МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна

Навчально-науковий інститут «Інститут державного управління»
Кафедра права, національної безпеки та європейської інтеграції

Кваліфікаційна робота магістра
на тему

ПУБЛІЧНЕ УПРАВЛІННЯ ФОРМУВАННЯМ МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Виконав студент 2 курсу,
групи ППГЗ-1-24
Спеціальності 281 – «Публічне управління та адміністрування»
Освітньо -професійної програми
«Публічне управління та адміністрування»
_____ Роман МЕЛЕШКО

Науковий керівник роботи:
доктор наук з державного управління, професор
_____ Володимир БУЛЬБА

Харків - 2025

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ ….3
ВСТУП …….4
РОЗДІЛ 1. НАУКОВІ ЗАСАДИ ПУБЛІЧНОГО УПРАВЛІННЯ ФОРМУВАЕННЯМ МОДЕЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ …….....9
1.1 Інформаційна сфера забезпечення національної безпеки ……...9
1.2 Закордонний досвід формування моделі інформаційної безпеки держави……...16
РОЗДІЛ 2. СУЧАСНИЙ СТАН ТА ВИКЛИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ……...23
2.1 Нормативно-правові засади інформаційної безпеки в Україні ..…23
2.2 Виявлення та обґрунтування існуючих загроз у сфері інформаційної безпеки України ……..……...32
РОЗДІЛ 3. НАПРЯМКИ ФОРМУВАННЯ СУЧАСНОЇ МОДЕЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ ……...40
3.1 Інформаційна агресія проти України: причини, наслідки та уроки гібридної війни ……40
3.2 Визначення напрямків формування сучасної моделі забезпечення інформаційної безпеки держави ……..….52
ВИСНОВКИ ……..….59
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ……62

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

АРК	Автономна Республіка Крим
АТО	антитерористична операція
ВРУ	Верховна Рада України
ГВ	гібридна війна
ДНР	так звана Донецька народна республіка
ДССЗЗІ	Державна спеціальна служба зв'язку та захисту інформації України
ЄС	Європейський Союз
ЗМІ	засоби масової інформації
ЗСУ	Збройні Сили України
ІВ	інформаційна війна
ІЗ	інформаційна зброя
ІП	інформаційне протиборство
ІТС	інформаційно-телекомунікаційні системи
КМУ	Кабінет Міністрів України
ЛНР	так звана Луганська народна республіка
НАТО	Північноатлантичний Альянс
РНБО	Рада національної безпеки і оборони України
СБУ	Служба безпеки України

ВСТУП

Актуальність теми дослідження. Драматичні події повномасштабного вторгнення російських окупантів в Україну довели, що в умовах швидкого формування і розвитку інформаційного суспільства та глобального інформаційного простору, широкого використання інформаційно-комунікаційних технологій у всіх сферах життя особливого значення набувають проблеми інформаційної безпеки. У наслідок відсутності дієвої системи забезпечення інформаційної безпеки в національному інформаційному просторі України спостерігається низка негативних явищ, які створюють реальні та потенційні загрози інформаційній безпеці людини і громадянина, суспільства і держави. Рівень розвитку та безпека інформаційного простору, які є системоутворюючими факторами у всіх сферах національної безпеки, активно впливають на стан політичної, економічної, оборонної та інших складових національної безпеки України. Таким чином, інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки, яка характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз і являє собою сукупність інформаційно-психологічної (психофізичної) та інформаційно-технологічної безпеки держави.

Глобальний поступ дистанційних комунікацій, інформаційних технологій та продуктів, ресурсів і послуг призводить до виникнення принципово нових суспільних відносин в інформаційній сфері, економіці, виробництві. Їх інтенсифікація стала найважливішою ознакою сучасної цивілізації. З їх допомогою глобалізація проникає в усі сфери людського життя. Відбувається розвиток процесів інформатизації, пов’язаний із розширенням доступу до інформаційних ресурсів та засобів їх виробництва всіх прошарків населення, і як наслідок, формування в останніх нових світоглядних та інших стереотипів суспільної поведінки, корегування

духовно-ціннісних орієнтирів, планів і перспектив. Інформація та інформаційні ресурси стають стратегічним здобутком і найважливішими чинниками поступу людини, суспільства і держави. Інформаційна сфера дедалі більше впливає на політичну, економічну, соціокультурну, оборонну, інші складові розвитку суспільства й держави, а врешті-решт, на забезпечення національної безпеки в сучасних умовах.

Інформаційна складова нині становить ключовий елемент війни проти України, що створює реальні загрози конституційному ладу, територіальній цілісності та національній безпеці України і характеризується цілеспрямованим знищенням української інформаційної інфраструктури на тимчасово окупованих територіях, здійсненням кібернетичних атак на об'єкти критичної інфраструктури нашої держави, спробами блокування каналів поширення проукраїнської позиції в інформаційному просторі, проведенням інформаційних операцій та окремих акцій на фоні потужної пропагандистської кампанії проти України.

Актуальність дослідження полягає в тому, що сьогодні інформаційна сфера складає інтегруючу основу життєдіяльності суспільства, а забезпечення інформаційної безпеки визнається однією з концептуальних засад його подальшого розвитку. За таких умов особливого значення набуває формування виваженої державної інформаційної політики, на основі системних наукових досліджень явищ інформаційної сфери, провідне місце серед яких займає інформаційна безпека.

Одним з важливих етапів системного дослідження інформаційної безпеки є глибокий аналіз загальної структури її забезпечення. Виокремлення та деталізація складових забезпечення інформаційної безпеки за різними ознаками сприятиме усвідомленню особливостей кожної з них, і, відповідно, формуванню комплексу адекватних заходів державного та недержавного характеру, спрямованих на підтримання оптимального інформаційного розвитку України та інтеграції у світовий інформаційний простір.

Теоретичне обґрунтування напрямів забезпечення інформаційної безпеки розглядалася лише через висвітлення окремих аспектів інформаційної безпеки вітчизняними та зарубіжними фахівцями у галузі державного управління, інформаційного права, національної безпеки, соціальних комунікацій та ін. У даному контексті слід згадати наукові розробки таких вчених, як З. Бжезінський, Е. Тоффлер, В. Гавловський, В. Гурковський, Г. Почепцов, В. Рижих, С. Расторгуєв, А. Селіванов, А. Семенченко, О. Соснін, В. Цимбалюк, І. Чиж, М. Швець, Ю. Шемшученко, О. Юдін та інші.

Водночас слід зазначити, що залишаються недостатньо розкритими питання особливостей загальної структури забезпечення інформаційної безпеки. Оскільки це гальмує процеси усвідомлення системності інформаційної безпеки та негативно позначається на формуванні державної інформаційної політики.

Тому в умовах викликів сьогодення та розвитку інформаційного суспільства проблема забезпечення інформаційної безпеки набуває якісно нового значення і в правовому вимірі виступає як невід'ємна складова сучасної системи управління на шляху до правової держави і як суттєвий чинник формування громадянського суспільства, забезпечуючи поступальний розвиток його інформаційної основи – національних інформаційних ресурсів. Все це вимагає зміни філософії забезпечення інформаційної безпеки.

Зазначене актуалізувало дослідження напрямів забезпечення інформаційної безпеки в сучасних умовах.

Мета і завдання дослідження. Мета роботи є полягає в обґрунтуванні публічного управління формуванням моделі інформаційної безпеки держави в сучасних умовах.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– дослідити систему забезпечення інформаційної безпеки України, її основні функції, об'єкти та суб'єкти;

– визначити основні елементи структури діючої моделі забезпечення інформаційної безпеки України

– обґрунтувати необхідність змін внутрішніх та зовнішніх засад вітчизняної інформаційної політика у сфері захисту державних (національних) інтересів;

– провести аналіз загроз інформаційній безпеці держави;

– проаналізувати сучасний стан нормативно-правового забезпечення інформаційної безпеки України;

– визначити напрямки і шляхи формування сучасної моделі інформаційної безпеки держави;

– надати рекомендації щодо пріоритетних шляхів забезпечення інформаційної безпеки в України.

Об'єктом магістерського дослідження є система забезпечення інформаційної безпеки держави.

Предметом магістерського дослідження є публічне управління формуванням моделі інформаційної безпеки держави.

Методологічна основа роботи. Методологічною основою дослідження стали сучасні загальні та спеціальні методи наукового пізнання.

Дослідження теоретичних і методичних положень магістерської роботи ґрунтуються на загальнонаукових принципах проведення комплексних досліджень, роботах провідних вітчизняних і зарубіжних вчених з питань з питань національної безпеки держави. Методи системного підходу та методи системного аналізу використовувались при дослідженні системи, що забезпечує формування інформаційної безпеки держави; у визначені методів забезпечення інформаційної безпеки – метод порівняльного аналізу та синтезу.

Правове поле дослідження склали чинні законодавчі та нормативні документи України, що регулюють діяльність галузі охорони здоров`я.

Науково-теоретичне підґрунтя дослідження становлять наукові праці фахівців у галузі державного управління національною безпекою, телекомунікаційних технологій, психології.

Інформаційну й емпіричну основу дослідження становлять матеріали парламентських слухань, довідкова література, статистичні матеріали, веб-сайти мережі Інтернет.

Теоретичне та практичне значення одержаних результатів полягає в розробці моделі процесу забезпечення безперервності функціонування системи інформаційної безпеки держави.

Висновки і рекомендації, що розроблені у магістерській роботі в результаті проведеного дослідження можуть бути основою для подальшої розробки проблем забезпечення інформаційної безпеки держави.

*Опис структури роботи***.** Логіка проведеного дослідження зумовила структуру роботи: вступ, три розділи, висновки. Загальний обсяг роботи складає 70сторінок. Список використаних джерел містить 79 найменувань.

РОЗДІЛ 1
НАУКОВІ ЗАСАДИ ПУБЛІЧНОГО УПРАВЛІННЯ ФОРМУВАННЯ МОДЕЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Інформаційна сфера забезпечення національної безпеки

Події 2014 року та розв'язана у лютому 2022 року проти України повномасштабна війна довели, що крім військових злочинів військового стану інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки. Більше того, інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку.

Сьогодні інформаційна сфера розглядається і як порівняно самостійна сфера, і як допоміжна стосовно інших видів діяльності. В останньому випадку йдеться про те, що інформаційна сфера обслуговує практично усі сфери суспільства (економіка, політика, управління, наука, культура, побут, сім'я), тобто займає «підлегле» становище у кожній з названих сфер. На думку І.В. Арістової, як у першому, так і в другому випадку мається на увазі вузьке тлумачення поняття «інформаційна сфера». Вчена зауважує, що нині політика держави в інформаційній сфері (вузьке тлумачення) спрямована як на розвиток безпосередньо інформаційної сфери, так і на підвищення ефективності розвитку державності, безпеки, оборони, пріоритетних галузей економіки, фінансової та грошової систем, соціальної сфери, галузей екології та використання природних ресурсів, науки, освіти і культури, міжнародної співпраці за допомогою інформаційної сфери. Пріоритетом є підвищення ефективності державного управління як однієї з функцій держави.

З усіх складових інформаційної сфери з-поміж розглянутих ключовими поняттями і такими, що найбільш виділяються, є інформація та інформаційні технології.

Сьогодні володіння інформацією стає одним з вирішальних чинників контролю над вирішенням будь-яких проблем світової спільноти.

Інформація стала чинником, здатним призвести до великомасштабних аварій, військових конфліктів і поразки в них, дезорганізувати державне управління, фінансову систему, роботу наукових центрів тощо. Водночас володіння інформацією сприяє розвитку всіх сфер діяльності держави та суспільства, і, врешті-решт, значним успіхам в економіці, бізнесі, фінансах. Однак володіння цінною інформацією покладає на суб'єктів, що мають на неї відповідні права, високий ступінь відповідальності за її збереження і захист від можливого зовнішнього впливу різнорідних чинників і подій, і навмисного, і випадкового характеру.

Поняття «інформація» використовується у всіх галузях науки і набуло різних інтерпретацій, які використовуються в залежності від сфери вживання.

В перекладі з латинської мови «інформація» – це роз'яснення, виклад [10]; «загальнонаукове поняття, що включає в себе обмін відомостями між людьми, людиною та автоматом, автоматом і автоматом; обмін сигналами у тваринному і рослинному світі; передачу ознак від клітини до організму, від організму до організму» [10].

Інформація, як сукупність фактів, подій, відомостей, характеристик явищ, предметів, які зібрані, узагальнені та систематизовані у відповідну для використання форму, складають основу управління. Загалом, всі управлінські процеси – це пошук, аналіз, узагальнення, оцінка та розповсюдження інформації, пов'язана з відображенням і пізнанням різних сфер діяльності суспільства. Тобто, якщо розглядати процес управління як рух потоків інформації і прийняття управлінських рішень, то такий процес можна назвати інформаційним.

В публічному управлінні під «інформацією» розуміють «документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі» [14].

Треба зазначити, що від обсягу, швидкості та якості обробки інформації значною мірою залежить ефективність управлінських рішень, зростає значення методів управління з використанням інформаційних технологій соціальними та економічними процесами, фінансовими і товарними потоками, аналізу та прогнозування розвитку внутрішнього і зовнішніх ринків. Використання інформаційних технологій визначає структуру і якість озброєнь, необхідний рівень їх достатності, ефективність дій збройних сил.

Інформаційні технології визначають можливість людини щодо формування, поширення та споживання інформації, накопичення суспільством соціально важливих відомостей [33].

Але доводиться констатувати, що внаслідок розвитку науково-технічного прогресу, зростання ролі інформаційних технологій у повсякденному житті, їх проникнення в усі сфери діяльності суспільства і держави зростає роль інформаційної безпеки особи, суспільства і держави, а її забезпечення займає особливе місце в діяльності всіх державних інститутів.

Одним із принципів правового регулювання відносин, що виникають у сфері інформації, інформаційних технологій та захисту інформації, є забезпечення безпеки держави під час створення інформаційних систем, їх експлуатації та захисту інформації, що міститься в цих системах, тобто – забезпечення інформаційної безпеки нашої держави.

У наукових джерелах запропоновано багато визначень інформаційної безпеки. Інформаційна безпека держави – це стан її інформаційної захищеності, за якого спеціальні інформаційні операції, акти зовнішньої інформаційної агресії та негласного зняття інформації (за допомогою спеціальних технічних засобів), інформаційний тероризм і комп’ютерні злочини не завдають суттєвої шкоди національним інтересам [18].

Специфіка інформаційної безпеки полягає в тому, що вона знаходить свій вияв у різноманітних сферах суспільного життя, оскільки збереження та захист інформації є важливою складовою їх функціонування в

інформаційному суспільстві. Інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки.

Так, Б. Кормич трактує інформаційну безпеку як стан захищеності встановлених законодавством норм та параметрів інформаційних процесів та відносин, що забезпечує необхідні умови існування держави, людини та суспільства як суб'єктів цих процесів та відносин [27, с. 15].

Деякі вчені розглядають інформаційну безпеку як стан захищеності життєво важливих інтересів особистості, суспільства і держави, при якому зводиться до мінімуму заподіяння шкоди через неповноту, несвоєчасність, недостовірність інформації чи негативний інформаційний вплив, через негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [36, с. 72]. Інформаційну безпеку суспільства також визначають як неможливість заподіяння шкоди його духовній сфері, культурним цінностям, соціальним регуляторам поведінки людей, інформаційній інфраструктурі й повідомленням, що передаються за її допомогою [74, с. 76].

Як зауважує І. Боднар, головна інформаційна загроза національній безпеці – це загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості з метою нав'язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної і державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони напрямку. Власне, це є загрозою суверенітету України в життєво важливих сферах суспільної й державної діяльності, що реалізовується на інформаційному рівні. Стратегічне інформаційне протистояння є самостійним і принципово новим видом протистояння,

здатним вирішувати конфлікт без застосування збройних сил у традиційному розумінні [6, с. 69].

Інформаційна інфраструктура є об'єктом національних інтересів у зв'язку з її використанням для реалізації: важливих функцій суспільства і, передусім, обміну інформацією, що циркулює у суспільстві; управління соціальними та технологічними процесами, військами і зброєю, убезпеченням критичної інфраструктури; комерційних операцій торговельного та банківського характеру, надання інформаційних послуг. Безпека інформаційної інфраструктури полягає у захищеності від загроз її здатності виконувати основні соціальні функції.

Національні інтереси в інформаційній сфері визначаються, насамперед, тією роллю, яку відіграє інформація, інформаційні технології та створена на їх основі інформаційна інфраструктура в забезпеченні сталого розвитку нації в конкретних історичних умовах, а також у збереженні національної ідентичності. Ці інтереси утворюються збалансованою сукупністю соціальних інтересів індивіда як особистості, інтересів суспільства і держави, що реалізуються в інформаційній сфері, ураховуючи їхні інтереси у використанні інформаційної сфери для збереження національної ідентичності [5].

Оцінюючи інформацію як ресурс національного розвитку, на нього варто подивитися в координатах проблем національних інтересів і безпеки. Насамперед на те, яке значення має інформація в реаліях інформаційної інфраструктури держави, як її функціонування підпорядковане забезпеченню сталого розвитку нації у конкретних історичних умовах і як збалансовано сукупність соціальних інтересів особистості, суспільства й держави, що реалізуються в інформаційній сфері.

Доцільно назвати чотири складові національних інтересів України в інформаційній сфері. Визначимо основний зміст кожної з них.

1. Вона полягає у дотриманні конституційних прав і свобод людини і громадянина в галузі одержання інформації і користування нею, забезпеченні

духовного відновлення України, збереження і зміцнення моральних цінностей суспільства, традицій патріотизму, гуманізму, культурного й наукового потенціалу країни.

2. Визначає доведення до громадян України та міжнародної громадськості достовірної інформації про державну політику України, її офіційні позиції до соціально значимих подій у житті держави і міжнародного життя, із забезпеченням доступу громадян до відкритих державних інформаційних ресурсів.

3. Полягає у розвитку сучасних інформаційних технологій, вітчизняної індустрії інформації, у тому числі індустрії засобів інформації, телекомунікації та зв'язку, забезпеченні потреб внутрішнього ринку її продукцією та вихід цієї продукції на світовий ринок, а також забезпеченні накопичення, зберігання та ефективного використання вітчизняних інформаційних ресурсів.

4. Ця складова національних інтересів України в інформаційній сфері полягає у захисті інформаційних ресурсів від технічних розвідок, несанкціонованого доступу, забезпеченні безпеки інформаційних і телекомунікаційних систем.[11, с. 148-150]

Таким чином, можна виокремити тріаду національних інтересів: людину та громадянина; суспільства; держави. Тобто національні інтереси України – це інтегрований вираз консолідованих інтересів і людини, і суспільства, і держави [18]. Зазначимо також, що об'єктом нашого наукового інтересу виступатимуть тільки національні інтереси людини, суспільства та держави в інформаційній сфері в контексті інформаційної безпеки, оскільки не всі інтереси в національній сфері є об'єктом забезпечення інформаційної безпеки.

Конституція України визначає закріплення основних прав та свобод людини в інформаційній сфері. Згідно ст. 15 суспільне життя в України ґрунтується на засадах політичної, економічної та ідеологічної багатоманітності. Жодна ідеологія не може визнаватися державою як

обов’язкова. Цензура заборонена. Ст. 31 зазначає, що кожному гарантується таємниця листування, телефонних розмов, телеграфічної та іншої кореспонденції. Ст. 32 Основного закону визначає, що не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Ст. 34, в свою чергу гарантує право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Кожен має право збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. Відповідно до ст. 54 громадянам гарантується свобода літературної, художньої, наукової і технічної творчості, захист інтелектуальної власності, їхніх авторських прав, моральних і матеріальних інтересів, що виникають у зв’язку з різними видами інтелектуальної діяльності. Кожен громадянин має право на результати своєї інтелектуальної, творчої діяльності; ніхто не може використовувати або поширювати їх без його згоди, за винятками, встановленими законом [25].

На основі здійсненого аналізу вищевикладених норм Конституції України, а також беручи до уваги національні інтереси, визначені законом України "Про основи національної безпеки України", доцільно показати основні національні інтереси в інформаційній сфері. До них віднесемо:

а) для людини:

– реалізація прав і свобод людини і громадянина, щодо одержання, використання, поширення, зберігання інформації;

– забезпечення права людини на захист від маніпуляції індивідуальною свідомістю;

– захист права інтелектуальної власності;

– захист інформаційної безпеки людини тощо.

б) для суспільства:

– побудова інформаційного суспільства;

– забезпечення плюралізму засобів масової інформації;

– захист від маніпуляції масовою свідомістю;

– розвиток духовності, моральних засад, інтелектуального потенціалу Українського народу, зміцнення психічного здоров'я нації.

в) для держави:

– забезпечення інформаційного суверенітету;

– унеможливлення монополізації інформаційного простору іноземними компаніями або транснаціональними корпораціями;

– створення конкурентоспроможних інформаційних технологій та технологій зв'язку;

– забезпечення та зміцнення науко-технічного потенціалу;

– інтеграція України в європейський інформаційний простір;

– боротьба з інформаційною злочинністю тощо[59].

Таким чином, визначимо, що основним питанням виживання України в питаннях національної безпеки, є створення сучасної моделі забезпечення ефективної системи протидії дезінформації та гібридним загрозам.

1.2 Закордонний досвід формування моделі інформаційної безпеки держави

Діюча система забезпечення інформаційної безпеки України та її структура призначені для реалізації державної політики у даній сфері. Ця система є частиною сфери забезпечення національної безпеки держави і будується на основі державно-правового механізму шляхом розмежування повноважень органів законодавчої, виконавчої та судової влади в даній сфері, а також поєднання зусиль зазначених органів з метою підвищення ефективності їх діяльності. Але формування сучасної моделі інформаційної держави в Україні проходить в умовах імплементації вітчизняних реалій до вимог Європейського Союзу і міжнародних стандартів та критеріїв, що характеризує демократичний світ. Тому доречно звернутися до вивчення закордонного досвіду у визначеній сфері.

У вітчизняній та закордонній літературі поняття «модель інформаційної безпеки держави» – це комплексна система організаційних, правових, технічних та процедурних заходів, спрямованих на захист національного інформаційного простору від внутрішніх і зовнішніх загроз. Така модель визначає архітектуру взаємодії державних інституцій, приватного сектору, громадянського суспільства та міжнародних партнерів у забезпеченні кібербезпеки та захисту критичної інформаційної інфраструктури.

Національна модель інформаційної безпеки охоплює стратегічне планування, законодавче регулювання, координацію діяльності уповноважених органів, механізми реагування на кіберінциденти, систему підготовки фахівців та міжнародну співпрацю. Вона формується з урахуванням специфіки загроз, рівня цифровізації економіки, геополітичного становища та наявних ресурсів країни.

Зазначимо, що діючі моделі інформаційної безпеки демократичних держав спираються на низку універсальних і специфічних принципів. Зробимо опис основних з них.

Принцип всеохопності та багаторівневості передбачає захист інформації на всіх рівнях – від персональних даних громадян до критичної державної інфраструктури. Це забезпечує системний підхід до безпеки, коли кожен елемент цифрової екосистеми отримує належний захист відповідно до свого значення.

Принцип превентивності та стримування орієнтує систему на випереджальне виявлення загроз та їх нейтралізацію до завдання шкоди. Важливість цього принципу полягає в економічній доцільності: запобігання інциденту завжди дешевше, ніж ліквідація його наслідків. Стримування передбачає формування потужних оборонних можливостей, що знижують привабливість держави як цілі для кіберагресії.

Принцип кіберстійкості означає здатність швидко адаптуватися до нових загроз, відновлюватися після атак та продовжувати функціонування

критичної інфраструктури навіть під час масованих кібератак. Цей принцип особливо актуальний в умовах гібридних війн, коли противник використовує кіберпростір для дестабілізації держави.

Принцип державно-приватного партнерства визнає, що більшість критичної інфраструктури перебуває у приватній власності, а найкращі технологічні рішення розробляються приватним сектором. Ефективна модель інформаційної безпеки неможлива без тісної співпраці держави з бізнесом, обміну інформацією про загрози та спільних дій у відповідь на інциденти.

Принцип міжнародної співпраці обґрунтовується транснаціональним характером кіберзагроз. Жодна держава не може самостійно протистояти глобальним викликам, тому обмін інформацією, спільні навчання та координація дій з міжнародними партнерами є критично важливими для національної безпеки.

Принцип постійного розвитку та інновацій забезпечує адаптацію системи до швидкого технологічного прогресу. Інвестиції в дослідження, підготовку кадрів та впровадження передових технологій гарантують, що система захисту не відстає від нових методів атак.

На визначених принципах побудовані різні моделі інформаційної безпеки, які сформувалися на різних підходах до забезпечення інформаційної безпеки, що відображають національні особливості та пріоритети. Коротко визначимо сутність деяких з таких моделей.

Централізована модель з військовим компонентом характеризується створенням спеціалізованого центрального органу, що координує всю діяльність у сфері кібербезпеки та інтегрує військові кіберздібності. Ця модель передбачає чітку вертикаль управління, швидке реагування на загрози та можливість проведення наступальних кіберопе рацій.

Розподілена координаційна модель базується на розмежуванні повноважень між різними відомствами при наявності координуючого органу. Така модель забезпечує баланс між ефективністю та демократичним контролем, залучаючи експертизу різних агенцій.

Багатосекторна екосистемна модель робить акцент на горизонтальній співпраці державних органів, приватного сектору, академічних установ та громадянського суспільства. Ця модель найбільш гнучка та інноваційна, оскільки використовує ресурси всіх секторів економіки.

Модель критичної інфраструктури зосереджується на захисті найважливіших систем життєзабезпечення (енергетика, транспорт, фінанси, охорона здоров'я) через встановлення жорстких стандартів безпеки та постійний моніторинг. Пріоритет надається об'єктам, порушення роботи яких може спричинити катастрофічні наслідки.

Кожна з визначених моделей з різним рівнем успіху використовується в системі публічного управління певних держав. Наведемо приклади з досвіду державного будівництва деяких демократичних держав.

Досвід Сполучених Штатів Америки: інтегрований підхід з акцентом на приватний сектор. США побудували одну з найпотужніших систем інформаційної безпеки, що поєднує державні можливості з інноваційним потенціалом Кремнієвої долини. Основою американської моделі є Національний інститут стандартів і технологій (NIST), який розробив Cybersecurity Framework – добровільний набір стандартів, що став де-факто світовим еталоном.

Координацію здійснює Агенція кібербезпеки та безпеки інфраструктури (CISA) при Міністерстві внутрішньої безпеки, яка фокусується на захисті цивільної інфраструктури. Національне агентство безпеки (NSA) та Кіберкомандування відповідають за військові аспекти та розвідувальні операції. ФБР розслідує кіберзлочини.

Ключова особливість американської моделі – потужна співпраця з приватним сектором. Великі технологічні компанії (Google, Microsoft, Amazon) надають хмарні рішення для урядових установ, беруть участь у розробці стандартів безпеки та обмінюються інформацією про загрози. Створено систему Information Sharing and Analysis Centers (ISAC) для галузевого обміну даними про кіберінциденти.

США інвестують масштабно у кібер-страхування, що зменшує вразливість організацій. Розвинена система підготовки фахівців через університети та спеціалізовані програми залучення талантів. Міжнародна співпраця включає допомогу партнерам через USAID та спільні операції з NATO.

Сильні сторони моделі: технологічне лідерство, залучення приватного сектору, потужна нормативна база. Виклики: складність координації через федеративний устрій, напруга між безпекою та приватністю, загроза монополізації ринку кібербезпеки великими корпораціями.

Модель Ізраїлю: екосистема стартапів та військові технології. Ізраїль останні роки перетворився на глобального лідера у сфері кібербезпеки завдяки унікальному поєднанню військового досвіду, інноваційної культури та необхідності протистояти постійним загрозам. Національний кібер-директорат (INCD) створений у 2015 році підпорядковується безпосередньо прем'єр-міністру та координує всі аспекти національної кібербезпеки.

Ізраїльська модель інформаційної безпеки базується на трирівневій операційній концепції: агрегована кіберстійкість (підвищення загального рівня захисту суспільства), системна кіберстійкість (швидке відновлення критичної інфраструктури) та національна кіберзахист (активна протидія масованим атакам).

Національне управління кібербезпеки (NCSA) керує Національним центром реагування на кіберінциденти (CERT-IL), який працює цілодобово та надає допомогу як корпораціям, так і звичайним громадянам. Створено галузеві центри для фінансового, енергетичного та урядового секторів.

Зазначимо, що унікальність ізраїльської моделі – в інтеграції військового досвіду з комерційним сектором. Підрозділ 8200 військової розвідки є кузнею талантів: після служби багато спеціалістів засновують стартапи з кібербезпеки. Це створило екосистему з сотень інноваційних компаній, що експортують рішення на мільярди доларів щорічно. Держава активно стимулює розвиток кібер-індустрії через Інноваційне управління,

створено шість дослідницьких центрів при провідних університетах. Спеціальні програми готують школярів до кар'єри в кібербезпеці. Міжнародна співпраця включає угоди з США, країнами ЄС та, після Авраамських угод, з ОАЕ.

До найбільш сильних сторін Ізраїльської моделі варто віднести високий рівень інновацій, синергія військової підготовки та комерційного сектору, швидкість впровадження нових рішень. Але варто зазначити і її обмеження: невеликий розмір ринку, залежність від експорту, етичні питання щодо використання кібертехнологій.

Аналіз діючих моделей інформаційної безпеки, які прийняли на озброєння демократичні держави, дозволив виділити ще одну з них – *Естоньську модель цифрової держави з розподіленою архітектурою*.

Так, Естонія, незважаючи на невеликий розмір, стала зразком цифровізації та кібербезпеки після руйнівних кібератак 2007 року. Естонська модель демонструє, що ефективна кібербезпека можлива навіть без великої вітчизняної IT-індустрії, якщо правильно організувати систему та залучити міжнародну допомогу.

Центральну роль відіграє Управління інформаційних систем (RIA), яке управляє державною IT-інфраструктурою та платформою X-Road – захищеною системою обміну даними між державними базами та приватними акторами. X-Road з'єднує всі державні реєстри, банки, лікарні, забезпечуючи безпечний доступ до електронних послуг. Естонія впровадила стандарт ISKE (адаптація німецького IT-Grundschutz), обов'язковий для державного сектору з 2008 року. Він використовує трирівневу оцінку вимог безпеки та балансує конфіденційність, цілісність і доступність даних. Естонський CERT-EE визначає пріоритети інцидентів за кількістю постраждалих користувачів, серйозністю, ціллю атаки та необхідними ресурсами.

Концепція "цифрової безперервності держави" передбачає резервування критичних даних за кордоном (у Люксембурзі) через програму "Data Embassy", що гарантує роботу електронних послуг навіть у разі

фізичної окупації території. Естонія регулярно проводить національні кібернавчання (2010, 2012, 2015, далі щорічно).

Країна тісно співпрацює з NATO, де розташований Центр передового досвіду з кіберзахисту (CCD COE) у Талінні. Естонські експерти навчають фахівців з країн Латинської Америки та інших регіонів. Міжнародне партнерство компенсує обмежені внутрішні ресурси.

Таким чином, аналіз закордонного досвіду дозволяє сформулювати рекомендації щодо оптимальної моделі інформаційної безпеки для України, враховуючи специфіку гібридної війни, обмежені ресурси та євроатлантичні прагнення.

РОЗДІЛ 2
СУЧАСНИЙ СТАН ТА ВИКЛИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Нормативно-правові засади інформаційної безпеки в Україні

Державна політика у сфері забезпечення інформаційної безпеки України реалізується за допомогою механізму правового регулювання. Такий механізм є сукупністю системи правових норм, методів та засобів, за допомогою яких держава впливає на інформаційні відносини в цілому та інформаційну безпеку зокрема.

Провідне місце в механізмі правового регулювання інформаційної безпеки займають нормативно-правові акти, в яких закріплені державно-правові засади формування та розвитку інформаційного суспільства, способи правової охорони та захисту прав та обов'язків суб'єктів інформаційних правовідносин, форми та способи забезпечення інформаційної безпеки тощо.

В Конституції України [25] закладені загальні засади збереження інформаційної безпеки. Конституційні норми охоплюють питання прав та свобод людини в інформаційній сфері, визначають роль держави у виборі способів і методів проведення політики інформаційної безпеки, гарантують державний захист інформаційної інфраструктури, закріплюють концептуальні положення національної безпеки України в усіх сферах її існування. Конституція України не тільки задекларувала забезпечення інформаційної безпеки справою всього Українського народу, а й гарантує кожному право на свободу думки й слова, свободу вираження своїх поглядів і переконань, можливість вільно збирати, зберігати, використовувати й поширювати інформацію будь яким способом, не забороненим законом.

У ст. 17 Конституції України, яка є основою формування інформаційного законодавства в Україні, вперше було задекларовано, що

захист "інформаційної безпеки є найважливішою функцією держави, справою всього українського народу".

Конституційні положення стали визначальними для розробки пакета нормативно-правових актів, необхідних для ефективного забезпечення інформаційної безпеки в Україні, в яких враховано основні положення міжнародних договорів та угод, ратифікованих Верховною Радою України. Нормативна база інформаційної безпеки спрямована на урегулювання відносин між суб'єктами інформаційної безпеки, закріплення їх правового статусу, порядку застосування сил та засобів забезпечення інформаційної безпеки тощо.

Стратегічними цілями розвитку інформаційного суспільства в Україні визнано захист інформаційних прав громадян, насамперед щодо доступності інформації, захисту інформації про особу, підтримки демократичних інститутів та мінімізації ризику "інформаційної нерівності". У цьому контексті важливим для забезпечення інформаційної безпеки України є Закон України "Про інформацію", яким утверджено інформаційний суверенітет України, закріплене право на інформацію і на доступ до неї, визначено систему відносин і зобов'язань у цій сфері, передбачено дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність за порушення інформаційного законодавства.

Разом з цим у Законі України "Про інформацію" визначення інформаційна безпека" взагалі немає. А в Законі України "Про основи національної безпеки України", який є основним орієнтиром забезпечення безпеки нашої держави, сутність "інформаційної безпеки" подано як невід'ємний складник національної безпеки України без точного визначення цього поняття [59].

Загрозами національним інтересам і національній безпеці України в інформаційній сфері цим Законом України "Про основи національної безпеки України" визнано [59]:

– прояви обмеження свободи слова та доступу громадян до інформації;

– поширення засобами масової інформації культу насильства, жорстокості, порнографії;

– комп'ютерна злочинність та комп'ютерний тероризм;

– розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– маніпулювання суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

До основних напрямів державної політики в інформаційній сфері віднесено:

– забезпечення інформаційного суверенітету України;

– удосконалення державного регулювання розвитку інформаційної сфери;

– забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації;

– недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;

– ужиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Закон України “Про Концепцію Національної програми інформатизації” проголошує, що “інформаційна безпека є невід’ємною частиною політичної, економічної, оборонної та інших складових національної безпеки” [56]. У ст. 23 “Воєнної доктрини України” прямо вказується, що “здійснення заходів щодо забезпечення інформаційної

безпеки є одним із основних завдань Збройних сил України в мирний час". А в ст. 20 зазначається, що характерними рисами сучасної збройної боротьби, серед іншого, є "зростання ролі і значущості протиборства в інформаційній сфері, використання новітніх інформаційних технологій" [56].

З метою протидії негативному впливу інформаційної пропаганди іноземних та вітчизняних засобів масової інформації та об'єднання українського суспільства навколо ідеї української державності Рада національної безпеки і оборони України прийняла Рішення "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України", яке введено в дію Указом Президента №449/2014 від 01.05.2014, у якому зазначила "що останнім часом Російська Федерація поширює недостовірну, неповну, упереджену інформацію про Україну, через що намагається маніпулювати суспільною свідомістю в Україні та за її межами". Тому виникла необхідність розроблення комплексу заходів, спрямованих на вдосконалення нормативно-правового забезпечення та попередження й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері, зокрема [54]:

– внесення змін до деяких законів України щодо протидії інформаційній агресії іноземних держав, передбачивши, зокрема, визначення механізму протидії негативному інформаційно-психологічному впливу, в тому числі шляхом заборони ретрансляції телевізійних каналів;

– розроблення і впровадження комплексних заходів організаційного, інформаційного і роз'яснювального характеру щодо всебічного висвітлення заходів з реалізації державної політики у сфері забезпечення інформаційної безпеки та посилення контролю за додержанням законодавства з питань інформаційно-психологічної та кібернетичної безпеки.

Як бачимо, у наведених документах надаються лише загальні визначення терміну "інформаційна безпека" до того ж, не узгоджені між собою. Але ці документи не містять системних підходів до забезпечення

інформаційної безпеки в Україні, не визначають суб'єктів інформаційної діяльності та не розподіляють повноважень між ними.

Внаслідок кібератаки на початку грудня 2016 року було виведено з ладу мережу Держказначейства і Міністерства фінансів України, унаслідок чого сталася надзвичайна подія в системі, де здійснюється біля 150 тисяч електронних транзакцій за добу. І як один з результатів, у грудні 2016 року на засіданні РНБО було затверджено Доктрину інформаційної безпеки України [71]. Доктрина визначає національні інтереси в інформаційній сфері, мету, завдання, принципи та механізми формування і реалізації державної інформаційної політики.

Основною метою реалізації положень Доктрини інформаційної безпеки України є створення в Україні розвиненого національного інформаційного простору і захист її інформаційного суверенітету. Доктрина визначає національні інтереси в інформаційній сфері, мету, завдання, принципи, напрями, пріоритети і механізми формування та реалізації державної інформаційної політики. Пріоритетними у документі названі такі напрямки:

– створення та розвиток структур, що відповідають за інформаційно-психологічну безпеку, насамперед у Збройних Силах України, з урахуванням практики держав-членів НАТО;

– розвиток і захист технологічної інфраструктури забезпечення інформаційної безпеки України;

– забезпечення повного покриття території України цифровим мовленням, передусім прикордонних і тимчасово окупованих територій тощо [69].

Слід відзначити, що Доктрина є першим вітчизняним нормативно-правовим документом, у якому проголошується особливе місце інформаційної безпеки в системі забезпечення національної безпеки, а саме з одного боку – як невід'ємного складника кожної зі сфер забезпечення національної безпеки і як важливої самостійної сфери забезпечення національної безпеки – з іншого боку [68].

Окрім того, важливою новацією Доктрини стало чітке виокремлення трьох головних напрямів державної політики у забезпеченні інформаційної безпеки України: технологічного розвитку, захисту інформації та "інформаційно-психологічного, зокрема щодо ...створення сприятливого психологічного клімату в національному інформаційному просторі" [69].

Стосовно інформаційно-психологічного напряму в Доктрині визначаються такі життєво важливі інтереси особи, як захищеність від деструктивних інформаційно-психологічних впливів; суспільства – щодо збереження і примноження духовних, культурних і моральних цінностей Українського народу; держави – недопущення інформаційної залежності та блокади України, інформаційної експансії з боку інших держав та міжнародних структур.

Логічним і необхідним у розвиток Доктрини мають бути розроблені та прийняті документи, які б послідовно деталізували її: Концепцію інформаційної безпеки України, Стратегію інформаційної безпеки України, Програму та плани імплементації положень попередніх документів. Маємо наді., що ці документи найближчим часом будуть розроблені і введені в дію.

У той же час, більш нормативно опрацьованими є питання кібернетичної безпеки. Так, наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 10.06.2008 р. № 94 затверджено "Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" (далі – ІТС) [44].

Метою цього Порядку є організація координації діяльності з питань запобігання вчиненню порушень безпеки інформації в ІТС, виявлення та усунення наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів в ІТС а також впровадження єдиної процедури

надання суб'єктами координації інформації про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в ІТС.

Проте цим документом не визначено механізм координації щодо діяльності з протидії інформаційним загрозам.

Ще одним із визначальних нормативних актів, яким було закладено підвалини для забезпечення захисту та здійснення контролю інформації в мережах передачі даних є постанова Кабінету Міністрів України від 8 жовтня 1997 року "Про затвердження Концепції технічного захисту інформації в Україні" [51]. Технічний захист інформації передбачає діяльність, спрямовану на забезпечення інженерно-технічними засобами порядку доступу, цілісності й доступності (неможливості блокування) інформації, що становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності й доступності відкритої інформації, важливої для особистості, суспільства й держави.

Відносини інформаційної безпеки урегульовані і Законом України "Про державну таємницю" [48], який регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [52] регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, визначає повноваження державних органів у сфері захисту інформації в інформаційно-телекомунікаційних системах.

На підзаконному рівні для забезпечення інформаційної безпеки держави актуальною є Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року [67]. Серед актуальних загроз національній безпеці Стратегія національної безпеки України виділяє загрозу інформаційній безпеці, складовою якої є ведення інформаційної

війни проти України, відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства, відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. Пріоритетним шляхами забезпечення інформаційної безпеки визначено:

– забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії;

– створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

– протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства;

– розробка і реалізація скоординованої інформаційної політики органів державної влади;

– виявлення суб'єктів українського інформаційного простору, що створені та/або використовуються Росією для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності;

– створення і розвиток інститутів, що відповідають за інформаційно-психологічну безпеку, з урахуванням практики держав - членів НАТО;

– удосконалення професійної підготовки у сфері інформаційної безпеки, упровадження загальнонаціональних освітніх програм з медіа культури. [67]

Законом України «Про захист суспільної моралі» [53] передбачено заходи щодо захисту суспільства від негативного інформаційного впливу, який спричиняє розповсюдження продукції, що негативно впливає на суспільну мораль. Цим Законом заборонено виробництво та обіг у будь-якій формі продукції порнографічного характеру в Україні, а також забороняються виробництво та розповсюдження продукції, яка:

– пропагує війну, національну та релігійну ворожнечу, зміну шляхом насильства конституційного ладу або територіальної цілісності України;

– пропагує фашизм та неофашизм;

– принижує або ображає націю чи особистість за національною ознакою;

– пропагує бузувірство, блюзнірство, неповагу до національних і релігійних святинь;

– принижує особистість, є проявом знущання з приводу фізичних вад (каліцтва), з душевнохворих, літніх людей;

– пропагує невігластво, неповагу до батьків;

– пропагує наркоманію, токсикоманію, алкоголізм, тютюнопаління та інші шкідливі звички.

Крім, того ним встановлюються спеціальний порядок виробництва та обігу у будь-якій формі продукції еротичного характеру та продукції, що містить елементи насильства та жорстокості, що дозволяються виключно за умови дотримання обмежень, встановлених законодавством, зокрема ліцензування такої діяльності.

Разом з цим, КМУ має розробити і внести на розгляд парламенту законопроекти про внесення змін до законів “Про основи національної безпеки України”, “Про інформацію”, “Про захист інформації в інформаційно-телекомунікаційних системах” та інші. Уряд має опрацювати питання щодо створення національної захищеної операційної системи, антивірусного програмного забезпечення, спеціальних програмних і технічних засобів захисту державних інформаційних ресурсів та інформаційно-комунікаційних мереж; ужити заходів щодо забезпечення поширення у світі об'єктивних відомостей про суспільно-політичну ситуацію в Україні, зокрема, шляхом створення відповідного медіа холдингу для підготовки якісного конкурентоздатного інформаційного продукту. І певна робота проводиться щодо розробки нормативно-правових актів. Проте, у проектах зазначених нормативно-правових актів, на жаль, не передбачаються

заходи щодо створення в державі цілісної системи національної інформаційної безпеки. Вважаємо проблему створення такої системи ключовою у питанні забезпечення надійної інформаційної безпеки України.

2.2 Виявлення та обґрунтування існуючих загроз у сфері інформаційної безпеки України

При розгляді проблеми інформаційної безпеки важливим кроком є виділення загроз інформаційній безпеці, а також аналіз захисту від цих загроз. Загроза інформаційній безпеці – явище, дії негативних чинників або процес, через які: соціальні об’єкти інформаційної безпеки частково або повністю втрачають можливість реалізувати свої інтереси в інформаційній сфері; а також, порушується нормальне функціонування, здійснюється руйнація або стримується розвиток технічних об’єктів інформаційної безпеки.

Наявна інформація щодо сучасного стану справ в інформаційній сфері дозволяє виділити такі типи інформаційних загроз: політичні; економічні; суспільні; військові та науково-технічні. Зосередимо увагу на характеристиці кожного з них.

В політичній сфері це:

- система державного управління;
- системи підготовки прийняття політичних рішень;
- виборчі системи;
- телекомунікаційні системи спеціального призначення.

В економічній:

- система прийняття рішень;
- банківська інфраструктура;
- управління економічним станом в умовах надзвичайних ситуацій;
- система управління державними комунікаціями, які мають економічний характер;

– корпоративні війни і промисловий шпіонаж.

В суспільній:

– загрози для системи формування громадської думки;

– структури політичних партій, громадських рухів, релігійних організацій;

– структури забезпечення основних прав і свобод людини.

У військовій:

– інформаційні ресурси збройних сил;

– системи управління військами;

– системи постійного контролю і спостереження;

– канали надходження інформації стратегічного, оперативного і розвідувального характеру.

В науково-технічній:

– системи накопичення ноу-хау;

– об’єкти інтелектуальної власності;

– структури фундаментальних і прикладних досліджень;

– структури аналізу та прогнозування тенденцій в науково-технічній сфері;

– бази і банки даних конфіденційного характеру.

Закон України “Про основи національної безпеки України” визначає наступні загрози національним інтересам і національній безпеці України в інформаційній сфері: прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації. [59]

Вітчизняні експерти [28] як правило, загрози інформаційній безпеці України за своєю загальною спрямованістю, поділяють на такі види: загрози конституційним правам і свободам людини і громадянина у сфері духовного життя й інформаційної діяльності, індивідуальній, груповій і суспільній свідомості, духовному відродженню України; загрози інформаційному забезпеченню державної політики України; загрози розвиткові вітчизняної індустрії інформації, включаючи індустрію засобів інформатизації, телекомунікацій і зв'язку; загрози безпеці інформаційно-телекомунікаційних систем на території України, як діючих, так і тих, що створюються.

Серед загроз інформаційному забезпеченню державної політики України виділяють наступні: монополізація інформаційного ринку України, його окремих секторів вітчизняними і закордонними інформаційними структурами; блокування діяльності державних засобів масової інформації з інформування української і закордонної аудиторій; низька ефективність інформаційного забезпечення державної політики України внаслідок дефіциту кваліфікованих кадрів, відсутність системи формування і реалізації державної інформаційної політики.

Серед загроз розвитку вітчизняної індустрії інформації можна виділити такі: протидія доступу України до новітніх інформаційних технологій, взаємовигідній і рівноправній участі українських виробників у світовому поділі праці в індустрії інформаційних послуг, засобів інформатизації, телекомунікацій і зв'язку, інформаційних продуктів, а також створення умов для посилення технологічної залежності України в галузі сучасних інформаційних технологій; закупівля органами державної влади імпортних засобів інформатизації, телекомунікацій і зв'язку за наявності вітчизняних аналогів, що не поступаються за характеристиками закордонним зразкам; витіснення з вітчизняного ринку українських виробників засобів інформатизації, телекомунікацій і зв'язку; відтік за кордон кваліфікованих фахівців.

Загрозами для безпеки інформаційно-телекомунікаційних систем на території України, як діючих, так і тих, що створюються, можуть бути: протиправні збирання та використання інформації; порушення технології обробки інформації; впровадження в апаратні і програмні вироби компонентів, що реалізують функції, не передбачені документацією на ці вироби; розробка і поширення програм, що порушують нормальне функціонування інформаційно-телекомунікаційних систем, зокрема систем захисту інформації; знищення, пошкодження, радіоелектронне придушення або руйнування засобів і систем обробки інформації, телекомунікацій і зв'язку; вплив на парольно-ключові системи захисту автоматизованих систем обробки і передачі інформації; компрометація ключів і засобів криптографічного захисту інформації; витік інформації по технічних каналах; впровадження електронних пристроїв для перехоплення інформації в технічні засоби обробки, збереження та передачі інформації, а також у службові приміщення органів державної влади, підприємств, установ і організацій незалежно від форми власності; знищення, пошкодження, руйнування або розкрадання машинних та інших носіїв інформації; перехоплення інформації в мережах передачі даних і на лініях зв'язку, дешифрування цієї інформації і нав'язування помилкової інформації; використання несертифікованих вітчизняних і закордонних інформаційних технологій, засобів захисту інформації, засобів інформатизації, телекомунікації і зв'язку під час створення й розвитку української інформаційної інфраструктури; несанкціонований доступ до інформації, що знаходиться в банках і базах даних; порушення законних обмежень на поширення інформації. [38].

Прикладами загроз інформаційній безпеці України, є, зокрема, протизаконна приватизація державних видавництв і поліграфічних комбінатів, свавільний розподіл радіочастот тощо. Найбільш вражаючим є те, що одна з головних загроз інформаційній безпеці лежить в сфері діяльності органів державної влади: невиконанні або неналежному виконанні органами

державної влади своїх повноважень у інформаційній сфері. Хоча, відповідно до Конституції України “забезпечення інформаційної безпеки є однією з найважливіших функцій держави та справою всього Українського народу”. [34,с. 17]

Розглядаючи проблему інформаційних загроз неможливо обминути поняття джерел загроз інформаційній безпеці. Експерти розрізняють внутрішні та зовнішні джерела загроз.

Під внутрішніми джерелами розуміють відсутність історичного, політичного та соціального досвіду життя у правовій державі, що торкається процесу практичної реалізації конституційних прав та свобод громадян, в тому числі в інформаційній сфері, а також посилення організованої злочинності та збільшення кількості комп'ютерних злочинів, зниження рівня освіченості громадян, що суттєво ускладнює підготовку трудових ресурсів для використання новітніх технологій, в тому числі інформаційних. Недостатню координацію діяльності вищого державного керівництва, органів влади та військових формувань в реалізації єдиної державної політики забезпечення національної безпеки теж можна вважати таким джерелом. До цього слід додати і відставання України від розвинутих країн за рівнем інформатизації органів державної влади, юридично-фінансової сфери, промисловості та побуту громадян. До зовнішніх джерел належать діяльність іноземних політичних, військових, економічних та розвідувальних структур в інформаційній сфері; політика домінування деяких країн в інформаційній сфері; діяльність міжнародних терористичних груп; розробка концепцій інформаційних війн будь-якими структурами; культурна експансія у відношенні до конкретної країни.

В наш час стало очевидним, що під впливом інформації зростає потенційна вразливість суспільних процесів від інформаційного впливу. Інформація стала чинником, здатним призвести до великомасштабних аварій, військових конфліктів, дезорганізації державного управління тощо. Розгляд питань інформаційної безпеки дозволяє виділити чотири групи

інформаційно-технологічних небезпек для суспільства і держави, зумовлених досягненнями науково-технічного прогресу. [29, с.127]

Перша група пов'язана з інтенсивним розвитком нового вигляду зброї - інформаційної, здатної ефективно впливати на психіку людей і інформаційно - технологічну інфраструктуру держави. Аналіз сучасних досліджень в цій області дозволяє говорити про ефективність програмування поведінки окремих людей під впливом на комп'ютерні банки даних знань і інформації.

Друга група являє собою новий вигляд соціальних злочинів, оснований на використанні досягнень сучасних інформаційних технологій: махінації з банківськими операціями; комп'ютерне хуліганство; незаконне копіювання технологічних рішень та інше. На думку провідних дослідників в цій області, комп'ютер стає провідним знаряддям злочину.

Третя група виявляється у вигляді електронного контролю за життям, настроєм, планами громадян, роботою політичних організацій, тотального комп'ютерного контролю за населенням країни. Інформаційні технології дозволяють накопичувати, зберігати і використовувати величезні масиви даних про здоров’я, соціальну активність, політичні думки, зв'язки, фінансові справи населення. Четверта група полягає у використанні інформаційних технологій в політичній боротьбі. Зростання впливу засобів масової інформації на хід і зміст політичних процесів, функціонування механізму влади - одна з домінуючих тенденцій сучасного суспільного розвитку.

Отже, можемо виділити основні реальні та потенційні загрози державній безпеці України, стабільності в суспільстві, наведемо ті, які тією чи іншою мірою реалізовуються через інформаційну сферу:

– посягання на державний суверенітет України та її територіальну цілісність, територіальні претензії з боку інших держав; спроби втручання у внутрішні справи України з боку інших держав;

– воєнно-політична нестабільність, регіональні та локальні війни (конфлікти) в різних регіонах світу, насамперед поблизу кордонів України;

– розвідувально-підривна діяльність іноземних спеціальних служб;

– загроза посягань з боку окремих груп та осіб на державний суверенітет, територіальну цілісність, економічний, науково-технічний і оборонний потенціал України, права і свободи громадян;

– злочинна діяльність проти миру і безпеки людства, насамперед поширення міжнародного тероризму;

– прояви сепаратизму, намагання автономізації за етнічною ознакою окремих регіонів України;

– недостатня ефективність існуючих структур і механізмів забезпечення міжнародної безпеки та глобальної стабільності;

– можливість втягування України в регіональні збройні конфлікти чи у протистояння з іншими державами;

– небезпечне зниження рівня забезпечення військовою та спеціальною технікою та озброєнням нового покоління ЗСУ, інших військових формувань, що загрожує зниженням їх боєготовності;

– порушення з боку органів державної влади та органів місцевого самоврядування Конституції і законів України, прав і свобод людини і громадянина, в тому числі при проведенні виборчих компаній, недостатня ефективність контролю за дотриманням вимог Конституції і виконанням законів України;

– можливість виникнення конфліктів у сфері міжетнічних і міжконфесійних відносин, радикалізації та проявів сепаратизму в діяльності деяких об’єднань національних меншин та релігійних громад;

– загроза прояву сепаратизму в окремих регіонах України;

– критична залежність національної економіки від кон’юнктури зовнішніх ринків, низькі темпи розширення внутрішнього ринку;

– зниження можливостей здобуття якісної освіти представниками бідних прошарків суспільства;

– прояви моральної та духовної деградації суспільства;

– наростаюче науково-технологічне відставання України від розвинутих країн;

– низька конкурентоспроможність продукції;

– відплив учених, фахівців, кваліфікованої робочої сили за межі України;

– прояви обмеження свободи слова та доступу громадян до інформації;

– поширення засобами масової інформації культу насильства, жорстокості, порнографії;

– комп’ютерна злочинність та комп’ютерний тероризм;

– розголошення інформації, яка становить державну та іншу передбачену законом таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації.

РОЗДІЛ 3
НАПРЯМКИ ФОРМУВАННЯ СУЧАСНОЇ МОДЕЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

3.1 Інформаційна агресія проти України: причини, наслідки та уроки гібридної війни

Збройна агресія Росії проти України, яка у повномасштабному виявленні почалася 22 лютого 2022 року, не є єдиним проявом кризових явищ у системі міжнародних відносин. Резонансні світові події останніх років, зокрема революційні зміни влади та збройні конфлікти в країнах Північної Африки, Близького Сходу та колишнього СРСР, свідчать про появу нових форм і методів, до яких вдаються провідні держави, намагаючись досягти своїх зовнішньополітичних цілей і владнати міждержавні розбіжності.

На заміну класичним військовим агресіям, коли застосовуються збройні сили, приходять так звані гібридні війни. Вони мають прихований характер та спостерігаються, переважно, у політичній, економічній і інформаційній сферах. Військо для вирішення окремих завдань залучається в невеликій кількості. Суттю такого підходу є зміщення центру зусиль з фізичного знищення противника в рамках масштабної війни до вживання засобів “м’якої сили” проти країни-противника з метою дезінтеграції та зміни її керівництва, включення до сфери свого впливу.

Причини та особливості гібридних війн (ГВ). Характерними особливостями гібридних війн є: агресія без офіційного оголошення війни; приховування країною-агресором своєї участі в конфлікті; широке використання нерегулярних збройних формувань (у т.ч. під прикриттям мирного населення); нехтування агресором міжнародними нормами ведення бойових дій та чинними угодами і досягненими домовленостями; взаємні заходи політичного та економічного тиску (за формального збереження

зв’язків між двома країнами); широка пропаганда та контрпропаганда із застосуванням “брудних” інформаційних технологій; протистояння у кібернетичному просторі.

Важливо розуміти причини виникнення самої концепції гібридних війн та пояснити, чому саме вона активно використовується різними країнами для досягнення своїх цілей.

Головною з причин виникнення ГВ є наявність нових потужних видів зброї (у т.ч. масового знищення), що робить класичні війни вкрай небезпечними, як для самого агресора, так і для всього світу. Адже це призведе до масових жертв серед мирного населення, з’являться масштабні потоки біженців, руйнуватимуться транспортні та промислові інфраструктури (включно з критично-небезпечними ядерними та хімічними об’єктами), розірвуться існуючі торгівельно-економічні зв’язки тощо.

Не менш важливим чинником є також бажання агресора применшити свою роль у розв’язанні конфліктів задля уникнення санкцій з боку інших країн та міжнародних організацій, а також для недопущення втрати свого авторитету та позицій на світовій арені.

Ще однією причиною відмови від масштабного застосування військової сили є намагання країн-агресорів встановити свій контроль над об’єктами агресії (у т.ч. інтегрувати їх до своїх політичних, економічних та безпекових систем) без надмірних для них збитків, що можуть зашкодити нападникам у реалізації власних геополітичних та економічних інтересів.

У той же час ведення гібридної війни потребує наявності або створення певних обов’язкових передумов внутрішнього та зовнішнього характеру. Насамперед, країна-агресор повинна мати сильну та дієву владу, спроможну, незважаючи на існуючі проблеми, згуртувати громадськість довкола єдиної національної ідеї. Це – по-перше.

По-друге, для успішного застосування методів гібридної війни у агресора має бути перевага над противником у військовій, економічній та інформаційній сферах, що надаватиме йому необхідні важелі тиску (впливу)

на об’єкт агресії, виснажуватиме цей об’єкт морально-психологічно та економічно.

По-третє, успіх у гібридній війні з об’єктом агресії можливий лише за умов слабкості його влади, міжнародної ізоляції, розколу у суспільстві, деградації економіки, а також зниження дієздатності та деморалізації силових структур.

У будь-якому випадку країна-агресор має бути готовою до відсічі з боку об’єкта агресії, а також до того, що останній матиме підтримку інших країн та міжнародних організацій (у т.ч. в плані надання політичної, економічної, інформаційної та військової допомоги і запровадження санкцій проти агресора).

Етапи типової гібридної війни. З урахуванням вищенаведеного, а також наявного досвіду, типова гібридна війна складається з трьох основних етапів**:** підготовчого, активного та завершального.

Етап перший – підготовчий. На підготовчому етапі (який може тривати кілька років) керівництвом країни-агресора, за активного залучення спецслужб, вживаються заходи з формування ідеологічних, політичних та військових передумов майбутньої агресії. Ці заходи включають:

– зміцнення системи державної влади в країні, включно з посиленням контролю над усіма сферами її життєдіяльності;

– ідеологічну обробку власного населення задля об’єднання довкола ідей націоналізму, великодержавного шовінізму, захисту так званих “національних цінностей та інтересів”, боротьби із “зовнішнім ворогом” та в умовах “обложеної фортеці” тощо, а також максимальне послаблення опозиції у всіх її проявах;

– захоплення інформаційного простору країни-противника та використання його у своїх інтересах для формування у суспільстві відповідного настрою;

– руйнація державної влади країни-об’єкта агресії, у т.ч.: підкуп впливових урядовців, політичних діячів та керівництва силових структур;

просування агентів впливу на посади у державних органах влади; розпалювання протистояння між різними політичними силами та встановлення контролю над ними (у першу чергу, з числа ідеологічно близьких і корумпованих партій та рухів);

– внесення розколу серед населення країни-противника шляхом стимулювання внутрішніх суперечностей політичного, міжнаціонального та міжрелігійного характеру (зокрема, у рамках створення та підтримки різних партій, рухів та організацій відповідного, у т.ч. екстремістського спрямування);

– всебічне послаблення країни-об'єкта агресії, підрив довіри населення до влади, а також поширення протестних та сепаратистських настроїв у суспільстві у спосіб провокування соціально-економічних та інших проблем (у т.ч. шляхом застосування елементів торгівельно-економічних та енергетичних війн);

– дискредитацію зовнішньої та внутрішньої політики країни-противника, нав'язування її керівництву та населенню певних ідей та цивілізаційних цінностей шляхом проведення активної інформаційної кампанії із застосуванням спеціальних методів "зомбування" суспільства.

Етап другий – активний. На активному етапі проводиться прихована агресія проти обраної країни з метою безпосередньої реалізації поставлених цілей. Для цього передбачаються наступні кроки:

– у країні-об'єкті агресії створюються незаконні збройні формування з представників місцевих антиурядових сил, до них залучаються співробітники спецслужб, найманці та бойовики;

– у країні провокується внутрішній конфлікт на політичній, соціально-економічній, конфесійній та міжнаціональній основі, а також стимулюються процеси його переростання у масові виступи населення, акції громадської непокори, безлад та сутички демонстрантів з правоохоронними органами;

– учасники акцій протесту захоплюють (у т.ч. за участю незаконних збройних формувань та спецслужб країни-агресора) урядові будівлі та важливі об’єкти транспортної і промислової інфраструктури, а також блокують діяльність силових структур (включно з використанням мирних жителів у вигляді “живих щитів”);

– на територію країни-об’єкта агресії вводяться регулярні збройні сили агресора під виглядом місцевих збройних формувань (“загонів самооборони”, “ополченців” тощо) з метою допомогти опозиції та сепаратистам захопити владу в державі або в її окремих регіонах. При цьому можлива прихована участь регулярних збройних сил країни-агресора у бойових діях на боці противників чинного уряду країни-об’єкта агресії;

– проводяться масштабні інформаційні кампанії з підтримки антидержавних сил в країні-об’єкті агресії, а також з дискредитації дій її керівництва щодо забезпечення конституційного ладу в державі.

Етап третій – заключний. На завершальному етапі агресором проводиться наступна робота щодо закріплення своїх позицій в країні-об’єкті агресії:

– надається всебічна підтримка новій) владі в країні-об’єкті агресії або сепаратистським режимам в її окремих регіонах (включно зі створенням органів влади та силових структур сепаратистів);

– надається допомога у проведенні “референдумів” щодо спрямованості зовнішнього та внутрішнього курсу країни-об’єкта агресії, статусу її регіонів, тощо, а також у проведенні “виборів” центральних та місцевих (у т.ч. сепаратистських) органів влади;

– легалізуються самопроголошені державні утворення в країні-об’єкті агресії, затягуються процеси врегулювання ситуації на її території під виглядом посередницької участі у мирних переговорах. При цьому, країна-агресор жодним чином не визнає себе стороною конфлікту;

– створюються умови для забезпечення військової присутності агресора в країні-об’єкті агресії на довготривалій/постійній основі (у вигляді

“миротворчих сил” або збройних формувань сепаратистів), а також для реалізації інших, у т.ч. економічних інтересів.

Починаючи з другої половини 90-х років минулого століття, елементи та технології концепції гібридних війн застосовувались Росією у Придністров’ї, Абхазії, Південній Осетії та Нагірному Карабасі. З початку XXI ст. аналогічний сценарій активно використовується Російською Федерацією також і щодо України (у рамках встановлення російського контролю над пострадянським простором під гаслом побудови “російського світу”).

Головна мета гібридної війни Росії проти України – послабити та децентралізувати нашу державу, привести до влади проросійське, підконтрольне Росії керівництво, зірвати її європейський курс, повернувши Україну під контроль Російської Федерації. При цьому стратегія та тактика дій Москви проти України включає послідовні кроки з реалізації розглянутих вище підходів.

Україна і Росія у попередні роки мали щонайменше три газові війни, безліч торгових війн, кожна з яких обов'язково мала інформаційний компонент, налаштований на вирішення якоїсь проблеми в фізичному просторі.

Росії для використання військової сили треба було розділити Україну на “правильну” і “неправильну”, оскільки всі ми виросли в радянській парадигмі “братерських народів”. А як можна застосовувати силу до братерського народу? Тому Україна весь час негативізувалася, що надало можливість в потрібний час заговорити про нелегітимну владу, про хунту, про бандерівців-неонацистів-фашистів. У цій моделі саме вони – “неправильні” – захопили владу, а жертвою став український народ, братерський, якого й треба захистити. Це модель "герой, жертва, злодій". Ця ж модель була використана і під час російсько-грузинської війни 2008 року

Для Росії інформаційна війна вигідна з двох боків. Перший – досягнення своїх геополітичних амбіцій, з іншого боку - це вигідний

пропагандистський інструментарій для власних потреб, оскільки всі проблеми, які існують в Росії, закрила Україна. Про власні проблеми не має часу говорити, весь негатив був перенаправлений виключно на Україну.

Перший етап. На першому (підготовчому) етапі – з початку 2000-х років до середини 2013 року, такі дії включали:

У період другого президентського терміну Л. Кучми – посилення російського впливу на керівництво України та проведення через нього вигідних для Росії рішень. Наслідком цього стала відмова української влади від курсу на вступ до НАТО та ЄС (у 2003 році після так званого "кольчужного скандалу"), а також "визначення" спадкоємцем Л. Кучми ставленика Росії В. Януковича. Однак через помаранчеву революцію Росія не досягла бажаного.

За президентства В. Ющенка – проведення масштабних заходів щодо дискредитації ідей помаранчевої революції, а також керівництва України та його європейського і євроатлантичного курсу; дестабілізація обстановки в Україні та поглиблення розколу в українському суспільстві на прихильників Заходу і Росії; підрив української економіки скороченням торгівельно-економічних зв'язків з Російською Федерацією та використанням енергетичного чинника в якості інструменту тиску на Україну (у т.ч. у рамках т. зв. газових війн). Це створило передумови для перемоги В. Януковича на президентських виборах та для "розвертання" вектору руху нашої держави із Заходу на Схід.

Під час президенства В. Януковича – закріплення досягнень Російської Федерації в Україні та остаточна її переорієнтація на Росію у спосіб:

– підкупу та корупціоналізації представників української влади (у т.ч. на вищому рівні); впровадження агентів російського впливу у керівництво України;

– послаблення та деморалізація українських силових структур, насамперед в Криму (керівниками майже всіх силових відомств України за часів В. Януковича були громадяни Росії);

– посилення російської присутності в українській економіці;

– поширення у нашій державі ідей приєднання до російських інтеграційних ініціатив в обмін на кредити та економічні преференції;

– розгортання масштабних проросійських рухів в Україні та її окремих регіонах (у першу чергу на Кримському півострові та у східних і південних областях).

І все це супроводжувалось потужною інформаційною кампанією з боку російського "агітпропу".

Наслідком такої політики Москви стала відмова керівництва України від підписання Угоди про асоціацію з ЄС у листопаді 2013 року та переорієнтація на Росію і Митний союз, що спровокувало розгортання в Україні.

Зазначимо, що масштабне “зомбування” як російського суспільства, так і частини українського населення на основі ідей російського великодержавного шовінізму сформували передумови для реалізації наступних етапів гібридної війни проти України в плані анексії Криму та провокування збройного конфлікту на сході нашої держави (у рамках проекту створення т.зв. Новоросії).

Другий етап. На другому (активному) етапі – орієнтовно з початку листопада 2013 року, вживаються наступні заходи:

У період підготовки до захоплення Криму та подальшої дезінтеграції України:

– розгортання нової масштабної інформаційної кампанії з дискредитації революції гідності в Україні (як “фашистського заколоту”) та нової влади нашої держави (як “військової хунти”), а також нав’язування ідеї щодо “необхідності захисту російськомовного населення на українській території”;

– організація в Криму та на Сході України т.зв. загонів самооборони з числа місцевих жителів та російських громадян, у т.ч. співробітників спецслужб, військовослужбовців сил спеціального призначення, членів козачих та інших напіввійськових формувань;

– створення угруповань військ, призначених для вторгнення до АР Крим та демонстрації сили поблизу кордонів України під виглядом проведення навчань та забезпечення безпеки Зимових олімпійських ігор у Сочі в січні-лютому 2014 року.

При цьому свої активні дії в українському Криму Росія розпочала у найбільш сприятливий для неї момент, який характеризувався послабленням української влади через об'єктивну тимчасову відсутність президента, прем'єр-міністра та керівників силових відомств (які втекли до Росії), а також деморалізацією особового складу українських правоохоронних органів в умовах революційних подій у нашій державі.

У такий спосіб Росія анексувала Крим та створила "підстави" для його інтеграції до складу Російської Федерації. У той же час російська анексія Криму не була визнана переважною більшістю країн та викликала негативну реакцію США, ЄС і їх партнерів, які ввели санкції проти Росії.

Під час створення т.зв. Новоросії та розв'язання збройного конфлікту на сході України :

– дестабілізація східних та південних областей України шляхом організації масових антивладних ("антимайданівських") акцій протесту, сутичок з правоохоронними органами та прихильниками єдності України, а також захоплення адміністративних будівель; реалізація "кримського" сценарію у Донецькій та Луганській областях, у т.ч. встановлення контролю над частиною їх територій, створення "загонів ополченців" з числа представників російських спецслужб, криміналізованих правоохоронних органів та місцевих проросійських сил; "легалізація" т.зв. Донецької та Луганської народних республік (ДНР і ЛНР) шляхом проведення відповідних "референдумів", а також "виборів" їх "органів влади";

– надання Росією всебічної підтримки сепаратистам, у т.ч. щодо фінансування їх діяльності, підготовки бойовиків та постачання їм зброї, військової техніки і боєприпасів, а також введення російських військ на територію ДНР і ЛНР;

– здійснення Російською Федерацією політичного та економічного тиску на Україну, а також нарощування угруповання збройних сил РФ поблизу українського кордону; дискредитація через ЗМІ військової операції України проти російсько-терористичних угруповань та дезінтеграція країни, намагання подати цю операцію як “каральну проти власного населення”.

У той же час, активна протидія України наведеним заходам Російської Федерації, у т.ч. із застосуванням військової сили, не дала можливості в повній мірі реалізувати “кримський” сценарій на сході нашої держави. Фактично, гібридна війна Росії проти України перетворилася у збройний конфлікт між двома країнами з безпосереднім залученням військ обох сторін. При цьому, незважаючи на спроби російської сторони приховати участь своїх збройних сил у зазначеному конфлікті, даний факт був визнаний переважною більшістю світової спільноти, що призвело до посилення санкцій США та ЄС у відношенні Росії.

Всі етапи гібридної війни РФ проти України супроводжувались потужною інформаційною війною. Потужні інформаційні атаки сусіда проти нашої держави розпочались задовго до анексії Криму. В історії нинішньої війни інформація дійсно стала реальною зброєю.

З 22 лютого 2022 року одночасно з повномасштабним вторгненням Росія намагається реалізувати другий етап гібридної війни проти України. Розглянемо методи та прийоми, що застосовуються в інформаційній агресії проти України, та цільові групи, які стали об'єктами інформаційних атак.

Можна виокремити такі основні методи інформаційної агресії проти України:

1) дезінформування та маніпулювання;

2) пропаганда;

3) диверсифікація громадської думки;

4) психологічний та психотропний тиск;

5) поширення чуток.

Дезінформування та маніпулювання інформацією – метод, який передбачає обман чи введення об'єкта спрямувань в оману щодо справжності намірів для спонукання його до запрограмованих суб'єктом дій.

На думку Валентина Петрика, кандидата наук з державного управління, доцента Київського національного лінгвістичного університету, найчастіше у світовій практиці застосовуються такі форми дезінформування та маніпулювання інформацією:

– тенденційне викладення фактів – форма дезінформування, яка полягає в упередженому висвітленні фактів або іншої інформації щодо подій за допомогою спеціально підібраних правдивих даних. Як правило, за допомогою цього методу спеціально сформована інформація подається дозовано, до постійно зростаючого напруження;

– дезінформування «від зворотного», що відбувається шляхом надання правдивих відомостей у перекрученому вигляді чи в такій ситуації, коли вони сприймаються об'єктом спрямувань як неправдиві. Внаслідок ужиття подібних заходів виникає ситуація, коли об'єкт фактично знає прав диву інформацію про наміри чи конкретні дії протилежної сторони, але сприймає її неадекватно, не готовий протистояти негативному впливу;

– термінологічне «мінування», яке полягає у викривленні первинної правильної суті принципово важливих, базових термінів і тлумачень загально світоглядного та оперативно-прикладного характеру;

– «сіре» дезінформування, що передбачає використання синтезу правдивої інформації з дезінформацією;

– «чорне» дезінформування, яке передбачає використання переважно неправдивої інформації [41].

Таким чином, можна констатувати, що в інформаційній війні проти України Росія застосовує практично весь арсенал впливу на свідомість людей.

Загалом інформаційний аналіз і моніторинг 2014–2020 рр. дає змогу дійти висновку, що в межах гібридної війни, яку веде РФ проти України, її

інформаційний складник характеризується певними тенденціями щодо напрямів і способів впливу. При цьому поміж основних трендів, що просувають РФ в інформаційному просторі, варто виокремити такі:

– формування іміджу РФ як могутньої держави, що обстоює принципи демократії та свободи, захищає своїх громадян та етнічних росіян;

– підрив морального здоров'я українців;

– формування уявлення про начебто широку підтримку жителями сходу України дій з боку РФ;

– деморалізування особового складу силових відомств України, зокрема Збройних сил і Національної гвардії;

– дезінформування власного населення та світового простору щодо перебігу подій, а також причин конфлікту;

– спростування інформації щодо присутності російських військових на території України;

– зомбування власного населення вигадками про американських військових, які ведуть бойові дії на сході України;

– підтримка проросійських громадян України.

На сьогодні Кремль розпочав нову інформаційну атаку, щоб підтримати новий виток ескалації конфлікту на сході України, чинити тиск на українське керівництво з метою змусити його приймати московський сценарій з урегулювання конфлікту.

Можна виокремити напрями, на яких ця атака зосередилася:

– нав'язування точок зору про неспроможність української влади керувати державою та приймати раціональні рішення;

– створення уявлень про те, що наразі для української еліти більш важливими є своє збагачення та утримання влади, ніж події на Сході України;

– формування негативних суджень про воєнно-політичне керівництво України;

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

– нав'язування думки про те, що Україна не зможе прожити зиму без російського газу та що сторонам необхідно повернутися до перегляду газових контрактів.

Цільовою аудиторією Кремля зараз є населення РФ, російськомовна діаспора за кордоном, населення України, в тому числі на тимчасово окупованих територіях України, громадяни західних країн, а також країн БРІКС та Митного союзу, близьких Росії за політичними поглядами. Тому сьогодні основну частину інформаційних заходів має взяти на себе влада та дипломатичний корпус за безумовної підтримки медіа.

У цілому ж слід зазначити, що обрання цілей і методів протидії конкретним загрозам та небезпекам інформаційній безпеці становить собою важливу проблему і складову частину діяльності з реалізації основних напрямів державної політики інформаційної безпеки [29]. У межах вирішення даної проблеми визначаються можливі форми відповідної діяльності органів державного управління, що потребує проведення детального аналізу економічного, соціального, політичного та інших станів суспільства, держави і особи, можливих наслідків вибору тих чи інших варіантів здійснення цієї діяльності.

3.2 Визначення напрямків формування сучасної моделі забезпечення інформаційної безпеки держави

Аналізуючи агресивну поведінку російської влади на різних напрямках забезпечення повномасштабного вторгнення в Україну, науковці підкреслюють, що інформаційна складова виглядає однією з пріоритетних. Наголошується, що головна інформаційна загроза національній безпеці – це загроза впливу іншої сторони на інформаційну інфраструктуру країни,

інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості, з метою нав'язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони напрямку.

Власне, це є загрозою суверенітету України в життєво важливих сферах суспільної й державної діяльності, що реалізовується на інформаційному рівні. Стратегічне інформаційне протистояння є самостійним і принципово новим видом протистояння, здатним вирішувати конфлікт без застосування збройних сил у традиційному розумінні.

Для вивчення закономірностей інформаційного протистояння та аналізу його кількісних характеристик необхідно формалізувати як поняття рівня інформаційної озброєності держави, так і механізм еволюції ресурсного потенціалу конкретної держави та вплив зовнішнього оточення.

Кожна держава, що є частиною світового інформаційного простору, має виробити комплекс заходів для власного сталого інформаційного розвитку в умовах жорсткої конкуренції з урахуванням чинників інформаційної безпеки. Для цього необхідно:

– розуміння інформаційних атак та протистояння ним.

– створення програмного забезпечення протистояння інформаційним атакам;

– аналіз показників інформаційних загроз з метою вдосконалення механізмів прийняття рішень в системах державного управління;

– забезпечення максимального захисту від зовнішніх впливів;

– аналіз стану і технічний аудит всіх засобів комунікації;

– консолідація діяльності органів державної влади та ЗМІ у сфері політичного інформування суспільства для нейтралізації негативного психологічного впливу в умовах криз та конфліктів.

Національну безпеку України в інформаційній сфері слід розглядати як інтегральну цілісність чотирьох складових – персональної, публічної

(суспільної), комерційної (корпоративної) й державної безпеки. Тому в процесі визначення характеру ризиків слід брати до уваги наступні елементи:

– концептуальне засади політичної безпеки [9], її принципів, стандартів та правил, погоджених із чинним законодавством й принципами забезпечення безперервності системи інформаційної безпеки особистості, суспільства, комерційних (корпоративних) структур та держави;

– визначення об’єктів та цілей;

– визначення прийнятних з погляду забезпечення інтересів усіх суб’єктів структур встановлення контролю над об’єктами безпеки, а також оцінки ризиків та управління ризиками;

– аналіз недоліків діючої моделі інормаційної безпеки держави.

Зазначимо, що проведене у магістерській роботі дослідження щодо основник ознак, внутрішнього змісту та функцій моделей інформаційної безпеки дерави дозволяє побудувати та обгрунтувати оптимальну модель інформаційної безпеки держави для України. Вона повинна базуватися на унікальному досвіді протидії масованим кібератакам в умовах повномасштабної війни. Так, тільки за 2024 рік Україна зафіксувала понад 1000 серйозних кібератак, спрямованих на державну, військову та цивільну інфраструктуру, проте кількість успішних атак драматично скоротилася завдяки розвинутій кіберстійкості. Виходячи з наявного досвіду і вивчення кращих практик у зазначеній сфері, спробуємо сформувати проєктні орієнтири такої моделі.

Модель має інтегрувати три парадигми:

1.Парадигма бойової ефективності – визнання кіберпростору повноцінним театром військових дій, де проводяться як оборонні, так і наступальні операції. Створення Кіберсил ЗСУ (затверджено Верховною Радою у жовтні 2025 року) як окремого виду військ підкреслює стратегічну важливість цього підходу.

2.Парадигма цифрової резильєнтності – здатність критичної інфраструктури швидко відновлюватися після атак та продовжувати

функціонування навіть під час масованих кібернападів. Українські державні мережі демонстрували відновлення протягом годин після використання wipers-програм, що нівелювало стратегічний ефект атак.

3.Парадигма державно-приватного симбіозу – органічна інтеграція державних структур, приватних ІТ-компаній, міжнародних партнерів (Microsoft, Palo Alto Networks, Google) та волонтерських кіберспільнот. Цей підхід забезпечив унікальну гнучкість та доступ до передових технологій.

Сучасна модель інформаційної безпеки України може будуватися на основних принципах, що закладає підґрунтя для наукового та інноваційного підходів. Зупинимося на характерних ознаках таких принципів.

Принцип подвійного призначення – кожен елемент системи має виконувати як військові, так і цивільні функції, забезпечуючи ефективне використання обмежених ресурсів в умовах війни.

Принцип вертикальної інтеграції та горизонтальної координації – централізоване стратегічне управління через РНБО при збереженні оперативної автономії галузевих структур та швидкого горизонтального обміну інформацією.

Принцип проактивної агресивності – не лише оборона, але й активні наступальні кібероперації проти агресора для стримування та виснаження його можливостей. Українські кіберпідрозділи завдали понад 160 ударів по російських нафтових об'єктах у 2025 році.

Принцип міжнародної взаємозалежності – визнання, що безпека України нерозривно пов'язана з безпекою євроатлантичного простору, що вимагає глибокої інтеграції з NATO, ЄС та стратегічними партнерами.

Принцип адаптивної еволюції – швидка трансформація структур та процедур на основі бойового досвіду, без бюрократичних перепон, що довели свою ефективність під час війни.

Визначені принципи складають теоретичні підвалини бажаної моделі інформаційної безпеки держави. Але її практичне застосування потребує розробки стійкої і розгалуженої структури, що забезпечить її

функціональною здібністю швидко і кваліфіковано реагувати на виклики щодо забезпечення інформаційної безпеки держави. Структура моделі повинна передбачати напрямки організації виконання державної стратегії інформаційної безпеки і спиратися на вже існуючі інституції, що є виконавцями такої стратегії.

Одна з основних вимог до такої моделі передбачає стратегічне управління та координацію в питаннях інформаційної безпеки України. Таку місію може виконувати *Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони* (*Штаб національної кіберстійкості*). До функцій Центру доцільно віднести:

- визначення національної стратегії та пріоритетів у сфері кібербезпеки;
- координація діяльності всіх державних органів, відповідальних за кібербезпеку;
- стратегічне планування та розподіл ресурсів між секторами;
- управління міжнародною співпрацею та залученням технічної допомоги;
- розроблення щорічних національних оцінок кіберризиків;
- координація національних кібернавчань та оцінка готовності до кризових ситуацій.

Важливою інституцією в загальній моделі інформаційної безпеки України повинна стати *Рада з кібербезпеки критичної інфраструктури, що перебере на себе наступні функції:*

- ідентифікація та класифікація об'єктів критичної інфраструктури;
- затвердження галузевих стандартів кібербезпеки;
- координація взаємодії операторів критичної інфраструктури;
- організація обміну інформацією про загрози між секторами;
- контроль за дотриманням вимог державних стандартів у критичних секторах.

Не менш важливу роль в структурі моделі інформаційної безпеки забезпечують її механізми, що відповідають за оперативне керівництво та виконання конкретних завдань.

До таких механізмів відносяться *Кіберсили Збройних Сил України* (проведення наступальних кібероперацій проти військової та критичної інфраструктури противника, збір розвідувальної інформації в кіберпросторі, захист військових інформаційних систем та систем зв'язку ЗСУ, координація з військами радіоелектронної боротьби для комплексних операцій, підготовка військових кіберфахівців та управління кіберрезервом, участь у міжнародних військових кібернавчаннях NATO) та *Державна служба спеціального зв'язку та захисту інформації* (захист державних інформаційних ресурсів та електронних комунікацій, управління державною системою виявлення та реагування на кіберінциденти, провадження базових профілів безпеки для держустанов, сертифікація засобів криптографічного захисту, технічний аудит систем кібербезпеки державного сектору).

Природно, що до наповнення сучасної моделі забезпечення інформаційної безпеки України ефективними інструментами докладуть зусилля діючи в політичній системі і органах публічного управління держави інститути.

Вони можуть увійти у запропоновані міжвідомчі центри і координаційні ради, а можуть долучитись до такої роботи спираючись на свої повноваження, цілі та завдання. До таких інститутів відносяться:

– Служба безпеки України (Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки), Міністерство цифрової трансформації (Управління кіберзахисту),

– Національна поліція України (Департамент кіберполіції),

– Галузеві структури та спеціалізовані центри та інш.

Формування сучасної інноваційної моделі забезпечення інформаційної безпеки держави дозволить підняти на необхідний рівень систему ефективної

протидії гібридним загрозам, стане важливим елементом національної безпеки держави.

ВИСНОВКИ

У магістерській роботі здійснено теоретичне узагальнення публічного управління забезпеченням інформаційної безпеки держави. На підставі здійсненого дослідження зроблено певні узагальнення та висновки.

Інформаційна безпека в загальній системі національної безпеки України посідає надважливе місце, адже інформація в сучасному світі, зазнаючи постійних якісних та кількісних змін, є найціннішим глобальним ресурсом, а інформаційні відносини – невід'ємною складовою будь-яких процесів у державі та суспільстві. За умов зростання уразливості сучасного інформаційного суспільства від недостовірної (іноді – свідомо викривленої) інформації, її несвоєчасного надходження, загалом від злочинів в інформаційній сфері, деструктивні впливи на інформаційну сферу можуть завдати значної шкоди життєве важливим інтересам держави. Відтак забезпечення інформаційної безпеки належить до пріоритетних напрямів державної політики.

Побудова сучасної моделі забезпечення інформаційної безпеки в Україні спирається на вивчення та вростання досвіду демократичних держав. Корисним у зв'язку з нашим дослідженням може бути приклади функціонування систем інформаційної безпеки у Сполучених Штатах Америки, Франції, Ізраїлі і Естонії. Механізми та задіяні в її реалізації інструменти можуть бути імплементовані до українських реалій.

Аналіз сучасного стану нормативно-правової бази та інструкційного забезпечення інформаційної безпеки держави свідчить про недосконалість діючої моделі у зазначеній сфері. Це і відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. Україна потребує законодавчих змін, які дозволять захистити інформаційне поле України. Нормативно-правове забезпечення у питаннях національної безпеки і оборони не відповідає загрозам національній безпеці України в

інформаційній сфері, та потребує доопрацювання або уточнення. Політичне управління сектором інформаційної безпеки і оборони, а також його реформування проводилось безсистемно, без створення цілісної системи взаємопов'язаних нормативно-правових актів, програм розвитку, планів та відповідного фінансового і матеріально-технічного забезпечення.

Недосконаліть системи забезпечення інформаційній безпеці негативно вплинула на дотримання конституційних прав і свобод громадян, зашкодила важливим інтересам суспільства і держави в політичній, економічній, оборонній та інших сферах. Реалізація загроз може створити перешкоди на шляху рівноправного співробітництва України з закордонними країнами, утруднити прийняття найважливіших політичних, економічних та інших рішень, підірвати авторитет держави на міжнародній арені, створити атмосферу напруженості і політичної нестабільності в суспільстві, порушити баланс інтересів особистості, суспільства і держави, дискредитувати органи державної влади, спровокувати соціальні, національні та релігійні конфлікти, ініціювати страйки і масові заворушення, порушити функціонування органів державної влади, а також систем експлуатації озброєння і військової техніки, управління військами і зброєю, об'єктами підвищеної небезпеки.

Обґрунтована необхідність змін внутрішніх та зовнішніх засад вітчизняної інформаційної політика у сфері захисту державних (національних) інтересів. Зокрема, слід відмовитись від виключно оборонних засад інформаційної безпеки України. Адже сучасні геополітичні реалії України підтверджують неефективність методів офіційного спростування представниками влади тієї чи іншої інформації, що потрапляє у ЗМІ. Необхідно вживати заходи активної протидії інформаційним компаніям проти України шляхом використання наступальних інформаційних операцій.

Обґрунтовано розробку сучасної моделі інформаційної безпеки держави і створення на її основі комплексної системи безперервного забезпечення інформаційної безпеки, оскільки інтеграція в міжнародний

інформаційний простір та динамічний процес інформатизації, притаманний сучасному суспільству, мають як позитивні, так і негативні наслідки.

Для адекватного реагування на виклики і загрози в інформаційній сфері актуальним постає завдання становлення й розвитку дієвої системи забезпечення інформаційної безпеки та її складових, побудови такої моделі. Тому, розглянуті в проєктному вигляді основні структурні елементи моделі інформаційної безпеки України, де визначені інститути, міжвідомчі центри і ради та сформовані їх функції і сфери відповідальності.

СПИСОК ВІКОРИСТОНИХ ДЖЕРЕЛ

1. Актуальні проблеми міжнародної безпеки: український вимір [матеріали круглих столів, семінарів та конф.] / Рада нац. безпеки і оборони України ; Нац. ін-т проблем міжнар. Безпеки, - 2014 р.

2. Арістова І. В. Державна інформаційна політика та її реалізація в діяльності ОВС України: організаційно-правові засади: дис. д-ра юрид. наук: 12.00.07 / Нац. ін-т внутр. справ. – Х., 2012. – 408 с.

3. Баровська А.В. Оптимізація структури керівних документів державної політики (на прикладі інформаційної політики). – Аналітична доповідь. – НІСД. – 2011 р. – 46 с.

4. Білоконь М.В. Формування європейської та євроатлантичної перспективи України у контексті реалізації національних інтересів. Державне будівництво. 2021. URL: https://periodicals.karazin.ua/db/issue/view/1182

5. Бжезинский Зб. Вибір. Світове планування чи глобальне лідерство / Зб. Бжезинский; [пер. с англ.] – Київ : Думка, 2005. – 253 с.

6. Боднар І. Р. Інформаційна безпека як основа національної безпеки / І. Р. Боднар // Механізм регулювання економіки. – 2014. – № 1. – С. 68–75.

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

8. Боднар І. Р. Сучасні реалії інформаційного суспільства: проблеми становлення та перспективи розвитку: монографія [Текст] / І.Р. Боднар. – Львів: Видавництво Львівської комерційної академії, 2013. – 320 с.

9. Быченок М.М., Дзюба Т.М., Рось А.О., Витковский В.В. Основы информационной борьбы: Учебник. – К.: НУОУ, 2014. – 265 с.

10. Великий тлумачний словник сучасної української мови (з дод., допов. та CD) / [уклад. І голов. ред. В.Т. Бусел]. – К.; Ірпінь: ВТФ «Перун», 2009. – 1736 с.: іл.

11. Голубєв В.О. Інформаційна безпека: проблеми боротьби з кіберзлочинами: Монографія. – Запоріжжя: ГУ “ЗІДМУ”, 2013. – 250 с

12. Гусарєв С.Д. Юридична діяльність: методологічні та теоретичні аспекти / С.Д. Гусарєв. – К.: Знання, 2005. – 357 с.

13. Гуцалюк М. Інформаційна безпека в сучасному суспільстві / М. Гуцалюк // Право України. – 2005. – № 7. – С. 71–74.

14. Державне управління: основи теорії, історія і практика: Навчальний посібник / В. Д. Бакуменко, П. І. Надолішній, М. М. Іжа, Г. І. Арабаджи / за заг. ред. П. І. Надолішнього, В. Д. Бакуменка. – Одеса : ОРІДУ НАДУ, 2009. – 394 с.

15. Довгань О.Д. Інформаційна безпека – гарант існування і розвитку національних інформаційних ресурсів/О.Д. Довгань/ Актуальні проблеми управління інформаційною безпекою держави: Збірник матеріалів науково-практичної конференції, 19 березня 2015. – К.: Центр навч.-наук. та наук.-прак.вид. НА СБ України, 2015. – С.40-45.

16. Довгань О.Д. Щодо окремих проблем правового врегулювання інформаційних відносин в умовах кіберцивілізації/О.Д. Довгань, О.М. Солодка/ Правове регулювання інформаційних відносин та сфери інтелектуальної власності в умовах кіберцивілізації: Матеріали науково-практичної конференції, 26 березня 2015. – К.: НДІІП НАПрН України, НТУУ «КПІ», 2015. – С.27-29.

17. Інформаційне суспільство в Україні: глобальні виклики та національні можливості: аналітична доповідь / Д. В. Дубов, О. А. Ожеван, С. Л. Гнатюк. – К. : НІСД, 2010. – 64 с.

18. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1 / С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с.

19. Карпенко О.В. Інформаційні війна як інноваційний механізм реалізації державної політики України / О.В. Карпенко // Інновації в державному управлінні: системна інтеграція освіти, науки, практики : матеріали наук.-практ. конф. за міжнар. участю, Київ, 27 трав. 2011 р. : у 2 т. /

за заг. ред. Ю.В. Ковбасюка, В.П. Трощинського, С.В. Загороднюка. – К. : НАДУ, 2011. – Т.1. – С. 176-177

20. Карпенко О.В. Наступальні інформаційні операції як сучасний механізм захисту державних інтересів України / О.В. Карпенко // Ефективність державного управління: зб. наук. пр. Львівського регіонального інституту державного управління Національної академії державного управління при Президентові України. – Вип. 27 / за заг. ред. чл.-кор. НАН України В. С. Загорського, доц. А. В. Ліпенцева. – Львів: ЛРІДУ НАДУ, 2011. – С. 276-281.

21. Коваль І.Д. Інформаційні ресурси: національні і державні, зміст, поняття/І.Д. Коваль/ Інформація і право. – 2015. – №3(15).– С.85-91.

22. Комп'ютерна злочинність і інформаційна безпека / А. П. Леонов ; за заг. ред. А. П. Леонова. – Мінськ : АРІЛ, 2000. – 552 с.

23. Конах В.К. Нормативно-правові засади державної політики України у сфері інформаційно-психологічної безпеки / В.К. Конах // Стратегічні приоритети. – 2012. – № 3(24). – С. 152-157.

24. Конституційне право України : підручник для студ. вищих навч. закл. / За заг.ред. Ю.М. Тодики, В.С. Журавського. – К. : Видавничий Дім «ІнЮре», 2012. – 544 с.

25. Конституція України // Відомості Верховної Ради України. – 1996. [Електрон. ресурс]. – Режим доступу : http://www.viche.info/journal/1159.

26. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України. – О., 2003. – 472 с., с. 148–149

27. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. На здобуття наук. ступеня докт. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Б. А. Кормич ; Нац. ун-т внутр. справ. — Х., 2004. — 42 с., с. 15

28. Кормич Б.А. Правова регламентація інформаційної безпеки держави / Б.А. Кормич // Держава і право: зб.наук. пр. Юридичні і політичні

науки. – Вип. 17. – К.: Ін-т держави і права ім. В.М. Корецького НАН України, 2002. – С. 193-198.

29. Косогов О.М. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору / О.М. Косогов // Збірник наукових праць Харківського університету Повітряних Сил. – Х.: ХУПС, 2014. – Вип. 3 (40). – С. 127-129.

30. Краснокульська Ю. Інтернет як засіб комунікації: теоретико-методологічний аналіз [Електронний ресурс] / Ю. Краснокульська. – Режим доступу: http://bibl.kma.mk.ua/pdf/ukrpolituk/-1/41.pdf.

31. Круглов В.В., Сутула О.А. Механізми державно-приватного партнерства у відбудові спортивної інфраструктури України. *Суспільство та національні інтереси*. 2025. №3(11). С. 813-823.

32. Ліпкан В.А., Ю.Є.Максименко, В.М.Желіховський Інформаційна безпека України в умовах євроінтеграції КНТ, 2016., – 279с.

33. Лужецький В. А. Інформаційна безпека : навч. посіб. / В. А. Лужецький, О. П. Войнович, А. В. Дудатьєв. – Вінниця : УНІВЕРСУМ-Вінниця, 2009. – 240 с.

34. Макаренко Е., Кирик В. Інформайційно-психологічний захист як складовий чинник інформаційної безпеки // Проблеми безпеки української нації на порозі XXI сторіччя. – К.-Чернівці, 2014

35. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України: дис. ... кандидата юрид. наук: 12.00.01 / Максименко Ю.Є. – К., 2007. – 186 с.

36. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки / А. І. Марущак // Державна безпека України. — 2011. — № 21. — С. 92—95., с. 72

37. Масляниця Й.У. Інформаційні ресурси України : проблеми державного управління : монографія / Й.У. Масляниця, О.В. Соснін, Л.Є. Шиманський. – К.: НІСД, 2002. – 141 с.

38. Морозов О. Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності. [Електронний ресурс] – Режим доступу: http://www.viche.info

39. Мотузка І.І. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України /І.І. Мотузка/ Інформаційна безпека людини, суспільства, держави. – 2015. – №3(19).–С.6-17.

40. Новицька Н.Б. Правове забезпечення інформаційної безпеки // Інформаційна безпека людини, суспільства, держави. – 2009. – № 1. – С. 44-47

41. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / В. Петрик. – Режим доступу : http://justinian.com.ua/article.php?id=3222

42. Положення про Державний комітет телебачення і радіомовлення України: Указ Президента України від 07.05.2011 р. № 559/2011

43. Попов М.О., Щербак В.А. Дезінформаційні заходи та їх вплив на функціонування системи добування даних і прийняття інформаційних рішень // Наука і оборона. – 2012. – № 4. – С. 42–51.

44. Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 10.06.2008 р. № 94

45. Почепцов Г. Інформаційна політика : навч. посібник [Текст] / Г.Г.Почепцов – К.: Знання, 2006. – 663 с.

46. Про внесення змін до деяких законів України з питань оборони: Закон України від 16.06.2016 № 1420-VIII // Відомості Верховної Ради (ВВР), 2016, № 31, ст.546

47. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України // Відомості Верховної Ради України. – 2006. – № 30. – С. 258.

48. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII / [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgibin/laws/main.cgi?page=1&nreg=3855-12.

49. Про Доктрину інформаційної безпеки України (втратила чинність): указ Президента України від 8.07.2009 р. № 514/2009. [Електрон. ресурс]. – Режим доступу: http://www.president.gov.ua/documents/9570.html.

50. Про доступ до публічної інформації : Закон України від 13 січня 2011 р. № 2939-VI [Електронний ресурс] : Верховна Рада України : за станом на 1 січня 2012 р. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/про%20доступ%20до%20публічної%20.

51. Про затвердження Концепції технічного захисту інформації в Україні: постанова Кабінету Міністрів України від 8 жовтня 1997 року № 1126 [Електронний ресурс]. Режим доступу: http://zakon0.rada.gov.ua/laws/show/1126-97-%D0%BF

52. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР // Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286

53. Про захист суспільної моралі: Закон України 20.11.2003 № 1296-IV // Відомості Верховної Ради України. – 2004. – № 14. – С. 192.

54. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України : Указ Президента України №449/2014 від 01.05.2014. [Електронний ресурс]. Режим доступу: http://zakon5.rada.gov.ua/laws/show/n0004525-14

55. Про інформацію: Закон України від 02.10.1992 № 2657-XII / [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12.

56. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 р. № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27-28. – Ст. 182.

57. Про Національну програму інформатизації: Закон України від 4 лютого 1998 р. № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27 – 28. – ст. 181.

58. Про Національну раду України з питань телебачення і радіомовлення Закон України: // Відомості Верховної Ради України. – 1997. – № 48. – С. 296.

59. Про основи національної безпеки України: Закон України від 19.06.2003 № 964-IV // Відомості Верховної Ради України (ВВР), 2003, № 39, ст.351

60. Про Положення про Державний комітет телебачення і радіомовлення України: Указ Президента України від 07.05.2011 р., № 559/2011 // Урядовий кур'єр. – 2011. – 25.05. – № 93

61. Про Раду національної безпеки і оборони України: Закон України від 05.03.1998 № 183/98-ВР // Відомості Верховної Ради України. – 1998. – № 35. – С. 237.

62. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року "Про нову редакцію Воєнної доктрини України": Указ Президента України №555/2015. [Електронний ресурс]. Режим доступу: http://www.president.gov.ua/documents/5552015-19443

63. Про розвідувальну діяльність: Закон України // Відомості Верховної Ради України. – 2001. – № 19. – С. 94.

64. Про Службу безпеки України: Закон України // Відомості Верховної Ради України. – 1992. – № 27. – С. 382.

65. Про Службу зовнішньої розвідки України: Закон України // Відомості Верховної Ради України. – 2006. – № 8. – С. 94.

66. Про Стратегію кібербезпеки України: Указ Президента України №96 / 2016 від 27 січня 2016 року. – [Електроний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/287/2015

67. Про Стратегію національної безпеки України: Указ Президента України від 26.05.2015 № 287/2015 [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/287/2015

68. Про телебачення та радіомовлення: Закон України від 21.12.1993 № 3759-XII // Відомості Верховної Ради України. – 1994. – № 10. – С. 43.

69. Рада Національної безпеки і оборони України: Офіційний веб-сайт. [Електронний ресурс]. Режим доступу: http://www.rnbo.gov.ua

70. Рак О. Політико-комунікаційні впливи на суспільство та засоби їх реалізації через засобі масової інформації. *Освіта регіону: політологія, психологія, комунікації.* 2012. № 3. С. 188.

71. РНБОУ схвалила Доктрину інформаційної безпеки України [Електронний ресурс]. Режим доступу: http://www.rnbo.gov.ua/news/2678.html

72. Семенченко А.І. Методологія стратегічного планування у сфері державного управління забезпеченням національної безпеки України: моногр. / А.І. Семенченко. – К.: Вид-во НАДУ, 2008. – 428 с.

73. Середа М.П. Сучасні інформаційні структури як компоненти інформаційної безпеки /М.П. Середа/ Інформація і право. – 2015. – №2(14).– С.75-85.

74. Соснін О. В. Державна політика в галузі управління інформаційним ресурсом України : автореф. дис. на здобуття наук. ступеня д. п. н. за спеціальністю 23.00.02 «Політичні інститути та процеси» / О. В. Соснін. – Одеса, 2005. – 45 с.

75. Соснін О.В. Інформаційна політика України: проблеми розбудови [Електронний ресурс] – Режим доступу: http://www.niisp.gov.ua/vydanna/panorama

76. Толубко В.Б. Складові інформаційної боротьби / В.Б. Толубко, А.О. Рось // Наука і оборона. – 2012. – № 2. – С. 23-28

77. Тоффлер Э. Третя Хвиля / 3 англ. пер. А. Євса. — К.: Вид. дім «Всесвіт», 2000. — 480 с.

78. Хмелевський Р.М. Тези. «Інформаційна безпека, як одна з основ забезпечення ефективності роботи державного управління». Матеріали міжнародної науково-технічної конференції «Сучасні інформаційно-телекомунікаційні технології» Том IV «Сучасні технології інформаційної безпеки» Київ, ДУТ. 17–20 листопада 2015 р. – С.155–158.

79. Юдін О.К., Богуш В.М. Інформаційна безпека держави: Навчальний посібник.- Харків: Консум, 2005. – 576 с.