі протистояння в інфосфері тощо.

Першочерговими заходами щодо реалізації державної політики забезпечення інформаційної безпеки України на сучасному етапі мають стати: 1) розробка та впровадження ефективних організаційно-правових механізмів регулювання відносин в інформаційній сфері, а також підготовка концепції громадського -приватне забезпечення інформаційної безпеки України; 2) розвиток системи підготовки кадрів, які використовуються у сфері забезпечення інформаційної безпеки держави та інформаційної інфраструктури; 3) створення системи культурно-освітньої безпеки інформаційної сфери тощо. Узагальнюючи думки фахівців у цій сфері [33, 34], можна сказати, що чинником, який визначає державну інформаційну політику в цілому, є наявність в інформаційній сфері джерел загроз інтересам держави, найнебезпечніші з яких полягають не лише в неконтрольованому поширенні «інформаційної зброї», активізації «комп'ютерного тероризму», але в недосконалості процесу організації та реалізації такої політики. Слід зазначити, що динаміка змін у системі державного управління потребує подальшого наукового дослідження всього комплексу проблем діяльності органів державної влади, вивчення практики розвинутих країн з цього питання з метою її застосування в Україна. Потребують вдосконалення організаційно-правові механізми державного впливу в цій сфері з метою соціально-економічного розвитку та забезпечення інформаційної безпеки. Невирішеною залишається проблема, по-перше, механізму розподілу сфер діяльності органів виконавчої влади загальної та спеціальної компетенції – Міністерства інформаційної політики України та місцевих державних

адміністрацій. І по-друге, щодо приведення системи та роботи Інформаційної політики України (Міністерства інформаційної політики України) у відповідність до світової позитивної практики у цій сфері, що передбачає узгодження її системи з суспільними та приватними інтересами, її ієрархія. Нині, згідно з положенням про це міністерство, питаннями інформаційної безпеки покликаний його відповідний сектор [37].

При цьому реалізація політики інформаційної безпеки покладається на місцеві органи виконавчої влади загальної компетенції, а не спеціальні органи (до якого має входити згадане міністерство), що порушує такі основоположні, загальновідомі принципи державного управління: 1) єдність і системність; 2) збалансоване виконання функцій, їх нерозпорошеність; 3) дієвість та ефективність; 4) збалансоване використання «портфеля» ресурсів; 5) публічність (прозорість і відкритість); 6) ефективність і соціальна спрямованість тощо.

Тому для України сьогодні є актуальними завдання розвитку інформаційного суспільства, аналізу загроз в інформаційній сфері, забезпечення інформаційної безпеки Української держави як частини світового інформаційного співтовариства. Розробка державних заходів щодо забезпечення інформаційної безпеки громадян, суспільства та держави є одним із найважливіших пріоритетів державного управління у цій сфері, що потребує ефективної міжгалузевої взаємодії, зокрема між державними органами та за участю приватний сектор.

2.3. Головні тренди та напрямки реалізації державної політики з інформаційної безпеки України

Ми повністю підтримуємо Є. Мануйлова, що в стратегічному плані держава має зміцнювати аксіосферу суспільства шляхом відтворення цінностей

через освіту та виховання, дбати про інформаційну безпеку та захист культурно-інформаційного поля країни від зовнішніх впливів. Інформаційна стабільність та реалізація чітких ціннісних пріоритетів демократичного розвитку держави забезпечить її конкурентоспроможність у глобальних процесах сучасності [38, с. 16]. До цього твердження слід додати важливе застереження відомого соціолога М. Вебера про те, що кожна історична епоха має свою систему цінностей, тобто ця категорія є принципово історичною [39, с. 64]. Варто погодитися з думкою С. Ларіна, що національні цінності – це певні концептуальні, світоглядні основи, консолідуючі фактори, важливі життєві орієнтири на шляху ефективного суспільного розвитку [40, с. 47]. Проблему національних цінностей ґрунтовно дослідили вітчизняні дослідники В. Горбулін та А. Качинський. Вони структурували систему національних цінностей, розділивши їх на цінності особистості, цінності суспільства та цінності держави [41, с. 107].

На думку дослідників, подальше існування держави і нації слід розглядати крізь призму її ціннісного ядра, що консолідує суспільство, а саме: національної безпеки, духовних надбань, добробуту, системи міжнаціональних відносин, патріотизму та соціальної справедливості. На нашу думку, до наведеної системи національних цінностей слід також додати такі індивідуальні цінності, як: мораль; релігійність; взаємна толерантність; миролюбність; добра воля; тяжка робота; родина (родинні цінності) тощо, які завжди були притаманні українцям і відображають сутнісні засади українського національного характеру. В. Горбулін особливо підкреслив Національні цінності в інформаційній сфері (найменш мобільні) Національні цілі в інформаційній сфері (найбільш мобільні) Національні інтереси в інформаційній сфері (порівняно динамічні) Державну політику у сфері правового захисту інформаційної безпеки Національні надбання в інформаційній сфері важливість національних цінностей, зазначаючи, що стратегія національної безпеки України формується на основі оцінок національних цінностей у контексті міжнародної ситуації [42, с. 5]. Така

обережність стала особливо актуальною з початком збройної агресії Росії проти України. Національні цінності в інформаційній сфері - це сукупність духовних і матеріальних цінностей людини, суспільства і держави, які характеризуються чітко визначеними світоглядними, соціокультурними, соціально-економічними, географічними та демографічними характеристиками. Вони формують правову, світоглядну та етичну основу для забезпечення подальшого існування суспільства і держави, дають змогу реалізувати національну мету держави в інформаційній сфері. Національні цінності в інформаційній сфері, виходячи з їх сутнісної інтерпретації, є найбільш особливим сегментом, тим, що потребує особливого захисту.

До національних цінностей в інформаційній сфері, зважаючи на сучасний стан державотворення в Україні, слід віднести:

- матеріальний добробут населення, у тому числі на основі розвитку ІКТ;

- інформаційна безпека людини, суспільства, держави;

- духовність (доступність релігії, відсутність загроз, недопущення релігійного фанатизму та екстремізму, неприпустимість використання релігії як психологічного чинника тероризму, розвиток традиційних українських релігійних течій);

- мова як головний ідентифікатор нації, як спосіб передачі інформації та знань, як пам'ять поколінь;

- культура інформаційних відносин;

- свобода інформації (захист прав людини на інформацію, доступ до інформації, нейтралізація негативних інформаційних впливів). Соціально-економічна складова інформаційної безпеки має стати первинною в структурі національних цінностей в інформаційній сфері. Таким чином, на наше глибоке переконання, добробут населення, як базова категорія економічної політики

держави, має стати основною складовою інформаційної безпеки держави, а особливо національної безпеки нашої держави.

На думку Г. Ситника, об'єктивне існування та вплив на безпеку особистості, суспільства, держави та людської цивілізації природних і суспільних явищ зумовлює можливість поділу цінностей на природні та соціальні [43], що в цілому відображено у запропонованому вище переліку національних цінностей в інформаційному полі. Відомий вчений у галузі філософії та національної безпеки Б. Парахонський ще на початку 90-х років минулого століття зазначав, що в сучасному світі захист національних інтересів уже не може спиратися лише на стратегію силове протистояння. Ефективнішою стає реалізація власних національних інтересів за допомогою економічної, духовної та інтелектуальної експансії. Це твердження підтверджує вітчизняна історія останнього десятиліття з кульмінацією у 2014 році [43].

Таким чином, до національних цілей в інформаційному полі належать:

– припинення порушення та спотворення поглядів людей на навколишній світ і себе, що здійснюється шляхом культивування уявних цінностей, насадження деструктивних пріоритетів, завдань і цілей перед суспільством і особистістю (духовна безпека);

– забезпечують впровадження інформаційних технологій у військову сферу та забезпечують їх захист (військова безпека);

– прискорити розробку та впровадження новітніх конкурентоспроможних ІКТ у соціально-економічній сфері (економічна безпека); досягти належного рівня культури інформаційних відносин (соціальної безпеки);

– створити загальнодержавні інформаційні системи постійного екологічного моніторингу стану довкілля (економічної безпеки);

– сприяти інтеграції національної інформаційної інфраструктури з глобальною інфраструктурою. посилити захист інформаційних прав людини;

– вжити невідкладних заходів щодо формування позитивного іміджу держави в умовах інформаційної глобалізації.

Дещо цікавою та привабливою є категорія «національне надбання», яка більше характерна для сфери культури та мистецтва. Проте, з огляду на стрімкий розвиток інформаційних технологій, їх визначальний вплив як на військову сферу, так і на інші суспільні відносини, насамперед медицину, економіку, ряд досягнень в інформаційній сфері можна віднести до національного надбання в інформаційній сфері. Водночас у зазначеній сфері вони відіграватимуть роль певного індикатора та критерію ефективності реалізації національних цілей в інформаційній сфері. Закон України «Про інформаційну безпеку України» визначив національні надбання в інформаційній сфері як найважливішу та найціннішу частину інформаційних ресурсів, передусім кінцеві результати інтелектуальної та творчої діяльності, кращі зразки вітчизняної (національної) інформаційної продукції без позбавлення права власності можуть бути оголошені національним надбанням України і незалежно від форм власності охоронятися державою як пам'ятки історії та культури. Не зовсім зрозуміло, чому автори цього законопроекту обмежилися лише пам’ятками історії та культури, адже ці активи мають значно ширший діапазон ціннісних орієнтацій [43].

На нашу думку, національні надбання в інформаційній сфері – це сукупність унікальних інформаційних продуктів, які мають виняткове військове, соціальне, економічне тощо значення для реалізації національних цілей в інформаційній сфері. Створити вичерпний перелік національних надбань в інформаційному полі неможливо, оскільки щодня такий перелік може доповнюватися відповідними розробками або, навпаки, виключатися через

моральне старіння чи втрату вартості. Визначальним критерієм для включення до такого переліку є особлива, стратегічна важливість інформаційного продукту як для забезпечення інформаційної безпеки держави безпосередньо, так і для розвитку інших сфер і є унікальною за своєю природою. Їх розвиток і позитивний вплив як на забезпечення інформаційної безпеки держави, так і на інші суміжні сфери значною мірою залежить від продуманої державної політики та ефективних правових механізмів її реалізації.

Варто підтримати позицію відомого українського дослідника державного управління національною безпекою Г. Ситник, який дійшов висновку, що національні цінності визначають сутність (зміст), цілісність і стійкість, національні інтереси – структуру та характер, а національні цілі – конфігурацію та спрямованість формування та функціонування цих систем [44, с. 46]. Це стосується загалом інформаційної безпеки держави.

РОЗДІЛ ІІІ
ПРОБЛЕМИ ТА НАПРЯМКИ УДОСКОНАЛЕННЯ ПОЛІТИКИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

3.1. Основні проблеми реалізації державної політики з інформаційної безпеки України

Інформаційна безпека України – це захист політичних, державних, суспільних інтересів країни, загальнолюдських і національних цінностей, передбачених Конституцією [45]. Важливість забезпечення інформаційної безпеки проголошена статтею 17 Конституції України [46] однією з найважливіших функцій держави і справою всього Українського народу поряд із захистом суверенітету, територіальної цілісності та економічного розвитку України. безпеки. У сучасних умовах найважливішим елементом інформаційної безпеки є кібербезпека. Запроваджена у 2016 році та затверджена Указом Президента України від 15 березня 2016 року № 96/2016 Стратегія кібербезпеки України [5] свідчить про пріоритетність забезпечення кібербезпеки в Україні. Отже, початок регулюванню інформаційної безпеки в Україні покладено, що, безперечно, є позитивним кроком. Проте шляхи реалізації прийнятих норм на практиці розвиваються дуже повільно і в більшості випадків не є правовим інструментом для практичного застосування та забезпечення ефективності заходів кібербезпеки. Головною метою державного управління є розробка та реалізація концептуальних засад державної інформаційної політики шляхом прийняття відповідних нормативно-правових актів з питань регулювання інформаційних відносин [47].

Останнім часом значно зросла потреба у комплексному та дієвому підході до процесу забезпечення безпеки національного інформаційного простору, який

чітко представлений у нормативних документах зарубіжних країн. У провідних країнах світу законодавство про інформаційну політику та інформаційну безпеку формувалося десятиліттями, і, як свідчить їх досвід, злагоджена діяльність відповідного державно-правового механізму, тобто системи взаємопов'язаних державних органів, організацій, установ щодо розроблення та реалізація комплексу норм і принципів права, які мають регулювати суспільні відносини в інформаційній сфері [47, 48].

При цьому основною метою державної політики у сфері інформаційної безпеки є управління реальними та потенційними загрозами з метою створення необхідних умов для задоволення інформаційних потреб людей і громадян, а також реалізації національних інтересів. Як зазначають Р. Шаповал та В. Клочко, державна політика у сфері забезпечення інформаційної безпеки України – це діяльність державно-правових інституцій щодо управління реальними та потенційними загрозами та небезпеками з метою задоволення інформаційних потреб людей та громадян, а також реалізації національних інтересів, тому державна інформаційна політика та державна політика у сфері забезпечення інформаційної безпеки співвідносяться як ціле та частина [49, с. 6]. Отже, інформаційна безпека забезпечується реалізацією єдиної державної політики в інформаційній сфері, системи заходів економічного, політичного та організаційного характеру, адекватних загрозам національній безпеці, а також можливостей держави управляти відповідними ризиками . Система інформаційної безпеки є інструментом реалізації державної політики у сфері інформаційної безпеки. Основною метою цієї системи є досягнення цілей національної безпеки в інформаційній сфері, а отже, її основною функцією є забезпечення збалансованого існування інтересів особи, суспільства та держави в інформаційній сфері. Державна політика у сфері забезпечення інформаційної безпеки має три основні вектори: захист інформаційних прав і свобод людини, захист державної безпеки в інформаційній сфері та захист національного

інформаційного ринку, економічні інтереси держави в інформаційній сфері, національний товаровиробник інформаційних продуктів [24, с. 146]. Враховуючи національні інтереси та загрози в інформаційній сфері, Закон України «Про національну безпеку України» визначає основні напрями державної політики у сфері забезпечення інформаційної безпеки [16].

Єдність та взаємозв'язок напрямів державної політики у сфері забезпечення інформаційної безпеки має забезпечуватися правовими механізмами, визначеними на законодавчому рівні, серед яких: чіткі цілі та завдання державної політики; взаємодія державних і громадських інституцій у реалізації міжвідомчих напрямів державної політики; організація системи інформування суб'єктів, що здійснюють діяльність у сфері інформаційної безпеки, про поточні проблеми, виявлення потенційних і реальних загроз та їх джерел, а також відповідних заходів і засобів щодо їх запобігання, нейтралізації та ліквідації можливих наслідків; скоординованих і цілеспрямованих дій суб'єктів, що діють у різних сферах життєдіяльності суспільства і держави, з питань адекватного реагування на виявлені потенційні та реальні загрози; національне керівництво, координація та контроль у сфері забезпечення інформаційної безпеки [16].

Органи державної влади та місцевого самоврядування змушені закуповувати імпортне обладнання із залученням іноземних фірм через недостатню державну підтримку розвитку вітчизняної індустрії інформаційних технологій, що підвищує ймовірність несанкціонованого доступу до інформації. Особливо небезпечним у цьому контексті є придбання програмно-технічного забезпечення виробництва країни-агресора. На жаль, при забезпеченні безпеки в інформаційно-психологічній сфері розглядається лише технічна сторона, а психологічна здебільшого залишається поза увагою. Це призводить до посилення інформаційної агресії з боку Російської Федерації, яка для просування своїх інтересів використовує суспільно-політичну ситуацію в нашій державі, в

тому числі і за участю українців. Події, що відбуваються в Україні, свідчать про використання іноземними акторами зарубіжних та вітчизняних ЗМІ та соціальних мереж для зміни стану інформаційного простору з метою впливу на хід подій, що завдає значних політичних та економічних збитків нашій державі. Відкритість національного інформаційного простору створює реальну загрозу негативного інформаційно-психологічного впливу на суспільну свідомість населення, що становить особливу суспільну небезпеку. Безконтрольність електронних ЗМІ та соціальних мереж, які використовуються як майданчик для вербування в екстремістські організації, злочинні угруповання, незаконні збройні формування тощо, негативно впливає на користувачів Інтернету, якими є переважно молодь та освічені люди. з активним способом життя. Слід також враховувати, що наразі українське суспільство розділене у ставленні до таких фундаментальних цінностей, як демократія, незалежність, приватна власність, ринок тощо. Існують розбіжності щодо уявлень про форму правління та правління, кількість мов офіційного спілкування та освіти, напрямів децентралізації, функцій і завдань місцевого самоврядування тощо. Існує ціла низка міжрегіональних, міжетнічних, міжрелігійних розбіжностей, різна шкала цінностей і пріоритетів, а тому важко говорити про єдність інформаційного простору та спільність ціннісних орієнтацій, що також є джерелом різноманітних внутрішніх загроз. Наразі в Україні на законодавчому рівні відсутні достатні гарантії захисту населення від негативних інформаційно-психологічних впливів, наслідком яких може стати руйнація єдиного інформаційно-духовного простору. Тому виникає необхідність формування державної системи забезпечення інформаційно-психологічної безпеки, яка має будуватися на основі тісної взаємодії всіх гілок влади, а також громадських організацій. У процесі реалізації державної політики у сфері безпеки необхідно приділяти увагу: розробці та реалізації комплексних заходів щодо запобігання, нейтралізації та попередження негативних інформаційно-психологічних впливів на суспільство і державу;

підготовка суспільства до активної інформаційної протидії; входження національного інформаційного поля у світовий інформаційний простір; вдосконалення системи масової інформації та комунікації; формування системи підготовки особового складу до інформаційно-психологічної протидії; духовна консолідація суспільства та відкриття нової соціальної ідентичності всіма верствами населення. У сучасних умовах інформаційну безпеку слід визнати основою інформаційної складової всіх сфер національної безпеки. До основних завдань системи інформаційної безпеки належать: прогнозування ризиків реалізації державної внутрішньої та зовнішньої політики, міждержавних і державних програм і проектів; визначення внутрішніх і зовнішніх потенційних і реальних загроз; розроблення та впровадження адекватних заходів і засобів реагування на виклики як історичного походження, так і сучасного цивілізаційного розвитку; нейтралізації або послаблення наслідків проявів гібридної війни та інших загроз національній безпеці України. Системний і комплексний підхід до вирішення цих проблем має належним чином визначати напрями державної політики у сфері інформаційної безпеки нашої країни [16].

Забезпечення інформаційної безпеки є визначальним напрямом державної політики, від якого залежатиме існування суверенної та незалежної держави, її національна безпека, соціально-економічний розвиток та належне місце у світовому співтоваристві.

Наприклад, у Молдові існує стратегія інформаційної безпеки, яка містить опис безпекових та правових питань, цілі, завдання, ключові показники ефективності (KPI), план впровадження з чітким розподілом відповідальних осіб. У Данії також на державному рівні розроблено стратегію інформаційної та кібербезпеки, яка всебічно охоплює питання реалізації – від найвищого державного рівня – до безпеки людини в мережі. Естонія, яка вважається європейським лідером у використанні цифрових технологій в економіці та управлінні, опікується захистом інформації з 1996 року.

Правова складова має встановлювати норми та гарантувати правові механізми системи захисту інформації в державі, забезпечувати відповідний механізм попередження, реагування та розслідування будь-яких порушень інформаційної безпеки. Технічна складова має забезпечувати конфіденційність, цілісність та доступність інформації за допомогою інженерно-технічних заходів. Комунікаційна складова – це забезпечення системи моніторингу та створення контенту в соціальних мережах. Освітня складова – це комплексне системне навчання інформаційній безпеці в навчальних закладах, а також підвищення кваліфікації працівників органів державної влади та місцевого самоврядування, які працюють з інформацією [50]. З метою реалізації національних інтересів в інформаційній сфері необхідно переглянути пріоритети державної політики, розробити нові концептуальні підходи щодо регулювання ринку інформаційно-комунікаційних технологій, інформаційної та інвестиційної політики, розвитку інформаційного законодавства та забезпечення інформаційної безпека [51]

Рівень інформаційної безпеки активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України, адже найчастіше реалізація інформаційних загроз означає завдання шкоди в політичній, військовій, економічній, соціальній, екологічній сферах тощо. На жаль, наразі в Україні немає реальних гарантів її інформаційної безпеки, відсутній комплекс нормативно-правових актів щодо захисту інформаційних ресурсів та інформаційної інфраструктури. При цьому процес інформатизації має стихійний, неконтрольований характер з переважним ухилом на використання засобів інформатизації іноземного виробництва [52]

Запропоновані заходи є лише першими необхідними кроками у зміцненні державного управління інформаційною безпекою. Потрібні подальші комплексні дослідження в цьому напрямі, пріоритетами яких мають бути аналіз загроз у національному інформаційному просторі та проблематика забезпечення інформаційної безпеки держави як частини світового інформаційного

співтовариства.

3.2. Напрямки реформування державної політики з інформаційної безпеки України

Порівняно з розвиненими країнами Західної Європи та Північної Америки проникнення Інтернету в Україні відбувається повільніше. Експерти вважають, що протягом наступних трьох років, порівняно з допандемічним періодом (2019), темпи зростання цифровізації економіки зростуть на 1-5%. Найбільше від впливу цифровізації виграє сектор комп'ютерного програмування, поштових і кур'єрських послуг, телекомунікацій та освіти [53].

Разом із зростанням рівня цифровізації зростають і загрози інформаційній безпеці, а саме кіберзагрози. Саме цей вид загрози інформаційній безпеці завдає найбільших фінансових втрат і, безперечно, впливає на рівень фінансової безпеки країни в цілому. Кіберзлочинці найчастіше атакують користувачів інтернету через месенджери. У 2021 році 45% опитаних українців стикалися зі спробами онлайн-шахрайства. У 2020 році цей показник становив 22%. З початку 2021 року найбільше кібератак зазнали жителі великих міст. Згідно з офіційними статистичними даними рівень кіберзлочинності в Україні постійно зростає (рис. 1) [53].

Зазначимо, що Україна є лідером за кількістю кібератак у світових рейтингах, що свідчить про низький рівень захисту інформаційного середовища. Розглядаючи структуру кіберзлочинів у 2020 році, виявилося, що найбільшу частку (54%) випадків шахрайства становив продаж неіснуючого товару на умовах передоплати. Фішингові атаки склали 28% кіберзлочинів, коли користувачам надсилали в повідомленнях шкідливі посилання на підроблену платіжну форму з метою викрадення персональних даних користувача. 11% – шахрайство, пов'язане з розсилкою підроблених скріншотів/квитанцій про

оплату товару. Основною причиною успіху кібератак є саме людський фактор – 91% зломів здійснюється в результаті успішного фішингу.

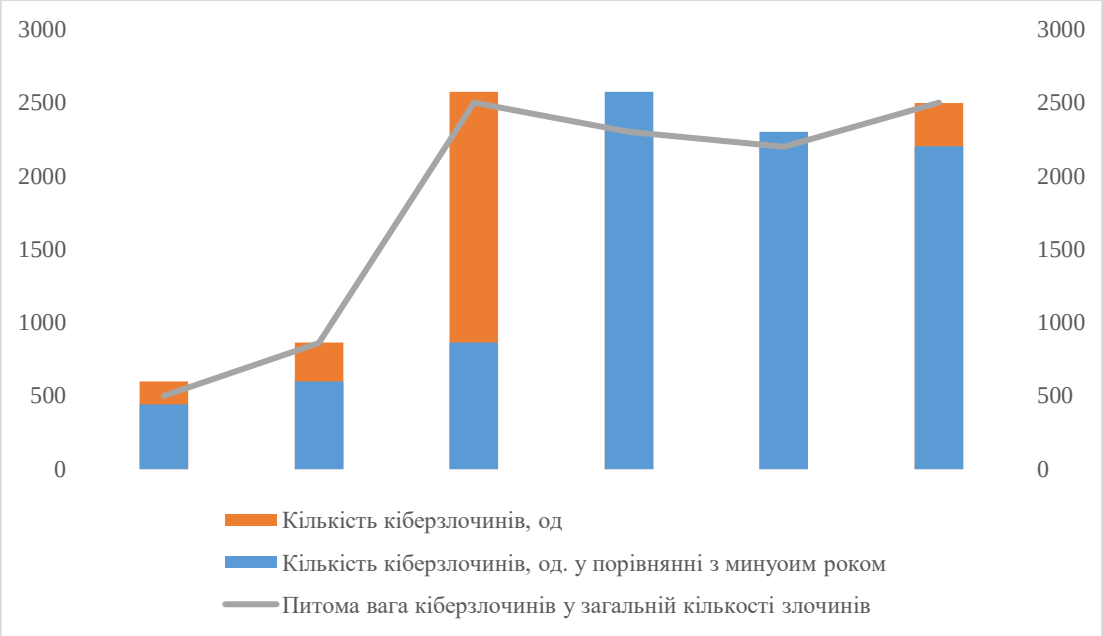

Рис. 1. Рівень та динаміка кіберзлочинів в Україні у 2015 - 2020 рр.

*Джерело: [52]

Згідно з опитуванням Harvey Nash/KPMG CIO Survey, 4 з 10 IT-лідерів повідомляють про збільшення кількості кібератак, причому понад три чверті цих атак викликані фішингом (83%) і майже дві третини через зловмисне програмне забезпечення (62%), доводячи, що масовий перехід на онлайн-роботу збільшив ризик і незахищеність праці працівників [54]. Так, за офіційними даними розробника програмного забезпечення у сфері захисту інформації та кібербезпеки ESET, у 2020 році кількість веб-загроз та кібератак в Україні зросла вдвічі, в тому числі через електронну пошту (шкідливе програмне забезпечення, програми-вимагачі сімейства WannaCryptor, завантажувачі та криптомайнери, експлойти EternalBlue тощо). Водночас фінансові втрати світової економіки через кіберзлочини у 2020 році перевищили 1 трлн. доларів, що майже вдвічі більше, ніж у 2018 році [55].

Ці дані підтверджують важливість інформаційної політики, як основної

складової інформаційної безпеки, для забезпечення фінансової безпеки держави. Таким чином, стрімкий розвиток інформаційних технологій ставить нові виклики не лише перед Україною, а й перед світовою спільнотою в цілому. Сьогодні розвинені країни йдуть шляхом цілеспрямованого правового регулювання відносин у національному інформаційному просторі, прийняття необхідних законодавчих актів, перебудови діяльності органів державної влади, відповідальних за реалізацію інформаційної політики. Наприклад, Велика Британія з метою покращення умов конкуренції на інформаційному ринку та підвищення ефективності інформаційних послуг реалізує інформаційну політику, засновану на принципах технологічної нейтральності законів, сприяння міжнародному співробітництву, захисту інтересів споживачів. в комп'ютерних системах і мережах. Німеччина націлена на безперешкодний транскордонний обмін інформацією, розвиток цифрових технологій, вільну конкуренцію в інформаційній сфері. Тим часом уряд Франції створив Фонд допомоги та співпраці для підтримки впровадження вітчизняних інформаційних технологій, стимулювання наукових досліджень у сфері IT-технологій, створення систем інформаційної безпеки та запобігання комп’ютерним злочинам. Сучасна інформаційна політика Європейського Союзу базується на доктрині європейського інформаційного суспільства, основною ідеєю якої є зміщення акценту з геополітики на технополітику, що реалізується в межах компетенції міжнародних регіональних організацій, які вирішують всю комплекс політичних, економічних і соціальних проблем європейських країн [56].

Нормативно-правова база ЄС в інформаційній сфері постійно доповнюється та розширюється, внаслідок чого є дуже широкою та розгалуженою. Інформаційна політика США спрямована на підтримку наукових досліджень і розробок у сфері інформації та телекомунікацій, сприяння обміну технологіями між університетами та компаніями, створення та вдосконалення

інформаційної інфраструктури, забезпечення балансу між основними інформаційними цінностями. США суворо контролюють питання державних таємниць, які зберігаються в урядових і комерційних телекомунікаційних мережах, унеможливлюючи їх витік за межі країни. У 1987 р. Конгрес США прийняв Закон «Про забезпечення комп'ютерної безпеки», який встановив пріоритет національних інтересів у вирішенні питань інформаційної безпеки, зокрема приватної інформації [57].

Слід зазначити, що аналіз досліджень наукових розвідок з питань інформаційної безпеки США показав, що, незважаючи на велику кількість нормативно-правових актів у сфері інформаційної безпеки, вони не завжди були ефективними, оскільки законодавство країн Сполучені Штати не охопили всіх загроз в інформаційній сфері держави, особливо після 11 вересня 2001 року (дата, відома як теракт у Лос-Анджелесі з найбільш масштабними наслідками). Тому захист інформаційного простору від кібертерористів та шахрайства сприяв розробці нормативно-правових актів з інформаційної безпеки США принципово нового, вищого рівня. Загалом, за останні 35 років у США сформувалася чітка, досконала система забезпечення інформаційної безпеки, яка характеризується поступовими тенденціями та радикальними заходами. Тому американський досвід державної політики у сфері інформаційної безпеки є важливим для української зовнішньої та внутрішньої політики, а особливо, найціннішим є ефективний підхід до регулювання ринку інформаційних технологій та забезпечення фінансової безпеки країни.

Важливо зазначити, що в умовах інформаційної агресії для України надзвичайно важливим є американський досвід використання інформаційних технологій для створення систем зв'язку та військового управління. Прийняття Стратегії інформаційної безпеки України у 2021 році стало важливим кроком у напрямку підвищення ефективності інформаційної політики. Водночас, враховуючи позитивний світовий досвід, правомірно виділити наступні

напрямки реалізації інформаційної політики в аспекті забезпечення фінансової безпеки України.

1. Розвиток національної інформаційної інфраструктури, здатної протидіяти зовнішнім і внутрішнім ризикам і загрозам, забезпечуючи захист національних інтересів, зокрема економічних.

2. Посилення інституційної спроможності у сфері стратегічних комунікацій, що передбачає формування механізму координації та взаємодії між органами державної влади, які здійснюють заходи щодо протидії ризикам і загрозам в інформаційній, фінансовій та інших сферах національної економіки.

3. Підвищення рівня інформаційної спроможності населення, а саме забезпечення вільного доступу до об'єктивної, неупередженої та правдивої інформації.

4. Забезпечення підвищення рівня інформаційної культури та медіаграмотності суспільства як основи протидії деструктивним інформаційним впливам. Державна інформаційна політика в умовах глобалізації буде ефективною лише за умови, що вона матиме комплексний, системний характер і, безперечно, буде відкритою, спрямованою на забезпечення економічних інтересів громадян, бізнесу та держави [53].

Держави, які мають потужний потенціал в інформаційному середовищі, можуть впливати на країни, в яких інформаційний простір є незахищеним. За останні три роки в Україні здійснено більше заходів щодо забезпечення інформаційної безпеки в інформаційному просторі, ніж за весь попередній період незалежності [31, с. 126].

Загалом існує з десяток різних видів інформаційного впливу. Тому слід розрізняти пропаганду, спеціальні інформаційні операції, психологічні операції, дезінформацію та інші види впливу, оскільки кожна з них має свій алгоритм, форми та методи здійснення. Досвід протидії інформаційним операціям

переконливо свідчить, що вони здебільшого плануються та організовуються з-за кордону, але з опорою на наявні оперативні позиції та можливості країни, де така операція проводиться. Зазвичай російські інформаційні операції відрізняються тим, що вони плануються і реалізуються в рамках єдиного оперативного плану і спільного стратегічного наративу, відрізняючись лише формами і методами реалізації, а також вибором цільової аудиторії. . Але безпосередні виконавці часто проживають в Україні, що дає можливість вітчизняній спецслужбі викривати конкретних осіб, мережі ботоферм чи ферм тролів та застосовувати до них відповідні заходи, передбачені чинним законодавством. Наприклад, ферми тролів – це більш складна структура, яка має свою ієрархію, де працюють «живі» люди. Найвища ланка – це ті, хто пише пости, виступає з «експертною» думкою, ініціює дискусію та визначає напрямок дискусії. Як правило, вони самостійно пишуть тексти на задану замовником тему, відповідно до затверджених методичних рекомендацій. Але в них складно знайти загальні фрази та приказки. Ви можете побачити лише емоційно забарвлені маркери, як-от «тарифний геноцид», «київська влада», «каратели» тощо. Знову ж таки, викривальною ознакою таких тролів є збіг повідомлень із часом порушення того чи іншого питання. Далі в ієрархії йдуть виконавці, які діляться публікаціями перших, додаючи власні слова та активно реагуючи на коментарі користувачів, щоб підтримати пост у стрічці новин. Нижча ланка – особи, які здійснюють позиційне коментування. Як правило, вони роздають заздалегідь написані коментарі (10-20 варіантів) і неохоче обговорюють. Вони не в змозі відповісти на більш-менш серйозне питання по темі, що коментується. Головне завдання тролів – ініціювати в мережі інформаційну хвилю на задану тему (або хвилю «флуду» чи «флейму»), до якої масово приєднаються реальні користувачі, яких росіяни на професійному жаргоні називають «пушечным м’ясом». Але ферми ботів чи тролів самі по собі не небезпечні. Їх вражаюча ефективність забезпечується тим, що практично всі сегменти бото- і трол-ферм (якщо мова йде

про російські) є функціональною складовою російських автоматизованих комплексів моніторингу Інтернету з прихованими функціями впливу на процеси в середовищі соціальних мереж. Так, в Російській Федерації діють системи моніторингу компаній «Крібрум», «Медіалогія», «Квант», «Бастіон», «Бранд Аналітика» та ін. Кількість автоматизованих облікових записів ботів, що працюють у всьому світі, становить понад 100 млн акаунтів. (тільки в системі Cribrum). Таке поєднання дає змогу реалізувати небезпечну технологію впливу на користувачів соціальних мереж, так званий «астротурфінг» – імітацію широкої суспільної підтримки певних ідей, думок, повідомлень, а також осіб чи політичних сил. Астротурфінг дозволяє створити фейкову громадську думку чи інтерпретацію події, яку користувачі Інтернету сприймуть як реальну. Наявність таких систем дозволяє Російській Федерації на основі моніторингу інтернет-контенту та аналітичної обробки «великих даних» виявляти вразливі місця противника, планувати, здійснювати та коригувати власні інформаційні атаки, а також контролювати їх ефективність і ефективність. За таких умов не можна недооцінювати роль і місце Служби безпеки України в забезпеченні інформаційної безпеки в Україні. Логічно, що в положеннях Стратегії інформаційної безпеки значну роль відведено діяльності вітчизняної спецслужби, яка в межах своєї компетенції здійснює моніторинг завдяки спеціальним методам і прийомам вітчизняних та іноземних ЗМІ та мережі Інтернет. з метою виявлення реальних та потенційних загроз безпеці держави в інформаційній сфері; організовує та забезпечує протидію проведенню спеціальних інформаційних операцій проти України, особливо з боку Російської Федерації, спрямованих на підрив конституційного ладу, порушення суверенітету та територіальної цілісності України.

Так, наприклад, за результатами успішної діяльності у сфері запобігання та протидії інформаційним загрозам вітчизняна спецслужба відзвітувала про такі досягнення за підсумками І півріччя 2021 року: відкрито 21 кримінальне

провадження за ст. 109 та ст. 110 КК України; 19 особам притягнуто до відповідальності за дії, відповідальність за які передбачена ст. 109 та ст. 110 КК України; заборонено в'їзд в Україну понад 50 іноземним громадянам; Заблоковано 8 ботоферм із загальною кількістю понад 35 тисяч акаунтів; припинено діяльність 16 інтернет-агітаторів; проведено понад 180 профілактичних заходів; заблокували 58 веб-ресурсів, на яких поширювався фейковий та деструктивний контент [58].

За перше півріччя 2021 року кіберфахівці Служби безпеки України локалізували майже 350 потенційних загроз інформаційній безпеці нашої країни. Притягнуто до кримінальної відповідальності 35 хакерів і ворожих пропагандистів, 14 зловмисників засуджено. На цьому тлі СБУ стала ефективним інструментом у роботі РНБО. Також зазначимо, що в липні 2021 року при Раді національної безпеки і оборони України була створена група з питань захисту вітчизняного інформаційного простору. Очікується, що напрацювання та результати робочої групи можуть бути використані для ініціювання впровадження відповідних регуляторних змін з урахуванням досвіду демократичних країн світу щодо забезпечення високого рівня захисту від трансформаційних гібридних загроз. Висновки. Цілеспрямоване маніпулювання громадською думкою із застосуванням технологій інформаційно-психологічного впливу є одним із найнебезпечніших проявів гібридної війни, яку держава-агресор веде проти України. Інформаційна безпека – це характеристика стійкого, стійкого стану загальної системи державного управління, яка зберігає свої важливі складові під впливом внутрішніх і зовнішніх загроз. Іншими словами, інформаційна безпека відповідає за захист інтересів громадянина і держави в інформаційній сфері від різних загроз, як реальних, так і віртуальних. Концепція інформаційної безпеки України розкривається через стратегію її існування як суверенної та стабільної держави, а також через розробку та реалізацію цілеспрямованої системної та виваженої політики захисту національних

інтересів від зовнішніх та внутрішніх інформаційних загроз. Важливим і актуальним нормативно-правовим актом, який узагальнює нагальні та декларує актуальні питання забезпечення безпеки у вітчизняному інформаційному просторі, є Стратегія інформаційної безпеки держави, яка розрахована на найближчі п’ять років (2022 – 2025 роки). Положення цієї Стратегії концептуально розкривають такі важливі для нашої країни аспекти, як: глобальні та національні загрози та виклики вітчизняній інформаційній безпеці; завдання та напрями реалізації основних положень Стратегії; принципи стратегічного планування в цій сфері; методику досягнення ефективності реалізації її основних положень; механізми успішної реалізації його положень у практичній площині в контексті побудови основ державної інформаційної політики.

Водночас важливим завданням держави є прискорення затвердження плану заходів щодо реалізації Стратегії інформаційної безпеки та забезпечення контролю за її виконанням. Актуальним завданням державного стратегічного планування залишається раціональний розподіл державою потенційних можливостей і наявних ресурсів (людських, інформаційних, фінансових, телекомунікаційних, технічних, технологічних), завдяки чому держава гарантує забезпечення національної безпеки та стабільної соціально-економічної ситуації. та цифровий розвиток громадянського суспільства в цілому. Для досягнення цієї мети необхідний достатньо високий рівень культури управління державним апаратом і використання методів системного аналізу та прогнозування, спеціальних методів забезпечення інформаційної безпеки тощо. Саме стратегічне планування у сфері забезпечення інформаційної безпеки дає змогу суттєво підвищити ефективність та якість державного управління у цій сфері. Стратегічне планування має розглядатися всіма органами державної влади та управління як універсальний інструмент, завдяки якому можна забезпечити виконання поточних державних завдань у сфері забезпечення інформаційної безпеки, в тому числі з використанням механізму державно-приватного

партнерства.

У сучасних умовах суспільство в цілому та державно-громадський сектор ІТ-сфери, зокрема, відчувають на собі наслідки триваючої агресії Російської Федерації, яка має гібридний характер, проникаючи в інформаційний простір, водночас завдаючи значної шкоди державні інтереси та приватний бізнес. Російська Федерація намагається маніпулювати свідомістю пересічних громадян, нагнітати соціальну напругу та поширювати заборонену законом інформацію за допомогою новітніх технологій, зокрема соціальних мереж та систем мікроблогів тощо. Найближчим часом прогнозується, що кількість подальших спеціальних інформаційних операцій Російської Федерації проти України збільшуватиметься з метою створення умов для соціальної напруги, формування загальної недовіри до чинної влади, шляхом поширення фейкової або викривленої інформації про діяльність центральних органів влади, військових командування, правоохоронних органів, а також стимулювання населення до участі в акціях непокори, використовуючи насамперед соціально-економічні та соціально-політичні питання. Кінцевою метою цієї діяльності є формування проросійської суспільно-політичної платформи та прихід до влади проросійських політиків для кардинальної зміни зовнішньополітичного курсу України. У сучасних реаліях гібридна війна стає все більш інтенсивною та набуває нових форм. Тому реформа СБУ має врахувати інноваційні гібридні загрози з боку Російської Федерації та надати спецслужбі додаткові механізми протидії таким загрозам. Запобігання та недопущення такого сценарію «керованого хаосу» з боку Російської Федерації потребує посилення можливостей вітчизняних спецслужб у здійсненні контррозвідувальних та оперативно-розшукових заходів, спрямованих, насамперед, на попередження та локалізація такої деструктивної діяльності на шкоду державним інтересам в інформаційній сфері. Важливими завданнями, які повинні залишатися в компетенції СБУ, є: здійснення заходів, спрямованих на виявлення,

попередження та припинення використання іноземними організаціями та їх посадовими особами, радикально налаштованими представниками вітчизняних ЗМІ на шкоду безпеці України. ; вжиття на системній основі додаткових заходів, спрямованих на блокування поширення у засобах масової інформації та мережі Інтернет матеріалів, що містять заклики до посягання на державний суверенітет, територіальну цілісність України, розпалювання міжнаціональних, міжконфесійних конфліктів, пропаганду війни тощо [32].

Важливе значення має інформаційна політика країни, адже від її ефективності залежить запобігання заподіянню шкоди національним інтересам, недопущення шкідливих змін у свідомості та поведінці людей, забезпечення фінансової безпеки України та національної безпеки в цілому. Державна інформаційна політика має забезпечувати свободу інформації, сприяти розвитку нових інформаційно-комунікаційних технологій, створювати більш відкрите управління державними програмами. Реалізація інформаційної політики має базуватися на реалізації комплексу заходів, спрямованих на розвиток інформаційного середовища, стійкого до зовнішніх і внутрішніх ризиків і загроз, які зростають в умовах цифровізації.

ВИСНОВКИ

На підставі проведеного дослідження можна запропонувати наступні висновки:

1. Інформаційна безпека – це складне, системне, багаторівневе явище, на стан і перспективи розвитку якого безпосередньо впливають зовнішні та внутрішні фактори, найважливішими з яких є: 1) політична ситуація у світі; 2) наявність потенційних зовнішніх і внутрішніх загроз; 3) стан і рівень інформаційно-комунікаційного розвитку країни; 4) внутрішньополітична ситуація в державі. Водночас інформаційна безпека є складною, динамічною, цілісною соціальною системою, складовими якої є підсистеми безпеки особистості, держави, суспільства. Саме взаємообумовлена, системна інформаційна єдність останніх становить якісну детермінацію, покликану захистити життєво важливі інтереси людини, суспільства і держави, забезпечити їх конкурентоспроможний, поступальний розвиток.

2. Наразі у вітчизняному інформаційному просторі спостерігається високий рівень зовнішніх загроз, зумовлений активною інформаційно-пропагандистською експансією з боку Російської Федерації. Зокрема, через інформаційну сферу здійснюються спроби вплинути на політичні та соціально-економічні процеси в нашій державі, підірвати авторитет легітимної української влади з метою деморалізації суспільства та посилення невдоволення та протестних настроїв. Також російська сторона активно впроваджує технології розміщення актуальної інформації в мережі Інтернет та ЗМІ, розповсюдження якої спрямоване на місцеве населення окупованих територій, громадян Російської Федерації та міжнародне співтовариство. Антиукраїнська інформаційна кампанія функціонально реалізується російською стороною за низкою напрямків, які спрямовані на: популяризацію ідей федеративного державного устрою України як альтернативи розпаду держави; забезпечення постійного потоку маніпулятивної дезінформації про події в Україні та на її

окупованих територіях; внесення розколу в середовище українських правлячих кіл, у тому числі шляхом публікації провокаційних та деструктивних матеріалів, критики центральної влади, яка «ігнорує інтереси регіонів», компрометації громадсько-політичних діячів, інспірації масових протестів; створення в Україні під виглядом представництв європейських організацій, підконтрольних російській стороні, громадських структур для проведення активної роботи в інформаційній, аналітичній та гуманітарній сферах в геополітичних інтересах Російської Федерації тощо. За таких умов при розгляді особливого значення набуває проблема організації забезпечення інформаційної безпеки, її структурна класифікація, яка є відносно умовною і побудована відповідно до певних цілей і завдань. У цьому аспекті інформаційну безпеку в залежності від джерел виникнення загрози доцільно розділити на два види – безпеку технічного характеру, зумовлену технологіями інформаційно-комунікаційних процесів, і безпеку, спричинену соціальними факторами. Отже, на сьогодні загрози інформаційній безпеці мають соціальний характер і зосереджені у внутрішньополітичній, економічній, соціальній, екологічній, інформаційній та духовній сферах нашого суспільства

3. Єдність та взаємозв’язок напрямів державної політики у сфері забезпечення інформаційної безпеки має забезпечуватися правовими механізмами, визначеними на законодавчому рівні, серед яких: чіткі цілі та завдання державної політики; взаємодія державних і громадських інституцій у реалізації міжвідомчих напрямів державної політики; організація системи інформування суб’єктів, що здійснюють діяльність у сфері інформаційної безпеки, про поточні проблеми, виявлення потенційних і реальних загроз та їх джерел, а також відповідних заходів і засобів щодо їх запобігання, нейтралізації та ліквідації можливих наслідків; скоординованих і цілеспрямованих дій суб’єктів, що діють у різних сферах життєдіяльності суспільства і держави, з питань адекватного реагування на виявлені потенційні та реальні загрози;

національне керівництво, координація та контроль у сфері забезпечення інформаційної безпеки

4. Серед основних складових інформаційної безпеки держави виділяють: обсяг виробленого в державі та державою інформаційного продукту; здатність мереж витримувати зростаюче інформаційне навантаження; здатність держави управляти розвитком виробництва та розповсюдження інформації; можливість доступу населення до всіх можливих джерел інформації, а також відкритість більшості з них.

5. Для України сьогодні є актуальними завдання розвитку інформаційного суспільства, аналізу загроз в інформаційній сфері, забезпечення інформаційної безпеки Української держави як частини світового інформаційного співтовариства. Розробка державних заходів щодо забезпечення інформаційної безпеки громадян, суспільства та держави є одним із найважливіших пріоритетів державного управління у цій сфері, що потребує ефективної міжгалузевої взаємодії, зокрема між державними органами та за участю приватний сектор.

6. До національних цілей в інформаційному полі належать: припинення порушення та спотворення поглядів людей на навколишній світ і себе, що здійснюється шляхом культивування уявних цінностей, насадження деструктивних пріоритетів, завдань і цілей перед суспільством і особистістю (духовна безпека); забезпечують впровадження інформаційних технологій у військову сферу та забезпечують їх захист (військова безпека); прискорити розробку та впровадження новітніх конкурентоспроможних ІКТ у соціально-економічній сфері (економічна безпека); досягти належного рівня культури інформаційних відносин (соціальної безпеки); створити загальнодержавні інформаційні системи постійного екологічного моніторингу стану довкілля (економічної безпеки); сприяти інтеграції національної інформаційної інфраструктури з глобальною інфраструктурою. посилити захист інформаційних

прав людини; вжити невідкладних заходів щодо формування позитивного іміджу держави в умовах інформаційної глобалізації.

7. З метою реалізації національних інтересів в інформаційній сфері необхідно переглянути пріоритети державної політики, розробити нові концептуальні підходи щодо регулювання ринку інформаційно-комунікаційних технологій, інформаційної та інвестиційної політики, розвитку інформаційного законодавства та забезпечення інформаційної безпека. Рівень інформаційної безпеки активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України, адже найчастіше реалізація інформаційних загроз означає завдання шкоди в політичній, військовій, економічній, соціальній, екологічній сферах тощо. На жаль, наразі в Україні немає реальних гарантів її інформаційної безпеки, відсутній комплекс нормативно-правових актів щодо захисту інформаційних ресурсів та інформаційної інфраструктури. При цьому процес інформатизації має стихійний, неконтрольований характер з переважним ухилом на використання засобів інформатизації іноземного виробництва.

8. Сьогодні розвинені країни йдуть шляхом цілеспрямованого правового регулювання відносин у національному інформаційному просторі, прийняття необхідних законодавчих актів, перебудови діяльності органів державної влади, відповідальних за реалізацію інформаційної політики. в умовах інформаційної агресії для України надзвичайно важливим є американський досвід використання інформаційних технологій для створення систем зв’язку та військового управління. Прийняття Стратегії інформаційної безпеки України у 2021 році стало важливим кроком у напрямку підвищення ефективності інформаційної політики. Водночас, враховуючи позитивний світовий досвід, правомірно виділити наступні напрямки реалізації інформаційної політики в аспекті забезпечення фінансової безпеки України:1. Розвиток національної інформаційної інфраструктури, здатної протидіяти зовнішнім і внутрішнім

ризикам і загрозам, забезпечуючи захист національних інтересів, зокрема економічних. 2. Посилення інституційної спроможності у сфері стратегічних комунікацій, що передбачає формування механізму координації та взаємодії між органами державної влади, які здійснюють заходи щодо протидії ризикам і загрозам в інформаційній, фінансовій та інших сферах національної економіки. 3. Підвищення рівня інформаційної спроможності населення, а саме забезпечення вільного доступу до об’єктивної, неупередженої та правдивої інформації. 4. Забезпечення підвищення рівня інформаційної культури та медіаграмотності суспільства як основи протидії деструктивним інформаційним впливам. Державна інформаційна політика в умовах глобалізації буде ефективною лише за умови, що вона матиме комплексний, системний характер і, безперечно, буде відкритою, спрямованою на забезпечення економічних інтересів громадян, бізнесу та держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про Концепцію Національної програми інформатизації»; Концепція від 04.02.1998 № 75/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80.

2. Форос Г.В., Жогов В.С. Особливості трактування поняття «кібербезпека» в сучасній юридичній науці. Правова держава. 2019. №33. С. 128–134.

3. Захаренко К. Основні суб'єкти та інститути інформаційної безпеки. Науковий вісник. Серія «Філософія». Харків: ХНПУ. 2017. Вип.48 (частина І). С. 212–219.

4. Лисовская Ю.П. Информационная безопасность в современном глобализованном мире. Веснік БДУ. 2015. № 2. С. 93–97

5. Панченко О.А. Державне управління інформаційною безпекою в епоху турбулентності. : дис ... д-ра юрид. наук. Національний університет цивільного захисту України. Харків, 2020. 521 с.

6. Золотар О.О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

7. Гуржій Т. Інформаційне право: виклики гібридної війни. Зовнішня торгівля: економіка, фінанси, право. 2018. № 4. С. 16–26.

8. Дмитренко М.А. Проблемні питання інформаційної безпеки України. Міжнародні відносини. Серія Політичні науки. 2017. № 17. С. 236–243.

9. Косогов О.М., Сірик А.О. Завдання захисту національного інформаційного простору за досвідом ведення гібридної війни РФ на Сході України. Системи озброєння і військова техніка. 2017. С. 38–41.

11. Доктрина інформаційної безпеки України : затверджено Указом Президента України від 25 лютого 2017 р. № 47/2017. URL:

http://zakon.rada.gov.ua/laws/show/47/2017.

12. Турчак А. В. Основні складові інформаційної безпеки держави. Аспекти публічного управління. 2019. Т. 7 № 5. С. 44-56

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

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

15. Закон України «Про національну безпеку України» від 21.06.2018 №2496: URL: http://zakon3.rada.gov.ua/laws/show/2469-19 (дата звернення: 27.05.2018).

16. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України. : дис ... д-ра юрид. наук. ДВНЗ «Ужгородський національний університет», Ужгород, 2019.487 с.

17. Лесков М.А. Гомеостатические процессы и теория безопасности. Безопасность. Инф. сб. 1994. №4(20). С. 66-67

18. Ожегов С.И. Словарь русского языка. М.: Рус.яз., 1988. 748 с.

19. Словник української мови: в 11-ти т. АН УРСР, Ін-т мовознавства ім.О.О. Потебні; редкол.: І.К. Білодід (голова) та ін. Т.3 [ред.: Г.М. Гнатюк, Т.К. Черторизька]. К.: Наукова думка, 1972. 744 с.

20. Гацко М. О соотношении понятий «угроза» и «опасност. Обозреватель – Observer: URL: observer.materik.ru/observer/N07_97/7_06.htm

21. Методика реагування на виклики, небезпеки та загрози національній

безпеці держави: навчальний посібник. К.: НАДУ, 2009. 40 с.

22. Брега А.. Риск в системе категорий, характеризующих антитезу национальной безопасности. URL: http://www.milpol.ru/data/2009/1-12/brega_risk_ doklad_ konf_nb.doc

23. Хілько О.Л. Визначення загроз національній безпеці в українській теоретико-політичній думці. URL: sevntu.com.ua/jspui/bitstream/123456789/1835/politolog.52.2003.48-56.pdf

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

25. Олійник О.В. Інформаційна безпека України: доктрина адміністративно-правового регулювання : дис ... д-ра юрид. наук. Київ, 2013. 203 с.

26. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» : Указ Президента України від 01.05.2014 р. № 449/2014 URL: www.president.gov.ua/documents/4492014-17157.

27. Гуржій Т. Інформаційне право: виклики гібридної війни. Зовнішня торгівля: економіка, фінанси, право. 2018. № 4. С. 16–26.

28. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий електронний журнал. 2020. № 2URL: http://lsej.org.ua/2_2020/54.pdf

29. Ткачук Т.Ю. Державна політика у сфері забезпечення інформаційної безпеки на сучасному етапі. Науковий вісник Ужгородського національного університету. 2017. № 46. С.39-42

30. Перун Т.С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: автореф. дис. …канд. юрид. Наук. Львів. 2019.

23 с.

31. Турчак А.В. Основні засади державної політики забезпечення інформаційної безпеки в Україні. Інвестиції: практика та досвід. 2019. № 11. С. 123-127.

32. Новицький В.Я.. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. Інформація і право. 2022. № 1(40). С. 111-118

33. Почепцов Г. Інформаційна політика : навч. посіб. / Г. Почепцов, С. Чукут. К. : Вид-во УАДУ, 2002. 88 с.

34. Домбровська С. М. Механізми інформаційної безпеки як складові державної безпеки України. Державне управління науково-освітнього забезпечення підготовки конкурентоспроможних фахівців у сфері цивільного захисту : матеріали Всеукраїнської наук.-практ. конф. / за заг. ред. В. П. Садкового. Х., 2015. С. 282–286.

35. Михайлов А. О. Оптимізація причинно-наслідкового зв’язку функцій держави та механізмів державного управління в Україні : автореферат дис. ... канд. наук з держ. упр. Акад. муніц. управління. К., 2015. 20 с.

36. Опанасенко Я. О. Роль і місце організаційної, соціальної й інформаційної складових у реалізації державної регіональної політики в умовах невизначеності регіонів. Вісник Національного університету цивільного захисту України (Серія: Державне управління), 2016. № 1 (4). С. 203–209.

37. Офіційний веб-сайт Міністерства інформаційної політики України URL: http://mip.gov.ua/ru/

38. Мануйлов Є.М., Калиновський Ю.Ю. Аксіологічний вимір інформаційної безпеки української держави. Вісник Національного університету “Юридична академія України імені Ярослава Мудрого”. № 3 (34) 2017. С. 13-30

39. Вебер М. Избранное. Образ общества / М. Вебер : пер. с нем. М. : Юристъ, 1994. 704 с.

40. Ларін С.В. Сутність та зміст поняття “національні цінності” в контексті сучасних дослідницьких підходів. Вісник НАДУ при Президентові України. 2016. № 2. С. 44-49.

41. Горбулін В.П. Засади національної безпеки України / В.П. Горбулін, А.Б. Качинський. К. : Інтер-технологія, 2009. 272 с.

42. Горбулін В. На захист національних інтересів. Політика і час. 1995. № 2. С. 3-8.

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

44. Ситник Г.П. Державне управління національної безпеки (теорія і практика) / Г.П. Ситник. К. : Вид-во НАДУ, 2004. 408 с.

45. Присяжнюк М., Бєлошевич Я. Інформаційна безпека України в сучасних умовах. Вісник Київського національного університету ім. Т. Шевченка. Військово-спеціальні науки. 2013. Вип. 30. С.29–33.

46. Конституція України від 28 червня 1996 р. Відомості Верховної Ради України. 1996. № 30. Ст. 17.

47. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. К.: КНТ, 2006. 280 с.

48. Малик Я.Й., Береза О.І. Забезпечення інформаційної безпеки України у контексті світового досвіду. Ефективність державного управління. 2012. Вип. 32. С.20–27.

49. Шаповал Р.В., Клочко В.О. Вдосконалення формування та реалізації

державної політики у сфері інформаційної безпеки України. Наше право. 2014. № 6. С. 5–9.

50. Апетик А. Інформаційна безпека. 2019. URL: https://webcache.googleusercontent.com/search?q=cache:nY_Tl2_Dян8J:https://www.prostir.ua/%3Flibrary%3Dinformatsijna-bezpeka-now-yakyh-elementiv-nevystachaje+&cd=3&hl=ru&ct=clnk&gl=ua.

51. Богуш В.М., Юдін О.К. Інформаційна безпека держави К.: МК-Прес, 2005. 432 с.

52. Панченко О. А. Проблеми правового забезпечення державного управління інформаційною безпекою URL: http://www.dy.nayka.com.ua/pdf/11_2019/5.pdf

53. Глушко А. Д., Пантась В. В., Бабенко С. Р. Інформаційна політика в системі забезпечення фінансової безпеки держави URL: http://www.economy.nayka.com.ua/pdf/2_2022/97.pdf

54. Офіційний сайт KPMG. URL: https://home.kpmg/ua/uk/home.html

55. The Hidden Costs of Cybercrime. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rphidden-costs-of-cybercrime.pdf

56. Мохова Ю.Л., Луцька А.І. Сутність та головні напрямки державної інформаційної політики України. URL: http://www.dy.nayka.com.ua/pdf/12_2018/27.pdf

57. Центр досліджень соціальних комунікацій НБУВ. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-sshazakonodavche-regulyuvannya-ta-perspektivi-spivpratsi-dlya-

ukrajini&catid=8&Itemid=350

58. “Україна – на вістрі гібридної атаки РФ у світі” – на міжнародній конференції в Академії СБУ обговорили досвід протидії інформаційним операціям РФ. URL: https://academy. ssu.gov.ua/ua/news-1-8-136-ukraina-–-na-vistri-gibridnoi-ataki-rf-u-sviti-–-na-mizhnarodniy-konferencii -v-akademii-sbu-obgovorili-d