Київський національний торговельно-економічний університет
Кафедра публічного управління та адміністрування

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

МОНІТОРИНГ ТА ОЦІНЮВАННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Студентки 2 курсу, 4 групи,
спеціальності 281 «Публічне управління та адміністрування» спеціалізації «Публічне управління та адміністрування» _____ (підпис студента) Гаврилюк Яни Миколаївна

Науковий керівник
кандидат екон. наук,
доцент _____ (підпис керівника) Сонько Юлія Анатоліївна

Гарант освітньої програми
д-р. екон. наук,
доцент _____ (підпис гаранта) Ладонько Людмила Степанівна

Київ 2020

Київський національний торговельно-економічний університет

Факультет економіки, менеджменту та психології
Кафедра публічного управління та адміністрування
Освітній ступінь: магістр
Спеціальність: публічне управління та адміністрування
Спеціалізація: публічне управління та адміністрування

Затверджую
Зав. кафедри _____

«28» лютого 2020 р.

Завдання
на випускну кваліфікаційну роботу (проект)
студентові

_____
(прізвище, ім'я, по батькові)

1. Тема випускної кваліфікаційної роботи (проекту): **«МОНІТОРИНГ ТА ОЦІНЮВАННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ»**

Затверджена наказом ректора від «27» лютого 2020 р. № 756

2. Строк здачі студентом закінченого роботи (проекту): 02.11.2020

3. Цільова установка та вихідні дані до роботи (проекту)

Мета роботи (проекту): дослідження стану захищеності інформаційної безпеки та аналіз наявних загроз національним інтересам держави в інформаційній сфері.

Об'єкт дослідження: процес проведення моніторингу та оцінки загроз інформаційної безпеки.

Предмет дослідження: теоретичні та прикладні основи забезпечення інформаційної безпеки за матеріалами Служби безпеки України.

4. Зміст випускної кваліфікаційної роботи (проекту) (перелік питань за кожним розділом):

ВСТУП

РОЗДІЛ 1 ТЕОРЕТИЧНІ ЗАСАДИ МОНІТОРИНГУ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Висновки до розділу 1

РОЗДІЛ 2. ДОСЛІДЖЕННЯ РОЗВИТКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

2.1. Механізми державного реагування на сучасні загрози інформаційній безпеці

2.2. Взаємодія державних і недержавних суб'єктів забезпечення інформаційної безпеки в сучасних умовах

2.3. Аналіз державної політики забезпечення інформаційної безпеки України

Висновки до розділу 2

РОЗДІЛ 3. ПРІОРИТЕТНІ НАПРЯМИ РОЗВИТКУ СИСТЕМИ МОНІТОРИНГУ ТА ОЦІНКИ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

3.1. Ідентифікація та захист об'єктів критичної інформаційної інфраструктури

3.2. Шляхи забезпечення безпеки інформації в Україні

3.3. Пропозиції для покращення ефективності функціонування Служби безпеки України у різних сферах діяльності держави для забезпечення інформаційної безпеки України

Висновки до розділу 3

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

5. Календарний план виконання роботи (проекту)

№ пор.	Назва етапів випускної кваліфікаційної роботи (проекту)	Строк виконання етапів роботи	
		за планом	фактично
1	2	3	4
1	Визначення напряму дослідження та затвердження теми випускної кваліфікаційної роботи	До 01.11.2019	01.11.2019
2	Складання плану та підготовка індивідуального завдання для виконання випускної кваліфікаційної роботи	До 28.02.2020	28.02.2020
3	Представлення на рецензування науковому керівнику рукопису першого розділу випускної кваліфікаційної роботи	До 19.06.2020	19.06.2020
4	Представлення на рецензування науковому керівнику рукопису другого розділу випускної кваліфікаційної роботи	До 01.09.2020	01.09.2020
5	Представлення на рецензування науковому керівнику рукопису третього розділу випускної кваліфікаційної роботи	До 01.10.2020	01.10.2020
6	Представлення закінченої випускної кваліфікаційної роботи на кафедру	До 02.11.2020	02.11.2020
7	Підготовка письмового відгуку на випускну кваліфікаційну роботу	До 06.11.2020	06.11.2020
8	Зовнішнє рецензування ВКР	До 16.11.2020	16.11.2020
10	Проведення попереднього захисту випускних кваліфікаційних робіт	23-27. 11.2020	23-27. 11.2020
11	Вирішення питання про допуск випускної кваліфікаційної роботи до захисту	До 01.12.2020	До 01.12.2020
12	Направлення випускної кваліфікаційної роботи із зовнішньою рецензією до ЕК для захисту	За графіком	За графіком

6. Дата видачі завдання « 28 » лютого 2020 р.

7. Науковий керівник випускної кваліфікаційної роботи (проекту)
Сонько Ю.А.
(прізвище, ініціали, підпис)

8. Керівник проектної групи
(гарант освітньої програми) Ладонько Л.С.
(прізвище, ініціали, підпис)

9. Завдання прийняв до виконання студент Гаврилюк Я.М.
(прізвище, ініціали, підпис)

10. Відгук наукового керівника випускної кваліфікаційної роботи (проекту):

Тема ВКР є актуальною, цікавою та відображає сучасні тенденції. В першому розділі ґрунтовно досліджено теоретичні засади інформаційної безпеки. В другому розділі проаналізовано державну політику забезпечення інформаційної безпеки та її розвиток. Автором виявлено основні загрози безпеки інформації в Україні в сучасних умовах. Безперечною перевагою роботи є її практичне значення, яке полягає в наданні рекомендацій щодо удосконалення роботи Служби безпеки України щодо забезпечення інформаційної безпеки. Робота є структурованою, висновки відповідають поставленим завданням. Автором використано сучасні напрацювання щодо інструментарію, який застосовується в організації інформаційної безпеки у світових практиках.

Загалом робота виконана на відповідному рівні, відповідає встановленим вимогам та може бути допущена до захисту.

Науковий керівник випускної кваліфікаційної роботи (проекту)
(підпис, дата)

Відмітка про попередній захист Ладонько Людмила Степанівна
(ПІБ, підпис, дата)

11. Висновок про випускну кваліфікаційну роботу (проект):
Випускна кваліфікаційна робота (проект) студента Гаврилюк Я.М.
(прізвище, ініціали)
може бути допущена до захисту екзаменаційній комісії.

Керівник проектної групи (гарант освітньої програми): Ладонько Людмила Степанівна
(прізвище, ініціали, підпис)

Завідувач кафедри: Новікова Наталія Леонідівна
(підпис, прізвище, ініціали)

«03» грудня 2020 р.

ЗМІСТ

ВСТУП

Сьогодні процеси розповсюдження інформації будь-якої країни світу має неабиякий вплив на усі сфери її життя суспільства. Саме тому забезпечення інформаційної безпеки – одне з найактуальніших завдань держави, тому що тільки збалансована політика інформаційної безпеки призведе до стабільної ситуації в державі та благополуччя її населення.

На Україну здійснюється потужний інформаційний вплив шляхом поширення неповної або упередженої інформації. Це зумовлено, насамперед, прагненням керівництва іноземних держав впливати на зовнішню та внутрішню політику України. Сьогодні актуальним завданням для України є моніторинг загроз інформаційній безпеці для реалізації інформаційної політики, спрямованої на забезпечення національних інтересів.

Актуальність контент-моніторингу інформаційного простору з метою виявлення ознак інформаційно-психологічних операцій для забезпечення інформаційної безпеки України у воєнній сфері обумовлена новими геополітичними викликами, що набули особливої гостроти в умовах інформаційної війни та військових конфліктів на сході України.

Інформаційний простір є однією з основних категорій інформаційної безпеки. Національний інформаційний простір являє собою сферу інформаційних обмінів щодо створення нової інформації, її захисту та використання. Розбудова власного інформаційного простору є однією з передумов соціально-економічного, політичного й культурного розвитку держави.

Метою роботи є дослідження стану захищеності інформаційної безпеки та аналіз наявних загроз національним інтересам держави в інформаційній сфері.

Поставлена мета зумовила необхідність вирішення таких завдань:

– розкрити теоретичні положення інформаційної безпеки;

- визначити загрози інформаційній безпеці України;
- розкрити своєрідність реалізації нинішньої політики інформаційної безпеки;
- дослідити механізми державного реагування на сучасні загрози інформаційній безпеці;
- висунути пропозиції для покращення ефективності функціонування різних сфер діяльності держави для забезпечення інформаційної безпеки України.

Об'єктом дослідження є процес проведення моніторингу та оцінки загроз інформаційної безпеки.

Предметом дослідження є теоретичні та прикладні основи забезпечення інформаційної безпеки за матеріалами Служби безпеки України.

Для вирішення визначених завдань, у процесі дослідження використано загальнонаукові та спеціальні методи.

У наукових працях з питань інформаційної безпеки та забезпечення кібернетичної безпеки таких фахівців, як А.Бабенко [2], В.Бурячок [4], В.Гавловський [6], О.Корочанський [18], Д.Дубов [13], Б.Кормич [17], В.Ліпкан [24], В.Цимбалюк [49], А.Марущак [27], В.Петрик [29], Г.Гулак [10], І.Валюшко [5] та інших науковців, дослідження інформаційної безпеки здійснювалося в контексті невід'ємної частини національної безпеки країни. Тому в даній роботі візьмемо собі за мету виокремити саме загрози інформаційної безпеки держави.

З метою реалізації поставлених завдань використано загальнонаукові та спеціальні методи дослідження: наукової абстракції – для розкриття сутності інформаційної безпеки (розділ 1), вивчення загроз безпеки інформації та механізм державного реагування (п.п. 2.1-2.2); кількісного та якісного аналізу – для формування удосконалення напрямів роботи Служби безпеки України в різних сферах для забезпечення інформаційної безпеки України (п.п. 2.3.-3.2) тощо.

Інформаційною базою дослідження стали: Закони України, Постанови Кабінету Міністрів, оперативна інформація міністерств та відомств, періодичні видання, праці вітчизняних і зарубіжних науковців з проблеми дослідження, а також інформаційні ресурси інформаційної мережі Internet.

Випускна кваліфікаційна робота складається зі вступу, 3-х розділів, висновків і пропозицій, списку використаних джерел. Основний текст роботи становить 68 сторінок, в т.ч. 1 таблиця, 10 рисунків. Список використаних джерел містить 50 найменувань, викладене на 6 сторінках.

Результати дослідження опубліковано: Гаврилюк Я. Теоретичні засади моніторингу загроз інформаційної безпеки України / Я. Гаврилюк // Публічне управління та адміністрування в умовах суспільних трансформацій : зб. наук. ст. студ. відп. ред. Н.Л. Новікова. – К.: Київ. нац. торг.-екон. ун-т, 2020. – 251 с., С. 18-27.

Розділ 1. ТЕОРЕТИЧНІ ЗАСАДИ МОНІТОРИНГУ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Важливу роль в розрізі національної безпеки сучасної України відіграє інформаційна безпека, а усі питання щодо її забезпечення є одними з найактуальніших. Адже збереження цілісності та суверенітету для незалежної України в умовах російсько-українського конфлікту є одним із головних пріоритетів.

Відповідно до законодавства України, інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [36].

Головним органом у системі центральних органів виконавчої влади у сфері забезпечення інформаційного суверенітету України, зокрема, з питань поширення суспільно важливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів є Міністерство інформаційної політики України (рис. 1.1).

Згідно з законодавством України поняття «інформаційна безпека» має наступне формулювання: «стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій» [41].

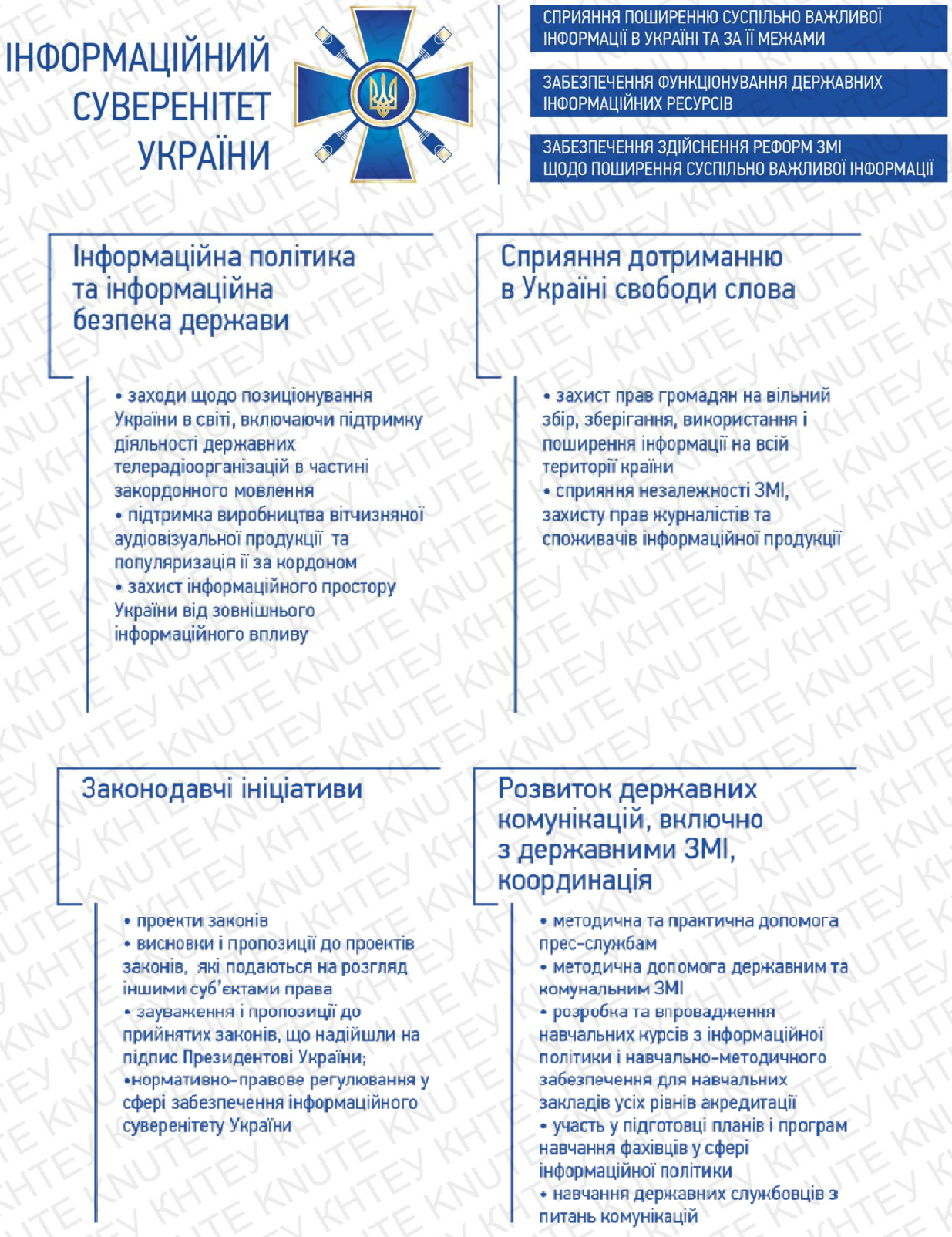

Рис. 1.1 Положення про Міністерство інформаційної політики України

Джерело: [37]

Проаналізуємо сутність інформаційної безпеки з різних джерел.

Інформаційна безпека України – це сукупність дієвих заходів

вповноважених державних органів у інформаційній сфері, спрямованих на захист національної безпеки та оборони України [15].

Інформаційна безпека – представляє собою стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [45].

Інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави [50].

Інформаційна безпека – безпека об'єкта від інформаційних загроз або негативних впливів, пов'язаних з інформацією та нерозголошення даних про той чи інший об'єкт, що є державною таємницею [21].

Інформаційна безпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства і держави [25].

Однак на мій погляд, ось найбільш обширне та оптимальніше визначення, що описує усі аспекти взаємодії суб'єктів інформаційних відносин:

Інформаційна безпека – стан захищеності життєво необхідних національних інтересів держави, суспільства та кожного громадянина, за якого ймовірні мінімальні збитки та їх наслідки функціонування у зв'язку з недостовірністю, неповнотою та невчасністю інформації, її негативний вплив і несанкціоноване розповсюдження застосування інформаційних технологій.

Аналізуючи процитовані вище тлумачення формулювання «інформаційна безпека» можемо окреслити її наступні ознаки. Отож, інформаційна безпека – це:

- стан захищеності інформаційного простору;
- безпека встановлених законом норм і правил, за якими здійснюються процеси інформації в країні;

- стан захищеності в середовищі інформації національних інтересів держави;
- невід'ємна частина політичної, оборонної, економічної та решти складових національної безпеки країни;
- суспільні відносини, які пов'язані із захистом життєво необхідних інтересів суспільства та держави від дійсних та можливих загроз в інформаційному просторі.

Одним з важливих питань в ході вивчення сутності інформаційної безпеки є оцінка загроз, які можуть позначатися на її ефективності.

Загрози інформаційній безпеці – існуючі та мислено ймовірні події і фактори, які несуть небезпеку життєво необхідним інтересам держави, суспільства та кожної особистості в інформаційній сфері.

Об'єднуючи багатоманітні підходи, виділимо наступні види загроз інформаційній безпеці:

- збій та відмова вироботі устаткування;
- порушення цілісності інформаційних ресурсів;
- розкриття інформаційних ресурсів;

Розберемо детальніше кожен з видів загроз.

Загроза збою та відмови в роботі самого устаткування. Дана загроза в роботі обладнання може статися під час блокування доступу як до одного, так і декількох ресурсів інформаційної системи. В дійсності блокування ресурсів може бути постійним, так щоб при запитуванні він ніколи не був отриманий або відповідь надходила з затриманням, що достатньо для того, щоб ресурс став некорисним.

Виділимо 3 категорії джерел загроз інформаційної безпеки:

1. Антропогенні джерела спричиненні діяльністю суб'єктаі (суб'єктів), що

   призводять до порушення інформаційної безпеки. Ці злочини кваліфікуються як навмисні та випадкові. Джерела таких дій бувають

як внутрішні, так і зовнішні. Проте їх можливо передбачити та вчасно застосувати ефективних запобіжних заходів;

2. Техногенні – менш прогнозовані та залежать практично від властивостей обладнання та техніки, а тому потребують постійного контролю та уваги. Такі джерела загроз інформаційній безпеці, також можуть бути внутрішніми і зовнішніми.
3. Стихійні джерела. Ця категорія відноситься до обставин непереборної сили (ураган, повінь, пожежа, землетрус та інші стихійні лиха) і спрогнозувати чи запобігти їх неможливо. Ці обставини носять об'єктивний та абсолютний характер і поширюється на всіх. Такі джерела загроз неможливо спрогнозувати, а відтак заходи їх уникнення повинні бути застосовані постійно. Оскільки стихійні джерела це саме природні катаклізми, вони відносяться до зовнішніх загроз.

Загроза порушення цілісності інформаційних ресурсів: умисний людський вплив, а саме редагування, передача до інших систем або знищення збережених данихів інформаційній системі певного суб'єкта управління.

Загроза розкриття інформаційних ресурсів: дані та інформація стають відомими тим, хто не повинен був це дізнатись. Також можна пояснити це як несанкціонований доступ до відкритих даних та даних з обмеженим доступом. Такі ресурси повинні бути збережені у єдиній інформаційній системі.

Зазвичай рівень інформаційної інфраструктури будь-якої цивілізованої країни переважно відображає рівень інформаційної безпеки країни. На превеликий жаль, безумовно низький рівень інформаційної інфраструктури нашої країни за роки незалежності посприяв навалі на цей ринок іноземним компаніям (в першу чергу російським) та створив придатні умови для «захоплення» ефірного часу, особливо в прайм-тайм, іноземними програмами, багато з яких забруднили інформаційних простір України своїм баченням подій. Вони активно пропагували та пропагують, нав’язували та нав’язують

«свою» політику і свій спосіб життя та традиції, що звичайно має пагубний вплив на державу і суспільство в цілому, таким чином фактично знищуючи генофонд української нації.

Недостатній, або свідомо недостатній, державний контроль за виконання законів України окремими політичними силами, багатьма ЗМІ та особами, які в інформаційній сфері здійснюють підприємницьку діяльністю, призвів до того, що час від часу відбувається багато випадків в ефірах теле- та радіопрограмам, які спрямовані на руйнування свідомості української нації та усіх моральних цінностей.

Крім того певною мірою низький чи середній інтелектуальний, творчий і професійний рівень виробництва вітчизняного інформаційного продукту, його не конкурентоспроможність веде до того, що аудиторія країни, надає перевагу іноземним продуктам. Таким чином, національний інформаційний простір України більш як два десятиліття зазнавав суттєвих загроз, що безумовно становили небезпеку функціонування країни, її політичного та економічного розвитку, інтеграції до Євросоюзу та НАТО.

Позиція Української держави щодо протидії загрозам національній безпеці в інформаційній сфері виражена у визначених Законом України «Про основи національної безпеки України» основних напрямах державної політики з питань національної безпеки (рис. 1.2).

Загрози національної безпеки України в інформаційній сфері – сукупність певних умов та факторів, що становлять небезпеку життєво необхідним інтересам держави, суспільства і особистості через ймовірну можливість негативного інформаційного впливу на поведінку та свідомість громадян, а також на інформаційно-технічну інфраструктуру та інформаційні ресурси.

Як зазначають науковці та фахівці з інформаційної політики України в сфері національної безпеки існує нагальна потреба негайного перегляду та удосконалення системи захисту, яка повинна бути спрямована на забезпечення захищеності національних інтересів держави.

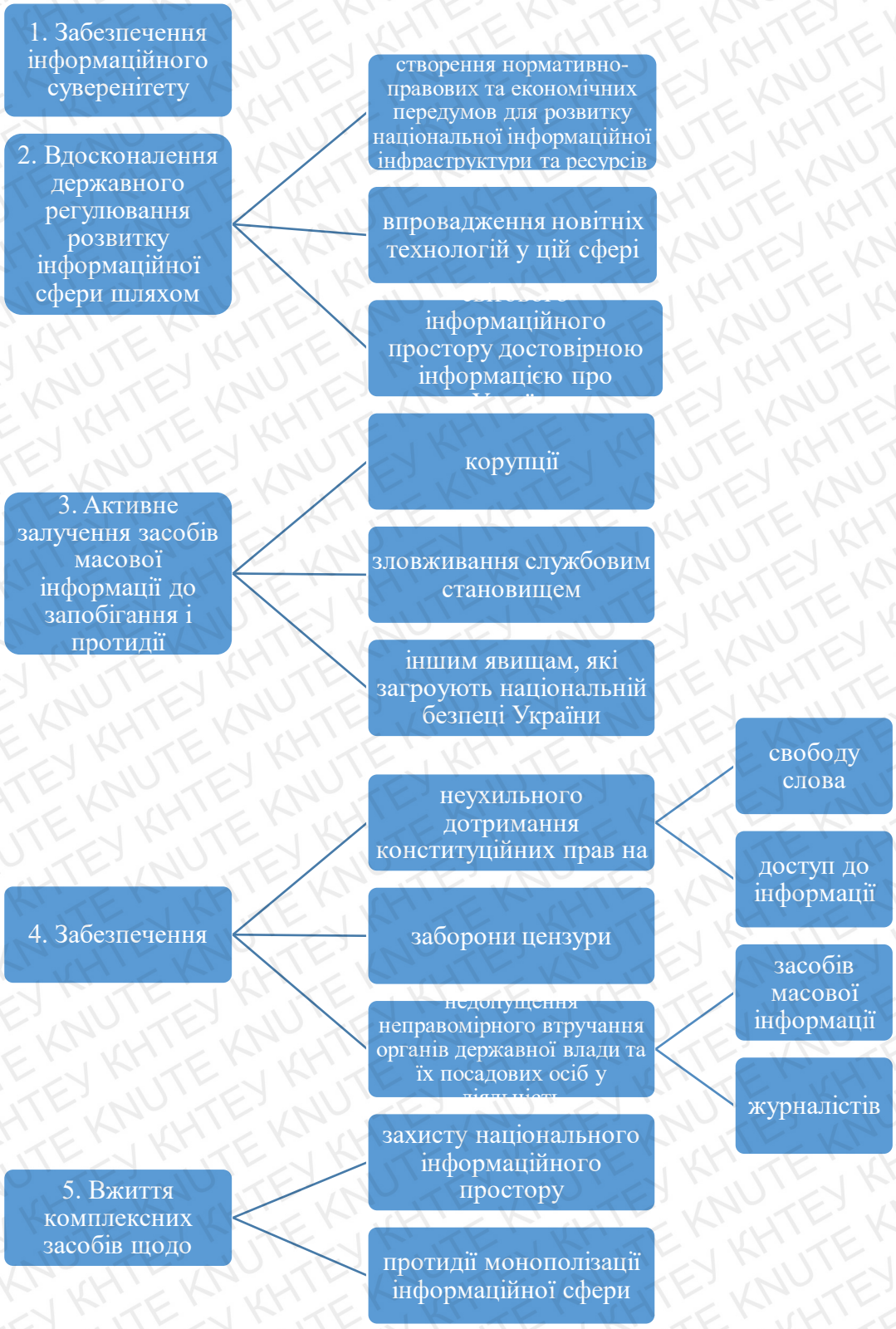

Рис. 1.2 Основні напрямки державної політики з питань національної безпеки в Україні в інформаційній сфері

Джерело: [39]

Найбільшою загрозою національній безпеці України в інформаційній сфері є реалізація іноземними державами через проведення спеціальних інформаційних операцій, кампаній та інформаційних акцій, потужного негативного інформаційно-психологічного впливу на громадськість всього світу, а особливо на свідомість громадян нашої країни. Це здійснюється шляхом постійного і систематичного поширення фейкової, упередженої, або неповної інформації про Україну та політичні, економічні і соціальні процеси, що точаться на її теренах. Усе це неодмінно впливає на зовнішню та внутрішню політику України та марнує міжнародний імідж нашої держави. Головною метою таких інформаційних операцій для інших держав є забезпечення своїх власних загальнодержавних інтересів.

Тому наслідком реагування нашої держави на такий перебіг подій стало Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Її метою є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни [34].

Зокрема Доктриною визначено актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері, а саме:

- здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;
- проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;

- інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;
- інформаційне домінування держави-агресора на тимчасово окупованих територіях;
- недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;
- неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства;
- поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [34].

Розглянемо пріоритети державної політики в інформаційному середовищі, що зазначені в Доктрині інформаційної безпеки України, отже:

В теперішніх умовах найбільша загроза інформаційної безпеки України є інформаційна війна з боку іншої держави, а саме Російської Федерації. Наміри агресора націлені нав’язувати за допомогою засобів масової інформації власну ідеологію, різні суспільні думки та стереотипи.

Інформаційна війна включає наступні дії:

- здійснення впливу на інфраструктуру країни (телекомунікації, транспортні мережі, електропостачання, банківська система, тощо);
- промисловий шпіонаж (розкрадання патентованої інформації, здійснення конкурентної розвідки, знищення важливих даних, порушення прав інтелектуальної власності);
- хакінг (умисне втручання в систему, злам і використання як особистих даних, так і інформації з обмеженим доступом).

До серйозних загроз інформаційній безпеці країни також відносяться кібертероризм та кібервійни. Такі дії передбачають протистояння в кіберпросторі загальнодержавних інтересів застосовуючи інтернер-технології для нанесення шкоди противнику. Найчастіше ці технології використовують для спрямування на сферу оборони державної безпеки і, відповідно, становлять серйозну загрозу цілісності держави та її суверенітету.

Висновки до розділу 1

На пій погляд, щоб покращити державну політику забезпечення інформаційної безпеки України, насамперед потрібно вдосконалити організаційні та правові процеси управління інформаційною безпекою та безупинно здійснювати забезпечення держави інтелектуальними та трудовими ресурсами.

Виділимо основні напрями удосконалення інформаційної безпеки:

- створення та впровадження загальнодержавних моделей та їх технічних інструкцій застосування інформаційно-комунікаційних технологій до відповідних європейських стандартів;
- створення та впровадження національної системи спостереження, оцінювання та виявлення показників різних сфер життєдіяльності, що аналізують та описують стан захисту інтересів держави та виявляють реальні загрози національній безпеці;
- розвиток правових засад управління національною безпекою (розробити відповідні закони, стратегії, доктрини, програми і концепції).

Отже, інформаційна безпека є однією з першочергових значень для соціально-економічного розвитку держави. Україна повинна посилити свої дії та активно працювати над створенням власної ефективної та потужної системи безпеки інформації, що є однією з ключових складових національної безпеки держави.

Розділ 2. ДОСЛІДЖЕННЯ РОЗВИТКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

2.1. Механізми державного реагування на сучасні загрози інформаційній безпеці

В ч.1 ст.17 Конституції України [16] визначено одну з норм як «найважливіша функція держави» – забезпечення інформаційної безпеки. Для формування державою чіткої політики інформаційної безпеки, оптимального застосування інструментів та засобів її реалізації, необхідна наявність інституціонального механізму, який втілює відповідний напрямок діяльності держави України.

Прийняття в установчому порядку стратегій, концепцій, програм та доктрин сприятимуть проведенню державної політики для комплексного забезпечення інформаційної безпеки.

Перелік установ, які беруть участь у проведенні політики, фактично невичерпаний і не обмежується лише органами місцевого самоврядування та державної влади. Крім Президента України, Верховної Ради і Кабінету міністрів до розв'язання проблем в політиці інформаційної безпеки долучаються фахівці різних наукових установ, групи експертів,тощо. Крім того неабиякий вплив на прийняття будь яких рішень має діяльність громадських організацій, політичних партій та рухів, а також неформальних фінансово-промислових та політичних груп.

Проте головний суб'єкт політики інформаційної безпеки безумовно держава, яка реалізує інституціональний механізм державної політики безпосередньо організувавши систему компетентних органів державного управління.

На наш погляд, інституціональний механізм являє собою багаторівневу систему, яка з однієї сторони об'єднана особливою функціональною спрямованістю, а з іншої сторони, розділена своєрідними особливостями, пов'язаними характером належних цілей та ступенем компетенції. Тобто, на

кожному рівні інституціональним суб'єктам відповідає окрема своєрідна функція – функція утворення державної політики інформаційної безпеки або функція втілення політики інформаційної безпеки. Функція утворення державної політики інформаційної безпеки містить в собі діяльність органів держави відносно формування стратегічних цілей та завдань, головних принципів та напрямів діяльності держави в даній сфері, а також розробку концепцій і рішень загальнодержавного значення.

Функція втілення політики інформаційної безпеки направлена на досягнення оперативних та тактичних цілей, забезпечує розв'язання визначених завдань, застосування доцільних засобів, методів та форм впливу держави на суспільні відносини в даній сфері.

Враховуючи вищевикладене можна констатувати, що для формування та реалізації політики держави в сфері інформаційної безпеки існує чіткий механізм – це організаційно-правовий механізм інформаційної безпеки.

Організаційно-правовий механізм державної політики інформаційної безпеки – це впорядкований комплекс інститутів держави, які задіяні у процесі утворення і втілення політики інформаційної безпеки, а їх ролі та відносини регулює система правових норм і принципів. Згідно з визначеними напрямками втілення політики інформаційної безпеки, організаційно-правовий механізм сформований із трьох елементів, які взаємопов'язані.

По-перше, це сукупність інституцій держави, які задіяні в процесі утворення і втілення політики інформаційної безпеки, інакше кажучи інституціональний механізм інформаційної безпеки.

По-друге, це сукупність відносин і ролей, яка включає правові відносини що з'являються під час провадження політики інформаційної безпеки і специфічні ролі, методи та форми діяльності суб'єктів провадження політики інформаційної безпеки.

По-третє, це ієрархічна сукупність правових принципів і норм, які регулюють зміст та процес проведення політики інформаційної безпеки,

іншими словами правовий механізм інформаційної безпеки. Саме два останніх елементи складають правовий механізм інформаційної безпеки.

Сукупність інститутів громадянського суспільства та інститутів публічної влади, які задіяні у процесі утворення і втілення політики інформаційної безпеки, складають інституціональний механізм інформаційної безпеки.

Ефективність кожної складової механізму інформаційної безпеки держави забезпечує її ефективність захисту інформаційної безпеки в цілому.

Проаналізуємо складову механізму політики безпеки, що репрезентована органами публічної влади. Варто відзначити, що цей механізм представляє саме ієрархічну сукупність органів влади різних гілок та різних рівнів, котрі в рамках свої повноважень вирішують певні завдання з утворення та втілення політики інформаційної безпеки.

Органи влади, які становлять частину механізму інформаційної безпеки, згідно ст.4 Закону України «Про основи національної безпеки» [39] є суб'єктами забезпечення національної безпеки, а саме:

Рис. 2.1 Механізм інформаційної безпеки

Джерело: [39]

Аналізуючи даний механізм, необхідно в першу чергу визначити керівні органи або орган у цій ієрархії. На мою думку в сфері інформаційної безпеки можна виділити відразу два претенденти на керівну роль, це Президент та Верховна Рада.

Можна констатувати той факт, що за часів незалежності країни формування законодавства, яке регулює безліч питань побудови структури апарату держави, відбувалося в умовах протистояння і політичної боротьби між двома гілками влади: законодавчою та виконавчою.

Функції Верховної Ради включають в себе визначення в державі ключових параметрів інформаційних процесів та ймовірних способів і форм забезпечення цих параметрів. Або іншими словами, Верховна Рада визначає зміст інформаційної безпеки і можливі способи та форми її захисту.

В сфері інформаційної безпеки Верховна Рада України виконує важливі контрольні функції. Нормами ст.85 Конституції України до повноважень Верховної Ради України належить здійснення: контролю за діяльністю Кабінету Міністрів України відповідно до Конституції та закону; контролю за виконанням Державного бюджету України, прийняття рішення щодо звіту про його виконання; парламентського контролю у межах, визначених Конституцією та законом; прийняття рішення про направлення запиту до Президента України на вимогу народного депутата України, групи народних депутатів України чи комітету Верховної Ради України. Також важливими інструментами контролю є утворення тимчасових слідчих комісій для проведення розслідування з питань, що становлять суспільний інтерес, в інформаційній сфері зокрема, та проведення парламентських слухань з питань свободи слова, діяльності ЗМІ, загальної ситуації в інформаційній сфері, тощо.

Президент України виконує свої повноваження у сфері інформаційної безпеки згідно норми визначеної у п.17 ст.106 Конституції України, а саме: Президент України здійснює керівництво у сферах національної безпеки та оборони держави [16]. Президент володіє ключовими функціями стосовно

організації забезпечення інформаційної безпеки. Згідно Конституції, Президент очолює Раду національної безпеки і оборони України, за поданням Кабінету Міністрів утворює, реорганізує та ліквідує міністерства та інші центральні органи виконавчої влади, які в інформаційній сфері здійснюють управління державне.

Головним завданням Адміністрації Президента є правове, організаційне, інформаційне, експортно-аналітичне, консультативне та інше забезпечення діяльності Президента, зокрема і в сфері інформаційної безпеки. Адміністрації Президента надані широкі повноваження для реалізації цих завдань, у тому числі й інформативного характеру.

В структуру Адміністрації Президента входять профільні підрозділи (департаменти) з питань інформаційної політики та інформаційної безпеки. Вони забезпечують напрямки діяльності Президента України в інформаційній сфері.

Згідно зі ст.107 Конституції України Рада національної безпеки і оборони України є координаційним органом з питань національної безпеки і оборони при Президентові України.

Рада національної безпеки і оборони України координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони.

Головою Ради національної безпеки і оборони України є Президент України.

Персональний склад Ради національної безпеки і оборони України формує Президент України.

До складу Ради національної безпеки і оборони України за посадою входять Прем'єр-міністр України, Міністр оборони України, Голова Служби безпеки України, Міністр внутрішніх справ України, Міністр закордонних справ України.

У засіданнях Ради національної безпеки і оборони України може брати участь Голова Верховної Ради України [16].

Крім того відзначимо, що серед контрольних, дорадчих та координаційних повноважень РНБО в сфері інформаційної безпеки згідно ст.4 Закону України Про Раду національної безпеки і оборони України, до компетенції РНБО входить визначення стратегічних національних інтересів України, концептуальних підходів та напрямів забезпечення національної безпеки і оборони у політичній, економічній, соціальній, воєнній, науково-технологічній, екологічній, інформаційній та інших сферах [42].

Також у сфері інформаційної безпеки до функцій Президента України додаються відповідні функції Кабінету Міністрів. Знаючи роль та місце даного органу в системі публічної влади України є сенс віднести його, як і Президента, до другого керівного центру політики інформаційної безпеки.

Отже, зміст організаційно-правового механізму державної політики забезпечення інформаційної безпеки складається з трьохелементної системи, в якій Верховна Рада визначає параметри безпеки інформаційної сфери, Президент вирішує питання стосовно визначення інструментів досягнення та забезпечення цих параметрів, а Кабінет Міністрів має завдання проводити в життя передбачені заходи застосовуючи вибраний інструмент впливу на суспільні відносини. Це є основні функції даних трьох органів у механізмі інформаційної безпеки, а їх ефективна реалізація залежить від додаткових повноважень та схем їх взаємодії.

Окремо хочеться виділити саме в рамках механізму державної політики забезпечення інформаційної безпеки ряд суб’єктів, які здійснюють планомірний вплив на інформаційну сферу, що є їхньою однією з головних чи головною функцією.

Вагомі функції щодо підтримки рівня інформаційної безпеки покладені на Міністерство культури та інформаційної політики України. Згідно п.1 Положення про Міністерство культури та інформаційної політики України, МКІП є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сферах культури,

державної мовної політики, популяризації України у світі, державного іномовлення, інформаційного суверенітету України (у частині повноважень з управління цілісним майновим комплексом Українського національного інформаційного агентства "Укрінформ") та інформаційної безпеки, а також забезпечує формування та реалізацію державної політики у сферах кінематографії, відновлення та збереження національної пам'яті, міжнаціональних відносин, релігії та захисту прав національних меншин в Україні, мистецтв, охорони культурної спадщини, музейної справи, вивезення, ввезення і повернення культурних цінностей [37].

Однією з важливих функцій Міністерства є процес регулювання порядку розповсюдження та демонстрування вітчизняних і іноземних фільмів на території нашої країни. Міністерство здійснює державну реєстрацію фільмів, а відмова в такій реєстрації означає заборону фільму до розповсюдження та демонстрації на території України.

Також в сфері інформаційної безпеки великий комплекс завдань покладено на Міністерством освіти і науки України. Згідно п.1 Положення про Міністерство освіти і науки України, МОН є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сферах освіти і науки, наукової, науково-технічної діяльності, інноваційної діяльності в зазначених сферах, трансферу (передачі) технологій, а також забезпечує формування та реалізацію державної політики у сфері здійснення державного нагляду (контролю) за діяльністю закладів освіти, підприємств, установ та організацій, які надають послуги у сфері освіти або провадять іншу діяльність, пов'язану з наданням таких послуг, незалежно від їх підпорядкування і форми власності [38].

МОН України виконує певний ряд дозвільних функцій, завдяки яким здійснюється регулювання наукової та освітньої діяльності на території України. Також Міністерство здійснює регулювання питань пов'язаних із захистом інтелектуальної власності та авторських прав, що мають величезний

вплив не тільки на ситуацію в інформаційній сфері держави, але і на її зовнішні відносини, згідно міжнародно-правових зобов'язань взятих на себе країною.

Виокремимо три основні напрямки діяльності Міністерства внутрішніх справ України в сфері інформаційної безпеки:

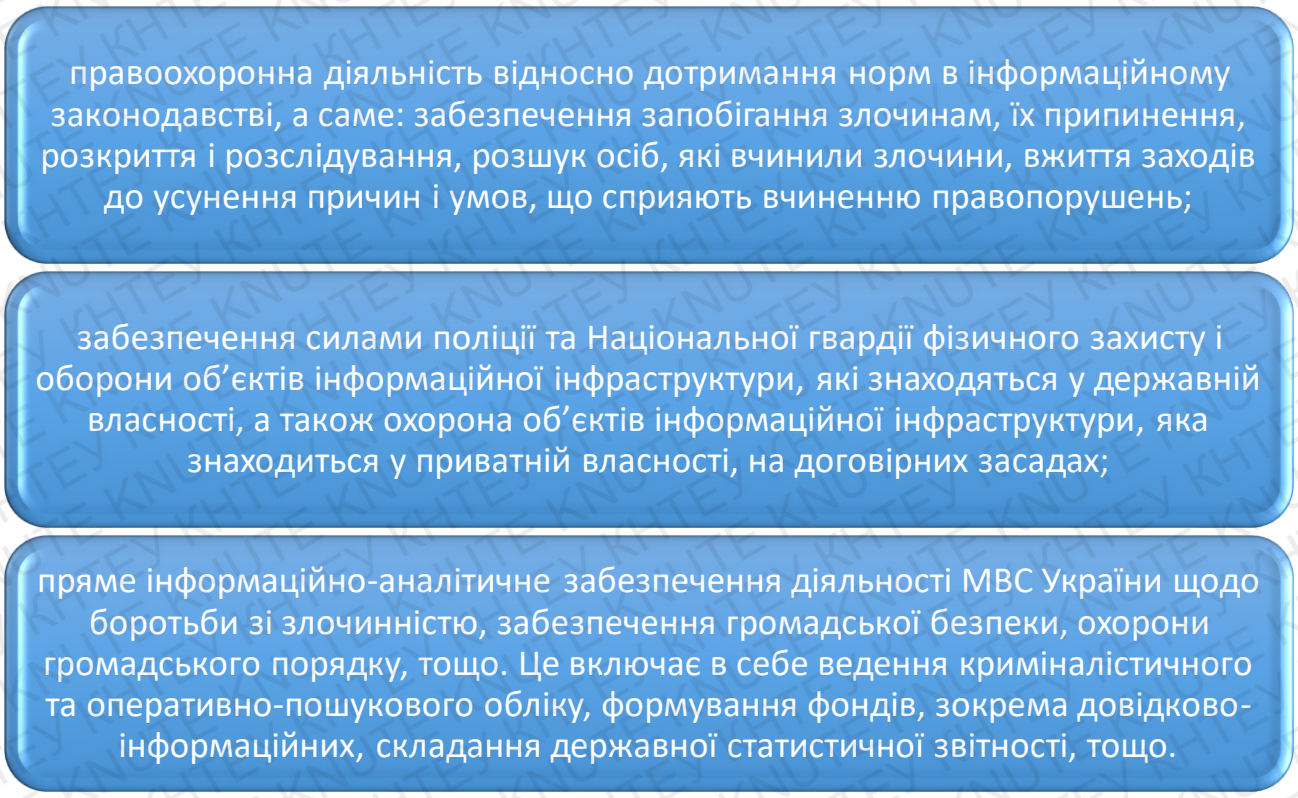

Рис. 2.2 Напрямки діяльності Міністерства внутрішніх справ України в сфері інформаційної безпеки

Джерело: [38]

Основним спеціалізованим відомством сектору безпеки з питань інформаційної безпеки, безумовно є Служба безпеки України. Згідно ст.1 Закону України «Про службу безпеки України» Служба безпеки України – державний орган спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку України [43]. Орган безпосередньо підпорядковується Президенту України та підзвітний Верховій Раді України. Переважна більшість напрямків діяльності спецслужби пов'язана безпосередньо з інформаційними процесами, причому в одних випадках інформація є метою їх діяльності, а в інших – засобом. В ст.10 Закону України

«Про Службу безпеки України» визначено функціональні підрозділи, серед яких виділимо ті, які питаннями інформаційної безпеки займаються безпосередньо. До них належать: контррозвідка, військової контррозвідка, контррозвідувальний захист інтересів держави у сфері інформаційної безпеки, інформаційно-аналітичний, оперативного документування та інші згідно з організаційною структурою Служби безпеки України.

До складу Служби безпеки України входить Департамент спеціальних телекомунікаційних систем та захисту інформації. Основне його завдання, це реалізації державної політики у сфері захисту державних інформаційних ресурсів у мережах передачі даних, криптографічного та технічного захисту інформації, забезпечення функціонування державної системи урядового зв'язку. Сьогодні Служба безпеки України реалізує весь комплекс заходів для інформаційної та кібербезпеки держави: протидіє кібертероризму, кібершпигунству, блокує хакерські атаки, спростовує фейки.

Також окремі питання пов'язані з провадженням у життя політики інформаційної безпеки вирішують цілий ряд відомств, які діють в системі органів виконавчої влади.

Одним з головних органів державного управління інформаційною сферою, безумовно, є Державний комітет телебачення і радіомовлення України.

Його значення і статус підкреслюється тим, що наявність даного комітету визначена нормами Конституції України (п.20 ст.85 та п.13 ст.106) [16], згідно з якими Верховна Рада України та Президент України призначають на посади та звільняють з посад половину складу Національної ради України з питань телебачення і радіомовлення відповідно.

Діяльність Держкомтелерадіо України, спеціально уповноваженого центрального органу виконавчої влади, координується та спрямовується Кабінетом Міністрів України. Крім контрольних функцій, Держкомтелерадіо України здійснює державну реєстрацію інформаційних агентств і друкованих засобів масової інформації, веде Державний реєстр України видавців,

виробників та розповсюджувачів видавничої продукції.

Наприкінці 2014 року в державі створено Міністерство інформаційної політики України, діяльність якого також координується та спрямовується Кабінетом Міністрів України. Міністерство є головним центральним органом виконавчої влади із формування стратегії інформаційної політики держави та забезпечення її дотримання у сферах просвітницької діяльності, створення інформаційної продукції, сприяння розвитку засобів масової інформації, формування і використання національних інформаційних ресурсів, створення умов для розвитку інформаційного суспільства та поширення суспільно важливої інформації, в тому числі в питаннях, що стосуються національної безпеки.

Проведення політики інформаційної безпеки на місцях здійснюється регіональними та місцевими відділеннями вищезазначених центральних органів виконавчої влади, державними адміністраціями районів та областей і органами місцевого самоврядування.

В загальному можемо констатувати, що за останні роки в Україні сформовано систему органів, яка здатна в галузі забезпечення інформаційної безпеки вирішувати найскладніші завдання. Проте ми розуміємо, що органи, які входять в цю систему, є складовими системи влади, що сформувалася в державі з усіма їй властивими недоліками та проблемами.

Серед основних факторів, які впливають на адекватність та ефективність механізмів державної політики інформаційної безпеки необхідно назвати в першу чергу в системі державного управління загальні негативні тенденції, які в переважній більшості наслідувані від колишньої радянської системи і набули найбільш потворних форм.

Сюди можна віднести такі явища, як бюрократизм, корупція шалених масштабів, низькі професійні та моральні якості певних керівників та їх орієнтованість на першочергове задоволення не потреб громадян і суспільства, а власних, незбалансованість, неузгодженість та недостатня визначеність

компетенції багатьох органів влади, які призводять до багатьох колізій і зіткнення їх інтересів. Також характерною проблемою для багатьох країн пострадянського простору є низька політична активність і нерозвиненість механізмів та інститутів громадського суспільства,, що призводить до неефективності або відсутності громадянського контролю у сфері інформаційної діяльності держави та її органів.

В цілому, можна констатувати, що зміст діяльності держави і її компетентних органів стосовно регулювання інформаційних процесів та правовідносин визначає політика інформаційної безпеки. Сьогодні значно розширилося значення та масштаб інформаційної діяльності держави, тому складно перелічити усі сфери державного і суспільного життя, на які впливають результати цієї діяльності, а саме на: державну і військову безпека, культуру, економіку, зовнішню та внутрішню політику, права людини, тощо.

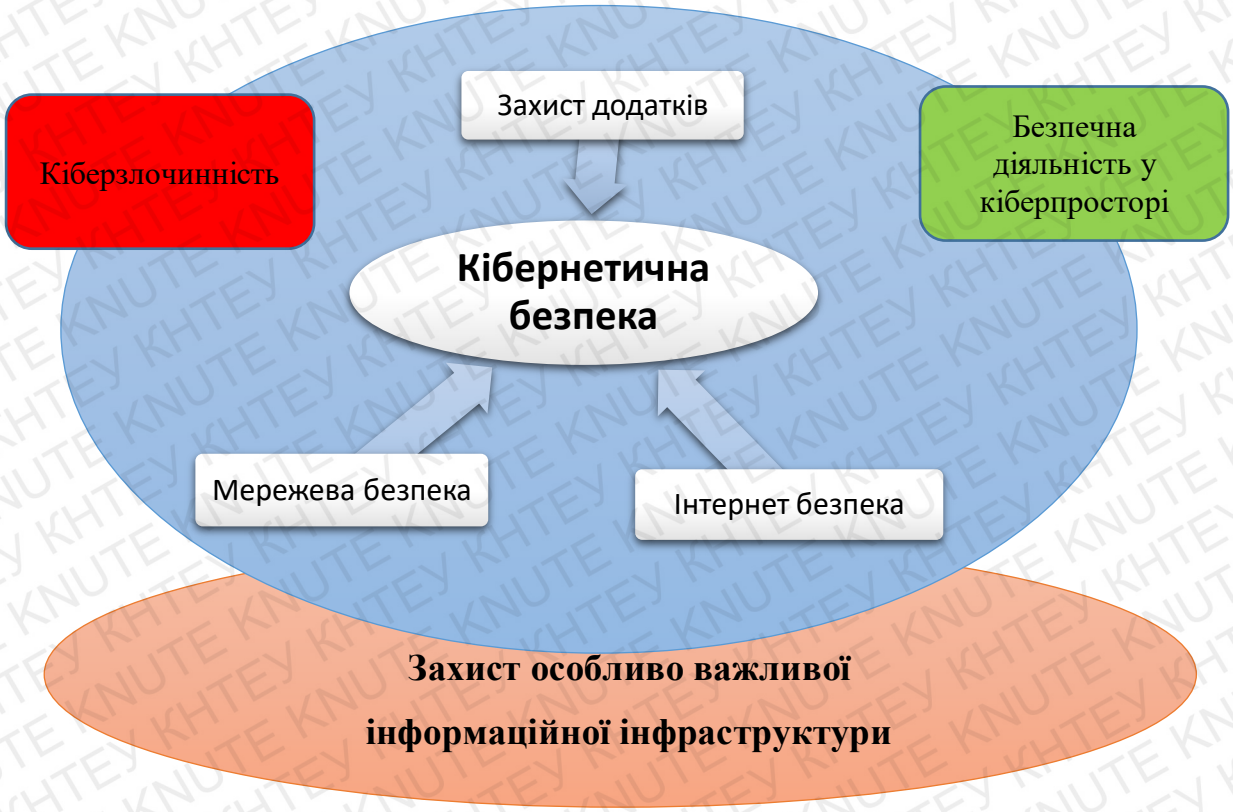

Рис. 2.3 Співвідношення понять безпеки в інформаційному та кіберпросторах

Джерело: [12]

2.2. Взаємодія державних і недержавних суб'єктів забезпечення інформаційної безпеки в сучасних умовах

Сучасна політика держави з питань забезпечення інформаційної безпеки має враховувати особисті, суспільні та державні інтереси у внутрішньому і зовнішньому середовищі, викривати небезпечні інформаційні загрози даним інтересам та включати відповідні засоби й методи для їх запобігання, нейтралізації та локалізації.

Забезпечення національної безпеки України є справою не лише органів державної влади, але й суспільства в цілому та кожного громадянина окремо.

Згідно ст.4 Закону України «Про основи національної безпеки України» суб'єктами забезпечення національної безпеки є громадяни України, об'єднання громадян, а відповідно ст.5 одним з пріоритетів національних інтересів є розвиток громадянського суспільства, його демократичних інститутів [39].

Проте на сьогодні науковцями в Україні системно не проведено дослідження недержавної системи безпеки як інституційного механізму забезпечення інформаційної безпеки, а громадські об'єднання – як суб'єктів забезпечення інформаційної безпеки держави.

Наразі в країні відбувається формування системи недержавних суб'єктів інформаційної безпеки, поява якої спричинена подіями останніх років в Україні: Революцією Гідності, анексією Криму та агресію Росії на Донбасі. Усі ці події призвели до плідної співпраці в даній сфері державних та недержавних суб'єктів забезпечення інформаційної безпеки, органів державної влади, громадянського суспільства і бізнесу. Прес-служби державних структур сектору безпеки налагодили співпрацю з приватними ЗМІ, які в свою чергу активно інформують громадськість з протидією держави російській агресії на Донбасі та спростовують різного роду медіа-фейки російських ЗМІ. У телеефірах, радіопередачах, друкованих і електронних ЗМІ надається об'єктивна та правдива інформація щодо агресії Росії, подіях в Криму, тощо. Як приклад, недержавними суб'єктами забезпечення інформаційної безпеки є

Міжнародний інформаційний консорціум «Бастіон», в структуру якого входять: «Інформаційний спротив» («ІС»), Центр «Миротворець», Міжнародна волонтерська мережа InformNapalm, Центр дослідження армії, конверсії та роззброєння; Український кризовий медіа-центр; Міжнародний центр протидії російській пропаганді; Бюро протидії гібридній війні, тощо.

Інформаційний спротив (ІС) – є неурядовим проектом, головне завдання якого, протидія в інформаційному просторі загрозам, що виникають у пріоритетних напрямках національної безпеки України: військовому, економічному, енергетичному та у інформаційній безпеці. «ІС» розпочав свою роботу у березні 2014 року, після вторгнення РФ до АК Крим. «ІС» перевіряє інформацію що надходить, з двох-трьох не пов'язаних між собою джерел, дає посилання на учасників та свідків подій, робить аналітику, яку готують як власні експерти, так і міжнародні.

Центр «Миротворець» теж є незалежною неурядовою організацією, яка створена вченими, журналістами та фахівцями з питань національної безпеки України, миру, безпеки людства та міжнародного правопорядку, які займаються творчою, науковою та журналістською діяльністю. Цікаво, що ресурс навіть популярний у РФ, де роботодавці через базу даних «Миротворця» перевіряють своїх співробітників.

Міжнародна волонтерська спільнота InformNapalm заснована у березні 2014 підчас збройної агресії Росії проти України у Криму. На даний час на волонтерських засадах у спільноту InformNapalm входять люди з 20 країн світу, які проводять OSINT-дослідження, перекладають та поширюють публікації іноземними мовами, ведуть важливу медійну, дипломатичну і просвітницьку роботу.

Засновником спільноти і головним редактором сайту InformNapalm.org є вимушений переселенець з Криму Роман Бурко. Співзасновником спільноти та

Деякі учасники спільноти, які постійно живуть в Україні, крім

волонтерської діяльності в команді також у певний період війни брали активну участь у захисті України у бойових діях на Донбасі. Частина волонтерів – це вимушені переселенці з Криму і Донбасу. У кожного з волонтерів є своя умовна спеціалізація в спільноті InformNapalm:

- проведення OSINT-розслідувань;
- аналіз масивів даних та перевірка інформації;
- технічний захист та збір інформації;
- написання статей і репортажів;
- графічний або відео дизайн;
- переклад публікацій на іноземні мови;
- поширення даних і стратегічні комунікації.

Всі розслідування спільноти розміщуються за вільною ліцензією Creative Commons BY 4.0 і можуть безперешкодно копіюватися і розповсюджуватися за умови активного посилання на джерело досліджень.

Місія спільноти InformNapalm:

Збір доказів та інформування світового співтовариства про реальну роль Росії в гібридних конфліктах та спецопераціях. Розкриття фактів про російське військове вторгнення в Україну. Викриття учасників агресії проти Грузії. Збір матеріалів про операції РФ в країнах Східної та Центральної Європи, і на Близькому Сході.

Головні цілі спільноти:

- Ідентифікація російських військовослужбовців. Виявлення осіб, які беруть участь в гібридних війнах, які РФ веде на території інших країн. Факти із зазначенням їх військових звань і підрозділів;
- Розкриття фактів нелегального експорту зброї та військової техніки з Росії в зони конфліктів;
- Збір доказів, що підтверджують участь російських державних чиновників у війні в Україні або в плануванні підривних операцій і ведення воєн в інших країнах;

- Аналіз і прогнозування військово-політичної ситуації в Центральній і Східній Європі. Аналіз ситуації на Близькому Сході;
- Розвінчання брехні російської пропаганди;
- Викриття чутливої для агресора інформації, яка змушує його змінювати свої агресивні оперативно-тактичні або стратегічні плани, нести значні фінансові витрати.

Центр дослідження армії, конверсії та роззброєння (ЦДАКР) – громадська не урядова організація, яка заснована у 1999 році. ЦДАКР був створений як добровільне об'єднання фахівців в області професійного аналізу процесів роззброєння і озброєння (переозброєння) армій держав регіону, реформування силових структур, діяльності окремих підприємств і активності України на міжнародному ринку озброєнь. Крім того, ЦДАКР періодично звертається до тематики військово-цивільних відносин і цивільного контролю над силовими структурами, а також розвитку в Україні технологій оборонного та подвійного застосування. Експерти ЦДАКР активно працюють у сфері дослідження участі України в міжнародних режимах контролю за озброєннями і критичними технологіями.

Центр досліджень армії, конверсії і роззброєння:

– досліджує темпи, напрямки та наслідки реформування силових структур України, співпрацює з ними;
– вивчає тенденції та перспективи трансформації національної оборонної промисловості;
– здійснює постійний моніторинг і аналіз експорту та імпорту озброєнь, продукції подвійного призначення і чутливих технологій на пострадянському просторі, а також їх розповсюдження в світі.

Основними цілями діяльності ЦДАКР протягом останніх п'яти років стали:

– проведення незалежних досліджень у галузі зовнішньоекономічної діяльності українських компаній на світовому ринку озброєнь;
– аналіз військово-технічного співробітництва України з іноземними

державами, в тому числі, в області спільних розробок і імпорту технологій військового і подвійного призначення;

– незалежна експертиза реформування Збройних сил України та аналіз тенденцій розвитку армій регіону і світу;
– незалежні оцінки розвитку підприємств оборонно-промислового комплексу;
– дослідження потенціалу реалізації різних проектів у сфері безпеки і оборони держави.

Всі дослідження ЦДАКР проводить виключно шляхом багатофакторного аналізу відкритої інформації: публікацій ЗМІ, виступів офіційних осіб та експертів, форумів, міжнародних виставок та конференцій.

За час своєї діяльності ЦДАКР виступив організатором і учасником цілого ряду міжнародних конференцій і круглих столів, його представники виступали на міжнародних форумах в області безпеки і оборони в державах Європи та Азії, США і РФ.

Експерти ЦДАКР регулярно здійснюють публікації статей, досліджень і книг [48].

Український кризовий медіа-центр (УКМЦ) створено задля зміцнення української державності та підтримки іміджу України закордоном. Ми обрали нелегкий шлях – працювати зі складними темами, і у нас немає ілюзій щодо швидких рішень. Ми розуміємо важливість трансформаційних процесів, що відбуваються у нашій країні останніми роками, та визнаємо, завдяки яким людським жертвам вони стали можливими.

Візія УКМЦ:

Вільний демократичний світ, у якому Україна – невід'ємна частина Заходу. Україна – аванпост свободи і демократичного розвитку Східної Європи, від якої залежить безпека і майбутнє світової демократії.

Місія УКМЦ:

Через управління стратегічними комунікаціями, вести Україну від

Революції Гідності до Країни Гідності та сприяти розвитку самодостатньої Української держави і суспільства. Ми віримо, що цього можна досягнути лише спільними зусиллями та через просвітницьку роботу у тісній співпраці з нашими міжнародними партнерами.

Цінності УКМЦ:

Українська державність, патріотизм, відвага, неповторність та креативність, чесність і відповідальність. Ми заявляємо, що ніколи не підтримуватимемо російські наративи та імперіалізм; тих, хто ставиться до України як до проєкту; не погодимось працювати на російські кошти або з українськими бізнесменами і політиками, які працюються проти суверенітету нашої країни; не говоритимемо неправди; не працюватимемо на шкоду державі; не братимемо участі у політичних кампаніях; не будемо дезінформувати і принижувати людську гідність; робити те, у що ми не віримо; не приймемо поразки. Ми підтримуємо діячів і діячок, які сприяють державотворенню, представників громадських організацій та спільноту незалежних медіа – неформальний консорціум усіх тих, хто працює на благо українського народу.

Що робить УКМЦ:

Громадська організація «Український кризовий медіа-центр» постала у часі і дусі Революції Гідності у березні 2014 року, як швидке реагування на російську окупацію Криму та з метою захистити суверенітет України, її національні інтереси у глобальному інформаційному просторі. Від часу свого заснування УКМЦ розвинувся у центр міжнародних стратегічних комунікацій з активним поширенням інформації на аудиторії як в Україні, так і закордоном. Експертиза УКМЦ охоплює унікальний медіа-центр, виняткові проєкти у сфері реформування урядових комунікацій, медіа підтримку великим іноземним ініціативам з допомоги Україні, глибинну роботу з регіональними журналістами, комунікацію реформ, що тривають, події та заходи у сфері культури, поширення медійної грамотності молоді, комплексний аналіз дезінформаційної діяльності у медійному просторі.

Прес-центр – головний підрозділ УКМЦ. Він працює як хаб, де перетинаються усі сфери діяльності нашої Організації і який відкритий для наших партнерів, яким потрібна професійна підтримка медіа-заходів.

Інші напрями діяльності УКМЦ:

- Група з аналізу гібридних загроз;
- UCHOOSE – Обираєш ти!;
- Національні аудиторії: перезавантаження регіональних медіа;
- Комунікація реформи децентралізації.

За роки діяльності УКМЦ та наші різноманітні проєкти підтримували: Українська Світова Фундація, USAID, NED, EED, NATO, UNICEF, German Marshall Fund/Black Sea Trust, UNHCR, Spirit of America, Heinrich Boll Stiftung, the Institute for Statecraft, Естонський Центр Східного Партнерства, чеський аналітичний центр «Європейські цінності», Міжнародний Фонд Відродження, GIZ, Посольства США, Нідерландів, Швейцарії, Фінляндії, Норвегії, Швеції та Німеччини, а також інші поважні організації.

УКМЦ цінує свою репутацію, тож дотримується високих професійних та етичних стандартів у своїй діяльності, не допускає конфлікту інтересів та спілкується з партнерами на рівні виняткової досконалості. На підтвердження цього УКМЦ регулярно проходить міжнародні аудити своєї проєктної діяльності. Усі 13 таких аудитів, що пройшли від 2014 року, дали позитивні висновки про роботу УКМЦ [17].

Міжнародний центр протидії російській пропаганді (МЦ ПРП) – це неурядова організація створена фахівцями з комунікацій, психологами, журналістами, соціологами, діячами в сфері культури.

Мета центру – захист інформаційного простору від російської інформаційної агресії, координація міжнародних зусиль з протидії впливу російської пропаганди.

Центр не фінансується жодним урядом і діє виключно завдяки волонтерській праці свої активістів.

Головні напрямки нашої діяльності МЦ ПРП:

– Моніторинг та аналіз;
– Просвітництво;
– Міжнародна взаємодія.

Основні продукти Центру, які будуть створені та доступні, для використання в забезпеченні інформаційної безпеки держави:

– Навчальні програми для підготовки фахівців;
– Унікального аналітичного контенту (тематичні доповіді);
– Майданчики обміну інформацією;
– Програми моніторингу інформаційних загроз;
– Мережа оперативного поширення інформації.

Бюро протидії гібридній війні – недержавний центр, який у грудні 2015 року утворився двома центрами – Центром суспільних відносин та Фондом національних стратегій.

Головною метою роботи Бюро є допомога у виробленні державної політики в Україні у сфері протидії технологіям гібридної війни, сприяння виробленню спільної стратегії з НАТО та ЄС стосовно її мінімізації у Європі та запобіганню її розгортанню на інших територіях.

2.3. Аналіз державної політики забезпечення інформаційної безпеки України

Ефективний захист національних інтересів держави напряму залежить від того, як успішно здатна реагувати на загрози та виклики система забезпечення національної безпеки. В цій ситуації важливим аспектом є детальний аналіз внутрішнього та зовнішнього безпекових середовищ. Враховуючи взаємопов’язаність та взаємозалежність цих ключових складових національної безпеки та можливості держави, створюються гарні умови для ефективного та позитивного вирішення проблемних питань захищеності інтересів держави, суспільства та особи.

Серед багатьох методів, що застосовуються при організації та плануванні державної політики забезпечення інформаційної безпеки віддамо перевагу наступним: PEST, SWOT, OSINT - аналіз.

PEST-аналіз (іноді позначають як STEP) — аналітичний метод, який призначений для виявлення політичних (P — political), економічних (E — economic), соціальних (S — social) і технологічних (T — technological) аспектів зовнішнього середовища, які впливають на об'єкт дослідження.

Політика вивчається, бо вона регулює владу, яка визначає в свою чергу середовище об'єкту дослідження та отримання ключових ресурсів задля її існування. Головною причиною вивчення економіки є створення картини розподілу ресурсів в державі, що є найважливішою умовою діяльності країни. Також важливі аспекти визначаються при допомозі соціального компонента PEST-аналізу. Останній чинник – технологічний компонент, метою дослідження якого вважають виявлення тенденцій у технологічному розвитку. Результати PEST-аналізу оформляються у вигляді матриці, що дозволяє оцінити зовнішню ситуацію, яка певним чином впливає на об'єкт дослідження.

PEST-аналіз має різновиди. PESTLE - аналіз є розширеною двома факторами (Legal і Environmental) версією PEST-аналізу. Іноді застосовуються й інші формати, наприклад, SLEPT-аналіз (плюс правовий фактор) або STEEPLE-аналіз: економічний, політичний, соціально-демографічний, технологічний, довкілля (природний), правовий та етнічні фактори. Також може враховуватися і географічний фактор.

У сфері національної безпеки основний метод дослідження є PESTLE(M), де M (military) – воєнний аспект.

Цей аналітичний метод потужно використовується структурами сектору безпеки Великої Британії. На основі методу будують мапу ризиків національній безпеці держави, яку щорічно оновлюють.

Ще однією з успішних технологій з 60-х років минулого століття й до сьогодення є SWOT-аналіз, який широко застосовується у процесі

стратегічного планування, і полягає в розділенні чинників та явищ на чотири категорії: сильних (Strengths) і слабких (Weaknesses) сторін проекту, можливостей (Opportunities), що відкриваються при його реалізації, та загроз (Threats), пов'язаних з його здійсненням.

За допомогою традиційного методу SWOT-аналізу проводяться детальні дослідження зовнішнього та внутрішнього середовищ. Результат раціонального SWOT-аналізу, який спрямований на формування загального інформаційного потенціалу, дає появу ефективних рішень, які стосуються відповідного впливу (реакції) суб'єкта (сильної, середньої й слабкої) відповідно до сигналу (сильному, середньому або слабкому) зовнішнього середовища. SWOT-аналіз – це складова частина стратегічних планувань та прийняття стратегічних управлінських рішень.

SWOT-аналіз дозволяє нам визначати сучасний стан зовнішнього та внутрішнього безпекових середовищ в сфері інформаційної безпеки України.

Проаналізувавши відповідність політики держави щодо забезпечення інформаційної безпеки України приведемо матрицю SWOT-аналізу сучасного стану зовнішнього та внутрішнього безпекових середовищ в сфері інформаційної безпеки України.

Таблиця 2.1

Матриця SWOT-аналізу сучасного стану зовнішнього та внутрішнього безпекових середовищ в сфері інформаційної безпеки України.

Сильні сторони	**Слабкі сторони**
1. Потужний науковий потенціал у сфері інформатизації та зв'язку. 2. Велика кількість провайдерів зв'язку – інформаційно-телекомунікаційних компаній. 3. Велика кількість магістральних оптоволоконних ліній зв'язку. 4. Висока прибутковість та привабливість телекомунікаційної галузі.	1. Низька на світовому ринку конкурентна спроможність національної інформаційної продукції. 2. Недостатній рівень розвитку вітчизняної інформаційної інфраструктури. 3. Відставання у сфері телекомунікаційних технологій і засобів вітчизняних високотехнологічних виробництв.

Політична воля керівництва країни. Зміна етнопсихології українського суспільства. 7. Зменшення контенту російських ЗМІ в інформаційному просторі України. 8. Інформативний супротив інститутами громадянського суспільства України деструктивним інформаційним впливам. 9. Реформа органів державної влади сектору безпеки. 10. Створенняголовного органу контрпропаганди – Міністерства інформаційної політики України.	4. Недосконалий захист інформації від несанкціонованого доступу в результаті використання іноземної техніки та інформацій технологій. 5. Технологічна залежность держави від іноземних інформаційно-комунікаційних технологій. 6. Брак матриці загроз інформаційній безпеці України. 7. Квола захищеність від експансії інформації іноземних ЗМІ національного інформаційного простору. 8. Недостатнє інформаційне покриття на окупованих територіях України (Схід та Крим). 9. Недосконала нормативно-правова бази з питань забезпечення інформаційної безпеки. 10.Відсутня гармонізація та координація міжнародного та національного законодавства у сфері інформаційної безпеки. 11. Недосконала комунікація між громадянським суспільством та урядовими структурами , як наслідок виникає соціальна напруга, яку використовують проти інтересів держави. 12. Відсутня інтегрованість в єдину систему міжнародної інформаційної безпеки.
Можливості	**Загрози**
1. Стимулювання конкурентоспроможного виробництва національного інформаційного продукту та введення новітніх інформаційних технологій. 2. Забезпечення ефективної безпеки інформаційно-телекомунікаційних систем, які працюють в інтересах управління країною, забезпечують потреби безпеки та оборони держави, усіх сфер економіки, систем управління всіма об'єктами критичної інфраструктури. 3. Розробка і впровадження державних стандартів та технічних регламентів	1. Поширення недостовірної, упередженої та спотвореної інформації в зарубіжному інформаційному просторі, що завдає прямої шкоди національним інтересам держави. 2. Загроза безпечному та стабільному функціонуванню національних інформаційно-технологічних систем від проявів кібернетичної злочинності та кібернетичного тероризму. 3. Негативні інформаційні впливи, які спрямовані на підрив суверенітету, конституційного ладу, недоторканості кордонів і територіальної цілісності

застосування й використання інформаційно-комунікаційних технологій, які відповідають та поєднуються з міжнародними стандартами. 4. Створення та впровадження національної системи кібербезпеки і нормативно-законодавчої бази її забезпечення. 5. Створення та впровадження систем швидкого реагування інформаційним атакам, спецпідрозділів сектору безпеки для ведення інформаційно-психологічних операцій. 6. Забезпечення державою у сфері зв'язку та інформатизації конкурентоспроможних технологій.	України. 4. Порушення регламенту збирання, зберігання, обробки та передачі інформації з обмеженим доступом на підприємствах оборонно-промислового комплексу держави, органах військового управління, в сфері національної економіки. 5. Інформаційно-психологічний вплив на військове керівництво, особовий склад армії й військових формувань та населення України. 6. Незахищеність персональних даних громадян держави та електронних баз даних. 7. Гібридна війна Російської Федерації проти України. 8. Не вироблена система забезпечення інформаційної безпеки України. 9. Відсутність широкого мовлення суспільного телебачення та радіомовлення.

У вищенаведеній матриці SWOT-аналізу вказана реальна оцінка стратегічного стану України в сфері забезпечення інформаційної безпеки, з огляду відповідності поточної стратегії державної політики нацбезпеки до її внутрішніх ресурсів та міжнародного становища. Сильні сторони держави трансформують зовнішні можливості у реальні, підвищуючи ймовірність їх реалізації. Держава повинна перетворювати загрози працюючи над слабкими сторонами і реалізувавши необхідні стратегічні кроки на придатні стратегічні альтернативи.

Розвідка відкритих джерел (англ. Open source intelligence, OSINT) — концепція, методологія і технологія добування та використання військової, політичної, економічної та іншої інформації з відкритих джерел, без порушення законів. Використовується для прийняття рішень у сфері національної безпеки та оборони, і у сфері інформаційної безпеки України зокрема (рис. 2.4).

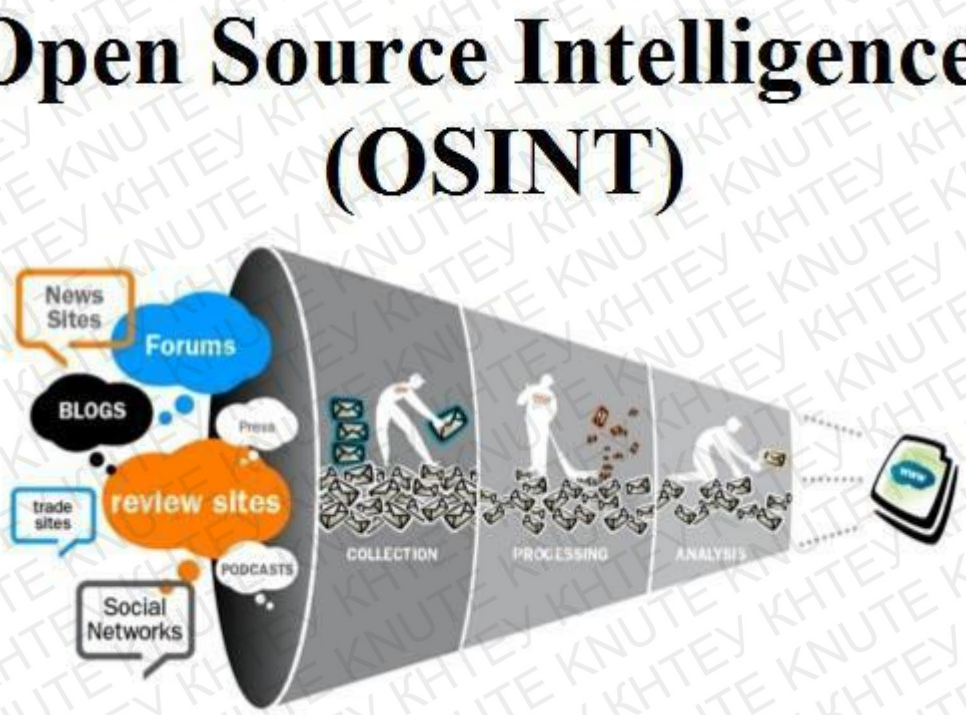

Рис. 2.4 Розвідка відкритих джерел

Джерело: [44]

OSINT включає в себе пошук інформації, її реєстрацію, облік та аналіз, аналітико-синтетичну переробку первинної інформації, зберігання й розповсюдження інформації, забезпечення безпеки інформації та презентація результатів досліджень. Первинна інформація з відкритих джерел після її аналітико-синтетичної переробки стають цінними знаннями, які після цього можуть стати секретними — якщо не відносяться до категорії інформації, яка не може бути віднесеною до державної таємниці.

Методи збору розвідувальної інформації в OSINT кардинально відрізняються від решти напрямів розвідувальної діяльності. До прикладу робота агентурної розвідки полягає в отриманні (добуванні) потрібної інформації з джерела, яке не завжди згодне до співпраці, що є головною проблемою в ії роботі. Натомість в OSINT головне питання – пошук надійних та змістовних джерел серед всієї кількості різнобічної інформації кібернетичного простору (рис. 2.5).

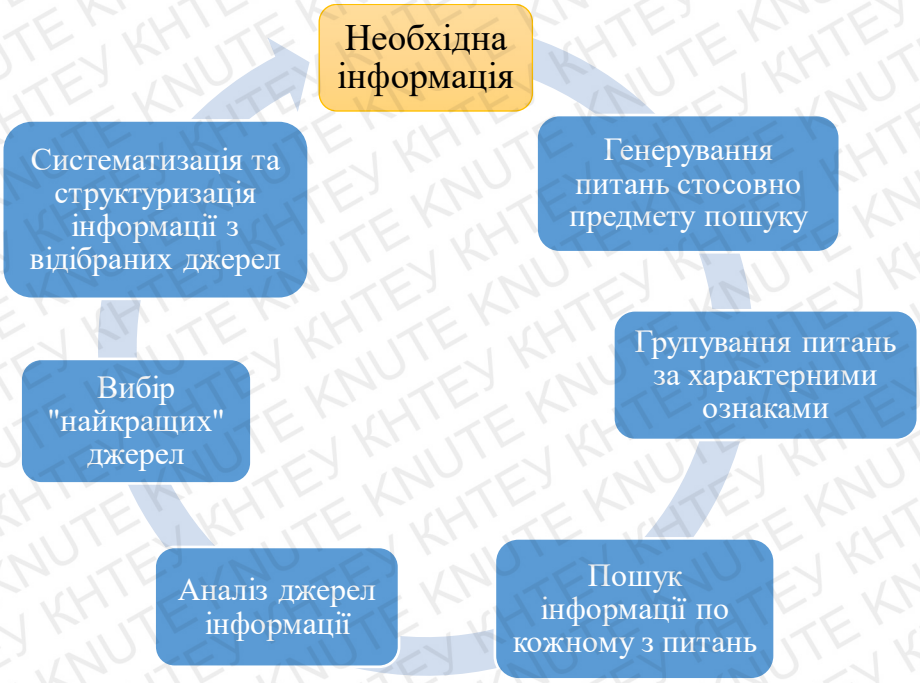

Рис. 2.5 Методика пошуку інформації з відкритих джерел за допомогою OSINT

Джерело: [44]

Сутність даної методики полягає у наступному: для отримання необхідної інформації стосовно проблеми необхідно сформувати велику кількість питань, класифікувати питання по специфічним ознакам, визначити залежності між групами і певними питаннями, виконати пошук інформації з усіх питань, проаналізувати на об'єктивність, достовірність, новизну джерела інформації, вибрати найкращі джерела, структурувати та систематизувати інформацію.

Як результат дослідження – отримання повної характеристики проблеми. Результати застосування даної методики кардинально відрізняються від звичайного пошуку інформації по проблемі, яка досліджується.

По різним оцінкам фахівців, розвідувальні служби США у відкритих джерелах кіберпростору дістають від 33% до 96% розвідувальної інформації, хоча витрати на OSTIN складають близько 1% всього американського розвідувального бюджету. Існує твердження аналітиків США, що майже 90% усіх розвідувальних даних добуваються з відкритих джерел та всього 10% припадає на роботу агентури [13].

Висновки до розділу 2

Отож, майбутнє держави Україна напряму залежить від ефективної державної політики, від здатності захистити та відстояти у власному інформаційному просторі національні й духовні цінності, від забезпечення стійкості та працездатності державних структур в надзвичайних ситуаціях і обстановці невизначеності.

Організація ефективного реагування державою на сьогоднішні виклики і загрози інформаційній безпеці повинно передбачати централізоване управління із детальними розпорядницькими функціями, що забезпечують моніторинг та контроль за усім національним інформаційним простором. У будь-яких ситуаціях система забезпечення безпеки інформації в Україні має бути скоординованою, багатобічною, багатоаспектною та володіти здатністю зберігання важливих параметрів свого функціонування.

Таким чином, щоб досягнути певного рівня безпеки інформації в Україні, необхідно сформувати єдиний механізм забезпечення інформаційної безпеки держави на основі вирішення наступних питань:

- створити системи нормативно-правових актів, які регулюватимуть відносини між об’єктами і суб’єктами діяльності, що виникають в області забезпечення інформаційної безпеки;
- організувати безпосередню діяльність державних органів влади і недержавних організацій стосовно забезпечення інформаційної безпеки держави, суспільства і особистості, а також через інтереси ефективно управляти цією діяльністю;
- побудувати системи забезпечення інформаційної безпеки України на основі головних принципів забезпечення безпеки;
- розробити механізм вироблення політичних рішень, їх виконання та контролю.

Розділ 3. ПРІОРИТЕТНІ НАПРЯМИ РОЗВИТКУ СИСТЕМИ МОНІТОРИНГУ ТА ОЦІНКИ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

3.1. Ідентифікація та захист об'єктів критичної інформаційної інфраструктури

Загрозу національній безпеці України несе збій у роботі інформаційно-комунікаційних систем і мереж, від яких повністю залежить сучасне суспільство. Дана ситуація безумовно може призвести до хаосу та навіть критичних втрат фінансових, матеріальних і людських ресурсів.

Сьогодні рівень та ефективність інформаційно-комунікаційних систем все більше визначає потенційні можливості розвитку сучасного суспільства. За допомогою найсучасніших інформаційних технологій держави можуть реалізовувати власні національні інтереси. Не застосовуючи воєнну силу до конкуруючої держави, яка не має чи в неї не достатня дієва система захисту від інформаційних впливів, можна послабити або завдати непомірної шкоди її безпеці.

Інформаційна складова в умовах розвитку суспільства стає дедалі більш вагомою та однією з найбільш важливіших елементів забезпечення національної безпеки. Власне тому питання забезпечення інформаційної безпеки в сучасному інформаційному суспільстві є першочерговими у порядку денному в системі управління національною безпекою державою. Для досягнення успіху та переваги у виконанні завдань у воєнно-політичній, інформаційній, соціальній, економічній та інших сферах потрібно ефективне проведення національної інформаційної політики. Матеріальна основа інформаційної інфраструктури кожної держави складається із засобів створення, пошуку, збору, прийому, поширення, зберігання, автоматизованої обробки та захисту інформації.

Стабільність розвитку цивілізованих країн залежить від стабільного функціонування об'єктів інфраструктури держави, які не в останню чергу

потребують забезпечення захисту. До таких об’єктів відносяться важливі для життєдіяльності держави, які отримали назву об’єкти критичної інфраструктури.

Об'єкти критичної інфраструктури — підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв (рис. 3.1).

Об'єкти критичної інфраструктури	урядові установи
	основна ресурсна база
	військові об'єкти
	морські порти
	нафто та газопроводи
	залізничні станції
	пам'ятки культурної спадщини
	інші об'єкти

Рис. 3.1 Об’єкти критичної інфраструктури

Джерело: [47]

Закон України «Про основні засади забезпечення кібербезпеки України» використовує термін «Критично важливі об'єкти інфраструктури», визначаючи їх як юридичні особи, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення

для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей.

Цей Закон також надає взаємопов'язане визначення об'єкт критичної інформаційної інфраструктури: комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури [32].

Аналізуючи досвід розвинених країн в питанні механізмів захисту критичної інфраструктури та ідентифікації елементів, секторів та об’єктів критичної інфраструктури, можемо констатувати, що провідні країни світу оприлюднили власні стратегії, які використовуючи різні методи, ідентифікують критичні інфраструктури своїх держав. Ідентифікувати критичність інфраструктури можна, наприклад, з огляду на можливості пошуково-рятувальних ресурсів та організацій, потік товарів і продукції, або елементів інфраструктури та вузлів. Однак не розроблено на сьогодні для ідентифікації критичних інфраструктур загальних критеріїв. Також суттєво різняться один від одного базові критерії та поняття критичних інфраструктур. Кожна країна з точки зору важливості послуг для держави, економіки та безпеки суспільства або критичності окремих галузей (секторів). Різні національні інтереси в залежності від рівня розвитку держави та регіону є головним бар’єром загальної стандартизації в сфері захисту критичної інфраструктури. Але серед усіх стратегій різних держав світу прослідковується ключова позиція критичної інфраструктури – безпека громадян, суспільства та держави.

Згідно Директиви Європейської Комісії кожна держава ідентифікує елементи критичної інфраструктури за наступними факторами, характеристиками, критеріями та ознаками:

– масштаб (географічно охоплена територія, на якій втрата хоча б одного з елементів критичної інфраструктури завдає серйозної шкоди);
– вплив на населення (кількість загиблих, постраждалих, осіб, які зазнали значних травм, а також число евакуйованого населення);
– економічна шкода (розмір прямих і непрямих економічних втрат, вплив на ВВП);
– екологічна шкода (вплив на навколишнє природне середовище та населення);
– взаємозв'язок з іншими елементами критичної інфраструктури;
– політичний ефект (втрата впевненості у дієздатності влади);
– тривалість впливу (як саме і коли проявляться наслідки, пов'язані з відмовою чи втратою об'єктів критичної інфраструктури).

Об'єкти інформаційної інфраструктури займають особливе місце в системі критичної інфраструктури держави. Їх ефективний захист є необхідним елементом забезпечення національної безпеки. До них слід віднести інформаційні системи та комп'ютерні мережі: сектора безпеки і оборони; органів місцевого самоврядування та державної влади; підприємства: енергетичні, хімічні, телекомунікаційні, транспортні, банківської системи та житлово-комунального господарства.

Враховуючи усі інформаційні компоненти можемо констатувати, що кожному об'єкту критичної інфраструктури необхідно:

- фізичний захист (захист від фізичного ураження);
- захист від кібератак та загроз;
- радіоелектронний захист (захисті від електромагнітного імпульсу та радіоелектронного подавлення);
- захист обслуговуючого персоналу (захист від інформаційно-психологічного впливу).

В Україні приділяється увага захисту надважливих об'єктів критичної інфраструктури. Для цього прийнято і введено в дію ряд законодавчих актів, які

визначають особливості та алгоритм забезпечення захисту критичної інфраструктури. До них можна віднести: Стратегію національної безпеки України, Воєнну доктрину України, Стратегію кібернетичної безпеки України, Указ Президента України №8/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури», проект Закону України «Про критичну інфраструктуру та її захист».

5 жовтня 2017 році Президент України Указом № 2163-VIII підписав Закон України «Про основні засади забезпечення кібербезпеки України» в змісті якого є визначення «критична інформаційна інфраструктура» та «об'єкт критичної інформаційної інфраструктури». Згідно п.15 Статті 1 критична інформаційна інфраструктура – сукупність об'єктів критичної інформаційної інфраструктури, а п.19 об'єкт критичної інформаційної інфраструктури - комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури [40].

3.2. Шляхи забезпечення безпеки інформації в Україні

Ефективними напрямками вдосконалення державної політики щодо забезпечення безпеки інформації в Україні під час агресії РФ проти України мають стати:

1. Впровадження у інформаційний простір національне суспільне мовлення, відновити суспільства до українських ЗМІ, впровадити прозорість медіа-ринку та провести його демонополізацію, що спричинить створення умов для розвитку незалежних ЗМІ. Необхідно розширити на території України можливості кабельних мереж країн ЄС та США, забезпечити присутність якісного українського інформаційного продукту в супутникових мережах, які доступні у мас-медійному просторі РФ та союзних їй держав пострадянського простору.

2. Постійний контроль за діяльністю українських Інтернет-ресурсів, які в

умовах інформаційної війни можуть бути створені в соціальних мережах російськими спецслужбами з метою організації та дестабілізації процесів в українському суспільстві, а також компаній, що діють в економічних, політичних, соціальних сферах і служать прикриттям для діяльності іноземних спецслужб.

3. Приділення уваги по роботі з елітами сусідніх країн (політиками, бізнесом, діячами культури). Створення інформаційного продукту для цієї категорії осіб, який повинен вирізнятися від звичайного інформаційного продукту споживання рівнем ерудованості. Організація для даної соціальної групи зустрічей, бізнес-конференцій, форумів, дискусій, прес-турів тощо. Створення спільних проектів з експертами громадських організацій інших країн для просування української позиції в світі.

4. Концентрування уваги по роботі з регіональними ЗМІ (область, район, місто тощо). Ініціювання заходів щодо їх добровільної організації у єдину команду і формування єдиної стратегії дій в інформаційній сфері.

5. Впровадження заходів із залученням представників ЗМІ щодо налагодження у військах політично-інформаційної роботи. Створення умов для ефективної співпраці представників ЗМІ з командуванням військових формувань.

6. Створення волонтерських політично-інформаційних бригад з числа представників центральних та регіональних ЗМІ, волонтерських організацій, творчої інтелігенції, студентів тощо. Головне завдання сформованих бригад – розголошення суспільно-важливої інформації та поширення проукраїнської позиції в суспільстві, підвищення до своєї держави рівня патріотизму у громадян, тощо.

7. Спрямування зусиль на формування політики історичної пам’яті держави Україна, в якій приділити увагу: національній пам’яті; розвінчуванню міфів «спільноруської» єдності; подоланню радянської, а на даний час і російської історичної міфології; презентації історичного минулого держави у

сучасний соціокультурний європейський простір тощо.

8. Розвінчування та викривання міфів російської пропаганди в Криму та на Сході України. Варто протидіяти пропагандистському впливу РФ не «оборонною» тактикою, а навпаки потрібно зайняти наступальну позицію. Для контрпропагандистського наступу державна інформаційна політика України, потребує ефективних стратегічних комунікацій, а саме побудову цілісного світосприйняття і просування його у всіх регіонах на всіх рівнях та будь якими державно-управлінськими методами.

Потрібно серед заходів із забезпечення інформаційної безпеки під час «гібридної війни» врегулювати доступ до національного інформаційного простору: ввести правовий режим, який передбачає заходи щодо заборони любого мовлення в інформаційному просторі України супротивника і організації радіоелектронної боротьби.

У разі прийняття необхідних нормативно-правових актів відбуватиметься етап впровадження цих положень в життєдіяльність держструктур, особливо структур сектора безпеки і оборони. Наступним етапом, не менш важливим, буде налагодження взаємодії між усіма суб'єкти забезпечення інформаційної безпеки, щоб усі працювали по єдиному плану та задуму. Даний «спеціальний режим» повинен стати ключовим інструментом стримування противника в інформаційному простору України.

На сьогодні можна констатувати, що:

- потужна пропагандистка компанія РФ є смисловою війною проти нашої держави, яка несе негативні наслідки для інформаційної безпеки України;
- громадянське суспільство та влада України повинні активніше використовувати потенціал інформаційної політики;
- великий відсоток населення має низьку довіру до інформаційної діяльності національних ЗМІ за необ'єктивне висвітлення подій в країні, незадоволений діяльністю влади;

– державна інформаційна політика має недоліки в контексті українсько-російської війни;
– у цільової аудиторії відсутнє цілісне сприйняття України як єдиної політичної нації та єдиної країни;
– побудова державної інформаційної політики не здійснюється як цілісна комунікативна кампанія;
– не враховуються і прогнозуються усі загрози інформаційній безпеці України та тенденції до їх появи, які виникають в інформаційному просторі;
– кібер-простір використовується переважно в цілях захисту, а не як простір для асиметричної відповіді противнику;
– державній інформаційній політиці України потрібно вдосконалення нормативно-правового та інституційного забезпечення розвитку інформаційного суспільства;
– весь хаотичний процес реалізації державної політики України необхідно змінити на системний.

Виходячи з вищезазначеного можна стверджувати, що пріоритетними напрямами державної політики забезпечення інформаційної безпеки України можна вбачати:

- формування та розвиток суб'єктів інформаційної безпеки на основі загальновизнаних цінностях нашого суспільства і основних принципах інформаційної безпеки;

- вдосконалення державної політики інформаційної безпеки з урахуванням реальних кількісно-якісних показників, що відображають життєво важливі інтереси держави, суспільства та особистості;

- встановлення недержавної системи страхування інформаційних ризиків, що гарантує захищеність життєво важливих інтересів держави, суспільства та особистості від загроз в інформаційній сфері.

Для впровадження політики забезпечення інформаційної безпеки у

найкоротші строки, необхідно здійснити ряд організаційних питань, а саме:

- реорганізація структури апарату РНБО, особливо тих підрозділів, які вирішують питання інформаційної безпеки на підприємствах та організаціях, що працюють з оборонним комплексом держави;

- використання у своїй діяльності принципи політико-адміністративного управління для підвищення рівня інформаційної безпеки

- обов'язково дублювати інформаційні системи та проводити резервування інформаційних ресурсів, враховуючи велику шкоду від застосування інформаційної зброї до державних систем управління;

- в діяльності РНБО пріоритетними напрямками визначити моніторинг рівня інформаційної безпеки, механізм реєстрації інформаційних загроз та мінімізацію небезпечних факторів, які породжують дані загрози;

- враховуючи сучасні завдання щодо захисту інформаційних ресурсів і комп'ютерних систем органів управління потрібен перегляд освітньої політики в цілому у державі та у військово-навчальних закладах зокрема.

3.3. Пропозиції для покращення ефективності функціонування Служби безпеки України у різних сферах діяльності держави для забезпечення інформаційної безпеки України

Функціонування різних сфер діяльності нашої держави в складних умовах сьогодення, як ніколи потребують покращення їх ефективності, саме для забезпечення інформаційної безпеки України. Пропонуємо розглянути пропозиції в наступних сферах, а саме: воєнній, зовнішньополітичній, внутрішньополітичній, економічній, науково-технологічній, законодавчій, протидії кібернетичній злочинності та функціонуванні органів державної влади.

Пропозиції у воєнній сфері. Розвиток інформаційної зброї зумовив виділення інформаційної боротьби в окремий інтегрований вид стратегічного забезпечення військових операцій які спрямовані на досягнення над противником інформаційної переваги завдяки комплексну використанню її складових за єдиним планом та замислом. Як наслідок у воєнній сфері

появилися нові форми ведення інформаційної боротьби: інформаційна операція та спеціальна оперативна інформація.

Підготовку висококваліфікованих фахівців для ведення кібернетичних війн та захисту інформаційного простору України від деструктивного інформаційного впливу сьогодні на відомчому рівні проводить Військовий інститут телекомунікацій та інформатизації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

Виходячи з вищенаведеного, пропонується:

1) удосконалити законодавство з усіх питань інформаційної безпеки у воєнній сфері з ціллю координації діяльності органів військового управління та органів державної влади під час рішення задач для забезпечення інформаційної безпеки;
2) безперервний аналіз застосування форм, засобів і способів інформаційної боротьби у воєнній сфері, окреслити напрямки забезпечення інформаційної безпеки;
3) удосконалити форми і способи протидії інформаційним операціям супротивника, спрямованими на послаблення обороноздатності держави; спеціальним інформаційним операціям, діям зовнішньої інформаційної агресії та різного деструктивного інформаційного впливу;
4) удосконалити від несанкціонованого доступу види і засоби захисту інформації у інформаційно-телекомунікаційних мережах, задіяних в управлінні військами та зброєю;
5) створити єдиний інформаційний простір України у воєнній сфері в інтересах функціонування і діяльності Збройних сил України (ЗСУ) та решти військових формувань Воєнної організації держави (ВОД);
6) міжвідомча кооперація та централізація підготовки кадрів з ведення інформаційної боротьби на базі Національного університету оборони України імені Івана Черняховського (керівний склад сектору безпеки) та

Військового інституту телекомунікацій та інформатизації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» (технічні спеціалісти).

Пропозиції у зовнішньополітичній сфері. Інформаційна політика України відкрита, орієнтована на дотримання прав громадян на інтелектуальну власність та інформацію. Держава повинна підтримувати вітчизняних виробників технологій, захищати внутрішній ринок від потрапляння на нього завуальованих елементів інформаційної зброї. Це насамперед важливо сьогодні, адже інформаційні технології здебільшого купуються за кордоном, в той час як існує тенденція до руйнування власного науково-технічного та виробничого потенціалу. З цією ціллю пропонується:

1) інтегрувати у міжнародні інформаційно-телекомунікаційні організації та системи на засадах економічної доцільності, рівноправності та збереження інформаційного суверенітету;
2) гарантувати на державному рівні вчасне виявлення загроз національному інформаційному суверенітету зовнішнього характеру, цілком відповідна реакція на них та нейтралізація;
3) приймати активну участь у створенні міжнародної законодавчої бази стосовно проблем інформаційної безпеки, де відображені були б найістотніші проблеми міжнародної спільноти і безумовно врахована специфіка національної інформаційної політики.

Пропозиції у внутрішньополітичній сфері. На державному рівні у внутрішньополітичній сфері пропонується:

1) створити і підтримувати мережеві соціальні структури, основне завдання яких – захист в інформаційному просторі національних інтересів України, формування громадської думки, нейтралізація негативних, підсилення позитивних та створення своїх інформаційно-психологічних впливів;

2) створити та розвивати у складі державного апарату професійні групи інформаційного-психологічного впливу із завданнями, як у мережевих соціальних структур, однак з більшими можливостями;
3) співпрацювати з громадськими організаціями, які налаштовані у патріотичному вихованні дітей та молоді, пропагують здоровий спосіб життя, виховують культуру сімейних та інших соціальних цінностей, підтримують творчість, екологічне виховання, відроджують українську культуру, цінності та традиції, пропагують їх та поширюють на міжнародному рівні, що безумовно підвищує рівень стабільності та соціальної гармонії в Україні, покращує міжнародний імідж нашої держави.

Пропозиції в економічній сфері. В економічній сфері пропонується:

1) підтримка державою вітчизняних виробників високотехнологічної продукції, в першу чергу комп'ютерно-телекомунікаційних технологій та засобів;
2) формувати вітчизняну індустрію інформаційних послуг, підвищувати ефективність використання державних, приватних і корпоративних ресурсів;
3) координувати законодавство України з питань інформаційної безпеки в економічні сфері з міжнародними стандартами і нормами;
4) забезпечити сталий розвиток національного медіа-ринку в період впровадження у державі цифрового телебачення;
5) посилити державний контроль за дотриманням вимог інформаційної безпеки у системах збирання, обробки, зберігання та передачі фінансової, біржової, статистичної, митної та податкової інформації;
6) комплексно інформатизувати процеси формування, розподілення та контролю по використанню бюджетних коштів;
7) удосконалити системи статистичної звітності з ціллю підвищення оперативності та достовірності звітної інформації.

Пропозиції в науково-технологічній сфері. З метою забезпечення конкурентоспроможності України в науково-технологічній сфері пропонується:

1) удосконалити системи захисту та охорони права інтелектуальної власності;
2) підтримка державою розвитку на міжнародному рівні науково-технічної співпраці в сфері забезпечення захисту інформації у системах телекомунікації;
3) враховувати вимоги забезпечення інформаційної безпеки України для науково-технологічного супроводу формування та розвитку інформаційного суспільства в Україні;
4) розширити можливості доступу громадян до наукової та науково-технічної інформації в світовому інформаційному просторі;
5) сприяти розвитку конкурентоспроможного вітчизняного виробництва засобів інформації та зв'язку, з ціллю зменшення, технічної, технологічної та стратегічної залежності від сторонніх держав.

Пропозиції в законодавчій сфері. Важливим фактором загроз національної безпеки України сьогодні є недовершеність нормативно-правового забезпечення в інформаційній сфері системи державного управління. Незважаючи на те, що більше 20 законів регулюють інформаційну сферу, їх переважна кількість в умовах розвитку новітніх технологій застаріла морально та суперечить один одному. Для вирішення цієї проблеми в комплексі пропонується:

1) Розробити та затвердити Концепцію національної інформаційної політики, розпочавши таким чином кодифікацію інформаційного законодавства;

2) Стратегію кібербезпеки України допрацювати відповідно до вимог Будапештської конвенція про кіберзлочинність (the Budapest Convention on Cybercrime) та більш виразно прописати повноваження і відповідальність державних суб'єктів забезпечення кібербезпеки.

Пропозиції щодо протидії кібернетичній злочинності. Стосовно протидії злочинам у кібернетичній сфері пропонується:

1) розробити нормативні документи, в яких описати загрози Україні у кіберпросторі, дати їх визначення та формувати єдину державну політику з кібербезпеки. Крім Стратегії кібербезпеки України потрібно розробити Закон України «Про кібербезпеку України», в якому уточнити: загрози кібернетичній безпеці; механізми розмежування повноважень та прийняття рішень; критерії зарахування об'єктів до критичної інформаційної інфраструктури, послідовність утворення переліку таких об'єктів; критерії віднесення до інформації з обмеженим доступом, інформації на об'єктах усіх форм власності, несанкціоновані дії стосовно якої викликають загрозу кібернетичній безпеці держави; повноваження державних структур стосовно впровадження заходів протидії кіберзагрозам на об'єктах усіх форм власності;

2) розробити механізми співпраці приватного та державного секторів у сфері забезпечення кібернетичної безпеки;

3) покращити кадрове забезпечення відомств належними фахівцями в сфері інформаційної безпеки;

4) створити державні міжвідомчі координаційні структури, які можуть координувати та узгоджувати діяльність усіх силових відомств в моменти здійснення слідчих дій у кіберпросторі та при створенні продуктивної системи захисту державного кіберпростору, насамперед у військовій сфері;

5) створити національну операційну систему для застосування в системі органів державної влади, відновити вітчизняні потужності з виробництва телекомунікаційної бази, стимулювати державою створення національного антивірусу;

6) створити Єдину загальнодержавну систему протидії кіберзлочинності;

7) змінити принципи фінансової підтримки державою вітчизняних досліджень у сфері боротьби та попередження кіберзлочинності;

8) підвищити у сфері боротьби з кібернетичними злочинами рівень технологічного і технічного оснащення та професійних знань працівників правоохоронних органів (СБУ, МВС, тощо).

Пропозиції щодо підвищення ефективності функціонування органів державної влади. Система державного управління в сфері інформаційної безпеки має низьку ефективність. Це зумовлено тим, що крім 6-ти провідних органів державної влади (Національна рада України з питань телебачення і радіомовлення, Міністерство інформаційної політики України, Міністерство інфраструктури України, Міністерство юстиції України, Державний комітет телебачення і радіомовлення України, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації) в країні діють понад 20, які у сфері інформаційної безпеки виконують завдання в тій чи іншій мірі. В таких умовах головні проблеми витікають з недосконалості нормативно-правової бази та складнощів координації й контролю за виконанням завдань стосовно забезпечення інформаційної безпеки та інформатизації. З огляду на те, натомість конструктивній роботі вищезазначені органи велику частку зусиль марнують на міжвідомчі суперечки.

Державна інформаційна політика в сфері інформаційного протиборства має базуватися на методологічних та наукових розробках, об’єднаних та систематизованих в одну концепцію. Вона може бути представлена як сукупність національних цілей, інтересів та цінностей, стратегії і тактики управлінських рішень та методів їх реалізації, які розробляються та реалізуються державною владою для регулювання та удосконалення як безпосередньо процесів інформаційної взаємодії в усіх сферах життєдіяльності суспільства та держави, так і процесів технологічного забезпечення такої взаємодії.

Висновки до розділу 3

Для покращення та посилення інформаційної безпеки держави

пропонуємо наступні кроки:

1. Необхідно розкрити специфічні сегменти, які потребують реорганізації у сфері інформаційної безпеки. До прикладу, здійснити комплексні аудити (комунікаційний, технічний, освітній та правовий) у сфері інформаційної безпеки в усіх державних органах із притягненням зацікавлених суб'єктів.
2. На підставі виявлених уразливостей та недоліків, з фахівцями в сфері інформаційної безпеки, виробити національну стратегію інформаційної безпеки та реальний план її виконання.
3. Почати виконання реформи інформаційної безпеки.

З метою покращення та посилення захисту інформації, яка становить державну таємницю, необхідно на об'єктах інформаційної діяльності:

- з боку міністерств та відомств посилити контроль за підпорядкованими установами стосовно питань охорони державної таємниці;
- в державному бюджеті передбачити статті видатків з криптографічного та технічного захисту інформації;
- виробити систему інвестування та державної підтримки вітчизняних проектів та виробництв, які спрямовані на створення новітніх інформаційно-технічних засобів та технологій захисту;
- покращити рівень підготовки фахівців у галузі захисту інформації, яка становить державну таємницю.

Для покращення протидії негативним інформаційно-психологічним впливам, операціям та війнам з боку владних органів держави пріоритетними напрямами та важливими кроками потрібно:

1) інтегрувати Україну до світового та регіонального європейського інформаційного просторів;
2) інтегрувати у міжнародні інформаційні та інформаційно-телекомунікаційні системи та організації;

3) створити власну національну модель інформаційного простору та забезпечити розвиток інформаційного суспільства;
4) модернізувати усю систему інформаційної безпеки держави та формувати й реалізовувати ефективну інформаційну політику;
5) удосконалити законодавство з питань інформаційної безпеки, узгодити національне законодавство з міжнародними стандартами та дієвим правовим регулюванням інформаційних процесів;
6) здійснити розвиток національної інформаційної інфраструктури;
7) підвищити конкурентоспроможність вітчизняної інформаційної продукції та інформаційних послуг;
8) впровадити сучасні інформаційно-комунікативні технології у процеси державного управління;
9) налагодити ефективну взаємодію органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригуванні державної політики в інформаційній сфері.

Для покращення інформаційної безпеки України та з метою недопущення інформаційної експансії, в інформаційному просторі держава повинна здійснювати за наступними напрямами:

1) реалізовувати упереджувальну стратегію та тактику (превентивні заходи);
2) здійснювати реагувальну стратегію (оперативне реагування на інформаційні атаки супротивника та активний наступ);
3) захищати національний інформаційний простір.

Головна ціль – забезпечення в інформаційному просторі домінування та медійної переваги. Окрім цього в пріоритеті інформаційних структур державних органів мають бути: контроль за інформаційними потоками; надання об’єктивної, вичерпної інформації, представлення фахових коментарів та пояснень щодо подій; систематичне висвітлення офіційної позиції посадових осіб та політичних лідерів.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

В роботі проаналізовано та узагальнено теоретичні підходи до визначення загроз інформаційної безпеки України. Проведено аналіз сучасного стану інформаційної безпеки в Україні. Виокремлено основні види загроз в сучасних умовах. Запропоновано напрями удосконалення інформаційної безпеки.

На основі результатів роботи сформульовано наступні висновки.

1. Узагальнено теоретико-методологічні підходи стосовно державної політики інформаційної безпеки України.

З позицій системного підходу доведено, що система забезпечення інформаційної безпеки держави являє собою відкриту систему зі специфічними функціональними і структурними елементами, яка має власні внутрішні зв'язки та зв'язки з навколишнім середовищем, розвивається й функціонує під впливом численних факторів (як соціальних, так і природних).

Розкрито своєрідність реалізації нинішньої політики інформаційної безпеки держави, яка з одного боку полягає у врахуванні, появи нових глобальних інформаційних загроз і викликів сучасного світу, геополітичної конкуренції в інформаційному просторі, відсутності міжнародного законодавства, що регулює зростання загроз міжнародній інформаційній безпеці, а з другого – національного виміру сучасних загроз, змістом яких є ведення проти України інформаційної та смислової війни Російській Федерації.

2. Досліджено механізми державного реагування на сучасні загрози інформаційній безпеці та шляхи забезпечення безпеки інформації в Україні.

Організаційні та нормативно-правові механізми державної політики забезпечення інформаційної безпеки знаходяться на стадії розвитку та становлення.

Встановлено, що в загальному організаційно-правовий механізм державної політики інформаційної безпеки є систематизованим комплексом інститутів держави, які задіяні в процесі створення та запровадження політики інформаційної безпеки, зовнішні й внутрішні відносити і ролі якої регулює

система правових норм і принципів. Вказаний організаційно-правовий механізм згідно до визначених напрямків впровадження політики інформаційної безпеки об'єднує три взаємопов'язані елементи.

По-перше, це сукупність інституцій держави (інститутів громадянського суспільства та інститутів публічної влади), задіяних в процесі створення та запровадження політики інформаційної безпеки, або інакше інституціональний механізм інформаційної безпеки.

По-друге, це сукупність відносин і ролей, яка містить правові відносини, що з'являються в процесі здійснення політики інформаційної безпеки, та характерні ролі, методі і форми діяльності суб'єктів здійснення політики інформаційної безпеки.

По-третє, це ступенева сукупність правових норм і принципів, які регулюють зміст та процес здійснення політики інформаційної безпеки.

Можемо стверджувати, що ефективність та продуктивність захисту інформаційної безпеки держави забезпечується ефективністю та продуктивністю кожної складової її механізму.

Одним з шляхів для досягнення високого рівня безпеки інформації в Україні, є формування єдиного механізму забезпечення інформаційної безпеки держави на основі вирішення наступних питань:

- створення системи нормативно-правових актів, які регулюватимуть відносини між об'єктами і суб'єктами діяльності, що виникають в області забезпечення інформаційної безпеки;
- організація безпосередньої діяльності державних органів влади і недержавних організацій стосовно забезпечення інформаційної безпеки держави, суспільства і особистості, а також через інтереси ефективно управляти цією діяльністю;
- побудова системи забезпечення інформаційної безпеки України на основі головних принципів забезпечення безпеки;
- розробка механізму вироблення політичних рішень, їх виконання та

контролю.

3. Обґрунтовано необхідність взаємодії недержавних і державних суб'єктів забезпечення інформаційної безпеки в умовах ведення військових та антитерористичних операцій. Зроблено висновок, згідно якого недержавна система забезпечення інформаційної безпеки України в умовах збройної агресії Російської Федерації проти України стала дієвим механізмом забезпечення інформаційної безпеки, яку визнано на найвищому міжнародному рівні.

4. Розкрито специфіку та сутність захисту об'єктів критичної інформаційної інфраструктури. На основі роботи можемо стверджувати, що кожен об'єкт критичної інформаційної інфраструктури потребує:

– фізичного захисту (від фізичного ураження);
– радіоелектронного захисту (від радіоелектронного подавлення та електромагнітного імпульсу);
– захисту від кіберзагроз;
– захисту обслуговуючого персоналу від інформаційно-психологічного впливу та соціальної інженерії.

Приведено визначення понять «критична інформаційна інфраструктура» та «об'єкт критичної інформаційної інфраструктури». Так критична інформаційна інфраструктура тлумачиться як комплекс інформаційно-телекомунікаційних та інформаційно-аналітичних систем державних і недержавних суб'єктів, знищення або ураження яких призведе до виникнення загроз національній безпеці, а об'єкт критичної інформаційної інфраструктури – як критично важливий об'єкт ІТ та ІА системи, порушення функціонування або знищення якого може призвести до втрати управління ним державними і недержавними суб'єктами, суттєвого зниження рівня безпеки людини, суспільства та держави, негативного впливу на природне середовище і великих фінансових збитків.

Однак уведення терміна «критична інфраструктура» в законодавство України не може бути кінцевою метою. Концепція критичної інфраструктури

повинна стати підґрунтям дієвого механізму координації зусиль органів влади та інститутів громадянського суспільства, які спрямовані на недопущення втрати чи завдання непоправної шкоди найважливішим для життєдіяльності держави об'єктам, з урахуванням негативних факторів будь-якого походження: соціально-політичного, техногенного, природного, або їх комбінації.

5. Здійснено аналіз застосування методів PEST, SWOT, OSINT-аналізу при організації та плануванні державної політики забезпечення інформаційної безпеки України. В процесі дослідження встановлено, що одним із найуспішніших системних технологій, який дає можливість оцінити у комплексі вплив внутрішніх та зовнішніх чинників, слабкі та сильні сторони і можливості держави, які впливають певним чином на стан захищеності інтересів держави, суспільства та особи в інформаційній сфері є SWOT-аналіз. У результаті застосування методу SWOT-аналізу побудована матриця сучасного стану зовнішнього та внутрішнього безпекових середовищ в сфері інформаційної безпеки України, яка дозволяє розробити рекомендації стосовно покращення ефективності функціонування різних сфер діяльності держави для забезпечення інформаційної безпеки України.

6. Сформульовані пропозиції для покращення ефективності функціонування різних сфер діяльності держави для забезпечення інформаційної безпеки України, а саме: воєнній, зовнішньополітичній, внутрішньополітичній, економічній, науково-технологічній, законодавчій, протидії кібернетичній злочинності та функціонуванні органів державної влади.

Також визначені кроки для покращення та посилення інформаційної безпеки держави, захисту інформації, яка становить державну таємницю, протидії негативним інформаційно-психологічним впливам, операціям та війнам з боку владних органів держави, інформаційної безпеки України та з метою недопущення інформаційної експансії, в інформаційному просторі держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Адаськов О.І. Рекомендації щодо проведення інформаційних заходів в мережі інтернет в інтересах виконання завдань інформаційно психологічних операцій. / Збірник наукових праць військового Інституту Київського національного університету імені Тараса Шевченка. - № 45 – К.: ВІКНУ, 2018. – С. 57 – 67.
2. Бабенко А.К. Паралельні алгоритми для вирішення задач захисту інформації / А.К. Бабенко // Інститут комп'ютерних технологій і інформаційної безпеки. – 2015. – 227 с.
3. Богуш В. Інформаційна безпека держави/ В. Богуш, О. Юдін // – К.: «МК-Прес», 2017. – 432 с.
4. Бурячок В.Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства / В.Л. Бурячок // Сучасна спеціальна техніка. – 2011. – № 3 (26). – С. 104-114.
5. Валюшко І.О. Основні виклики і загрози в епоху інформаційних війн. / І. О. Валюшко // Науковий вісник Дипломатичної академії України. Зовнішня політика і дипломатія: традиції, тренди, досвід. Серія«Політичні науки» / За заг. ред. В.Г. Ціватого, Н.О. Татаренко. – 2019. – Випуск 23. Частина ІІ. – С. 142–147.
6. Гавловський В.Д Щодо проблем боротьби із злочинами, що вчиняються з використанням комп'ютерних технологій / В.Д. Гавловський //Боротьба з контробандою: проблеми та шляхи їх вирішення. -К. НДІ «Проблем людини»., 2018. – С.148-154.
7. Гаврилюк Я.М. Теоретичні засади моніторингу загроз інформаційної безпеки України / Н.Л. Новікова. // Публічне управління та адміністрування в умовах суспільних трансформацій : зб. наук. ст. студ. відп. ред. – К.: Київ. нац. торг.-екон. ун-т, 2020. – 251 с.

8. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть / О.М. Горбатюк // Вісник Київського університету імені Т.Шевченка. – 2015. – Вип. 14: Міжнародні відносини. – С. 46-48.
9. Горбулін В.П. Проблеми захсту інформаційного простору / В.П. Горбулін // Інтертехнологія – К.: Київ, 2017. – 134 с.
10. Гулак Г.М. Завдання, форми та способи ведення воєн у кібернетичному просторі / Г.М. Гулак // Наука і оборона. – 2011. – № 3. – С. 35-42.
11. Данільян О.Г. Національна безпека України: сутність, структура та напрямки реалізації / О.Г. Данільян, О.П. Дзьобань, М.І. Панов. – Х.: «ФОЛІО», 2018. – 296 с.
12. Дмитренко М.А. Спеціальні інформаційні впливи // Збірник наукових праць Інституту СЗРУ – 2017. - № 8. – С. 156-167.
13. Дубов Д.В. Інформаційне суспільство в Україні : глобальні виклики та національні можливості : аналіт. доп. / Д. В. Дубов // – К.:НІСД, 2017. – 64 с.
14. Ільницька У.В. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам: [Електронний ресурс] / Ільницька Ульяна – Режим доступу: science.lpnu.ua/sites/default/files/journal.../ilnicka0.pdf
15. Інформаційна безпека: [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0
16. Конституція України : [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
17. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України / Б.А. Кормич: [монографія]. – Одеса: Юридична література, 2016. – 472 с.
18. Корочанський О.Е. Проблеми юридичної деліктології в інформаційних відносинах / О.Е. Корочанський // Бізнес і безпека. – 2018. – № 6. – С.19-21.

19. Косогов О.М. Модель динаміки зміни рівня інформаційної безпеки системи / О.М. Косогов // Зб. наук. праць. – К.: ЦВСД НУО імені І. Черняховського, 2018. – №2 (54). – С. 76-79.
20. Краус Н.М. Інституційні аспекти кластеризації в інноваційній економіці під впливом системної та комплексної модернізації / Н.М. Краус // Інституційні аспекти кластериза – К.: Київ, 2014 – 150 с.
21. Ларін С.В. Сутність та зміст поняття "національні цінності" в контексті сучасних дослідницьких підходів / С.В. Ларін. // Вісник НАДУ при Президентові України. – 2016. – №2. – 44-49 с.
22. Левченко О.В. Погляди на створення системи інформаційної безпеки України та її Збройних Сил / Ю. Радковець, О. Левченко, О. Косогов // Наука і оборона. – 2016. – № 1. – С. 38-42.
23. Лєнков С.В. Метод предикативної ідентифікації процесів для захисту від прихованих загроз в середовище хмарних обчислень. / В.М. Джулій, О.В. Селюков, І.В. Муляр //Збірник наукових праць військового Інституту Київського національного університету імені Тараса Шевченка. - № 55 – К.: ВІКНУ, 2017. – С. 145-155.
24. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський // – К.: КНТ, 2018. – 280 с.
25. Мануйлов Є.М. Калиновський Ю.Ю. Аксіологічний вимір інформаційної безпеки української держави / С.В. Мануйлов. // Вісник Національного університету "Юридична академія України імені Ярослава Мудрого". – 2017. – № 3 (34). – 13-30 с.
26. Марутян Р.Р. Рекомендації щодо вдосконалення політики забезпечення інформаційної безпеки України [Електронний ресурс] / Р.Р. Марутян. – Режим доступу: http://www.dsaua.org/index.php?option=com_content&amp view=article&id=198%3A2014-08-13-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk

27. Марущак А.І. Щодо поняття «інформаційні ресурси держави» / А.І. Марущак // Інформаційна безпека людини, суспільства, держави. – 2016. – №1 (1). – С. 11-15.
28. Нікіфоров М.М. Аналіз загроз воєнної безпеки держави в інформаційній сфері / М.М. Нікіфоров // – К.: Київ, 2019. – 187 с.
29. Петрик В.К. Сутність інформаційної безпеки держави, суспільства та особи: [Електронний ресурс] / В.К. Петрик. – Режим доступу: http://www.justinian.com.ua/article.php?id=3222
30. Пєвцов Г.В. Концептуальні підходи щодо забезпечення інформаційної безпеки у воєнній сфері / Г.В. Пєвцов, С.В. Залкін, А.О. Феклістов // Системи обробки інформації. – Х.: ХУПС, 2017. – Вип. 2 (92). – С. 57-59.
31. Погорецький М.А. Оперативно-розшукова інформація: до визначення поняття / М.А. Погорецький // Вісник Харківського національного університету внутрішніх справ. – 2007. – № 36. – С. 13-19.
32. Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави: Постанова : [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF#n10
33. Почепцов Г.Г. Сучасні інформаційні війни / Г. Почепцов. – К. : Вид.дім “Києво-Могилянська академія”, 2016. – 497 с.
34. Про Доктрину інформаційної безпеки України: [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/514/2009
35. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України : [Електронний ресурс]. – Режим доступу: http://www.zakon5.rada.gov.ua /laws/ show/n0004525- 14.
36. Про інформацію: Закон України [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2657-12

37. Про Міністерство: Міністерство інформаційної політики України [Електронний ресурс]. – Режим доступу : https://mip.gov.ua/content/pro-ministerstvo.html?PrintVersion
38. Про Міністерство освіти і науки України: Положення : [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/630-2014-%D0%BF#n8
39. Про основи національної безпеки України : Закон України [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/964-15#Text
40. Про основні засади забезпечення кібербезпеки України: Закон України : [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19
41. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/537-16
42. Про Раду національної безпеки і оборони України: Закон України : [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text
43. Про Службу безпеки України: Закон України : [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2229-12#Text
44. Розвідка відкритих джерел: [Електронний ресурс]. – Режим доступу : https://www.in4sec.com.ua/razvedka-na-osnove-otkry-ty-h-istochnikov-open-source-intelligence-osint/osint/
45. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір /Т.Ю. Ткачук. : [Монографія]. – Київ: «Видавничий дім «АртЕк», 2018. – 422 с.
46. Угрімов В.В. Кібернетична безпека: характерні ознаки, існуючі поняття і визначення. стан питання в ГУР МО України, на державному рівні та у світі / В.В. Угрімов // Вісник воєнної розвідки. – 2013. – 227 с.

47. Український кризовий медіа-центр : [Електронний ресурс]. – Режим доступу : https://uacrisis.org/uk/
48. Центр дослідження армії, конверсії та роззброєння: [Електронний ресурс]. – Режим доступу : https://cacds.org.ua/
49. Цимбалюк В.С. Інформаційне право України. / В.С. Цимбалюк // Навчально-методичний комплекс. – К.: Київ, 2017. – 258с.
50. Шемчук В.В. Теоретико-правові засади дослідження інформаційної безпеки. Європейські перспективи / В.В. Шемчук // – Тернопіль: «Джура», 2019. – 5–11 с.

Київський національний торговельно-економічний університет
Кафедра публічного управління та адміністрування

РЕФЕРАТ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на тему:

«МОНІТОРИНГ ТА ОЦІНЮВАННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ»

Студентки 2 курсу, 4 групи,
спеціальності 281 «Публічне управління та адміністрування»
спеціалізації «Публічне управління та адміністрування» _____ (підпис студента) Гаврилюк Яни Миколаївни

Науковий керівник
кандидат екон. наук,
доцент _____ (підпис керівника) Сонько Юлія Анатоліївна

Гарант освітньої програми
д-р. екон. наук,
доцент _____ (підпис гаранта) Ладонько Людмила Степанівна

Київ 2020

Випускна кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел (50 найменувань). Основний зміст роботи викладено на 68 сторінках комп'ютерного тексту. Робота містить 8 рисунків, 1 таблицю.

Метою роботи є дослідження стану захищеності інформаційної безпеки та аналіз наявних загроз національним інтересам держави в інформаційній сфері.

Поставлена мета зумовила необхідність вирішення таких дослідницьких завдань:

– розкрити теоретичні положення інформаційної безпеки;
– визначити загрози інформаційній безпеці України;
– розкрити своєрідність реалізації нинішньої політики інформаційної безпеки;
– дослідити механізми державного реагування на сучасні загрози інформаційній безпеці;
– висунути пропозиції для покращення ефективності функціонування різних сфер діяльності держави для забезпечення інформаційної безпеки України.

Об'єктом дослідження є процес проведення моніторингу та оцінки загроз інформаційної безпеки.

Предметом дослідження є теоретичні та прикладні основи забезпечення інформаційної безпеки за матеріалами Служби безпеки України.

Для вирішення визначених завдань, у процесі дослідження використано загальнонаукові та спеціальні методи.

У першому розділі розкриваються багатогранність сутності інформаційної безпеки та розглядаються види загроз.

У другому розділі здійснюється дослідження розвитку та удосконалення інформаційної безпеки, оцінка шляхів забезпечення безпеки інформації.

У третьому розділі розкриваються напрями розвитку інформаційної безпеки, застосовано PEST, SWOT, OSINT – аналізу аналізу при організації та плануванні державної політики забезпечення інформаційної безпеки України та викладено пропозиції щодо покращення ефективності функціонування різних сфер діяльності держави для забезпечення інформаційної безпеки України.

Одержані результати можуть бути використані при удосконаленні безпеки інформації в Україні.

Анотація

У випускній кваліфікаційній роботі проаналізовано та узагальнено теоретичні підходи до визначення загроз інформаційної безпеки України. Проведено аналіз сучасного стану інформаційної безпеки в Україні. Виокремлено основні види загроз в сучасних умовах. Проведено дослідження розвитку та удосконалення інформаційної безпеки, оцінка шляхів забезпечення безпеки інформації та викладено пропозиції щодо покращення ефективності функціонування різних сфер діяльності держави для забезпечення інформаційної безпеки України.

Annotation

In the final qualification work it is analyzed and summarized theoretical approaches to identifying threats to the information security of Ukraine. The analysis of the current state of information security in Ukraine is carried out. The main types of threats in modern conditions are singled out. It was helt the development and improvement of information security, assessment of ways to ensure information security and proposals are set out for improving the efficiency of various areas of the state to ensure information security of Ukraine.

Ключові слова: інформаційна безпека, загрози, захист інформації, кіберпростір, моніторинг, ідентифікація, інформаційна інфраструктура.

Завідувачу кафедри публічного управління та адміністрування Новіковій Н.Л.

Заява

Я, Гаврилюк Яна Миколаївна,

повідомляю, що за результатами здійснення самостійної перевірки з використанням програмно-технічних засобів у наданій випускній кваліфікаційній роботі на тему: «Моніторинг та оцінювання загроз інформаційній безпеці України» не міститься елементів академічного плагіату. У випадках використання прямих запозичень з друкованих та електронних джерел, вказані відповідні посилання.

Робота для перевірки надається у друкованому та електронному варіантах. Електронна версія роботи ідентична з друкованою.

«13» листопада 2020 року

(підпис)

Згода

Я, Гаврилюк Яна Миколаївна,

цим засвідчую, що є автором випускної кваліфікаційної роботи на тему: "Моніторинг та оцінювання загроз інформаційній безпеці України"

несу повну відповідальність за достовірність, точність та повноту поданої у роботі інформації, жодна частина роботи не була скопійована, за винятком випадків, коли робиться належне підтвердження в присвоєнні. Я підтверджую, що у роботі не міститься державної таємниці або інформації для службового користування.

Цим засвідчую, що жодна частина цієї роботи не була опублікована мною раніше.

Я даю дозвіл на те, що моя робота буде направлена в інституційний депозитарій Київського національного торговельно-економічного університету і збережена в базі даних для майбутньої перевірки плагіату.

«23» листопада 2020 року _____ (Гаврилюк Я.М.)

Підпис *Прізвище, ініціали*

РЕЦЕНЗІЯ

на випускну кваліфікаційну роботу на тему

«Моніторинг та оцінювання загроз інформаційної безпеки України»,

студентки ОС «Магістр»

спеціальності «Публічне управління та адміністрування»

Київського національного торговельно-економічного університету

Гаврилюк Яни Миколаївни

Випускна кваліфікаційна робота виконана на актуальну тему. Інформаційна безпека є однією з важливіших складових національної безпеки держави. Майбутнє держави Україна безпосередньо залежить від ефективної державної політики в цій сфері, від здатності захистити та відстояти у власному інформаційному просторі національні й духовні цінності, від забезпечення стійкості та спроможності державних структур в умовах впливу зовнішніх та внутрішніх загроз.

Інформаційний простір є однією з основних категорій інформаційної безпеки. Національний інформаційний простір являє собою середовище інформаційного обміну задля створення нової інформації, її захисту та використання. Розбудова власного інформаційного простору є однією з передумов соціально-економічного, політичного й культурного розвитку держави.

На думку автора, на урядовому рівні необхідно остаточно врегулювати питання захищеності основних інформаційно-телекомунікаційних ресурсів, вдосконалити організаційні та правові процеси управління інформаційною безпекою та безупинно здійснювати забезпечення держави інтелектуальними та трудовими ресурсами. щоб досягнути певного рівня безпеки інформації в Україні, необхідно сформувати єдиний механізм забезпечення інформаційної безпеки держави.

Випускна кваліфікаційна робота є актуальною та містить практичні рекомендації. Робота відповідає основним вимогам та може бути допущеною до захисту.

Заступник керівника Служби з питань інформаційної безпеки та кібербезпеки – керівник управління інформаційної безпеки Апарату Ради національної безпеки і оборони України
кандидат технічних наук, с.н.с

В.П.Звєрєв

Підпис Звєрєва засвідчую
Державний експерт служби управління персоналом Апарату Ради національної безпеки і оборони України
11 2020 р.

ПРОВЕРКА ТЕКСТА НА УНИКАЛЬНОСТЬ > **РЕЗУЛЬТАТЫ**

PRO Купить за 79,00 ₽ | Зарегистрированные | Гости | Время пр

Новый текст | 0 текстов в очереди | 1 текст в очереди | 2 текста в очереди

Проверка уникальности

Уникальность: 88.98%

www.president.gov.ua/documents/472017-2... 11%
zakon.rada.gov.ua/go/47/2017 10%

Подробнее

Проверка орфографии

В данном тексте ошибки не найдены.

Подробнее

SEO-ана

Всего
Без
Колич

Подсвечено: Неуникальные фрагменты

можливості комунікації;
• постійно підвищувати медіа-грамотність громадян, сприяти підготовці компетентних працівників-професіоналів для медіа-сфери;
• необхідно замість аналогового мовлення покрити усю територію країни цифровим та інтернет-мовленням та надати однакових можливостей доступу кожному громадянину до інформаційних ресурсів мережі Інтернет;
• оперативно задовольняти об'єктивною та достовірною інформацією населення тимчасово окупованих територій.
4) Щоб забезпечити інформаційну безпеку:
• повинна бути створена інтегрована система оцінки інформаційних загроз та механізм (протокол дій) реагування на них;
• потрібно на законодавчому рівні затвердити механізм (нормативні акти, протокол дій, тощо) по виявленню фіксації, блокуванню та видаленню з інформаційного простору держави будь-якої інформації, яка є прямою загрозою життю та здоров'ю громадян країни, а також державному суверенітету, пропагує воєнні дії, ворожнечу на релігійному і національному підґрунті, тоталітарні режими і їхню символіку, зміну конституційного ладу і порушення територіальної цілісності України;
• щоб досягти оптимального рівня можливостей держави дати відсіч потенційним та реальним загрозам національним інтересам України, потрібно удосконалити повноваження державних органів, що здійснюють діяльність;

свобод людини і громадянина, Верховний Головнокомандувач Збройних Сил України і Голова Ради національної безпеки і оборони України здійснює загальне керівництво у сферах національної безпеки та оборони України;

Верховна Рада України в межах повноважень, визначених Конституцією України, визначає засади внутрішньої та зовнішньої політики, основи національної безпеки, формує законодавчу базу в цій сфері, схвалює рішення з питань введення надзвичайного і воєнного стану, мобілізації, визначення загальної структури, чисельності, функцій Збройних Сил України та інших військових формувань, створених відповідно до законів України [Закон України «Про основи національної безпеки»].
Згідно ст.124 Конституції України правосуддя в Україні здійснюють виключно суди, тому судові органи слід розглядати лише за рамками системи безпеки. В усіх інших випадках судові органи здійснюватимуть не характерну їм функцію, що порушить принципи судочинства передбачених ст.129 Конституції України: незалежність судів, змагальність та рівність сторін. Тому дякуючи саме дотриманню принципів судочинства суди відіграють значну роль у дотриманні балансу інтересів згідно закону різних об'єктів та суб'єктів політики інформаційної безпеки.
Отже в Україні за законодавчою владою щодо головних аспекті безпеки постала роль визначення завдань.
Функції Верховної Ради включають в себе визначення в державі ключових параметрів інформаційних процесів та ймовірних способів і форм забезпечення цих параметрів. Або іншими словами, Верховна Рада визначає зміст інформаційної безпеки і можливі способи та форми її захисту. Іншим вектором діяльності Верховної Ради створення правових принципів політики держави в інформаційній сфері. На виконання цих питань відповідно до ст.85 Конституції України Верховна Рада має такі повноваження: визначення засад внутрішньої і зовнішньої політики, реалізації стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору; затвердження загальнодержавних програм економічного, науково-технічного, соціального, національно-культурного розвитку, охорони довкілля; розгляд і прийняття рішення щодо схвалення Програми діяльності Кабінету Міністрів України; заслуховування щорічних та позачергових послань Президента України про внутрішнє і зовнішнє становище України. Верховна Рада уповноважена також визначати структури та призначати до органів державної влади ряд посадових осіб що виконують завдання по захисту інформаційної безпеки, зокрема згідно ст.85 Конституції України: призначення за поданням Президента України Прем'єр-міністра України

Уникальность текста: 100.0%

Править этот текст | Новая проверка