МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут «Інститут державного управління»

До захисту

В.о. завідувача кафедри публічного управління
та державної служби
к.держ.упр., доц. Набока Л.В.
_____
/Підпис/

ПУБЛІЧНЕ УПРАВЛІННЯ ФОРМУВАННЯМ МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Кваліфікаційна робота на здобуття освітнього ступеня «магістр»
281 Публічне управління та адміністрування
28 Публічне управління та адміністрування

Виконавець
здобувач 2 курсу, гр. ЗПУА- 4-23 О.М. Петренко

Науковий керівник
д.держ.упр., проф. В.Г. Бульба

Харків – 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

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 пртиборство
ІТС	інформаційно-телекомунікаційні системи
КМУ	Кабінет Міністрів України
ЛНР	так звана Луганська народна республіка
НАТО	англ. North Atlantic Treaty Organization (Північноатлантичний Альянс)
РНБО	Рада національної безпеки і оборони України
РФ	Російська Федерація
СБУ	Служба безпеки України

ВСТУП

Актуальність теми дослідження. В умовах швидкого формування і розвитку інформаційного суспільства в Україні 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 гібридної війни проти України, що створює реальні загрози конституційному ладу, територіальній цілісності та національній безпеці України і характеризується цілеспрямованим знищенням української інформаційної інфраструктури в окремих районах Донецької і Луганської областей та Автономній Республіці Крим, 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.

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 роботи є полягає в обґрунтуванні особливостей розвитку інформаційної безпеки України та з'ясуванні напрямів і шляхів забезпечення 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;

– проаналізувати сучасний стан нормативно-правового 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;

– визначити методи забезпечення інформаційної безпеки держави;

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

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

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

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

*Структури роботи***.** Логіка проведеного дослідження зумовила наступну структуру роботи: вступ, три розділи, висновки та перелік джерел посилання.. Загальний обсяг роботи становить 72 сторінки. Список використаної літератури нараховує 79 джерел. В роботі вміщено 3 рисунки.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Національні інтереси України в інформаційній сфері як об'єкт національної безпеки

За умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби різновекторних національних інтересів держав стає інформаційний простір. Сучасні інформаційні технології дають змогу державам реалізувати власні інтереси без застосування воєнної сили, послабити або завдати значної шкоди безпеці конкурентної держави, яка не має дієвої системи захисту від негативних інформаційних впливів.

Збройна агресія проти України, якій передували події на Сході України та в Криму у 2014 році підтверджують, що 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.

Водночас І. В. Арістова звертає увагу на те, що сьогодні в національному законодавстві не легалізовано поняття «інформаційна сфера». На її думку, сьогодні як на побутовому, так і на науковому рівні інформаційна сфера розглядається як сфера, що формується та розвивається під час інформаційної діяльності [2].

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].

В даній роботі під інформацією розуміється багатофункціональний об’єкт, що створюється і застосовується у всіх сферах діяльності і забезпечує виконання багатоманітних функцій і завдань, що постають перед органами влади, перед юридичними і фізичними особами, іншими соціальними утвореннями [37].

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. Також 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].

Натомість 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].

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]. 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].

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].

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 (рис. 1.1).

Рисунок 1.1- Національні інтереси в інформаційній сфері.

Можна виділити чотири основні складові національних інтересів України в інформаційній сфері:

1) Перша складова національних інтересів України в інформаційній сфері 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) Друга складова національних інтересів України в інформаційній сфері полягає у інформаційному забезпеченні державної політики України, доведенні 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) Третя складова національних інтересів України в інформаційній сфері 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) Четверта складова національних інтересів України в інформаційній сфері полягає у захисті інформаційних ресурсів від технічних розвідок, несанкціонованого доступу, забезпеченні безпеки інформаційних і телекомунікаційних систем.[11]

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.

Аналіз Конституції України дозволив говорити про закріплення основних прав та свобод людини в інформаційній сфері. Так згідно з 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].

Загалом, на основі здійсненого аналізу вищевикладених норм Конституції України, а також беручи до уваги національні інтереси, визначені законом України "Про основи національної безпеки України", можна виокремити основні національні інтереси в інформаційній сфері, а саме:

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].

Коротко підсумовуючи вищевикладене основним питанням виживання України є створення адекватної сучасному стану України, її національним інтересам і загрозам системи інформаційної безпеки, яка б включала сили та засоби ведення виграшних інформаційних війн.

1.2 Система забезпечення інформаційної безпеки України, її основні функції, об'єкти та суб'єкти

Забезпечення інформаційної безпеки України як найважливішої функції держави реалізується за допомогою відповідної системи як органів державної влади, так і ряду недержавних інституцій. Отже, система забезпечення інформаційної безпеки України призначена для реалізації державної політики в даній сфері. Ця система є частиною системи 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.

Б. Кормич оперує декількома поняттями: «державно-правовий механізм інформаційної безпеки» й «інституційний механізм інформаційної безпеки». При цьому, якщо державно-правовий механізм інформаційної безпеки автор визначає як сукупність державних інституцій, задіяних у процесі формування та впровадження політики інформаційної безпеки, їх ролей і відносин, що підпорядковані чіткій ієрархії правових норм та принципів, то інституційний механізм інформаційної безпеки, що є складовим елементом державно-правового механізму, має декілька визначень. Відповідно до першого, інституційний механізм інформаційної безпеки України – це сукупність державних інституцій, задіяних у процесі формування та впровадження політики інформаційної безпеки [26]. Згідно з другим, інституційний механізм інформаційної безпеки представляє собою сукупність інститутів публічної влади й інститутів громадянського суспільства, до компетенції яких входить вирішення питань щодо забезпечення умов функціонування та розвитку інформаційної сфери [28,].

Таким чином, поняття «інституційний механізм інформаційної безпеки» має широке та вузьке розуміння. У вузькому значенні інституційний механізм інформаційної безпеки охоплює виключно державні

інституції, задіяні в процесі формування та впровадження політики інформаційної безпеки. У широкому значенні, крім інститутів публічної влади, до його складу входять також інститути громадянського суспільства.

Перелік інституцій, які можуть брати участь у проведенні політики або виробленні конкретних політичних рішень, практично невичерпний і він не обмежується лише органами державної влади та місцевого самоврядування. Так, опрацювання будь-якої проблеми, пов’язаної з політикою інформаційної безпеки, може бути доручене певним науковим установам, групам експертів [26].

Компетенція органів державної влади України, інших державних органів, що входять до складу системи забезпечення інформаційної безпеки держави та її підсистем, визначається законами України, нормативними правовими актами Президента України і Кабінету Міністрів України.

Об’єктами інформаційної безпеки України є:

– людина і громадянин – їхні конституційні права і свободи, фізичне та психологічне здоров’я, захищеність від негативного впливу інформаційних технологій та інформації;

– суспільство і держава – захищеність їх законних інтересів в інформаційній сфері;

– інформаційні ресурси та інформаційна інфраструктура – їх цілісність, доступність та захищеність.

Суб’єктами системи забезпечення інформаційної безпеки України є:

– Президент України, Верховна Рада України (далі – ВРУ), Кабінет Міністрів України (далі – КМУ), Міністерство інформаційної політики України, Рада національної безпеки і оборони України (далі – РНБО), Державний комітет телебачення і радіомовлення України, Державна служба спеціального зв'язку та захисту інформації України, визначені законодавством центральні органи виконавчої влади, державні адміністрації та органи місцевого самоврядування, прокуратура України та інші органи

охорони правопорядку, судові органи, які віднесені до суб'єктів забезпечення національної безпеки України;

– Служба безпеки України (далі – СБУ), Служба зовнішньої розвідки України, розвідувальний орган Міністерства оборони України, Державна прикордонна служба України, Збройні Сили України (далі – ЗСУ) та інші військові формування, утворені відповідно до законів України;

– державні і недержавні засоби масової інформації, підприємства, заклади, установи та організації різних форм власності, що здійснюють інформаційну діяльність;

– наукові установи і навчальні заклади України, які здійснюють наукові дослідження та підготовку фахівців за різними напрямами інформаційної діяльності, в сфері інформаційного права та інформаційної безпеки.

Розглянемо функції деяких з них.

Перший рівень – загальнодержавний. Президент України як глава держави, гарант державного суверенітету і територіальної цілісності України, додержання Конституції України, прав і свобод людини і громадянина, Верховний Головнокомандувач Збройних Сил України та Голова РНБО, здійснює загальну координацію з питань забезпечення інформаційної безпеки України.

ВРУ в межах повноважень, визначених Конституцією України, формує державну політику і законодавчу базу в інформаційній сфері та здійснює контроль за практичним застосуванням законодавчих актів у діяльності суб'єктів забезпечення інформаційної безпеки та їх посадових осіб.

КМУ як вищий орган у системі органів виконавчої влади в межах повноважень, визначених Конституцією і законами України реалізує державну політику в інформаційній сфері, координує і контролює діяльність центральних органів виконавчої влади щодо забезпечення інформаційної безпеки України.

Міністерство інформаційної політики України забезпечує реалізацію єдиної державної політики, здійснює державне регулювання з питань інформаційної безпеки та функціональну координацію діяльності державних органів щодо забезпечення інформаційної безпеки.

РНБО проводить роботу з виявлення та оцінки загроз інформаційній безпеці України, оперативно розробляє проекти рішень Президента України по недопущенню таких загроз, розробляє пропозиції в сфері забезпечення інформаційної безпеки України, а також пропозиції по уточненню окремих положень нормативно-правових актів.

Враховуючи порядок організації роботи РНБО України та притаманні їй переважно координаційні і контрольні функції, для забезпечення її роботи необхідне її якісне функціонування суб'єктів забезпечення національної безпеки, діяльність яких координується.

До другого рівня системи забезпечення інформаційної безпеки ми пропонуємо віднести центральні й місцеві органи виконавчої влади та інші державні органи, що виконують спеціальні повноваження.

Однією з основних складових системи забезпечення національної безпеки в механізмі держави є СБУ, діяльність якої регулюється Законом України «Про Службу безпеки України» [64]. Відповідно до статті першого цього Закону, СБУ, це державний правоохоронний орган спеціального призначення, який забезпечує державну безпеку України.

Серед завдань, покладених на СБУ ст.2 цього Закону, можна виділити забезпечення охорони державної таємниці. СБУ відповідно до своїх основних завдань зобов'язана: здійснювати інформаційно-аналітичну роботу, здійснювати контррозвідувальну діяльність, брати участь у розробці і здійсненні заходів щодо забезпечення охорони державної таємниці та конфіденційної інформації, що є власністю держави, сприяти у порядку, передбаченому законодавством, підприємствам, установам, організаціям та підприємцям у збереженні комерційної таємниці, розголошення якої може завдати шкоди життєво важливим інтересам України [64].

Завдання щодо забезпечення інформаційної безпеки також покладено і на Службу зовнішньої розвідки України, діяльність якої регулюється Законом України «Про Службу зовнішньої розвідки України» [65], яким на зазначений орган покладається:

– добування, аналітична обробка та надання розвідувальної інформації споживачам;

– здійснення спеціальних заходів впливу, спрямованих на підтримку національних інтересів і державної політики України в інформаційній сфері;

– участь у забезпеченні безпечного функціонування установ України за кордоном, безпеки співробітників цих установ та членів їх сімей у країні перебування, а також відряджених за кордон громадян України, які обізнані з відомостями, що становлять державну таємницю;

– участь у боротьбі з незаконною торгівлею технологією виготовлення зброї.

Зазначені завдання здійснюються в порядку, визначеному Законом України «Про розвідувальну діяльність» [63], який визначає правові основи організації і діяльності державних органів, які здійснюють розвідувальну діяльність з метою захисту національних інтересів України від зовнішніх загроз.

Згідно цього Закону розвідувальна діяльність – діяльність, яка здійснюється спеціальними засобами і методами з метою забезпечення визначених законом органів державної влади розвідувальною інформацією, сприяння реалізації та захисту національних інтересів, протидії за межами України зовнішнім загрозам національній безпеці України.

Здійснення розвідувальної діяльності у інформаційній сфері покладається на Службу зовнішньої розвідки України та розвідувальний орган Міністерства оборони України.

Розвідувальна діяльність є одним із найважливіших засобів забезпечення інформаційної безпеки, спрямованим на здобуття розвідувальної інформації – відомостей про події і обставини, що стосуються

національної безпеки і оборони, які неможливо отримати офіційним шляхом, на підставі яких можна провадити прогнозування та планування заходів забезпечення інформаційної безпеки.

Найбільшу кількість функцій щодо забезпечення інформаційної безпеки покладено на Державну спеціальну службу зв'язку та захисту інформації України (далі – ДССЗЗІ), діяльність якої регулюється Законом України «Про Державну службу спеціального зв'язку та захисту інформації України» [47].

Відповідно до цього закону, ДССЗЗІ є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації.

Завдання ДССЗЗІ можна умовно розбити на такі групи:

– забезпечення функціонування державних систем спеціального зв'язку: державної системи урядового зв'язку та Національної системи конфіденційного зв'язку;

– захист державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

– криптографічний та технічних інформації.

Таким чином, як вбачається з завдань та функцій, покладених Законом на ДССЗЗІ, її діяльність зосереджена по-перше на технічних складових інформаційної безпеки: технічний та криптографічний захист інформації (конфіденційної і таємної), яка перебуває у власності держави, захист державних інформаційних ресурсів в інформаційно-телекомунікаційних мережах, забезпечення функціонування державних систем спеціального зв'язку: державної системи урядового зв'язку та Національної системи конфіденційного зв'язку, по-друге її діяльність переважно спрямована на захист держави, як суб'єкта інформаційних відносин, залишаючи поза

увагою таких суб'єктів інформаційних відносин, як суспільство, людина та громадянин. Такі акценти діяльності ДССЗЗІ є очевидними з огляду на те, що ДССЗЗІ є, в першу чергу, суб'єктом забезпечення національної безпеки, головним об'єктом якої є інтереси держави в інформаційній сфері.

Повноваження щодо захисту суспільної моралі покладаються також на Національну раду України з питань телебачення і радіомовлення (далі – Національна рада). Відповідно до Закону України «Про Національну раду України з питань телебачення і радіомовлення» [58] Національна рада є конституційним, постійно діючим колегіальним органом, метою діяльності якого є нагляд за дотриманням законів України у сфері телерадіомовлення, а також здійснення регуляторних повноважень, передбачених законом.

Крім нагляду за додержанням законодавства щодо захисту суспільної моралі Національна рада здійснює інші функції, пов'язані із забезпеченням інформаційної безпеки шляхом здійснення нагляду та контролю за діяльністю телерадіоорганізацій, інформаційному просторі, зокрема Національна рада здійснює забезпечення і сприяння конкуренції у діяльності телерадіоорганізацій усіх форм власності відповідно до вимог законодавства, створення умов щодо недопущення усунення, обмеження чи спотворення конкуренції у телерадіоінформаційному просторі.

Відповідно до ч.4 ст.7 Закону України «Про телебачення та радіомовлення» [68] Національна рада є єдиним органом державного регулювання діяльності у сфері телебачення і радіомовлення незалежно від способу розповсюдження телерадіопрограм і передач, на який покладено функції щодо забезпечення інформаційної безпеки в телерадіоінформаційному просторі держави.

Водночас, ч.3 ст.7 цього Закону визначено, що забезпечення формування та реалізація державної політики у сфері телебачення і радіомовлення покладаються на центральний орган виконавчої влади. Таким органом є Державний комітет телебачення і радіомовлення України (далі – Держкомтелерадіо). Відповідно до Положення про Державний комітет

телебачення і радіомовлення України, затвердженого Указом Президента України від 07.05.2011 р. № 559/2011 [60], Держкомтелерадіо є головним у системі центральних органів виконавчої влади з формування та реалізації державної політики у сфері телебачення і радіомовлення, в інформаційній та видавничій сферах.

Виходячи з положення Держкомтелерадіо, він є головним в системі органів виконавчої влади в сфері забезпечення інформаційної безпеки, на який покладається, зокрема, формування державної інформаційної політики, розробка заходів щодо запобігання інформаційному впливу, який загрожує інформаційній безпеці держави, суспільства, особи, реалізація завдання щодо забезпечення інформаційної безпеки, розробка пропозицій щодо вдосконалення системи державного управління інформаційній сфері, при цьому на законодавчому рівні на Держкомтелерадіо завдань і функцій щодо забезпечення інформаційної безпеки не покладено, що значною мірою нівелює його статус в цьому питанні.

Центральні органи виконавчої влади забезпечують виконання законодавства України, рішень Президента України в сфері забезпечення інформаційної безпеки; у межах своєї компетенції розробляють нормативно-правові акти в цій сфері і представляють їх у встановленому порядку Президентові України та до КМУ.

Міжвідомчі та державні комісії, що створюються Президентом України та КМУ, вирішують відповідно до наданим їм повноваженням завдання забезпечення інформаційної безпеки України.

Органи місцевого самоврядування забезпечують дотримання законодавства України в сфері забезпечення інформаційної безпеки держави.

Органи внутрішніх справ виконують завдання попередження, припинення, розкриття та розслідування злочинів та інших правопорушень в інформаційній сфері, а органи судової влади здійснюють правосуддя за справами про злочини, пов'язані із зазіханням на законні інтереси людини,

суспільства і держави в інформаційній сфері і забезпечують судовий захист громадян та суспільних об'єднань.

Практично кожен з державних органів на різних рівнях виконує конкретні функції організаційного та практичного характеру у сфері інформаційної безпеки.

До третього рівня системи забезпечення інформаційної безпеки ми відносимо підприємства, установи й організації критично важливих інфраструктур, які функціонують на основі використання електронних, телекомунікаційних засобів та інформаційних технологій, виведення з ладу яких може призвести до тяжких наслідків для особи, суспільства, держави. Відповідно до світової практики, передусім США, до критично важливих інфраструктур відносять системи телекомунікацій і мережі зв’язку, енергетики і промислового виробництва, соціальної сфери, державного управління тощо. Це найактуальніша проблема сучасності, що переконливо підтверджено трагічним українським та японським досвідом, пов’язаним з експлуатацією атомних електростанцій, та іншими подіями і процесами у світі. При цьому доцільно звернути увагу на те, що основи безпечного функціонування об’єктів критично важливих інфраструктур формуються і забезпечуються, насамперед, на інформаційному рівні.

До четвертого рівня системи забезпечення інформаційної безпеки ми відносимо громадян та їх об’єднання, а також державні і приватні ЗМІ.

Громадяни України та їх об’єднання мають виконувати такі функції з питань забезпечення інформаційної безпеки:

– громадяни України привертають увагу суспільних і державних інституцій до небезпечних інформаційних явищ і процесів у різних сферах життєдіяльності країни; захищають власну інформаційну безпеку всіма законними способами й засобами;

– політичні і громадські організації здійснюють заходи захисту своїх прав і свобод, а також прав і свобод громадян і певних верств населення; захищають політичні, економічні, соціальні, інформаційні та інші інтереси; у

межах, визначених законом, здійснюють громадський контроль за забезпеченням законності в діяльності виконавчо-розпорядчих органів та для розгляду актуальних проблем у сфері забезпечення інформаційної безпеки ініціюють проведення загальних зборів громадян за місцем проживання;

– ЗМІ України відповідно до чинного законодавства забезпечують захист прав, свобод і законних інтересів усіх суб'єктів України та легітимно визначених національних інтересів.

Державні телерадіоорганізації та друковані ЗМІ здійснюють інформаційне забезпечення державної внутрішньої й зовнішньої політики, напрямів і програм соціально-економічного розвитку, державного будівництва й забезпечення національної безпеки України із залученням із цією метою політичних і державних діячів, учених і спеціалістів; заходи протидії та нейтралізації відповідно до чинного законодавства зовнішніх і внутрішніх негативних безпекогенних інформаційних впливів на Україну.

Приватні ЗМІ здійснюють взаємодію з органами державної влади й органами місцевого самоврядування з питань об'єктивного висвітлення їхньої діяльності щодо реалізації державної внутрішньої та зовнішньої політики, державного будівництва, захисту національних інтересів; звертають увагу органів державної влади й місцевого самоврядування на проблемні аспекти в їхній діяльності та піддають конструктивній критиці порушення чинного законодавства й прав, свобод і законних інтересів суб'єктів України.

Таким чином, формування й реалізація державної політики інформаційної безпеки має здійснюватися шляхом вдосконалення організаційно-функціональної системи, суттєвої оптимізації структури державних органів, чіткого визначення й розмежування їх повноважень, налагодження ефективної взаємодії, координації діяльності всіх суб'єктів та контролю за виконанням чинного законодавства.

РОЗДІЛ 2
ВИКЛИКИ ТА ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ

2.1 Аналіз загроз інформаційній безпеці держави

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.

Проаналізувавши праці науковців та експертів, можна виділити такі типи інформаційних загроз: політичні; економічні; суспільні; військові та науково-технічні [75].

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]

Розглядаючи проблему інформаційних загроз неможливо обминути поняття джерел загроз інформаційній безпеці. Експерти розрізняють внутрішні та зовнішні джерела загроз [32].

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]

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.

2.2 Інформаційна війна як форма ведення інформаційного протиборства

Національна безпека України опинилася нині перед викликами й загрозами інформаційного протиборства. Надзвичайної гостроти для України набуває стратегія національної безпеки держави, коли недостатній динамізм і мобільність підготовки до інформаційних війн та відсутність належної уваги до питань інформаційної безпеки призводять до небажаних і навіть драматичних зрушень. Звідси зрозуміло, чому розвинені країни надають виняткової уваги питанням інформаційної складової державної безпеки.

Інформаційні війни (далі – ІВ) є формами ведення інформаційного протиборства (далі – ІП) (державами, неурядовими, економічними або іншими структурами), який передбачає проведення комплексу заходів з нанесення шкоди інформаційній сфері конфронтуючої сторони і захисту власної інформаційної безпеки [45].

Види ІП: інформаційно-технічне й інформаційно-психологічне. Головними об'єктами впливу інформаційно-технічного протиборства є системи телекомунікацій і зв'язку, радіоелектронні засоби тощо. Об'єктом інформаційно-психологічного впливу залишаються свідомість і психіка населення й особового складу збройних сил, спецслужб противника та системи формування суспільної думки і прийняття стратегічних рішень.[20]

ІВ передбачає цілеспрямовану розробку та поширення спеціальної актуальної інформації, здатної зробити безпосередній або непрямий вплив на суспільну свідомість, психологію і поведінку населення, військовослужбовців. При цьому інформація психологічного і пропагандистського типу може бути не тільки усного, друкованого, письмового, аудіо та візуального походження, а й екстрасенсорного, телепатичного й іншого, розрахована насамперед на підсвідомість реципієнта впливу.

ІП ведеться на трьох рівнях: стратегічному, оперативному та тактичному. На стратегічному рівні ІП планують і координують найвищі органи державної влади. На оперативному та тактичному рівнях ця діяльність проводиться силами і засобами збройних сил, спецслужб, а також суспільно-політичних інститутів держави.

За словами автора книги Г. Почепцова «Сучасні інформаційні війни», інформаційні війна веде до наступного кроку – війни фізичної. За його визначенням сучасні інформаційні війни – це квазі-агресивний інструментарій мирного життя, а не лише збройного конфлікту між державами. І постійний розвиток інформаційного простору продукує нові

можливості для застосування цього інструментарію. Поява інтернету здійняла його до нових висот.

Інформаційні війна – це слово з журналістського лексикону. Військові використовують термін інформаційна операція.

Завдання інформаційної війни:

- створення атмосфери бездуховності, негативного ставлення до культури та історичної спадщини у суспільстві конкурента чи ворога;

- маніпулювання громадською думкою і політичною орієнтацією населення держави з метою створення політичного напруження та стану, близького до хаосу;

– дестабілізація політичних відносин між партіями, об'єднаннями та рухами з метою розпалення конфліктів, стимулювання недовіри, підозри, загострення ворожнечі, боротьби за владу;

– провокування, застосування репресивних дій з боку влади щодо опозиції;

– зниження рівня інформаційного забезпечення органів влади та управління, інспірація помилкових управлінських рішень;

– введення населення в оману щодо роботи державних органів влади, підрив їх авторитету, дискредитація їхніх дій;

– провокування соціальних, політичних, національно-етнічних і релігійно-конфесійних зіткнень;

– ініціювання страйків, масових заворушень, інших акцій протесту та непокори;

– підрив міжнародного авторитету держави, її співпраці з іншими державами;

– дискредитація фактів історичної, національної самобутності народу; зміна системи цінностей, які визначають спосіб життя і світогляд людей;

– формування передумов до економічної, духовної чи військової поразки, втрати волі до боротьби та перемоги;

– підрив морального духу населення і, як наслідок, зниження обороноздатності та бойового потенціалу;

– нанесення шкоди безпеці інформаційно-технічної інфраструктури держави.

Основне завдання ІВ (між державами) – здійснення безпосереднього негативного руйнівного впливу на сукупну політичну могутність держави шляхом послаблення її реальних і потенційних можливостей щодо забезпечення власної безпеки, створення труднощів у внутрішньому розвитку й проведенні активної зовнішньої діяльності, а також, завдання шкоди політичному іміджу, тобто ослаблення правлячої еліти чи навіть сприяння усуненню останньої від влади.

Вперше, термін «інформаційна війна» з'явився в середині 80-х років XX ст., коли, після закінчення «Холодної війни», перед Збройними силами США постали нові завдання. Це був результатом роботи групи американських військових теоретиків у складі: Г. Е. Экклза, Г. Г. Саммерза та ін.

Хоча ще у стародавньому Китаї декілька тисяч років тому було систематизовано стратегії, які застосовувалися в політиці та військовій діяльності. Такі стратегії в сучасній літературі отримали назву «стратагеми» (від грецького зігаїедегпа, що означало військові хитрощі). Застосовуючи її, можна було ввести противника в оману.

Одним з найдавніших історичних джерел, де йдеться про застосування прийомів інформаційного протиборства, можна вважати «Трактат про військове мистецтво» китайського полководця Суньцзи (VI ст. до н. е.). У ньому наводиться опис і яскраві приклади застосування прийомів і методів психологічного впливу, які давали змогу досягати перемоги без битв або з мінімальними втратами. «У всякій війні, як правило, найкраща політика зводиться до захоплення держави цілісною... Війна - це шлях омани... Здобути сотню перемог у боях - це не край мистецтва. Підкорити суперника без бою - ось вінець мистецтва».

Особливо показовою є діяльність наполеонівського пропагандистського апарату. Наполеон був одним із перших можновладців Європи, хто по-справжньому оцінив роль преси у формуванні громадської думки. Широковідомим є його висловлювання: «Чотири газети зможуть заподіяти ворогові більше шкоди, ніж стотисячна армія» [14].

Вдосконаленню прийомів інформаційної війни, зокрема терористичних операцій як їх різновиду, сприяли певні зміни, що відбулися в житті суспільства, пов'язані зі зміною статусу преси та започаткування нових напрямків у науковому пізнанні.

Характерною рисою інформаційно-пропагандистської діяльності в європейських країнах періоду Першої світової війни стало те, що вона набула централізованого характеру, для чого були створені спеціальні органи і установи, які утримувалися коштом урядових бюджетів. Війна велася не лише зброєю, здатною фізично уражати супротивників та їх матеріальну базу, а й такою, що ранила душі, руйнувала боєздатність ворожих військ ще до вступу в бій.

Англійці першими високо оцінили руйнівну міць психологічної зброї. Поширення всіляких листівок і публікацій підбурювальних за змістом, розповсюдження панікерських чуток, закликів здаватися в полон - усе це деморалізувало противника та визнавалося важливою складовою у справі підготовки до наступальних операцій. Визнання пропагандистського напрямку одним із пріоритетних викликало зміни й у самому апараті пропаганди. Так, на початку Другої світової війни, в Англії існувало лише бюро воєнної пропаганди при Міністерстві закордонних справ, а наприкінці війни вже було створено Міністерство інформації та Департамент пропаганди на противника.

Перелом в ІПВ відбувся у міжвоєнний період (1918-1939 рр.) і був тісно пов'язаний зі становленням двох потужних тоталітарних держав: СРСР і нацистського Третього Рейху.

Зіткнувшись у жорстокому військовому конфлікті, обидві ворогуючі сторони активно застосовували різні методи психологічної війни. Але ці дії не дуже відрізнялися за формою і методами, які були продемонстровані в Першій світовій війні, відмінність полягала лише в масштабності.

Закінчення Другої світової війни знаменує завершення II періоду розвитку інформаційного протиборства. Якщо другий період розвитку форм і методів інформаційного протиборства відзначається зростанням значення останнього як ефективного допоміжного засобу у вирішенні питань військового, політичного чи економічного характеру, то особливість третього полягає в оновленні такого значення: з допоміжного інформаційна боротьба перетворюється на один із основних засобів досягнення успіху у зазначених сферах. Відповідно, різняться і стулені наукового та матеріально-технічного забезпечення у цьому виді боротьби. Для другого періоду характерними є постійна технізація інформаційних процесів у суспільстві та розгортання наукових досліджень останніх з метою теоретизації таких знань.

З кінця 1940 до середини 1980-х рр., в епоху так званої холодної війни, протистояння двох супердержав - СРСР і США - спричинило подальше вдосконалення форм і методів пропаганди та психологічної війни.

За цей же період у світі відбулося чимало локальних воєн і військових конфліктів (війни в Кореї, В'єтнамі, Афганістані, військові операції проти Іраку), де теж активно застосовувалася інформаційна зброя.

У 1970-х рр. у світі відбулася інформаційна революція пов'язана з винаходом мікропроцесорної технології і появою персонального комп'ютера. Бурхливий розвиток комп'ютерної техніки й інформаційних технологій став поштовхом до розвитку суспільства, яке одержало назву «інформаційного». В Інформаційному суспільстві продукується та споживається інтелект, знання, завдяки чому зростає частка розумової праці. Матеріальною і технологічною базою Інформаційного суспільства є різного роду системи на базі комп'ютерної техніки та комп'ютерних мереж, Інформаційних технологій, телекомунікацій та зв'язку.

Отже, геополітичний авторитет держави на міжнародній арені та її можливість впливати на світові події нині залежить не тільки від економічної і військової могутності. Усе більшого значення набувають не силові, а інформаційні фактори: можливість ефективно впливати на інтелектуальний потенціал інших країн, поширювати І впроваджувати в суспільну свідомість відповідні духовні й ідейні цінності, трансформувати і підривати традиційні підвалини націй і народів. У військовій справі відбувається перехід від стратегії ядерного стримування до високоточної контрсилової інформаційної зброї, що не загрожує людству глобальною катастрофою.

Низка країн, передусім США, починаючи з 1990-х р. активізують вивчення і вирішення проблем, пов'язаних з протиборством в інформаційній сфері та інформаційною війною. Таким чином, інформаційна війна перетворилась з футурологічної примари на реальну військову дисципліну, яку вивчають і розробляють у відповідних академічних закладах.

З новим витком історії воєн особливе місце займає широкомасштабна ІВ. У ході війни в Перській затоці з боку США мало місце масове застосування нової високотехнологічної інформаційно-вогневої зброї і засобів радіоелектронної боротьби. Під інформаційно-вогневою зброєю розуміється така зброя, у якій для доставки боєприпасів до цілі використовується інформаційний канал. Тим самим війна стає «над технологічною», де вирішальне значення в завоюванні перемоги належить системам інформатизації та автоматизації.

Розглянемо об'єкти посягань ІВ. Головний об'єкт, на якому концентрується безпосередній інформаційний деструктивний вплив у межах заходів ІВ, – громадська думка та свідомість окремої людини.

Об'єкти посягань ІВ поділяються на:

- загальні об'єкти;
- спеціальні об'єкти;
- об'єкти розвідувальних спрямувань [19].

До загальних об'єктів можна віднести правопорядок, нормальне функціонування органів влади та управління, мобілізаційну готовність і боєздатність збройних сил, органів безпеки та правоохоронних структур, налагоджені зовнішньополітичні зв'язки, міжнародний авторитет держави.

До спеціальних об'єктів – можна віднести суспільство загалом та окремі його верстви, прошарки, групи осіб, окремих їх представників.

До категорії об'єктів розвідувальних спрямувань ІВ належать:

– засоби масової інформації та комунікації, інформаційні агентства, незалежні аналітичні центри та дослідні установи, які постійно займаються висвітленням ситуацій, що виникають у державі, регіоні та світі, здійснюють аналіз і прогнозування можливого перебігу подій, тенденцій у різних суспільно-політичних, геополітичних, геоекономічних та геостратегічних процесах;

– відповідні підрозділи міністерств, відомств чи інших органів державного управління, на які покладається обов'язок налагодження і підтримання зв'язків із громадськістю та інформування останньої щодо діяльності зазначених установ, а також інші об'єднання громадян, які виступають від імені своїх членів. Такими структурами є політичні партії та блоки, громадські організації, профспілки тощо, які певним чином впливають на політичні процеси у державі.

Отже, основними об'єктами деструктивного інформаційного впливу є:

– ідеологічно-психологічне середовище суспільства, пов'язане з використанням інформації, інформаційних ресурсів та інформаційної інфраструктури для здійснення впливу на психіку й поведінку людей;

– інформаційні ресурси, які розкривають духовні, культурні, історичні, національні цінності, традиції, надбання держави, нації в різних сферах життя суспільства;

– інформаційна інфраструктура, тобто абсолютно всі проміжні ланки між інформацією та людиною;

– система формування суспільної свідомості (світогляд, політичні погляди, загальноприйняті правила поведінки тощо);

– система формування громадської думки;

– система розроблення та прийняття політичних рішень;

– свідомість та поведінка людини.

Попри все, головним об'єктом ураження залишається людина, прихований вплив на яку здійснюється через її нервову систему та психіку, здебільшого на підсвідомому рівні. Цілеспрямований інформаційний вплив на населення передбачає пануюче становище суб'єкта ІВ у всіх сферах життєдіяльності іншої держави: економічній, політичній, психологічній, релігійній, науково-технічній, мистецькій, а також міжнаціональних і міжнародних зв'язків. Зростання ефективності заходів безпосереднього підриву, зокрема ІВ, досягається за рахунок встановлення контролю над інформаційним простором іноземної країни, точності та цілеспрямованості таких акцій з урахуванням необхідного обсягу та рівня достовірності інформації, що доводиться, ступеня диференціації населення за системами матеріальних і духовних цінностей, здатності адекватно сприймати відомості та реагувати на них, а також політичної, економічної, етнорелігійної та іншої ситуації в державі й регіоні.

Нині є величезна кількість різноманітних технологій здійснення негативного впливу на духовно-ідеологічну сферу життєдіяльності суспільства. їх можуть застосовувати спецслужби іноземних держав, терористичні організації, політизовані радикальні угруповання, кримінальні структури, транснаціональні корпорації та інші формальні й неформальні учасники сучасних міжнародно-правових відносин.

Інститут національно-стратегічних досліджень США та деякі західні експерти і вчені виділяють сім складових елементів ІВ :

1) Стратегія і тактика нейтралізації органів управління противника (командна війна).

2) Розвідувальна війна.

3) Електронна війна.

4) Психологічна війна.

5) Комп'ютерна війна.

6) ІВ в економічній сфері.

7) Інформаційний тероризм.

Основними компонентами ІВ у військовій сфері прийнято вважати:

– розвідку;

– контррозвідку (насамперед протидію розвідці противника, включаючи маскування і дезінформацію);

– радіоелектронну боротьбу;

– автоматизоване управління військами і зброєю;

– з'ясування державної приналежності військових об'єктів, їх ідентифікацію;

– навігаційне забезпечення своїх військ (сил) і засобів;

– морально-психологічне забезпечення дій власних військ (сил), психологічну боротьбу (придушення) противника.

Інформаційний вплив на особистість, суспільство і державу під час ІВ здійснюється за допомогою інформаційної зброї (далі – ІЗ). Теоретики відносять до цього виду зброї широкий спектр заходів і засобів інформаційного впливу на противника – від дезінформації й пропаганди до засобів радіоелектронної боротьби.

Наведемо деякі найуживаніші в публікаціях визначення інформації зброї:

– комплекс специфічних програмно-інформаційних засобів, створених для ураження інформаційного ресурсу противника;

– засоби знищення, викривлення або викрадення інформаційних масивів, добування з них потрібної інформації після подолання систем захисту, обмеження або заборони доступу до них незаконних користувачів, дезорганізації роботи технічних засобів;

– засоби подолання систем захисту, засоби дезорганізації роботи технічних засобів та комп'ютерних систем.

У деяких джерелах сутність ІЗ визначається через розвиток інформаційних технологій, які забезпечують можливість системам (індивідам, суспільним або політичним угрупованням, державам) з більш високим рівнем інформатизації керувати системами з дещо нижчим рівнем інформатизації, спрямовуючи їх діяльність у своїх інтересах під постійним інформаційним контролем.

Інформаційна зброя у ширшому розумінні – це комплекс програмних і технічних засобів, призначених для контролю інформаційних ресурсів об'єкта впливу і втручання в роботу його інформаційних систем. Інформаційна зброя можливо класифікувати за методами впливу на інформацію, інформаційні процеси та інформаційні системи противника. Цей вплив може бути фізичним, інформаційним, програмно-технічних або радіоелектронним. Інформаційні методи впливу реалізуються за допомогою всієї сукупності засобів масової інформації та глобальних інформаційних мереж типу «Інтернет», станціями голосової дезінформації. Так як основним елементом інформаційної інфраструктури є люди, мотивація діяльності яких базується на їх фізіологічних, соціальних та інформаційних потребах, то правильно розраховане застосування так званих інформаційно-психологічних методів впливу надає прямий вплив на рівень безпеки держави [11].

За ще одним визначенням інформаційна зброя – комплекс технічних та інших засобів, методів і технологій встановлення контролю над інформаційними ресурсами потенційного супротивника, втручання у роботу його систем управління та інформаційних мереж, систем зв’язку тощо з метою виведення їх з ладу, спотворення чи спрямоване введення спеціальної інформації, поширення вигідної інформації та дезінформації у системі формування громадської думки і ухвалення рішень тощо [16].

Найбільш лаконічним та точним, на наш погляд, є таке визначення: інформаційна зброя – це різновид зброї, головними елементами якої є

інформація, інформаційні технології (зокрема технології інформаційного впливу), інформаційні процеси та технічні засоби, що застосовуються.

Інформаційна операція – цілісна подія (акт) інформаційної війни, яка відбувається із застосуванням інформаційної зброї шляхом використання інформаційної атаки або захисту для забезпечення реалізації інтересів учасника інформаційного протистояння. Інформаційні операції мають як наступальний, так і оборонний характер [76].

Інформаційний захист – це комплекс оборонних заходів учасника інформаційної війни із застосуванням інформаційної зброї з метою протидії інформаційній атаці та виникненню загрози його інформаційній безпеці.

На сьогодні за допомогою інформаційної зброї протиборчі сторони здатні вирішувати стратегічні завдання, зокрема:

– завдавати серйозної шкоди національним інтересам, підривати основи державності;

– дискредитувати органи влади й ускладнювати прийняття ними важливих рішень, паралізувати управління країною в кризових ситуаціях;

– створювати атмосферу напруженості в суспільстві, провокувати соціальні, політичні, національні і релігійні безладдя, ініціювати страйки, масові заворушення й інші акції економічного протесту;

– створювати атмосферу бездуховності й аморальності, негативного ставлення до культурного спадку; дезорганізовувати техносферу, економіку, систему комунікацій;

– підривати міжнародний авторитет держави, перешкоджати її співробітництву з іншими країнами.

В оборонній сфері об'єктами ІЗ є:

– інформаційні ресурси стратегічного управління, науково-дослідних підрозділів, військово-промислового комплексу,

– системи зв'язку та управління військами і зброєю, їх інформаційне забезпечення,

– інформаційні інфраструктури, зокрема центри обробки й аналізу інформації штабів, пункти управління, вузли та лінії зв'язку силових структур,

– морально-психологічний стан військ.

РОЗДІЛ 3
НАПРЯМКИ ФОРМУВАННЯ МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

3.1 Визначення складових моделі безпеки інформаційної інфраструктури держави

Діяльність із забезпечення інформаційної безпеки здійснюється за допомогою різних способів, засобів і прийомів, які у своїй органічній сукупності складають методи. Сукупність означених інструментів формують модель, яка вже виступає у ролі комплексного механізму безпеки інформаційної інфраструктури держави. З метою побудови такої моделі визначимо основні методи забезпечення інформаційної безпеки.

Метод передбачає певну послідовність дій на підставі конкретного плану. Методи можуть значно змінюватися і варіюватися в залежності від типу діяльності, в якій вони використовуються, а також сфери застосування [72].

По-перше, пропонуємо спочатку користуватись методами аналізу стану інформаційної безпеки – це методи опису та класифікації. Для здійснення ефективного захисту інформаційного середовища України слід, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів по здійсненню управління ними.

Розповсюдженими методами аналізу стану інформаційної безпеки є методи дослідження причинних зв’язків. За допомогою цих методів потрібно виявити причинні зв’язки між загрозами, ризиками, викликами та небезпеками; також здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи щодо їх нейтралізації та протидії їм.

У числі даних методів причинних зв’язків пропонуємо використовувати такі: метод схожості, метод відмінності, метод сполучення схожості і відмінності, метод змін, що супроводжують, метод залишків.

Вибір методів аналізу стану інформаційної безпеки залежить від конкретного рівня і сфери організації захисту та протидії. У залежності від загрози уможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів протидії. Що стосується сфери інформаційної безпеки, то у ній, зазвичай, виділяють: фізичний, програмно-технічний, управлінський, технологічний, рівень користувача, мережний, процедурний. Розглянемо дещо детальніше кожний з цих рівнів.

На фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються, а також управлінських технологій. На програмно-технічному рівні здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності.

На управлінському рівні здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях управління з боку системи інформаційної безпеки держави.

На технологічному рівні здійснюється реалізації стратегії інформаційної безпеки держави шляхом застосування комплексу сучасних автоматизованих інформаційних технологій. На рівні користувача реалізація стратегії інформаційної безпеки держави спрямована на зменшення рефлексивного впливу на державне інформаційне середовище.

На рівні інформаційно-телекомунікаційних мереж ця політика реалізується у форматі координації дій суб’єктів системи інформаційної безпеки, які пов’язані між собою однією метою.

На процедурному рівні вживаються заходи, що реалізуються суб’єктами. Серед них можна виділити такі групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності,

реагування на порушення режиму безпеки, планування відновлювальних робіт.

Можна виокремити декілька типів методів забезпечення інформаційної безпеки:

– однорівневі методи будуються на підставі одного принципу управління інформаційною безпекою;

– багаторівневі методи будуються на основі декількох принципів управління інформаційною безпекою, кожен з яких слугує вирішенню окремого завдання. При цьому часткові технології не пов’язані між собою і спрямовані лише на конкретні чинники інформаційних загроз;

– комплексні методи – багаторівневі технології, які об’єднані до єдиної системи координуючими функціями на організаційному рівні з метою забезпечення інформаційної безпеки, виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв’язок або генеруються з єдиного інформаційного центру інформаційного впливу;

– інтегровані високоінтелектуальні методи – багаторівневі, багатокомпонентні технології, які побудовані на підставі могутніх автоматизованих інтелектуальних засобів із організаційним управлінням [72].

Загальні методи забезпечення інформаційної безпеки активно використовуються на будь-якій стадії управління загрозами. До таких стадій належать:

– прийняття рішення з визначення типу та змісту інформаційної загрози і складу суб’єктів, які ведуть протидію;

– ухвалення загальної стратегії і алгоритму дій адекватного сприйняття загрози;

– виділення необхідних ресурсів, достатніх для реалізації протидії інформаційним загрозам і збереження сталого розвитку інформаційних ресурсів держави;

– трансформації результатів оцінки ризиків у відповідну стратегію інформаційної безпеки.

Вельми важливим є застосування аналітичних методів пізнання і дослідження стану професійної свідомості у сфері інформаційної безпеки. Наприклад, усвідомлення важливості забезпечення інформаційної безпеки на рівні носія інформації, структурного підрозділу і державного органу в цілому заважає розповсюджена думка про те, що захист інформації і криптографія одне й те ж саме. Водночас таке розуміння є наслідком використання застарілих підходів до інформаційної безпеки, коли інформаційна безпеки лише ототожнюються із захистом інформації шляхом її шифрування.

Нині важливою умовою забезпечення інформаційної безпеки є не стільки секретність, конфіденційність інформації, скільки її доступність, цілісність, захист від загроз. Отже, система має відповідно реагувати та гарантувати ефективну діяльність у цьому напрямі. Іншим завданням захисту є забезпечення незмінності інформації під час її зберігання або передавання, тобто забезпечення її цілісності.

Таким чином, конфіденційність інформації, яка забезпечується за допомогою криптографічних методів не є головною вимогою при проектуванні систем захисту інформації державних органів. Виконання процедур криптокодування і декодування може уповільнити передачу даних та зменшити доступ до них, через те, що співробітник буде позбавлений можливості своєчасного та швидкого доступу до цих даних та інформації, через функціонування механізму захисту. Саме тому, забезпечення конфіденційності інформації має відповідати можливості доступу до неї.

Таким чином, управління в сфері інформаційної безпеки має здійснюватися на підставі принципу доступності, конфіденційності та цілісності інформації.

Основним методом аналізу інформаційних ризиків є кількісний та якісний аналіз, факторний аналіз та інші. Мета якісної оцінки ризиків – ранжувати інформаційні загрози та небезпеки за різними критеріями, система яких дозволить сформувати ефективну протидію їм.

Важливим методом забезпечення інформаційної безпеки є також метод критичних сценаріїв. У зазначених сценаріях аналізуються ситуації, коли противник паралізує роботу органу управління і відповідно знижує здатність підрозділів виконувати завдання за призначенням.

Також можна зазначити на метод моделювання, за допомогою якого можна проводити навчання з інформаційної безпеки. Серед методів забезпечення інформаційної безпеки важливе значення має метод дихотомії. Для протидії загрозам інформаційній безпеці потрібно вживати необхідні заходи як в напрямку надання певного впливу на джерело загрози, так і в напрямку зниження вразливостей об’єкта безпеки. Відповідно можна виділити дві предметні області протидії. Одна з них утворюється сукупністю джерел загроз, а інша – сукупністю заходів із забезпечення інформаційної безпеки органу управління.

Вплив на джерело загрози інформаційної безпеки спрямований на зміну чинників та умов, здатних нанести шкоду об’єкту безпеки. Метою захисту є переконання противника у недоцільності здійснення загроз. Що стосується органів державного управління, то джерело загроз може бути спрямовано на створення умов, за яких здійснення небезпечних дій щодо об’єкта безпеки стає невигідним унаслідок виникнення небажаних наслідків або неможливим. Основним предметом за даного випадку є інформація, яка є у противника у вигляді відомостей, знань, оцінок. У свою чергу, інформація, що надходить від противника і становить собою загрозу, може бути піддана впливу для зміни її здатності завдавати шкоду, нейтралізації, трансформації або ліквідації її небезпечних властивостей. Вплив на інформаційну інфраструктуру важливий у тому випадку, коли загрозу може представляти середовище розповсюдження небезпечної інформації.

Методи впливу на інформаційну інфраструктуру можуть поділятися на інформаційні та неінформаційні. Інформаційні методи впливу орієнтовані на порушення формування інформаційно-телекомунікаційних систем, мереж зв’язку, засобів автоматизації управління, систем автоматизованої обробки

інформації, і таким чином, на попередження завдання шкоди предметам суспільних відносин, що захищаються.

На підставі викладеного можна визначити концептуальну модель безпеки інформаційної інфраструктури держави (рис. 3.1).

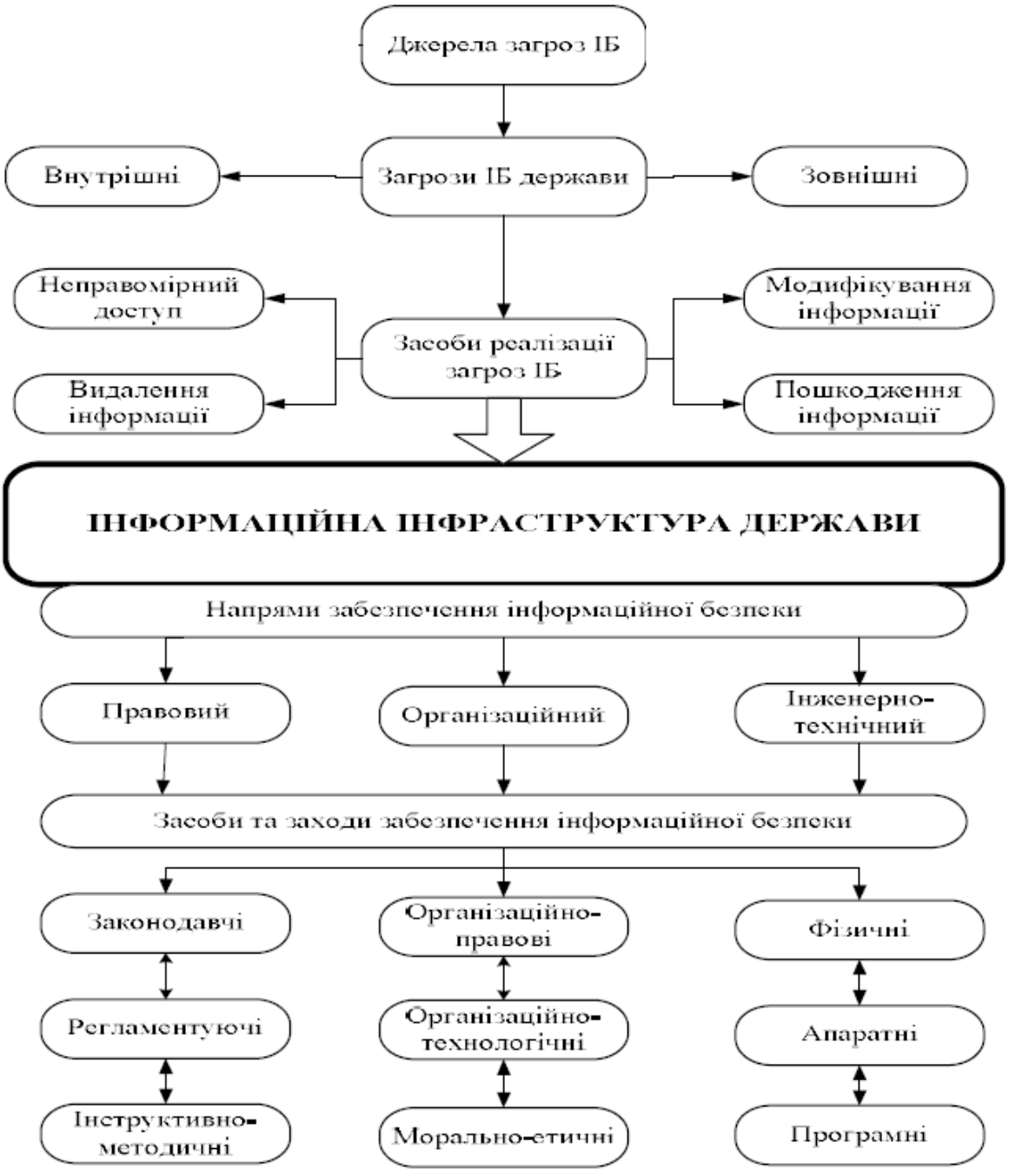

Рисунок 3.1– Модель безпеки інформаційної інфраструктури держави

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 Основні напрямки забезпечення інформаційної безпеки держави

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)
- державної безпеки.

Тому в процесі визначення характеру ризиків слід брати до уваги наступні елементи:

- концептуальне засади політичної безпеки, 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;
- визначення статусно-функціональних ролей, очікувань та міри відповідальності задіяних суб’єктів включно зі звітністю про події, які несуть потенційні загрози.

Процес забезпечення безперервності гарантування інформаційної безпеки можна поділити на шість основних стадій, які взаємопов’язані в рамках державної системи забезпечення інформаційної безпеки. Державна політика забезпечення інформаційної безпеки країни визначає основні напрямки діяльності органів державної влади у цій сфері (рис. 3.2.).

1) Розуміння безперервності функціонування системи забезпечення інформаційної безпеки держави. Ця фаза пов’язана з ідентифікацією критично важливих точок (об’єктів) захисту. Йдеться також про виокремлення основних внутрішніх та зовнішніх загроз, що можуть стати критичними для системи.

2) Стратегії забезпечення безперервності функціонування системи. В цьому випадку завдання зосереджуються на визначенні та доборі альтернативних рішень щодо відновлення системи з метою мінімізації загроз.

Пошук рішень балансує між собівартістю систем захисту та їхньою ефективністю.

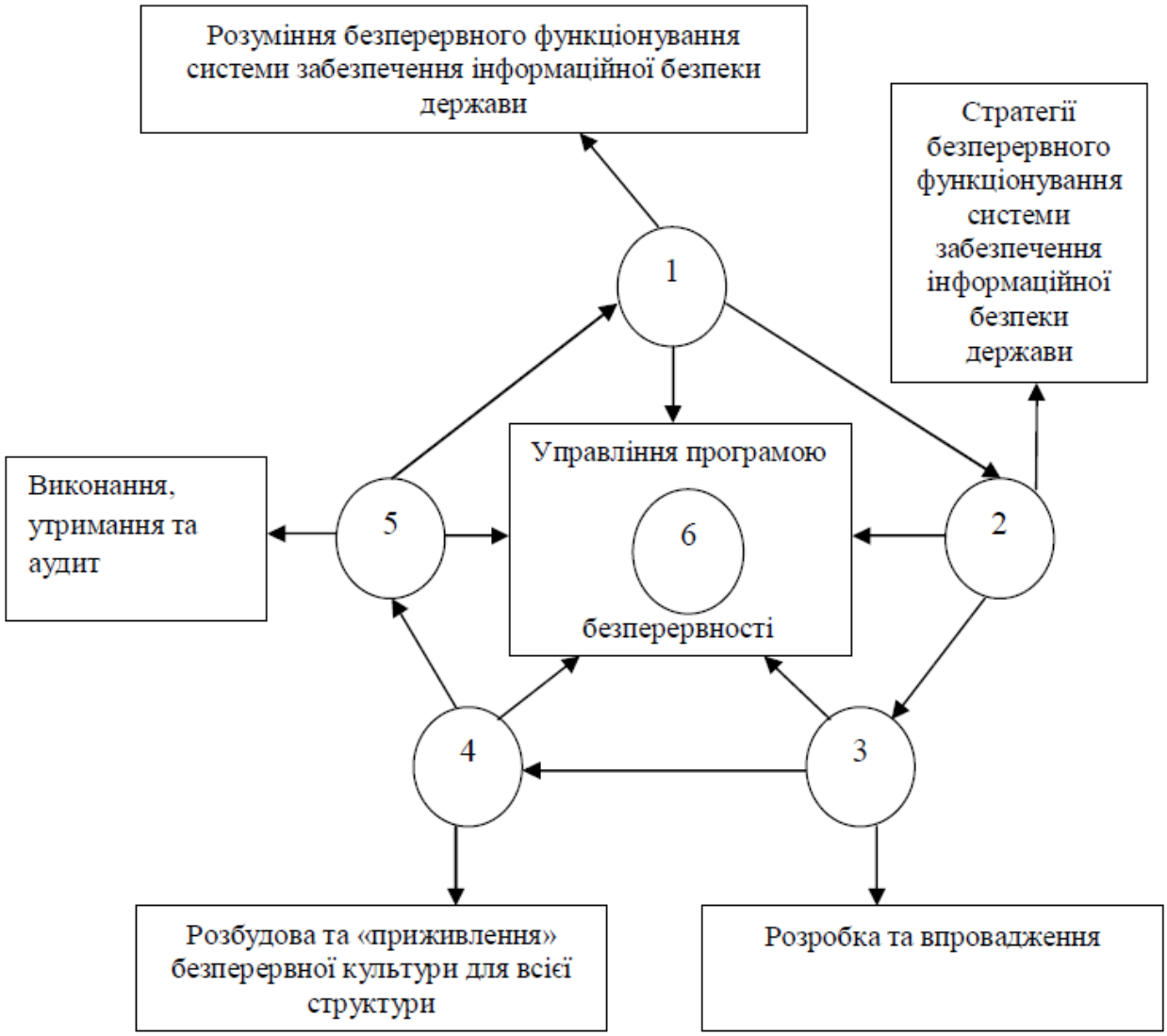

Рис. 3.2 – Процес забезпечення безперервності функціонування системи інформаційної безпеки держави

3) Розробка та впровадження. На цій фазі зусилля зосереджуються на структуруванні та документуванні Програми безперервності державного управління.

4) Розвиток культури інформаційної безпеки держави передбачає забезпечення процесу розробки державної інтегральної системи захисту інформації.

5) Виконання, підтримка та аудит процесу регулювання безперервного функціонування системи інформаційної безпеки держави за умов різноманітних криз та конфліктів.

6) Управління програмою інформаційної безпеки держави шляхом розподілу функцій, що передбачає відповідальність, страхування (гарантії) та керування у контексті реалізації загального плану безперервності функціонування системи забезпечення інформаційної безпеки держави.

Ці напрями обумовлені змістом національних інтересів держави, суспільства та особистості. По суті це є вірним, оскільки завданням заходів з інформаційної безпеки є мінімізація шкоди через неповноту, несвоєчасність або недостовірність інформації чи негативного інформаційного впливу через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації. Саме тому інформаційна безпека передбачає наявність певних державних інститутів і умов існування її суб'єктів, що встановлені міжнародним і вітчизняним законодавством.

З метою удосконалення правових основ державної інформаційної політики та політики забезпечення інформаційної безпеки України, а також управління з боку держави цими процесами, запропоновано організувати розробку й подання до Верховної Ради України законопроектів «Про національні інформаційні ресурси України», «Про засади державної інформаційної політики», «Про інформацію з обмеженим доступом», «Про захист інформації».

Для створення ефективної системи управління інформаційними ресурсами доцільно розробити і впровадити низку нормативно-правових документів, що регламентуватимуть:

– порядок і правила формування, поширення, використання і захисту інформаційних ресурсів, що не містять інформації з обмеженим доступом, окремо, що містять інформацію з обмеженим доступом;

– затвердження переліку документованої інформації, що в обов’язковому порядку надається для державної реєстрації (окремо як для відкритої інформації, так і з обмеженим доступом);

– порядок і правила державного обліку і реєстрації баз та банків даних.

Сучасна система вітчизняних інформаційних ресурсів є дуже складною за призначенням, засобами вираження, системою носіїв та ін. Відповідно забезпечення інформаційної безпеки потребує використання напрацювань різних аспектів теорії інформації, починаючи від теорій математичних, надто важливих для характеристик насамперед технічних показників розвитку інформаційних процесів. Вагомим для дослідження безпекових проблем є дослідження понятійного апарату інформаційної сфери, зокрема змісту поняття інформації, соціальної інформації, соціальних інформаційних баз, а також активізації глобальних процесів в інформаційній сфері.

Державна політика у сфері забезпечення інформаційної безпеки повинна бути відкритою і передбачати інформування суспільства про діяльність державних органів і суспільних інститутів у цій сфері з урахуванням обмежень, встановлених чинним законодавством України. Державна політика має виходити з принципу безумовної правової рівності всіх суб’єктів інформаційних відносин незалежно від їх політичного, соціального та економічного статусу, ґрунтуватися на обов’язковому забезпеченні прав громадян і організацій на вільне створення, пошук, отримання, накопичення, зберігання, перетворення і поширення інформації у будь-який законний спосіб.

Державна політика, спрямована на забезпечення інформаційної безпеки України, має ґрунтуватися на конструктивному поєднанні зусиль і діяльності держави, громадянського суспільства і людини за трьома головними напрямами:

– інформаційно-психологічному – щодо забезпечення конституційних прав і свобод людини і громадянина, створення

сприятливого психологічного клімату в національному інформаційному просторі задля утвердження загальнолюдських та національних моральних цінностей;

– технологічного розвитку – щодо розбудови та інноваційного оновлення національних інформаційних ресурсів, впровадження новітніх технологій створення, обробки та поширення інформації;

– захисту інформації – щодо забезпечення конфіденційності, цілісності та доступності інформації, у тому числі технічного захисту інформації в національних інформаційних ресурсах від кібернетичних атак.

ВИСНОВКИ

У магістерській роботі здійснено теоретичне узагальнення організаційно-правового забезпечення інформаційної безпеки держави. На підставі здійсненого дослідження зроблено певні висновки.

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 життєво важливим інтересам держави. Відтак забезпечення інформаційної безпеки належить до пріоритетних напрямів державної політики.

Події, що пов'язані зі збройною агресією проти України показали непідготовленість моделі інформаційної безпеки нашої держави до оперативного реагування на інформаційні загрози. Життя засвідчило, що законодавство у сфері національної безпеки і оборони не відповідає загрозам національній безпеці України в інформаційній сфері, та потребує переопрацювання 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.

Існує низка проблем у сфері інформаційної безпеки, не подолавши яких неможливо сформувати сучасну модель інформаційної безпеки держави. Перш за все це:

– недосконалість галузевої нормативно-правової бази;

– недостатня розвиненість національної інформаційно-комунікаційної інфраструктури;

– гострий брак системної, комплексної та ефективної державної політики щодо забезпечення інформаційної безпеки, громіздка й непродуктивна система державного управління та регулювання даної сферою.

– відсутність механізмів здійснення інформаційно-психологічних операцій, системи активного кіберзахисту інформаційного простору країни, якій призваний діяти не тільки в цілях захисту, а й як простір асиметричної відповіді агресору;

– концентрація загальнодержавних ЗМІ в руках олігархічних, фінансово-промислових кіл;

– спроби дезінформації громадян України, використання проти них інформаційно-психологічних маніпулятивних технологій.

Аналіз внутрішніх та зовнішніх загрози інформаційній безпеці держави дозволив встановити, що у наслідок існуючих проблем у зазначеній сфері бути завдано серйозної шкоди конституційним правам і свободам окремих громадян, життєво 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.

Дослідження показало 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 (інформаційних атак).

Виходячи із засад внутрішньої і зовнішньої політики, з урахуванням характеру актуальних загроз національній безпеці основними завданнями державної політики України у найближчий час і в середньостроковій перспективі, зокрема є:

– удосконалення державної інформаційної політики (особливо у воєнній сфері);

– попередження та ефективна протидія інформаційно-психологічним впливам іноземних держав, спрямованим на думки громадян України, порушення суверенітету і територіальної цілісності України, дестабілізацію внутрішньої соціально-політичної обстановки, провокування міжетнічних та міжконфесійних конфліктів в Україні.

У магістерському дослідженні обґрунтована необхідність створення 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.

Діяльність щодо забезпечення інформаційної безпеки повинна ґрунтуватися лише на нормах права, правовідносини будуватися в правовому полі і зосереджуватися на захисті життєво важливих інтересів людини,

суспільства і держави в інформаційній сфері та конструктивному поєднанні діяльності держави і всього українського народу.

Розвиток системи забезпечення інформаційної безпеки повинен передбачати питання стратегічного мислення, прогнозування і планування з метою запобігання чи нейтралізації правовими, організаційними, технічними та іншими засобами реальних і потенційних загроз в інформаційній сфері.

Розробка проблеми дозволила сформулювати пропозиції щодо здійснення пріоритетних кроків забезпечення інформаційної безпеки в Україні:

– 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 використовуються для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності;

– підвищення системи державного управління в інформаційній сфері;

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

– сприяння з боку держави активізації розвитку науково-технічних шкіл з метою створення і впровадження сучасних інформаційних технологій

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

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

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. – Харків, 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. Белл Д. Прихід постіндустріального суспільства/ Сучасна зарубіжна соціальна філософія: Хрестоматія. – Київ: Либідь, 1996. – С. 194 – 250.

5. Бжезинський Зб. Вибір: світове панування чи світове лідерство – К:, Києво-Могилянська Академія, 2006 р. –203 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. Боднар І. Р. Основні критерії інформаційної політики України : монографія. – Львів, Вид-тво Львівського торговельно-економічного університету, 2023. – 144 с.

10. Великий тлумачний словник сучасної української мови (з дод., допов. та CD) / [уклад. І голов. ред. В.Т. Бусел]. – Київ; 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. – Київ: 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. – Київ: 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. – Київ: 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. – Київ: 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. – Київ: 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. – Київ: Видавничий Дім «ІнЮре», 2012. – 544 с.

25. Конституція України // Відомості Верховної Ради України. – 1996. URL: http://www.viche.info/journal/1159.

26. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України. – Одеса, 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. — Харків, 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. – Київ: 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. – Харків: ХУПС, 2014. – Вип. 3 (40). – С. 127-129.

30. Краснокульська Ю. Інтернет як засіб комунікації: теоретико-методологічний аналіз / Ю. Краснокульська. URL: http://bibl.kma.mk.ua/pdf/ukrpolituk/-1/41.pdf.

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

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

33. Морозова В. О. Державна політика та стратегії США у сфері інформаційної безпеки в умовах глобальних викликів. URI: http://enpuir.npu.edu.ua/handle/123456789/13746

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

35. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України: дис. ... кандидата юрид. наук: 12.00.01 / Максименко Ю.Є. – Київ, 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. – Київ: НІСД, 2002. – 141 с.

38. Морозов О. Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності. URL: 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. URL :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. URL : https://zakon.rada.gov.ua/laws/show/559/2011#Text

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. URL : https://zakon.rada.gov.ua/laws/show/z0603-08#Text

45. Почепцов Г. *Сучасні інформаційні війни*. Київ : Києво-Могилян. акад.,. 2015. 496 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 / URL : 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. URL : 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. – URL : 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 URL :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. URL :http://zakon5.rada.gov.ua/laws/show/n0004525-14

55. Про інформацію: Закон України від 02.10.1992 № 2657-XII / URL : 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. URL : 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. URL :http://zakon3.rada.gov.ua/laws/show/287/2015

67. Про Стратегію національної безпеки України: Указ Президента України від 26.05.2015 № 287/2015/ URL: 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. URL: http://www.rnbo.gov.ua

70. РНБОУ схвалила Доктрину інформаційної безпеки України. URL : http://www.rnbo.gov.ua/news/2678.html

71. Семенченко А. І. Сучасний стан державної політики захисту національних інтересів: національні цінності, інтереси, цілі, загрози, обґрунтування геополітичної моделі // Вісник державної служби України. — 2008. — № 1

72. Семенченко А.І. Методологія стратегічного планування у сфері державного управління забезпеченням національної безпеки України: моногр. / А.І. Семенченко. – Київ: 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 URL : 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 Е. Третя Хвиля / З англ. пер. А. Євса. – Київ: 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.