МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

Факультет економіки та управління
Кафедра національної економіки та публічного управління

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА	Цифрове врядування
ГАЛУЗЬ ЗНАНЬ	28 «Публічне управління та адміністрування»
СПЕЦІАЛЬНІСТЬ	281 «Публічне управління та адміністрування»

Форма навчання: **заочна**

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему **«Цифрова розвідка в умовах інформаційних війн: державно-управлінський аспект»**

здобувача ***Рєпка Артема Сергійовича*** _____
(підпис)

Науковий керівник: ***к.е.н, доц. Федірко Н.В.*** _____
(підпис)

Робота допущена до захисту перед екзаменаційною комісією з атестації здобувачів вищої освіти (ЕК)

Завідувач кафедри: ***д.держ.упр., доц. Карпенко О.В.***_____
(підпис)

Київ 2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДВНЗ «КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАДИМА ГЕТЬМАНА»

Факультет економіки та управління

Кафедра національної економіки та публічного управління

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА	Цифрове врядування
ГАЛУЗЬ ЗНАНЬ	28 «Публічне управління та адміністрування»
СПЕЦІАЛЬНІСТЬ	281 Публічне управління та адміністрування

ПОГОДЖЕНО
Керівник проектної групи (гарант)
освітньо-професійної програми
О.В. Карпенко
(підпис)
2022 р.

ЗАТВЕРДЖУЮ
Завідувач кафедри
О.В. Карпенко
(підпис)
2022 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувачу вищої освіти *Рєпку Артему Сергійовичу*

заочної форми навчання

на підготовку кваліфікаційної магістерської роботи

на тему **«Цифрова розвідка в умовах інформаційних війн: державно-управлінський аспект»**

Тему затверджено наказом ректора Університету від «*25» жовтня 2022 р .№ 1854ст*

Кваліфікаційна магістерська робота виконується на матеріалах Міністерства оборони України.

План кваліфікаційної магістерської роботи

Розділ 1	Теоретико-правові засади організації цифрової розвідки органів державної влади в умовах інформаційних війн
Розділ 2	Практика організації цифрової розвідки в умовах інформаційної війни
Розділ 3	Удосконалення організації цифрової розвідки в умовах інформаційної війни України з Російською Федерацією

Об'єкт дослідження:	державне управління у сфері національної безпеки
Предмет дослідження:	державно-управлінський аспект цифрової розвідки в умовах інформаційних війн
Мета кваліфікаційної магістерської роботи:	обґрунтування шляхів удосконалення цифрової розвідки в умовах інформаційної війни в Україні

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

У розділі 1	1. Дослідити сутність та види розвідувальної діяльності органів влади як елементу державного управління у сфері національної безпеки, розкрити поняття та особливості цифрової розвідки 2. Дослідити характерні особливості інформаційних війн як чинника формування національної безпеки 3. Дослідити нормативно-правове забезпечення розвідувальної діяльності органів влади
У розділі 2	1. Дати характеристику системи, функцій та завдань розвідувальних органів державної влади в Україні 2. Проаналізувати український досвід організації цифрової розвідки в умовах інформаційної війни з Російською Федерацією 3. Проаналізувати зарубіжний довід організації цифрової розвідки в умовах інформаційних війн
У розділі 3	1. Дослідити виклики Російсько-Української інформаційної війни у найближчі роки 2. Обґрунтувати перспективні напрямки удосконалення нормативно-правового забезпечення цифрової розвідки органів влади в Україні 3. Обґрунтувати методи та ресурсне забезпечення для удосконалення цифрової розвідки органами державної влади в Україні

Завдання підготував науковий керівник Н.В. Федірко

«25» жовтня 2022 р.

Завдання одержав здобувач А.С. Рєпко

«25» жовтня 2022 р.

РЕФЕРАТ

Кваліфікаційна магістерська робота містить 85 сторінок, 5 таблиць, 10 рисунків, список використаних джерел з 56 найменувань, 2 додатки.

«Цифрова розвідка в умовах інформаційних війн: державно-управлінський аспект»

Об'єкт дослідження – державне управління у сфері національної безпеки.

Предмет дослідження – державно-управлінський аспект цифрової розвідки в умовах інформаційних війн.

Мета кваліфікаційної магістерської роботи – обґрунтування шляхів удосконалення цифрової розвідки в умовах інформаційної війни в Україні.

Відповідно до поставленої мети були визначені такі *завдання*:

- дослідити сутність цифрової розвідки та особливості її реалізації;
- дослідити нормативно-правову базу цифрової розвідки;
- проаналізувати світовий досвід реалізації цифрової розвідки в умовах інформаційних війн;
- проаналізувати практику реалізації цифрової розвідки в умовах інформаційної війни в Україні;
- обґрунтувати пріоритети удосконалення цифрової розвідки в умовах інформаційної війни в Україні.

Практичне значення отриманих результатів: полягає у тому, що представлені висновки можуть бути корисні для розвитку цифрової розвідки в Україні.

Описані пропозиції можуть бути використані в практичній діяльності органів цифрової розвідки.

Рік виконання кваліфікаційної магістерської роботи 2022.

Рік захисту роботи 2022.

Ключові слова: розвідка, цифрова розвідка, органи державної влади, інформаційна розвідка.

ВІДГУК

про кваліфікаційну магістерську роботу
здобувача факультету економіки та управління освітньо-професійної програми
«Цифрове врядування» Рєпка Артема Сергійовича
на тему «Цифрова розвідка в умовах інформаційних війн:
державно-управлінський аспект»

1. Актуальність теми. Загрози національній безпеці України, зумовлені військовою агресією Російської Федерації проти України, супроводжуються також загрозами інших сфер супільного життя, серед яких вагоме місце займає інформаційна безпека. Ключовим чинником впливу на інформаційну складову національної безпеки є цифрові засоби розвідувальної дільяності, що використовуються органами влади. З огляду на безпекові та цифрові виклики для системи публічного управління актуальність теми дослідження має вагомі підстави.

2. Позитивними рисами кваліфікаційної роботи є дослідження змісту процесу розвідуальної діяльності, його видів та ролі цифрових засобів в його реалізації (п.1.1), характеристика інформаційної війни в теоретичному аспекті (п.1.2) та в практиці України (п. 2.2) з огляду на формування інформаційної безпеки, дослідження засд діяльності органів цифрової розвідки в Україні (п.2.1), аналіз цифрових засобів розвідуальної діяльності та проведення кібернетичної розвідки (п.2.2), аналіз наукових підходів та авторське узагальнення сучасних викликів російсько-української інформаційної війни (п. 3.1), а також характеристика перспектиних напрямів, методів та ресурсів щодо удосконалення цифрової розвідки в Україні за умова поточної інформаційної та військової агресії Російської Федереації проти України.

3. До *самостійних розробок автора* можна віднести узагальнення та систематизацію правових засад розвідувальної діяльності в практиці України (п.1.3), авторське представлення особливостей організації розвідувальної діяльності в різних країнах світу (п. 2.3), авторське обгрунтування чинників, що впливають на цифрову розвідку в Україні з висновками щодо протидії потенційним загрозам, що здійснено з використанням методології СВОТ-аналізу (п.3.2, с.60).

4. Цінність теоретичних висновків та практичних рекомендацій полягає в узагальненні автором сучасного стану, викликів та рекомендації для системи публічного управління щодо протидії в Україні ризикам інформаційної безпеки засобами цифрової розвідки, що є корисним для обгрунтування рішень в практиці управління розвідувальною діяльністю.

5. До *недоліків роботи* можна віднести: дещо фрагментарний аналіз сучасної системи цифрової розвідки, який варто було б посилити за рахунок представлення цілісного авторського бачення елементів системи цифрової розвідки в Україні (п. 2.2); окремі частини аналітичного матеріалу мають недостатньо глибоке пояснення з точки зору їх ролі при реалізації цифрової розвідки в Україні (п.2.1, п.2.2); недостатньо повний аналіз прогнозних обсягів ресурсів та засобів, необхідних для подальшої організації цифрової розвідки в Україні (п.3.3).

6. Загальна оцінка кваліфікаційної магістерської роботи та її допущення до захисту перед ЕК. В цілому робота відповідає вимогам, містить достатньо повне виконання індивідуальних завдань та допускається до захисту перед ЕК з рекомендованою оцінкою «добре».

Науковий керівник:
доцент кафедри національної економіки
та публічного управління
к.е.н., доцент Н.В. Федірко
09 грудня 2022 року

РЕЦЕНЗІЯ

на кваліфікаційну магістерську роботу

здобувача другого (магістерського) рівня вищої освіти
Київського національного економічного університету імені Вадима Гетьмана
освітньо-професійної програми «Цифрове врядування»
за спеціальністю 281 «Публічне управління та адміністрування»
Репко Артема Сергійовича

на тему: «Цифрова розвідка в умовах інформаційних війн: державно-управлінський аспект»

Актуальність теми кваліфікаційної магістерської роботи і доцільність її розроблення обумовлюється тим, що з огляду на сучасні виклики національній безпеці України, що особливо загострились під час широкомасштабної війни Російської Федерації проти України, прихована інформаційна війна набула нового розмаху та більш глибоких проявів. За цих умов з метою кращої протидії інформаційній пропаганді та забезпечення інформаційної безпеки сучасні механізми цифрової розвідки потребують більш удосконалених навичок.

Якість проведеного дослідження. Дослідження, виконане в роботі, має достатній масштаб та глибину. У роботі було використано вітчизняні та міжнародні аналітичні дані, узагальнення якого дозволило автору зробити власні висновки та узагальнення щодо подальших викликів удосконалення цифрової розвідки в Україні.

Позитивні риси кваліфікаційної магістерської роботи. В кваліфікаційній магістерській роботі здійснено детальний аналіз світового досвіду реалізації цифрової розвідки в умовах інформаційних війн. Серед позитивних якостей, можна відзначити дослідження сутності цифрової розвідки та особливості її реалізації, нормативно-правової бази організації цифрової розвідки в Україні.

Практична значимість висновків і рекомендацій. Результати виконаного магістрантом дослідження можуть бути корисні для подальшого розвитку системи управління цифровою розвідкою в Україні в контексті забезпечення інформаційної безпеки. Описані пропозиції можуть бути використані в практичній діяльності органів, що здійснюють цифрову розвідку.

Зауваження. Недоліком роботи можна вважати недостатньо ґрунтовне розкриття питання практики організації цифрової розвідки в умовах інформаційної війни з точки зору її фінансового забезпечення. Також варто було більш детально розкрити питання стратегічних перспектив розвитку цифрової розвідки в Україні. Однак, це суттєво не впливає на загальний достатній рівень проведеного дослідження.

В цілому, кваліфікаційна магістерська дипломна робота «Цифрова розвідка в умовах інформаційних війн: державно-управлінський аспект» відповідає діючим вимогам та заслуговує позитивної оцінки. Робота рекомендується до захисту перед ЕК для отримання кваліфікації магістра з публічного управління та адміністрування.

Старший науковий дослідник
факультету прикладної математики
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
Доктор філософії прикладної математики ..... Максим СОХАЦЬКИЙ

ЗМІСТ

ВСТУП

Актуальність теми. XXI століття – епоха інформаційного суспільства, технічного прогресу та національні інтереси кожної країни перш за все забезпечується завдяки розвідувальної діяльності. Кожна країна має свої національні інтереси і їх захист - це найголовніше завдання. Забезпечення воєнно-політичного суверенітету без якісної розвідки - неможливо.

Безумовно, «розвідка» виступає ґрунтовним поняттям, що поєднує у собі величезну різноманітність діяльності як таємного, так і відкритого отримання найрізноманітнішої інформації. Не буде перебільшенням сказати, що поняття «розвідка» є відображенням багатовікового досвіду боротьби за інформацію. І ця боротьба триває протягом усієї історії людства. Тому можна з упевненістю сказати, що робота з інформацією є ключовим елементом розвідувальної діяльності у цілому. Загальновідомий факт, що політика виникла у світі безпосередньо в один момент з появою держави, а разом із політикою з’явилася і розвідувальна діяльність.

Актуальність роботи полягає в тому, що сучасні механізми цифрової розвідки потребують більш удосконалених навичок в умовах інформаційних війн.

Аналіз останніх досліджень і публікацій. О. Левченко та І. Захарова присвятили наукові дослідження висвітленню ключових питань безпеки та функціонування цифрової розвідки. Окремі питання щодо розвідувальної діяльності розглядали О. Золотар, В. Голота. Науковими дослідженнями щодо правового регулювання організації розвідки займалися В. Задирака, В. Рєзнік. Втім, невирішеним залишається питання стосовно забезпечення ефективності цифрової розвідки.

Мета і завдання дослідження. Метою дослідження є обґрунтування шляхів удосконалення цифрової розвідки в умовах інформаційної війни в Україні.

Відповідно до мети дослідження в процесі виконання роботи були поставлені наступні *завдання*:

- дослідити сутність цифрової розвідки та особливості її реалізації;
- дослідити нормативно-правову базу цифрової розвідки;
- проаналізувати світовий досвід реалізації цифрової розвідки в умовах інформаційних війн;
- проаналізувати практику реалізації цифрової розвідки в умовах інформаційної війни в Україні;
- обґрунтувати пріоритети удосконалення цифрової розвідки в умовах інформаційної війни в Україні.

Об'єктом дослідження виступає державне управління у сфері національної безпеки.

Предметом дослідження є державно-управлінський аспект цифрової розвідки в умовах інформаційних війн.

Методи дослідження. теоретичний – для пояснення сутності понять «розвідка» та «цифрова розвідка» та їх взаємозв'язку; порівняльний – для обґрунтування наявної державної політики у сфері цифрової розвідки в України і країнах світу; емпіричний – для обґрунтування впливу цифрової розвідки на національну безпеку країни та пояснення впливу державної політики на цифрову розвідку; логічний – для формування авторських оціночних суджень; узагальнення – для обґрунтування напрямків удосконалення державної політики у сфері цифрової розвідки в системі національної розвідки України. Для виконання дослідження були використані наступні методи:

Теоретична, методична значущість отриманих результатів полягає у дослідженні аспектів теоретичних понять та змісту цифрової розвідки.

Практична значущість отриманих результатів полягає у тому, що висновки щодо удосконалення цифрової розвідки можуть бути використані у безпосередній діяльності органів цифрової розвідки.

Інформаційною базою дослідження є матеріали Міністерства цифрової трансформації України, Міністерства оборони України, Міністерства у справах ветеранів України, Міністерства соціальної політики України, а також монографічні дослідження та наукові статті вітчизняних та зарубіжних вчених.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків та списку використаних джерел. *У першому розділі* досліджуються теоретико-правові засади організації цифрової розвідки органів державної влади в умовах інформаційної війни. *У другому розділі* здійснено аналіз українського і зарубіжного досвіду організації цифрової розвідки в умовах інформаційних війн. У *третьому розділі* здійснено обґрунтування перспектив удосконалення організації цифрової розвідки умовах інформаційної війни.

Апробація дослідження. Результати дослідження представлені автором на науково-практичній конференції «Публічне управління та кібербезпека: теорія та практика» (м. Київ, 15 вересня 2022 року) [56].

РОЗДІЛ 1
ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ОРГАНІЗАЦІЇ ЦИФРОВОЇ РОЗВІДКИ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ В УМОВАХ ІНФОРМАЦІЙНИХ ВІЙН

1.1 Сутність та види розвідувальної діяльності органів влади як елементу державного управління у сфері національної безпеки

Для початку потрібно дати визначення поняттю розвідка. Розвідка – це «діяльність, яку здійснюють за допомогою спеціальних засобів і методів аби забезпечити органи державної влади розвідувальною інформацією, сприяти реалізації та захисту національних інтересів, протидіяти за межами держави загрозам зовні нацбезпеці» [15]. На думку О. О. Золотар [32] розвідка – це «збір інформації політичного, економічного, науково-технічного характеру, що стосується обстановки в окремих країнах чи коаліціях країн, що представляють розвідувальний інтерес об'єктам, для забезпечення своєї безпеки та отримання переваг в області збройних сил, військових дій, політики або економіки».

Розвідувальні служби виступають у ролі інструмента влади, який ефективно займається вирішенням цілої низки проблем в інтересах держави. Активними учасниками політичного процесу в країні як зовнішньополітичного, так і всередині держави є розвідувальні служби.

Розвідувальні служби – це елемент виконавчої влади, проте елемент не у стандартному розумінні. Перш за все, варто зазначити наявність суттєвого впливу на три гілки державної влади. По-друге, розвідувальні служби впливають на аспекти формування зовнішньої політики держави та її геополітичних принципів. Розвідувальні служби отримують завдання не лише від керівництва держави, а й навпаки. Через надання інформаційно-аналітичних матеріалів певного спрямування розвідувальні служби впливають

на формування у керівництва держави бачення зовнішньополітичного оточення та тенденцій його розвитку.

Розвідки здійснюються з метою добування розвідувальних даних та поділяються на декілька видів, що представлено в таблиці 1.1.

Таблиця 1.1 – Види розвідки органів державної влади

Види розвідки	Особливості розвідки
За об'єктами	
Воєнна	військово-політична обстановка в окремих країнах
Політична	внутрішня та зовнішня політику, науково-технічний потенціал окремих держав
Економічна	промисловість, транспорт, фінансова та грошово-кредитна системи, екологія, природні ресурси
Зовнішня	розвідувальні служби іноземних держав, добування відомостей про їх діяльність
За територіальною ознакою	
Зовнішня	іноземні держави та їх території
Внутрішня	злочинна діяльність в середині країни
За використовуваними методами і засобами	
Розвідка на основі відкритих джерел (Open source intelligence, OSINT)	військова, політична, економічна та інші види інформації.
Агентурна	з допомогою агентурної мережі
Радіоелектронна	прийом і аналіз електромагнітних випромінювань радіоелектронних засобів противника
Видова	повітряна та космічна
Геопросторова	аналіз зображень і геопросторових даних
Військова	тактична розвідка частин сухопутних військ

Джерело: сформовано автором за даними [12].

Продуктом цілеспрямованого збору та опрацювання інформації про ситуацію, можливості та наміри сторін є розвідувальна інформація, яка використовується задля виявлення загроз та надання керівникам можливості скористатися цим продуктом. Розвідувальна інформація, яку збирають суперники, може вплинути на боєздатність країни. Інформація, яку збирають суперники може привести до зниження ступеню актуальності власної розвідувальної інформації країни.

Розвідка включає в себе збирання та оцінювання даних, які відносяться до роботи урядових структур різного рівня та військових. Подібна

інформація може використовуватися для того, аби прийняти стратегічні чи тактичні рішення.

Р. Кларк [26] стверджував, що розвідка «має певні розвідувальні цикли. Класичний цикл розвідки починається з вимог, далі збір, обробка, аналіз інформації. І останнє - донесення остаточного продукту до осіб чи організацій, які його замовили».

На тактичному та стратегічному рівнях функціонує той самий цикл для цифрової розвідки. За визначенням М. Мельника, цифрова розвідка – це «процес збирання даних та аналізу відомостей для керівників сил військових та урядових структур. Цифрова розвідка здійснюється та керуються урядовими відомствами, її використовують аби оцінити можливості і наміри противників та разом з тим аби підвищити ефективність систем озброєнь країни».

Не можна стверджувати, що цифрова розвідка безпосередньо впливає на боєздатність. Аби цифрова розвідка була ефективною, її необхідно інтегрувати до системи озброєння та особового складу.

Стрімкий розвиток соціальних мереж, які стали джерелом вільних даних, спричинив появу нової методологічної одиниці інформаційної аналітики – розвідки на відкритими джерелами – OSINT.

Через активний вплив Інтернету та соціальних медіа концепція OSINT отримала статус більш комплексного явища. Кожен користувач мереж власноруч залишає у мережі багато інформації: фото, особисті дані, публікування дописів, зазначення геолокації. Активне накопичення зазначеної інформації разом із зростанням більш широких можливостей комп'ютерного аналізу створили можливості для аналітиків, які збирають та аналізують дані.

На рисунку 1.1 зображена візуальна концепція можливої розвідувально-аналітичної розвідки за відкритими джерелами - OSINT. Таким чином, можна зробити висновок, що OSINT виступає у ролі важливого джерела інформації, який доповнює дані, що вже отримані з інших джерел.

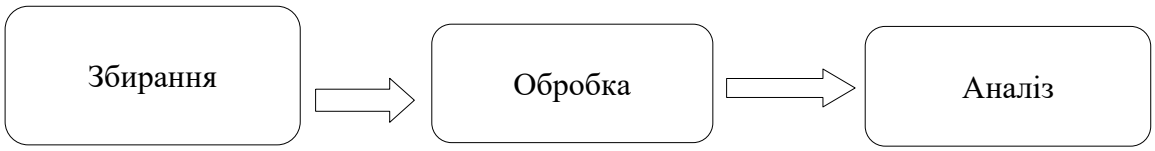


Рисунок 1.1 – Етапи розвідки за відкритими джерелами (OSINT)

Джерело: сформовано автором за даними [13].

Принципи не залежать одне від одного, і комбінуються лише у окремих ситуаціях. OSINT займає проміжну ланку серед інших типів та дає змогу отримати більш комплексну відповідь при використанні інших різновидів розвідки. Для прикладу, GEOINT може виступати як частина цифрової розвідки за відкритими джерелами. Для цього необхідно використовувати дані з супутників та різноманітних комерційних установ (Google, Bing) та додатково отримувати інформацію з військових супутників.

Під терміном цифрової розвідки згідно з визначенням М. Вертузаєва [5] розуміється «організаційна структура, яка бере на себе наступні питання: збір, перевірка, обробка, аналіз даних з різних аспектів господарської діяльності підприємства для подальшого використання отриманої інформації, щоб вирішити конкретні завдання його господарської діяльності» [32]. За умов ринкової економіки підприємство не має змогу здійснювати ефективну роботу без глибокого розуміння її рушійних сил. У розпорядженні варто мати новітню інформацію про події, які відбуваються в конкретному сегменті ринку. Варто розуміти, що наявні у підприємства можливості, базуються на емоціях, симпатії та антипатії. Ці можливості продиктовані навколишнім середовищем представляють собою баланс інтересів різних спільнот, угруповань та окремих особистостей.

За визначенням О. Рєзніка, центр цифрової розвідки – «структурний підрозділ організації, на який покладені завдання єдиного, в рамках суб'єкта господарювання, інформаційного центру з завданнями обробки та аналізу інформації, що забезпечує прийняття вищим керівництвом обґрунтованих рішень з найважливіших для питань» [31].

Створення цифрової розвідки визначається наступними чинниками:

– недостатність неформальних засобів спостереження за навколишнім середовищем;

– система цифрової розвідки повинна орієнтуватися на конкретних осіб, за якими зберігається право приймати рішення;

– головне завдання цифрової розвідки полягає у забезпеченні осіб, які приймають управлінські рішення, а також інформацією, як потрібна для прийняття оптимальних рішень;

– збір інформації з різноманітних джерел, порівняння, аналіз отриманих даних, що стане у нагоді для прийняття рішень;

– легітимна робота цифрової розвідки без використання незаконних та неетичних методів отримання інформації;

– враховувати, що конкуренти також мають певні розвідорган і можуть використовувати незаконні способи отримання інформації.

Центр цифрової розвідки по факту повинен працювати на випередження. Тобто навіть коли невідомо, які рішення необхідно буде приймати. Щоб швидко привести до мінімуму обсяг робочих моментів, важливо разом з керівництвом країни прийти до єдиного спільного розуміння проблеми та шляхів її вирішення. Разом з тим необхідно домовитися про особливості термінології, яка буде використовуватися в роботі.

Під час впровадження системи цифрової розвідки важливим є баланс інтересів. Кожен співробітник, що має певний обсяг інформації, яка стосується його діяльності намагається поділитися нею з оточуючими. Статус співробітника залежить від рівня доступу до інформації. Тому перед тим як почати реалізацію програми щодо створення системи цифрової розвідки варто здійснити глибоке осмислення ситуації, дослідження інтересів всіх учасників подій. І тільки після цього варто переходити до моделювання сприятливих умов для здійснення відповідних робіт.

Як зазначає В. Варенко [4], «інформаційний чинник є одним із найважливіших елементів цифрової розвідки країни» [12]. Його суть полягає у тому, аби надавати необхідні дані військовому керівництву. Це у свою чергу допомагає ефективно застосовувати ресурси під час військових операцій. Завдяки великому арсенал засобів інформаційного забезпечення інформація стає свого роду метою, зброєю, ресурсом.

Інформаційне супроводження протягом воєнно-політичного конфлікту дозволяє побудувати дієву систему, яка необхідна для того, аби інформувати усіх кого потрібно: особовий склад збройних сил, військове керівництво, міжнародне співтовариство, власних громадян усередині країни та на окупованих територіях.

Розробка інформаційної кампанії повинна, згідно з висновками В. Бойко [2], «відповідати позиціям та потребам сторони у воєнно-політичному конфлікті. Засоби інформаційного впливу здатні чинити потужний морально-психологічний тиск на війська та населення, прагнучи зламати волю до спротиву та досягти політичної мети обмеженими засобами» [42].

Безумовно, що ворожа інформаційна діяльність потребує протидії. Це є одне з важливих завдання інформаційної політики. Зазначене завдання допомагає виробити ефективні інструменти для нейтралізації ворожої пропаганди.

Задля отримання інформаційної переваги необхідно підготувати висококваліфіковані кадри та застосовувати сучасні технології. Підприємливість, новаторство – саме ці характеристики виступають як ключові фактори успіху та ґрунтовної ефективності розвідки. Зазначимо, що більшу частину розвідувальних даних неможливо купити, адже вона відноситься до конкретних персоналіїв. Тому кожна країна повинна проводити власні воєнні дослідження та працювати над створенням внутрішніх джерел та можливостей для збору, аналізу та надання інформації тим, кому вона потрібна.

Складність у виконанні завдань розвідки виникає через невизначеність. Її можливо мінімізувати якщо вдосконалити процедури та підготувати кваліфіковані кадри.

На інформаційну сферу життєдіяльності людей впливає стрімкий розвиток інформаційних технологій, створення віртуальних середовищ, які отримали вагоме значення у державних та міжнародних відносинах певних організацій. Серед подібних віртуальних середовищ варто виокремити кіберпростір - особлива область соціальних взаємодій, яка включає в себе сукупність процесів, що відбуваються в інформаційно-комунікаційних мережах світу. Кіберпростір сьогодні став ще одним середовищем діяльності людини» [19]. Кіберпростір – це поєднання важливих галузей інформаційної, економічної, політичної, воєнної діяльності окремих людей, корпорацій, держав та їх спільнот, наднаціональних структур і утворень.

Після свого утворення, кіберпростір став свого роду полем для зіткнення воєнних та політичних сил.

У кіберпросторі відбуваються протистояння між розвідками різних країн, їх структурами воєнного сектору, проводяться інформаційні та економічні війни, та навіть диверсії та шпигунство.

Кібербезпека – це «властивість захищеності активів від загроз конфіденційності, цілісності, доступності, але в деяких абстрактних рамках – кіберпросторі» [14]. Особливості організації простору кібербезпеки нами представлено у Додатку А. Отже комунікаційний простір складається з:

- соціопростору;
- інфопростору;
- технопростору;
- віртуального простору.

Комунікаційний простір знаходиться під впливом кібернетичним впливом. Все це будує інформаційну та кібербезпеку.

Що стосується питання забезпечення кібербезпеки, то пріоритет залишається за взаємодією між організаціями. Саме вони формують кіберпростір. Автономні дії не створюють ефективний захист від кіберзагроз. Кібербезпека, як можна простежити завдяки Додатку Б об'єднується з наступними поняттями: інформаційна безпека, безпека застосування, мережева безпеки, безпека глобальної мережі, а також безпека критичної інформаційної інфраструктури.

Відповідно до Закону України «Про основи національної безпеки України» національна безпека відповідає за захищеність життєво важливих інтересів людини і громадянина, суспільства і держави. Забезпечує сталий розвиток суспільства, своєчасно виявляє, запобігає і нейтралізує реальні та потенційні загрози національним інтересам» [3]. Розвідка виступає у ролі формуючого чинника національної безпеки країни. Завдяки розвідувальним діям є можливість попередити виникнення ситуацій, що можуть загрожувати національній безпеці країни.

Враховуючи останні події в України термін військової розвідки набуває вагомого значення. Отже, військова розвідка – це діяльність, яка стосується збору військової інформації. В контексті національної безпеки розвідка виступає у ролі аналітичного дослідження, яке організовано державою по відношенню до інших країн.

Відповідно до положень Закону України «Про розвідку», розвідка – це «організаційно-функціональне поєднання розвідувальних органів та діяльності, яку вони здійснюють самостійно або у взаємодії між собою та з іншими суб’єктами розвідувальної співпраці з метою гарантування національної безпеки й оборони України» [5].

Нижче ми розглянемо основні види розвідки за масштабом поставлених завдань (табл. 1.2).

Таблиця 1.2 – Види розвідки за масштабом поставлених завдань

Вид розвідки	Характеристика
Тактична	Збір розвідувальної інформації, аналізування тактичної ситуації й розробка рекомендацій, які стосуються підготовки і здійснення бойових дій на конкретних напрямках.
Оперативна	Збір розвідувальної інформації про противника, яка знадобиться для підготовки і здійснення військових операцій. Також оперативна розвідка аналізує оперативну ситуацію та розробку рекомендацій щодо можливої підготовки і здійснення відповідно наступу чи контрнаступу.
Стратегічна	Збір інформації, яка стосується військової політики противника, її сильних та слабких сторін і стратегії здійснення власне військових дій. Подібна інформація можемо стосуватися особового складу, стану, розміщення сил противника, плани бойових дій, рівень озброєння, військовий потенціал противника. Ще одне з завдання стратегічної розвідки - це виявити можливі шляхи та підготовка пропозицій щодо можливостей уникнення війни чи припинення агресії шляхом проведення дипломатичних переговорів.

Джерело: сформовано автором за даними [14].

З розвитком інформаційної аналітики та комп`ютерних технологій набуває розповсюдження новий різновид розвідувальних операцій – цифрова. Цифрова розвідка – це різновид розвідки, що для отримання даних використовує відкриті джерела, інноваційні технології, комерційні та державні данні. Події в Україні розвиваються непередбачувано. Змінюються типи загроз, агресором використовуються неоднозначні стратегії і тактики . Ці фактори, на думку В. Голоти [8], спонукають розвідку до рішучих дій, аби отримати інформацію і спрацювати на випередження».

1.2 Інформаційні війни як чинник формування національної безпеки

Сьогодні інформація відіграє дуже важливу роль в житті людей. Вона стала вагомою складовою сучасного життя. Інформація у XXI столітті постає у ролі регулятора різноманітних відносин: економічних, соціальних, політичних. Процес інформатизації стрімко розвивається, що призводить до формування єдиного інформаційного простору. Це явище носить позитивний характер, адже процес обміну різного роду інформацією сприяє швидкому розвитку людства. Але разом з тим, створення інформаційного суспільства спричинило інформаційні катастрофи, руйнування духовних складових суспільства і може стати причиною великих масштабних технічних катастроф.

Негативні аспекти інформаційного суспільства створюють умови для формування такого поняття, як «інформаційна війна», яка сьогодні стала загрозою безпеці усього людства. Аналізуючи хід і наслідки війн та конфліктів, що відбувалися протягом XX та XXI століть, ми бачимо, що роль інформаційного забезпечення зростає. Це вказує на формування нового рівня ведення інформаційної боротьби. Інформаційна війна складається з різноманітних аспектів. Основні серед них: вплив на свідомість людини з використанням різних засобів, які засновані на зміні світогляду людей.

За твердженням В. Варенко [46], «інформаційна війна вирізняється всебічним, цілісним характером, що демонструє значимість того, як важливо володіти інформацією в процесі керування, командування і реалізації політики країни. Інформаційна війна – це війна за знання, за те хто матиме відповіді на важливі питання, що дозволять управляти масами. Звичайно, за такої війни кількість жертв мінімальна, але участь у ній беруть усі люди, що може спричинити зміну світогляду людей».

Відповідн до В. Задіраки [33], «життєдіяльність суспільного організму залежить від рівня розвитку, якості, безпеки інформаційного середовища. Витік і розповсюдження інформації, яка може бути шкідливою для інформаційної і національної безпеки країни».

Вперше термін «інформаційна війна» з'явився наприкінці 70-х років XX століття. Він з'явився як результат плодотворної співпраці теоретиків збройних сил США. Набув розповсюдження після вдало проведеної роботи щодо ліквідації СРСР. У 1991 році під час воєнної компанії США в Іраку цей термін почав активно застосовуватися. Саме тоді вперше застосувалися інформаційні технології, при чому відкрито, що спричинило суттєвий резонанс. Цьому досвіду не приділили необхідної уваги, хоча саме він зробив внесок у розпад СРСР, держави, яка була найбільш помітним конкурентом для США. Все це точно вказує на необхідність займатися розробкою концепції інформаційного стримування.

Якщо говорити про історичні приклади інформаційних війн, то можна вказати на події 2001 року, пов'язані з касетним скандалом. Саме тоді з'явилися звинувачення у постачанні комплексів радіотехнічної розвідки «Кольчуга» в Ірак у лютому 2004 року. Мали місце інформаційні протистояння на тлі «газових війн». І це не включаючи майже щоденних провокацій на інформаційному фронті з боку ЗМІ Росії. Якщо проаналізувати сучасну геополітичну обстановку можна зробити висновок, що Україна зазнає інформаційних диверсій, які мають на меті дискредитувати, підірвати імідж та дестабілізувати ситуацію у країні. Перш за все, цього впливу зазнає система забезпечення національної безпеки.

Інформаційна війна впевнено стає воєнним поняттям. Тому можна з упевненістю сказати, що розвинена система інформаційної безпеки закладає фрагмент для стійкої роботи системи держуправління за допомогою цифрової розвідки, яка входить до складу оперативної розвідки.

Стрімкий розвиток інформаційних технологій може стати причиною призвести нових типів війн, які відбуватимуться без пострілів. Сучасні інформаційні війни вражають у більшій мірі економічну інфраструктуру. Цілі інформаційної війни інші, аніж у війни у класичному розумінні. Мова йде не про фізичне знищення противника і ліквідацію його збройних сил. Це масштабна руйнація функціонування транспортних, фінансових і комунікаційних мереж і систем, руйнування економічної інфраструктури і захоплення населення країни, що була атакована.

Інформаційна війна складається з наступальних та оборонних частин. Одна з ключових її цілей, за висновками С. Мельника [20] – «забезпечити особам, що мають відношення до прийняття рішень, відчутну інформаційну перевагу у різноманітних конфліктах. Інформаційна війна може спрямовуватися проти комп'ютера, програмного забезпечення та людини» [11]. Головна ціль та завдання інформаційної війни – пригнітити в людині моральні якості, втрутитися в аспекти її світогляду.

На міжнародному рівні інформаційні проводять держави між собою, корпорації міжнародного рівня, терористичні організації та злочинні угруповання. Варто підкреслити прогресивні технології інформаційного віку поставили на один щабель індустріальні, постіндустріальні і доіндустріальні країни. Всі вони мають певний інструментарій для проведення заходів інформаційної війни. Тому можуть бути як суб'єктами, так і об'єктами інформаційної війни. І працювати задля забезпечення внутрішньої інформаційної безпеки.

Для впливу інформаційного характеру використовується технологія дозованої присутності правди.

Дозована присутність правди – технологія, яка використовується для інформаційного впливу. На такому фоні маніпулятор отримує неправдиві дані. В науковій літературі цей спосіб називається «перетасовка» або «підтасовка карт». Зміст даного способу полягає в наступному: тенденційний відбір фактів, певних даних, аби продемонструвати правильність або

неприйнятність певної точки зору, програми, ідеї. Як зазначає Р. Шай [54] , останнім часом цей спосіб частіше за все використовується у видозміненому вигляді під назвою «акцентування» [17].

До засобів сучасної інформаційної війни входять різні прийому аби впливати на соціальні відносини, ресурси, свідомість та психіку окремих людей. Для цього застосовуються наявні інформаційні ресурси та новітні технології з метою створення чинників які гальмують розвиток людини, суспільства та держави. Також здійснюється контроль над інформаційними ресурсами супротивника. Таким чином можна отримати перевагу у різних сферах суспільного життя.

Коли проходить інформаційна війна та будь-яка операція розглядається, В. Окіпнюк [23] «як комплекс заходів, які потрібні аби маніпулювати інформацією, досягати та утримувати перевагу. Це є можливим якщо впливати на інформаційні процеси в системах супротивника. Але є маленьке уточнення - інформаційні системи розглядаються в широкому сенсі, включаючи державу і суспільство».

Основні ознаки та суб’єкти інформаційних війн представлено на рис.1.2.

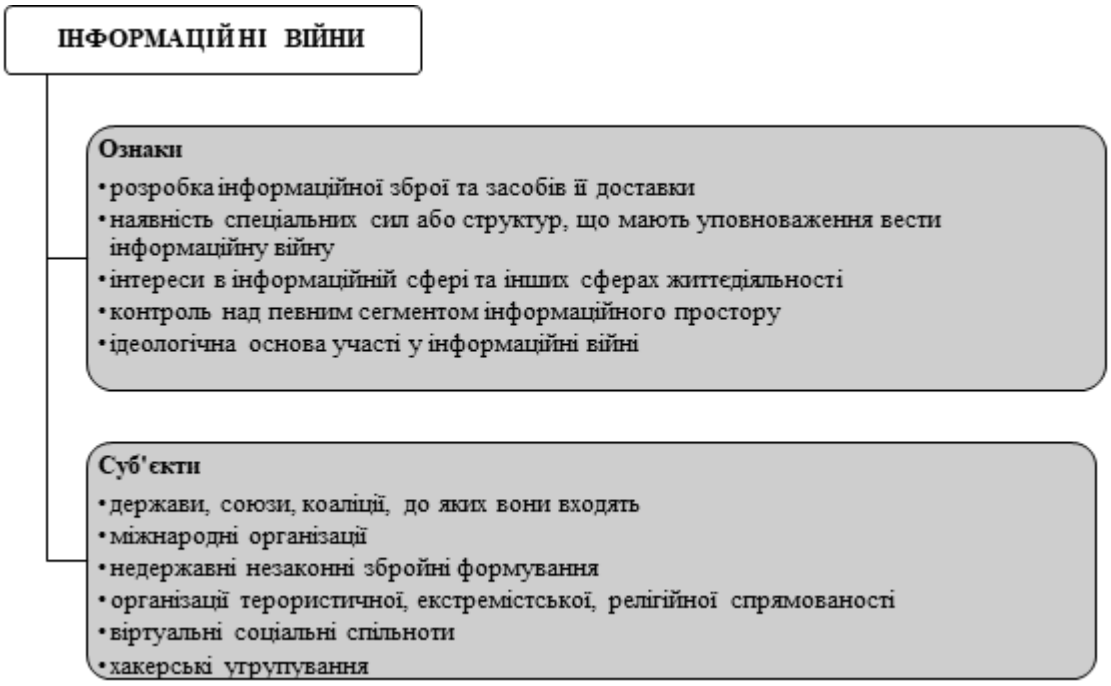


Рисунок 1.2 – Основні ознаки та суб’єкти інформаційних війн

Джерело: сформовано автором за даними [17].

Інформаційні війни проводяться не завжди, лише у виняткових випадках. Адже вони наносять суттєву шкоду економіці обох сторін, негативно впливають на культурне та соціальне життя, загрожують інформаційній та національній безпеці. При цьому ключовою ознакою сучасного світового розвитку стале саме інформаційне протистояння «мирного» характеру.

Суб’єкти інформаційної війни і більшості випадків об’єднані на основі спільних інтересів або інших ознак: мова, національність, територія, професія.

Держави, їх союзи та коаліції за умов інформаційного протистояння займаються розробкою наступних заходів:

– інтегрують власне інформаційне середовище до глобального інформаційного простору;
– розроблюють нормативно-правову базу, що регламентує участь в інформаційній війні, окреслює принципи та форми;

– створюють цивільні та військові системи аби проводити інформаційну війну;
– розроблюють та закупляють за кордоном зброю інформаційного характеру.

Варто підкреслити, що захиститися від інформаційних маніпуляцій неможливо, при чому навіть розвинених країнам. Враховуючи ці умови людство, з високою долею ймовірності, найближчі роки буде шукати менш агресивні способи співіснувати на планеті.

З цього питання О. Соснін слушно зазначає: «Прийшов час, коли міжнародному товариству необхідно чітко зрозуміти проблеми глобальної взаємозалежності національних інформаційних ресурсів. Необхідно визнати, що успішність національних зусиль щодо охорони свого інформаційного ресурсу залежить від того, наскільки будуть захищені і «не агресивні» інформаційні простори інших держав, із якими їхні інформаційні ресурси об’єктивно пов’язані» [16].

Незаконні збройні формування та організації прагнуть створити власний інформаційний простір аби в подальшому захопити чи зруйнувати глобальні та національні інформаційні простори. Саме для цього створюється власний науково-технічний потенціал або використовують потенціал держав чи організацій, що їх підтримують у відкритому чи прихованому форматі. Агресивність суб’єктів інформаційних війн може нанести суттєву шкоду. Новітні технології, які використовують зазначені суб'єкти, зумовлює наступне: «виникнення нових терористичних угруповань важко передбачити, оскільки їх ініціатори досить мобільні, дуже підготовлені й надзвичайно жорстокі, про що свідчать основні характеристики терористичних угруповань: нездатність до підпорядкування, відсутність дисципліни, військових традицій; перетворення інститутів громадянського суспільства» [27].

Інформаційна безпека виступає як складова національної безпеки. І на даний час її розглядають у якості пріоритетної функції держави. Інформаційна безпека, з одного боку, забезпечує якісне всебічне інформування громадян.

Надає доступ до різних джерел інформації. Проте з іншого боку – це контроль аби не поширювалася дезінформація, робота щодо забезпечення цілісності суспільства, укріплення інформаційної незалежності, протидія негативну інформаційно-психологічному пропагандистському впливу. Разом з тим, це механізм захисту національного інформаційного простору від маніпуляцій, інформаційних операцій. Вирішуючи комплексну проблему інформаційної безпеки відкриється можливість «захисту інтересів суспільства і держави, а також гарантування прав громадян, які зможуть отримати всебічну, об'єктивну та якісну інформацію» [31].

Інформаційна безпека охоплює ціле коло питання. Їх головна спрямованість у тому, аби вивчити нові можливості для розбудови правової держави та розвитку громадянського суспільства.

1.3. Нормативне-правове забезпечення розвідувальної діяльності органів влади

По-перше варто зазначити, що нормативна база цифрової розвідки менш розвинута та не така публічна, якщо порівнювати з іншими розвідувальними службами. Міжнародні стандарти прав людини та верховенства права висувають певні вимоги. І головна з них полягає у тому, щоб права та повноваження розвідувальних служб визначались законодавством. Закон повинен бути у зрозумілому і доступному форматі. Служби внутрішньої та зовнішньої розвідки вирізняються автономністю роботи. Їх функціонування підпорядковано закону, де чітко зазначено завдання, повноваження та обмеження у використанні особливих повноважень. У зазначених законах прописані певні заборони на самовільні дії, що дозволяє врівноважити секретність і не допустити свавілля.

17 вересня 2020 року ухвалено Закон України «Про розвідку», який встановив організаційні, правові засади функціонування розвідки, правовий статус та соціальні гарантії співробітників розвідувальних органів України й осіб, залучених до виконання розвідувальних завдань. Крім того, цим Законом запроваджено порядок здійснення контролю за розвідкою. Закон України «Про розвідку» чітко «розмежовує повноваження і сфери відповідальності розвідувальних органів із зосередженням їхніх зусиль на пріоритетних напрямах забезпечення національної безрпеки, унеможливлює дублювання їхніх завдань і функцій та одночасно забезпечує комплексний підхід до виконання розвідувальними органами пріоритетних завдань розвідувальної діяльності у відповідних сферах» [7].

Відповідно до статті 20 Закону України «Про національну безпеку України», розвідувальні органи України здійснюють розвідувальну діяльність з метою сприяння реалізації національних інтересів України та протидії зовнішнім загрозам національній безпеці України у визначених законом сферах [5].

У межах аналізу чинного законодавства необхідно враховувати рекомендації Парламентської Асамблеї Ради Європи № 1713 (2005) «Про демократичний нагляд за становищем у сфері безпеки в державах-членах». Там, зокрема, йдеться про те, що «функціонування спеціальних служб повинно бути засноване на ясному і належному законодавстві під наглядом судів» [10].

Серед нормативно-правового забезпечення розвідувальної діяльності варто виділити також Указ Президента України №685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». Цим указом було затверджено Стратегію інформаційної безпеки. Контроль за дотриманням умов указу покладений на покласти на Секретаря Ради національної безпеки і оборони України.

Таблиця 1.3 – Правові засади розвідувальної діяльності в Україні

Нормативно-правовий акт	Предмет регулювання	Що визначає
Закон України «Про розвідку» від 17 вересня 2020 року	Організаційні, правові засади функціонування розвідки, правовий статус та соціальні гарантії співробітників розвідувальних органів України й осіб, залучених до виконання розвідувальних завдань.	Розмежовує повноваження і сфери відповідальності розвідувальних органів із зосередженням їхніх зусиль на пріоритетних напрямах забезпечення національної безпеки, унеможливлює дублювання їхніх завдань і функцій та одночасно забезпечує комплексний підхід до виконання розвідувальними органами пріоритетних завдань розвідувальної діяльності у відповідних сферах»
Стаття 20 Закону України «Про національну безпеку України»	Розвідувальні органи України	Сприяння реалізації національних інтересів України та протидії зовнішнім загрозам національній безпеці України у визначених законом сферах
Рекомендації Парламентської Асамблеї Ради Європи № 1713 (2005) «Про демократичний нагляд за становищем у сфері безпеки в державах-членах».	Національна безпека	Функціонування спеціальних служб повинно бути засноване на ясному і належному законодавстві під наглядом судів
Закон України «Про розвідувальні органи України» від 22.03.2005 №17	Розвідувальні органи України	Всебічне зміцнення української розвідки (кадровий, агентурний (оперативний), технічний (сюди входять також авіація, безпілотні літальні апарати), зокрема космічний для воєнної розвідки, компонент стратегічного, оперативного, тактичного рівня) має бути одним із першочергових пріоритетів реального, відновлення Воєнної організації України.
Указ Президента України №685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки».	Інформаційна безпека	Затверджено стратегію інформаційної безпеки. Контроль за дотриманням умов указу покладений на покласти на Секретаря Ради національної безпеки і оборони України.рй

Джерело: розроблено автором.

Діяльність розвідувальних органів регулюється Законом України «Про розвідувальні органи України», який є регулює кадровий, агентурний та технічний компоненти їх роботи стратегічного, оперативного і тактичного рівнів. Якщо порівнювати з автономними розвідувальними службами, то цифрова розвідка є організаційним елементом збройних сил та міністерства оборони (або ж може охоплювати одразу кілька підрозділів збройних сил і міністерства оборони). Функціонал розвідки регулюється статтями, законами, підзаконними актами. Але часто громадськість про них не інформована. Розглянемо нижче основні закони, що регулюють роботу розвідки.

РОЗДІЛ 2
ПРАКТИКА ОРГАНІЗАЦІЇ ЦИФРОВОЇ РОЗВІДКИ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

2.1 Система, функції та завдання розвідувальних органів державної влади в Україні

Сьогодні Україна перебуває на етапі розвитку національної державності. Цей етап вирізняється заснуванням та розбудовою демократичних інституцій, які повинні забезпечити передумови для існування розвиненого громадянського суспільства та створити можливості безпосереднього доступу до державного управління.

Україна прагне посісти чільне місце в європейській системі колективної безпеки. Це висуває перед країною певні зобов'язання, а саме прийняття у національному секторі безпеки євроатлантичних цінностей та стандартів, а також механізмів їх імплементації. Через актуальні виклики та загрози, які постають перед національної безпекою України, спеціальні служби отримують нові завдання. Виконання останніх може призвести до певних обмежень прав і свобод людини. Виходячи з цього посилюється необхідності у прозорій роботі вказаних служб.

За визначенням В. Окіпнюк [15] «спеціальні служби, до яких відносяться державні органи, мають повноваження проводити розвідувальну та контррозвідувальну діяльність. Вони повинні забезпечувати внутрішню безпеку, безпеку інформації і системи управління державою, ставати на захист національних інтересів та виступає у ролі важливого елемента системи забезпечення національної безпеки певної країни».

До системи контролю за діяльністю спецслужб входить парламентський, президентський та судовий контроль. Якщо поглянути на

досвід дієвого та професійного контролю за роботою спецслужб, який здійснюють країни-члени НАТО, то можна помітити, що ґрунтовних стандартів для організації такого контролю немає. Кожна держава бере за основу національні інтерес, аспекти геополітики та форму державного правління. Демократичний цивільний контроль включає в себе співпрацю, діалог, взаємодію, спільний пошук способів вирішення проблем, готовність до порозуміння і бажання діяти ефективно. Надзвичайно важливо зберігати баланс між правом сили і силою права. Адже це один з основних принципів демократії. Все це підводить до думки про те, що до пріоритетних напрямів реформування безпекового сектору країни відноситься створення системи демократичного цивільного контролю над спецслужбами. Очевидно, що «наскільки ефективним буде демократичний цивільний контроль за діяльністю спеціальних служб залежить від того, як обізнані всі його суб'єкти щодо сутності системи контролю, механізмів її впровадження, враховуючи національні особливості, узгоджені з євроатлантичним баченням» [18].

Важливе значення отримує інформаційно-аналітичний супровід та забезпечення наукового плану. Урахування незалежної громадської думки, ґрунтовна наукова експертиза повинні бути засновані на взаємодії спецслужб з членами Комітетів Верховної Ради України, Рахункової плати, Уповноваженим з прав людини, суддями тощо. Тому варто зазначити, що суттєвою ознакою роботи сектору безпеки і оборони у правовій державі виступає діючий інститут демократичного цивільного контролю за діяльністю спеціальних служб. У контексті «розвитку системи забезпечення національної безпеки України цей інститут буде позитивно впливати на формування позитивного мислення громадянського суспільства щодо функцій і повноважень спеціальних служб та розуміння необхідності впроваджувати в організацію їхньої діяльності європейські стандарти» [12].

Варто підкреслити, що в Україні відносини між розвідувальними органами і державними інституціями ще не сформувалися остаточно. «Розвідувальні органи та їх інформпродукт залишаються міноритарною

ланкою у політичному процесі прийняття та реалізації політичних рішень. В суспільстві триває дискусія, що стосується ролі та завдань певних розвідувальних органів, формується система демократичного цивільного контролю над їх діяльністю» [16].

Розвідка здійснюється уповноваженими державою розвідувальними органами, які можуть діяти як самостійний державний орган в Україні. Структура розвідки України, виглядає таким чином (рис. 2.1).

Рисунок 2.1 – Структура розвідки України

Джерело: сформовано автором за даними [20].

Так, розвідувальні органи України (Служба зовнішньої розвідки України та Головне управління розвідки Міністерства оборони України), передають інформаційні та аналітичні матеріали основним посадовим особам як виконавчої, так і законодавчої влади, а саме Президенту України, Прем'єр-міністру України, Голові Верховної Ради України та іншим визначеним законодавством споживачам.

19 березня 2015 Верховна Рада України було ухвалено Закон України «Про внесення змін до деяких законів України щодо розвідувальних органів України». Його розробив Комітет Верховної Ради України з питань національної безпеки і оборони спільно з розвідкою України. Закон удосконалює правові основи організації та регламентує діяльність розвідувальних органів України за умова збройної агресії з боку РФ. Таким чином розвідувальні органи можуть проникати в міжнародні терористичні організації, злочинні групи чи організації, а також організацій, що займаються підривною діяльністю проти України, з метою запобігання їх протиправній діяльності або припинення та встановлення осіб, які їм сприяють. Прийняття закону відкрило можливості щодо застосування закріплених на законодавчому рівні спеціальних методів та засобів діяльності для протидії на тимчасово окупованих територіях України підривної діяльності іноземних спецслужб. Перш за все це стосується РФ. Водночас в умовах російської агресії отримали чіткіших обрисів сфери відповідальності суб'єктів сектору безпеки і оборони держави, зокрема Служби зовнішньої розвідки Україна. Службою зовнішньої розвідки України у взаємодії МЗС України та міжнародними організаціями було доведено до відома світової спільноти численні факти участі регулярних військ Росії в окупації Автономної Республіки Крим та окремих районів Донбасу, фінансуванні та озброєнні бойовиків, діяльності в Україні агентури РФ.

У Збройних силах України та Національної гвардії України наявні наступні бойові підрозділи військової розвідки:

– 10-й окремий загін спеціального призначення;
– 49-й окремий навчальний розвідувальний батальйон;
– 54-й окремий розвідувальний батальйон;
– 74-й окремий розвідувальний батальйон;
– 129-й окремий розвідувальний батальйон;
– 130-й окремий розвідувальний батальйон;
– 131-й окремий розвідувальний батальйон;
– 132-й окремий розвідувальний батальйон;
– 140-й окремий розвідувальний батальйон;
– 143-й окремий розвідувальний батальйон.

Служба безпеки України в якості державного органу спеціального призначення з правоохоронними функціями керується конфіденційним співробітництвом під час виконання завдань, які стосуються протидії загрозам державного рівня. Згідно з положеннями законодавства України держава «гарантує конфіденційний характер відносин з особами, які допомагають СБУ. У свою чергу, конфіденти зобов'язуються зберігати таємницю, що стала їм відома під час виконання завдань. Забезпечення конфіденційності відносин з особами, які надають допомогу СБУ, особливо важлива та актуальна через складну оперативну обстановку» [5].

Початком парламентського нагляду є право законодавців приймати закони та затверджувати політику уряду. Цей нагляд також характеризується постійним на регулярній основі їх реалізації. Відстежуючи виконання законів та аспектів проведення політиків, депутати парламенту визначають на виявлять законодавчі недоліки. Це можуть бути погане керівництво, зловживання, корупція. Варто підкреслити, що парламентський нагляд є функцією всього парламенту. Все це підводить до виокремлення 3 рівнів парламентського нагляду: пленарні сесії, комітети та діяльність окремих депутатів парламенту.

Пленарна сесія – одна з форма парламентської діяльності, яка привертає багато уваги з боку ЗМІ. За висновком О. Золотар [12], вона є відправним пунктом парламентської влади та впливає на визначення майбутньої політики. Всі парламентські акти та рішення, обов'язкові для інших державних органів, проходять обговорення та голосування на пленарній сесії. В парламенті приймають закони, заслуховують політичні декларації та дають оцінки діями уряду» [4].

Нижче розглянемо рівні парламентського нагляду та завдання, які вони виконують.

Пленарна сесія:	затверджує політики/стратегію та урядову політику безпеки і оборони;
	ухвалює закони;
	затверджує використання державних коштів (закон про державний бюджет);
	обговорює та приймає рішення з пропозицій, проголошує вотум довіри;
	дає згоду на призначення на ключові посади (міністрів, директорів розвідслужб).
Комітети:	надають звіти та офіційні висновки щодо законопроєктів;
	проводять слухання, візити та інспекції на місцях;
	проводять розслідування (найчастіше – лише за згодою пленарної сесії);
	розглядають скарги громадян;
	видають звіти про нагляд для обговорення на пленарних засіданнях;
	надають рекомендації організаціям, за якими вони наглядають;
	надають висновки щодо кандидатів, за якими вони наглядають;
	у деяких країнах можуть заслуховувати та надавати висновок щодо кандидатів на посади керівників з розвідки.
Окремі депутати парламенту:	пропонують нові законопроекти чи поправки до законів;
	розглядають офіційні питання та запити до керівників виконавчої влади (на пленарних засіданнях, усно чи письмово).

Рисунок 2.2 – Рівні парламентського нагляду за розвідкою

Джерело: сформовано за даними [23].

Під час пленарних дебатів парламенти іноді можуть офіційно затверджувати урядову політику у сфері безпеки. Програма уряду, стратегія національної безпеки, оборонний огляд та інші стратегічні документи пролонгують політику національної безпеки. Зазначені документи визначають інтереси національної безпеки та виокремлюють завдання, які будуть пріоритетними у відомствах безпеки. У них може відзначатись рівень оборонних витрат, максимальна чисельність персоналу сил безпеки, необхідність закупівлі озброєнь і рівень участі країни у військових та цивільних операціях з підтримання миру. Навіть без окремої згадки, документи програми створюють загальні межі роботи воєнної розвідки, а також можуть окреслювати роль, яку мають розвідувальні служби та їх функціонал у безпековому секторі. Однак, нагляд більш ефективно й помітно проявляється на рівні комітетів. Для чинного парламенту важливою є добре організована структура постійних комітетів. І вона повинна повторювати структуру уряду. Саме за сильними комітетами закріплено формування незалежної культури, здатність незалежно, неупереджено мислити та діяти. Вони виступають у ролі головного інструмента парламентського впливу на процес вироблення політики та нагляду за виконавчою владою [17].

Комітети виступають у ролі найновішої гілки парламентського нагляду мають справу з секретними, складними, унікальними питаннями. Вони беруть на себе відповідальність наглядати за розвідкою. При цьому вони організовані по-різному і володіють різними повноваженнями.

Виходячи з порівняльного аналізу парламентів Європи, інші сфери парламентського нагляду не володіють різноманітністю у питанні організації. Можна виокремити три підходи до організації нагляду за розвідкою в порядку збільшення спеціалізації та ускладнення організації [40]:

- комітети з питань оборони та безпеки;
- комітети з нагляду за розвідкою;
- експертні органи з нагляду за розвідкою.

Експертні органи з нагляду за розвідкою зазвичай працюють поза межами парламента. Їх члени не виступають у ролі депутатів, проте призначаються парламентом. Далі варто приділити увагу характеристиці цих трьох типів органів нагляду за розвідкою та їхні порівняні переваги [3].

Парламентський комітет деяких країн, що має широкі повноваження, займається законодавством і наглядає за усім сектором безпеки. Під його наглядом перебувають міністерство оборони, міністерство внутрішніх справ, військові та правоохоронні служби, які знаходяться під керуванням цих двох міністерств. До цього списку також варто віднести інші органи безпеки, серед яких розвідувальні служби та міністерські департаменти, що займаються розвідувальною діяльністю. Ще десятиріччя тому, в багатьох демократичних державах комітет з питань оборони та безпеки мав статус єдиного комітету, що займався питаннями безпеки та розвідки. Така система зберігається і сьогодні у невеликих країнах: Молдова, Чорногорія, Албанія. Комітети з питань оборони та безпеки можуть виконувати лише поверховий нагляд за розвідслужбами. Все це через велику кількість установ та питань, які входять до їх компетенції. Для прикладу, у багатьох країнах сектор безпеки є одним із найбільших роботодавців і споживає велику частину державного бюджету. Часто вони приділяють увагу багатьом іншими питанням, більш важливим для суспільства. Але часто їм не вистачає ресурсів, часу, доступу до секретної інформації та знань, щоб звернути увагу на розвідку.

Комітети з широким колом повноважень вдаються до створення підкомітетів. Останні приділяють увагу конкретній установі або колу питань. Користь підкомітетів тому, що вони дають можливість групі членів комітети прослідковувати та оцінювати певне питання і після надавати комітету інформацію у вигляді звітів. Проте дієздатність підкомітетів доволі сумнівна через обмежений склад та відсутність мотивації аби організувати тривалу роботу.

Також варто виділити позапарламентські експертні органи, які створюють держави. До цих органів відносяться громадські активісти, діячі, колишні судді, політики у минулому. Члени таких органів призначаються парламентом і звітують перед ним та виконавчою гілкою влади. Про експертні органи можуть автономно приймати рішення, визначатися, які питання розглядати і по яких аспектах звітувати. Вони мають потужний секретаріат і фаховий допоміжний персонал, що працює на постійній основі, і тому можуть здійснювати нагляд постійно й на умовах повної зайнятості.

Експертні органи мають повноваження «відслідковувати законність роботи розвідувальних служб і дотриманнями ними прав людини. Проте їх повноваження можуть також включати в себе стеження за ефективністю операцій, адміністративною практикою чи застосуванням методів збирання інформації, що пов'язані із втручанням» [5]. Зазвичай вони доповнюють роботу парламентських комітетів (тобто комітетів з питань оборони та безпеки). Проте в окремих випадках парламенти перекладають повноваження нагляду на спеціалізований автономний орган і не мають спеціального парламентського комітету з нагляду за розвідувальними службами. Переваги цієї моделі протилежні недолікам, пов'язаним із парламентськими комітетами нагляду. Не рідко це професійні органи, які не мають інших обов'язків. Тому вони можуть присвяти нагляду більший відрізок часу. У членів непарламентських наглядових органів більший термін повноважень., що відкриває перспективи для отримання досвіду. Зазначимо, що їх посада не залежить від балансу влади в парламенті чи зміни уряду.

Як зазначає Є. Стратегопулос [51], нагляд непарламентських органів відбувається на постійній основі, навіть коли парламент на канікулах чи його розпускають для нових виборів. Вибір членів відбувається на основі їхньої кваліфікації. Їх досвід необхідний для того аби здійснювати дієвий нагляд. Вважається, що вони більш незалежні, аніж члени парламентських органів, бо не мають політичних посад. Разом з тим, вони не діють у середовищі, де нагляд може бути задіяний задля отримання політичної вигоди. Існують певні суворі

запобіжники, які відповідають за те, що їхні члени не братимуть участь у іншій діяльності, яка може вплинути на їхню позицію. Наприклад, виборна посада чи приватний бізнес може бути заборонені на період терміну членства.

Через обмежені ресурси ускладнене розуміння проблематики воєнної розвідки депутатами та працівниками парламентів. Відсутність чіткого аналізу цифрової розвідки для парламенту відбувається через залежність від інформації, наданої самим оборонним відомством. Монополія на інформацію не впливає позитивно на дієвий нагляд. Демократичний контроль недостатньо концентрується на питанні воєнної розвідки. Різниця від служб внутрішньої розвідки помітна. У кількох країнах Південно-Східної та Східної Європи служби внутрішньої розвідки контролюються через підтримку ними попередніх комуністичних та авторитарних режимів. Громадськість підозрює, що на них здійснюють тиск аби провести реформи.

У більшості країн воєнна розвідка отримала суттєву вигоду від довірливого ставлення суспільства до збройних сил. Також від підтримки військовослужбовців країни, що базуються за кордоном аби підтримувати мир чи проводити антитерористичні операції. Служби внутрішньої розвідки підвищили рівень прозорості для громадськості та здійснюють добрі рекламні кампанії. Але незважаючи на це воєнна розвідка все ще непомітна.

Секретність безпосередньо стосується керівництва. Контролювати та наглядати за урядовою бюрократичною організацією досить складно через вимогу секретності. Основні проблеми парламентського нагляду за розвідкою представлені на рис. 2.3.

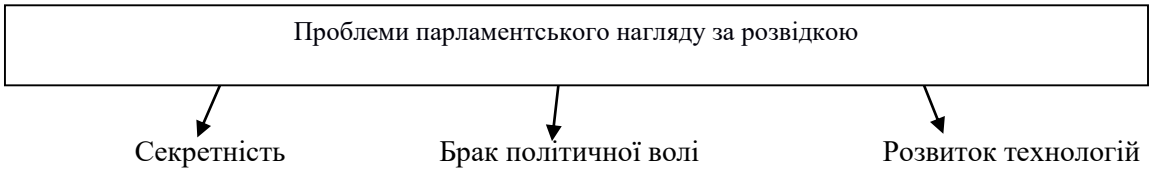


Рисунок 2.3 – Проблеми парламентського нагляду за розвідкою

Джерело: сформовано за даними [19].

За професійним розвідниками зазвичай залишається право самостійно приймати рішення під час своєї роботи на власний розсуд. Для дієвого нагляду за таємними операціями та самостійними рішеннями необхідні певні знання, доступ до інформації, зусилля і час. У вирішенні цієї проблеми можуть допомогти додаткові незалежні органи нагляду з чіткими повноваженнями доступу до секретної інформації.

Враховуючи рівень секретності у розвідувальних службах більша частина аспектів нагляду за розвідкою не обговорюються публічно. Тому можна стверджувати, що вони не мають вагомої користі в процесі боротьбі за увагу та голоси громадян. Деякі обрані представники можуть бути не зацікавлені витрачати час, аби наглядати за розвідкою.

Швидкий розвиток технологій знаходить застосування в діяльності розвідки. Це відбувається досить швидко, що органи нагляду не встигають адаптувати свої юридичні повноваження та досвід. Це призводить до прорахунків в підзвітності. Аби надавати органам нагляду важливу інформацію потрібно задіяти технічних експертів, й парламенти мають забезпечити своєчасну зміну юридичної бази паралельно з технічним розвитком. Рівні парламентського нагляду за розвідкою [7].

Стратегічна розвідка отримує розвідувальну інформацію і впливає на державну політику України, зміцнює обороноздатність, економічний й науковий, технічний розвиток України. Об’єднавшись з розвідувальними й правоохоронними органами України департамент бореться з міжнародною організованою злочинністю: тероризм, протизаконний обіг наркотиків, незаконна міграція, протизаконна торгівля зброєю і її виготовлення.

Інформаційне забезпечення проводить аналітичну обробку добутих даних, аби дати оцінку реальним й потенційним можливостям, намірам й діям іноземних держав, організацій і окремих осіб, які можуть загрожувати інтересам України. Також надає оцінку військово-політичній обстановці довкола України, виявляє загрози нацбезпеки держави. Отримана інформація від департаменту подається до вищого державного й військового керівництва. Структурні підрозділи департаменту організують заходи міжнародного військового співробітництва з розвідувальними органами інших держав.

2.2 Український досвід організації цифрової розвідки в умовах інформаційної війни з Російською Федерацією

Для новітньої історії української державності сучасні події стали найбільш разючим випробуванням. Через проведення РФ низки спеціальних операцій Україна вже втратила контроль над частиною своїх територій.

Сепаратизм та іноземне військове вторгнення об'єктивно загрожують Україні новою втратою територій. Уся ця ситуація продемонструвала, що система національної безпеки України неефективна, неефективна, слабка і не може протистояти багатовекторній агресії. Найбільш сильно та дієво на сьогоднішній день Російська федерація використовує зброю інформаційної війни.

Відповідно до законодавства України, поняття «інформаційна безпека» має таке визначення: «захист життєво важливих інтересів людини, суспільства і держави, запобігання нанесення шкоди державі через невчасність та невірогідність інформації, що використовується; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації» [7].

Тому можна стверджувати, що інформаційна безпека - діяльність органів державного управління. З цього випливає важливий висновок, що варто діяти активно, впливати на джерела інформаційної небезпеки. Відносно змісту інформаційної безпеки варто керуватися поняттям «цінності». Саме у цінностях виражаються інтереси суб’єктів суспільних відносин. Коли вони стикаються - виникають загрози. Інформаційні війни – одна з найбільш загроз для нормального функціонування системи органів державного управління.

Рисунок 2.4 – Види розвідки України за масштабами застосування

Джерело: сформовано автором за джерелом [23].

До складу цифрової розвідки відноситься комп'ютерна розвідка, за якою розвідувальні дані можуть бути отриманні з інформації, що присутня в засобах електронно обчислювальної техніки, локальних та глобальних обчислювальних мережах. Сюди також відноситься інформація, яка отримана через несанкціонований доступ.

Згідно з О. Шевчуком [53], цифрова розвідка проводиться на основі двох груп завдань:

1. добування розвідувальних відомостей з комп'ютерних систем або інформаційних мереж та їх обробка за допомогою апаратно програмних засобів;
2. добування і систематизація даних про потенційні джерела кіберзагроз за допомогою різних методів цифрової розвідки.

Перша група завдань вирішується завдяки реалізації комплексу заходів: несанкціоноване проникнення в мережі та комп'ютери іноземних державних та урядових організацій. Аби вирішити другу групу завдань (добування інформації про кібернетичні загрози) використовуються нові джерела, технології і прийоми. Йдеться про апаратно-математичне моделювання кібернетичних атак.

Засоби і методи розвідки у кібернетичному просторі впливають на процес реалізації кібернетичних атак. Вони надають можливість здійснювати планування наступальних кібероперацій аби домінувати у кіберпросторі над противником та наперед запобігти спрямованому кібернетичного впливу на

критично-важливі об’єкти. Задля забезпечення інформаційної безпеки слугують такі принципи як доступність, конфіденційність, цілісність інформації. А також комплекс заходів, спрямованих на забезпечення захищеності інформації. Певний вплив на будь-яку з цих складових можна розцінювати як кібернетичну атаку. В якості об’єкту атаки може виступати персональна електронно-обчислювальна машина, інформаційна система або мережевий пристрій. Передумова для успішної кібернетичної атаки – це перш за все ґрунтовна розвідка кібернетичного простору противника, яка характеризується часовим та якісним критерієм добування інформації, характеристик одного або більше віддалених комп’ютерів противника.

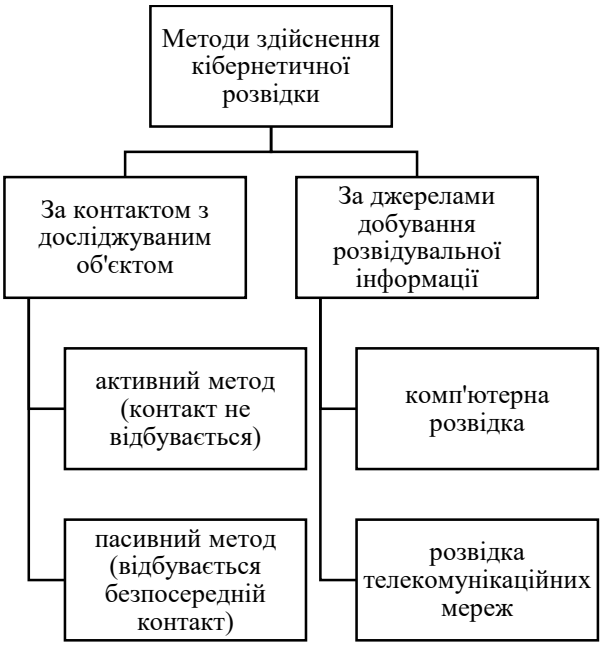


Рисунок 2.5 – Методи здійснення кібернетичної розвідки

Джерело: сформовано автором за джерелом [42].

Отримана інформація може використовуватися для створення моделі атакуючої системи та дозволяє полегшити майбутні спроби проникнення.

Розвідка кібернетичного простору противника поділяється на наступні етапи (рис. 2.6).

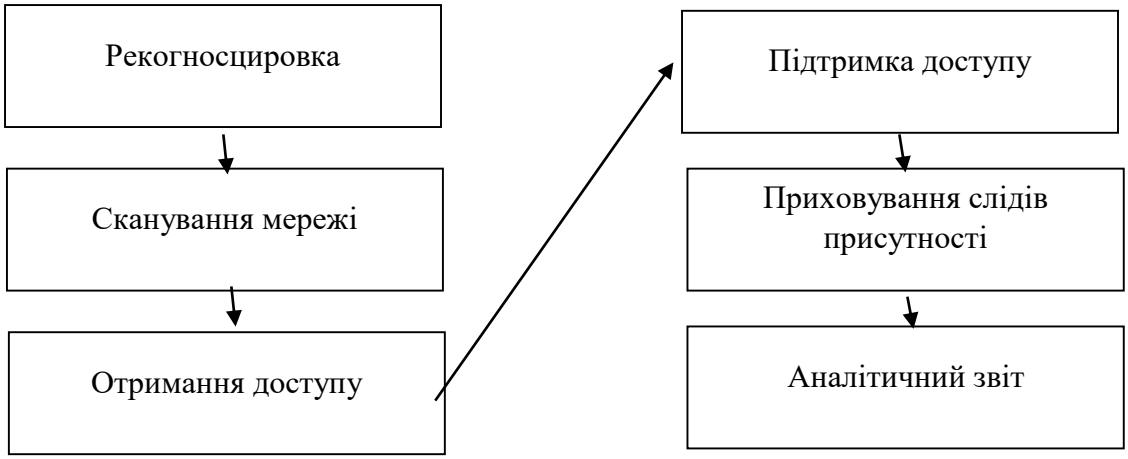


Рисунок 2.6 – Етапи проведення кібернетичної розвідки в Україні

Джерело: сформовано автором за джерелом [42].

Отже розглянемо більш детально кожен з етапів кібернетичної розвідки

1. Рекогносцировка відноситься до підготовчого етапу. Суб'єкт атаки має прагнення отримати інформацію про ціль до здійснення кібератаки. Рекогносцировка поділяється на два види:

- активна рекогносцировка – активна взаємодія з об'єктом атаки , що включає в себе використання будь-яких засобів. Наприклад телефонні дзвінки в службу підтримки певного органу, аби отримати певну інформацію;
- пасивна рекогносцировка – отримання інформації, для якої не потрібна взаємодія з об'єктом кібернетичного впливу. Наприклад пошук інформації на викинутих документах, записках, накопичуваних пристроях, комп'ютерах.

2. Сканування мережі належить до етапу попередньої атаки на противника. Це ситуація за якої атакуючий проводить сканування мережі аби отримати певну інформацію під час рекогносцировки. Сканування включає:

- сканування портів та IP-адрес;
- топологію мережі, сервісів, вразливості;
- визначення типу операційної системи.

3. Отримання доступу. На цьому етапі атакуючий отримує доступ до операційної системи або додатків на комп’ютері. І в подальшому може отримати повний контроль над системою. І це в свою чергу дає можливість приєднатися до проміжних систем, які пов'язані з нею. Атакуючий може заволодіти доступом на рівні операційної системи, рівні додатків або мережевому рівні. Це може виражатися у зламі паролів, переповнення буфера, відмові у обслуговуванні.

4. Підтримка доступу. Етап, на якому атакуючий намагається зберегти доступ до системи. Атакуючий може використати вразливості нульового дня з використанням Backdoor, Trojan, RootKit. Атакуючий може вдатися до завантаження, вивантаження або маніпулювання даними додатків або конфігурацією над атакуючою системою, користуватися системою аби запускати нові кібератаки.

5. Приховування слідів присутності. Етап, на якому атакуючий вдається до спроб здійснити непомітну атаку, приховавши докази, які могли б стати причиною кримінального переслідування.

6. Аналітичний звіт. Отримані розвідувальні дані піддаються аналізу , на основі якого формуються певні пропозиції та висновки, щодо реалізації кібернетичного впливу на противника. Аналітичний звіт - це опис, де зазначається ретельне дослідження противника, а також зображаються результативні показники та підсумки у кількісному та якісному вимірі. За ними залишається пріоритетна позиція в оцінці ефективності здійснення розвідувальних заходів під час отримання інформації про противника. Кожен з етапів кібернетичної розвідки має власну ціль та мету, яка в результаті дозволяє отримати інформацію про противника.

Якщо порівнювати з пасивним методом добування даних, активний метод виключає ймовірність помилкової ідентифікації віддаленого об’єкта зменшується врази. Це позитивно впливає на точність розвідувальної інформації та ефективність подальшого формування кібернетичного впливу на основі добутих розвідувальних даних про об’єкт дослідження.

До найбільш сприятливого засобу цифрової розвідки відноситься map-карта. Остання відкриває можливості для проведення розвідувальних заходів для дослідження віддаленого об’єкта противника. За умов обмеженого часу представлений інструмент не може за короткий час отримати необхідну розвідувальну інформацію про противника. Саме це спонукає до подальших досліджень, які необхідно зосередити на розробці та впровадженні розподіленої системи кібернетичної розвідки досліджуваного об’єкта противника. Це дозволить скоротити час на здобування інформації у ході проведення розвідувальних заходів. Метод активного добування - це безпосередній контакт з досліджуваним об’єктом розвідки, для якого використовуються методи прихованого сканування, що дає можливість бути непомітним при здійсненні впливу на противника (рис. 2.7).

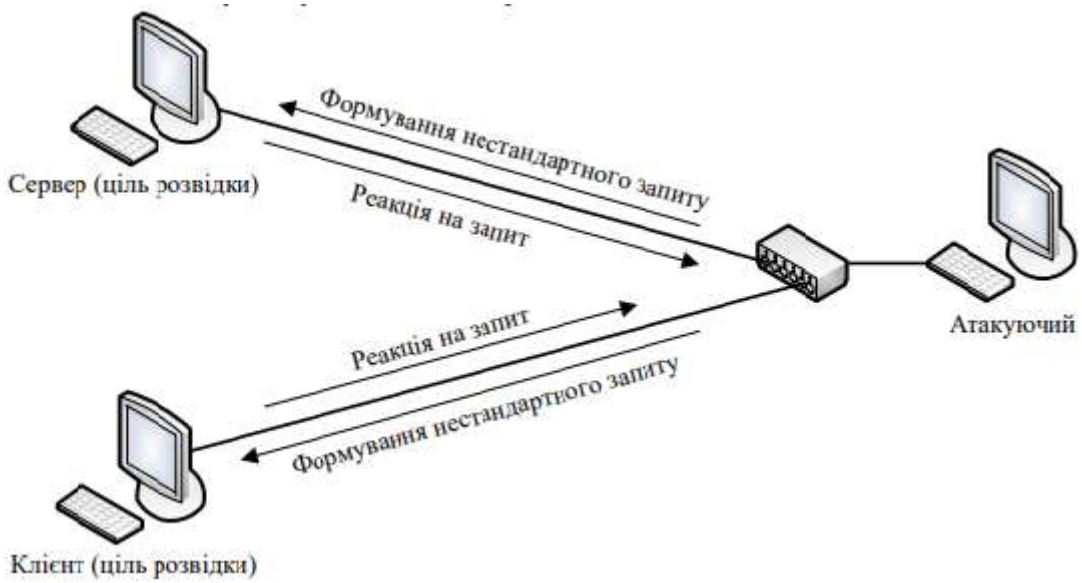


Рисунок 2.7 – Активний метод добування розвідувальних даних

Джерело: сформовано автором на основі [17].

Україна здійснює помітні кроки аби розвивати національний інформаційний простір та захищати свій інформаційний суверенітету.

Зокрема О. Резнік була проведена реалізація окремих положень вироблених рекомендацій:

- розвиток нормативного та правового забезпечення нацбезпеки в інформаційній сфері;
- вдосконалення системи підготовки фахівців з інформаційної та кібербезпеки, з підготовки й підвищення кваліфікації кадрів. Причому це стосується як державних, так і недержавних суб'єктів, з питань обміну інформацією щодо кіберінцидентів.

Указ Президента України від 14 вересня 2020 року № 392/2020 затвердив нову стратегію національної безпеки України. У документі окреслено актуальні та можливі загрози для нацбезпеки та націнтересів України, зокрема:

– зростає роль інформаційних технологій у всіх сферах суспільного життя;

– розроблюється система озброєння, для якої беруться за основу фізичні принципи, для яких використовуються квантові, інформаційні, космічні, гіперзвукові, біотехнологій, технологій у сфері штучного інтелекту тощо;

– уможливлюється поширення міжнародного тероризму та міжнародної злочинності у кіберпросторі, буде виявляти критичні проблеми в інформаційній та інших сферах, що можуть потенційно загрожувати національним інтересам та національній безпеці України. Нова стратегія національної безпеки України окреслює пріоритети національних інтересів України та національної безпеки і напрями забезпечення цих пріоритетів.

Відповідно до стратегії національної безпеки України визначаються пріоритетні завдання для правоохоронних, спеціальних, розвідувальних та інших державних органів спираючись на їх компетенцію. Зокрема – активна та ефективна протидія розвідувально-підривній діяльності, спеціальним інформаційним операціям та кібератакам з боку Росії та іншій підривній пропаганді. Основне завдання розвитку системи кібербезпеки- це гарантія

кіберстійкості та кібербезпеки національної інформаційної інфраструктури в за умов сучасної цифрової трансформації. Відповідно до нової стратегії національної безпеки України визначено завдання щодо реформування й розвитку сектору безпеки і оборони. Наголошується на завершенні створення національної системи кібербезпеки, формуванні сучасних спроможностей суб'єктів у питаннях забезпечення кібербезпеки і кібероборони та зміцнення системи їх координації. Враховуючи актуальну ситуацію, що склалася в державі, нові виклики та вимоги нормативно-правових актів висуваються певні вимоги, для виконання яких потрібно ще більше зусиль та наполегливої роботи у питанні забезпечення національних інтересів та національної безпеки України в інформаційній та кіберсфері. Для розв'язання зазначених завдань необхідно здійснити конструктивні наукові дискусії та обмінятися набутим досвідом на науково-практичних форумах аби напрацювати пропозиції для майбутнього розвитку інформаційного суспільства. Це також допоможе вдосконалити систему забезпечення інформаційної та кібербезпеки України, захистити її від агресивного інформаційного впливу з боку Російської Федерації.

Варто відмітити, що в Україні з 2016 по 2020 роки активно працювала національна розвідувальна програма. Головне завдання, яке закріплене за програмою – розвиток розвідки в України, організація розвідувальної діяльності відповідно до світових стандартів. На національну програму було покладено наступні завдання:

– фінансування розвідувальних органів України та контроль за використанням матеріально-технічно забезпечення;

– створення сприятливих умов для ефективної роботи розвідувальних органів;

– запозичення досвіду розвідок прогресивних країн;

– залучення інноваційний технологій у роботу розвідувальних служб.

Разом з тим, проводилися робота щодо нових методик та способів отримання та обробки секретної інформації. Відбувалася заходи щодо

підвищення кваліфікації кадрів розвідки. Безумовно, всі дії розвідки підпорядковувалися чинному законодавству міжнародним договорам та Конституції України.

Розвиток розвідувальної діяльності України за підтримки національної програми позитивним чином вплинув на зміцненні обороноздатності країни на інформаційному фронті.

Але безумовно багато над чим потрібно і надалі працювати, аби більш швидко та ефективно боротися з кібератаками противників, вираховувати потенційні загрози заздалегідь, формувати власну потужну систему отримання даних.

Проаналізувавши актуальні джерела ми визначали, що нової програми з цього питання немає. Тому вважаємо доцільним запропонувати розробку нової, більш досконалої розвідувальної системи. Варто враховувати аспекти, які не були включені до минулої версії програми. Розвідка України за умов активної підтримки уряду та іноземних партнерів має всі шанси стати потужною системою.

2.3 Зарубіжний досвід організації цифрової розвідки в умовах інформаційних війн

Якщо поглянути на розвинути країни, то їх розробка стратегій нацбезпеки заснована на системі оцінювання ризиків і загроз. Методологія оцінювання ризиків і загроз виступає у ролі системи оцінки ризиків і загроз у сфері нацбезпеки. Виходячи з цього вважаємо доцільним дослідження методологічних аспектів зарубіжного досвіду оцінювання ризиків і загроз у сфері національної безпеки.

Велика Британія, для прикладу, оцінює ризики у сфері національної безпеки використовуючи трьохетапну методологію. Перши і другий етап дозволяють виявити ризики всього спектру та ранжування ризиків відповідно до критеріїв тотожності і взаємодоповнення та їх розподілення по групам в категорії типових ризиків. Третій етап відповідає за формування шести класів ризиків. Візуалізувати ризики допомагає таблична матриця, яка побудована на основі двох параметрів виміру рівнів імовірності та наслідків надзвичайних ситуацій.

У документі «Оцінювання ризиків у сфері національної безпеки» [1, с. 14-15] представлені зовнішні та внутрішні ризики для національних інтересів, безпеки та оборони Великої Британії в інтервалі їх прояву від п’яти до двадцяти років, на основі якого розробляють Стратегію національної безпеки. Подібний підхід дає змогу прогнозувати ризики через імітаційне моделювання, для якого залучаються експерти та формується бібліотека моделей поширення ризиків, яку можна поповнювати.

У Королівства Нідерланди є власна система оцінювання ризиків і загроз, що є базою для стратегічного планування та розробки Стратегії національної безпеки. Вона включає в себе щорічну оцінку ризиків, а також сканування горизонту національної безпеки. Аналізуються тренди і загрози національній безпеці на перспективу. Методологія оцінювання ризиків і загроз у Королівстві Нідерландів визначена рядом керівних настанов, зокрема, «Настановою з питань комплексного аналізу та оцінювання ризиків для національної безпеки» від 2019 р. [1, с. 19-20].

Інформаційна сфера має важливе значення для забезпечення політики в цілому. Але процес інформатизації призвів до виникнення безпекової проблеми, що знаходить вираження у збільшенні вразливості суспільств перед зовнішніми впливами. У минулому столітті основною загрозою національної безпеки була військова агресія, то сьогодні термін «війна» вже отримує інше значення. Війна відбувається не лише з залученням зброї, а включає в себе економічний тиск, дискредитацію на міжнародній арені, дипломатію, а також

інформаційне протиборство. Тому інформаційний вплив за актуальних умов має статус вирішального для досягнення результату.

Організація діяльності британської розвідки пов'язана з різноманітними принципами, формами, методами, засобами роботи в інтересах досягнення цілей забезпечення національної політики і ефективного вирішення поставлених перед розвідкою завдань. Створюючи британську таємну служби та її принципи базувалися на певних вимогах. Британські фахівці, які займаються вивченням принципів ведення війни і розвідки, неодноразово відзначали, що ці принципи легко використовуються при вивченні боїв від найдавніших часів Сунь Цзи і Ганнібала до епохи Наполеона і новітньої історії періоду Черчилля.

Британські політики наголошуються на тому, що принципи повинні бути загальними, аби мати статус безпосереднього керівництва до дії за різних обставин. Але при цьому ніхто не стверджує, що принципи введення війни можна назвати універсальними. Кожен з принципів повинен мати чітку зрозумілу структуру. Це полегшить розуміння та подальше використання принципів. Важлива умова - це гнучкість формулювань, простота викладення і переважна відсутність спеціальної юридичної або філософської термінології. Принципи діяльності британської розвідки поділяються на такі групи:

- стратегічні;
- тактичні;
- адміністративно-управлінські;
- оперативні;
- інформаційно-аналітичні;
- кадрові.

У своїх дослідженнях О. Золотар [32], підкреслює, що «різні країни мають різні моделі служб воєнної розвідки, їх сфери діяльності перетинаються у відповідному міністерстві оборони та розвідувальної спільноти. Цифрова розвідка відрізняється від цивільних розвідувальних служб, ти що підпорядковується сектору оборони та належить до структури відповідного

міністерства». До прикладу, відповідно до закону про організацію сил оборони України: «Центр воєнної розвідки виступає у ролі структурного підрозділа Сил оборони. Його основне завдання - проводити воєнну розвідку й прослідковувати розвідувальні операції та заходи безпеки інших структурних підрозділів, надавати міністру оборони, командувачу Сил оборони та заступнику командувача Сил оборони розвідувальну інформацію та інформацію з питань безпеки, а також виконувати інші функції, передбачені законодавством» [11]. Помітна різниця між підрозділами воєнної розвідки, які є частиною Збройних сил, та служб, які не є частиною армійської структури, мають цивільний статус, проте виконують завдання воєнної розвідки.

У більшості випадків одночасно діють різні види підрозділів воєнної розвідки, які підпадають під різні режими нагляду. Те, що воєнна розвідка підпорядковується командним структурам є проблемою для парламентського нагляду. Венеціанська комісія Ради Європи зазначає: «Військові відомства мають суттєву різницю від цивільних відомств. Головне завдання перших - це збір розвідувальної інформації, яка охоплює загрози державі та безпеці лояльності збройних сил. Проте межу між цим завданням та завданням цивільного відомства доволі важко провести. У підзвітності виникають великі проблеми якщо служба безпеки організаційно належить до структури військового командування» [14]. Служби воєнної розвідки на національному і міжнародному рівнях проводять співпрацю з різними відомствами сектору безпеки. Вони підтримують збройні сили, організовують тренування за кордоном у межах спільних миротворчих місій чи на двосторонній основі, беруть участь у міждержавних інформаційних системах. Проводять обмін розвідувальною інформацією із закордонними військовими розвідувальними службами.

На думку В. Варенко [46] «В контексті сучасних транскордонних загроз виникає необхідність у більш тісній постійній співпраці з іншими службами безпеки та правоохоронними органами». Разом з тим завдання та обов’язки служб воєнної розвідки, а також засоби, якими вони керуються у

своїй роботі отримують більш складний характер. Військові розвідувальні служби здійснюють повний спектр розвідувальних операцій: агентурна розвідка, радіо- і радіотехнічна розвідка, візуальна розвідка, розвідка з відкритих джерел та інші її види.

Великий обсяг завдань, широка міжнародна співпраця, а також вагомий обсяг видів операцій служб воєнної розвідки призводять до не лише фундаментальних проблем з точки зору дієвості парламентського нагляду. Це може призвести до появи непропорційної й невиправданої перешкоди для реалізації основних прав. Якщо говорити про методи роботи, то служби воєнної розвідки керуються широким спектром засобів, які присутні і в цивільних розвідувальних служб. В процесі розробки механізму нагляду слід брати до уваги складність і спектр операцій воєнної розвідки. А також пам'ятати про адміністративно-керівну структуру. В одному відомстві можуть об’єднуватися засоби та керівництво цифрової та воєнної розвідки. Разом з тим, вони можуть розподілятися по всій системі збройних сил та оборонному сектору.

Враховуючи останні світові події можна зробити висновок, що країни намагаються забезпечити кращу координацію, діюче керівництво та нагляд, а також більш ефективний обмін інформацією між розвідувальними службами. Для того, аби реалізувати подібні завдання створюються нові координаційні структури та змінюється нормативна база.

Стосовно Канади було зазначено, що «управління воєнною розвідкою є складною через делікатність, а також через те, що досвід і ресурси воєнної розвідки сильно розділені по організаціях Міністерства оборони та командуваннях Збройних сил Канади» [13]. Річний звіт за 2018 рік вказує на те, що необхідно регулювати воєнну розвідку на державному рівні. Саме це відкриє можливості для ефективного захисту основних прав.

Таблиця 2.1 – Світовий досвід організації розвідувальної діяльності

Країна	Особливості
США	Створення загальносвітової агентурної мережі. Беруться до уваги передусім інформаційні, символічні та віртуальні стратегії корпорацій і держав як корпорацій, а не індустріальні чи військові в їх архаїчному розумінні; Орієнтація на на корпорації та корпоративний підхід. Контактування з креативним класом по всьому світу, а представники цього класу, зокрема журналісти, стають агентами в усіх країнах світу.
Велика Британія	Лідер у наданні приватних розвідувальних послуг. Бюджет галузі — близько 20 млрд. доларів. Приватні розвідувальні компанії ВБ вивчають масову поведінку людей та способи її зміни, здійснюють акції впливу. Втручалися у вибору у таких країнах як Нігерія, Індія, Індонезія, Тайвань, Колумбія. Використовують технології глибинного аналізу даних.
Ізраїль	Приватними розвідувальними компаніями використовуються такі методи: проникнення в цільову аудиторію в соціальних мережах спеціально створених фейкових учасників; поширення оманливої інформації через вебсайти, що імітували новинні портали; дискредитація політичних опонентів завдяки організації вручення хабарів чи звинувачень у сексуальних домаганнях. Також вдавалися до наступних способів: онлайн-управління сприйняттям, вплив через соціальні мережі, маніпулятивні кампанії, стратегічна дезінформація (наприклад, підготовка фейкових новин чи пропагандистської продукції),
Об'єднані Арабські Емірати	Характеризуються «наступальними» заходами (тобто злам комп'ютерних мереж, кібернетичних атак, незаконне отримання доступу до даних в мережі Інтернеті), зокрема в інтересах уряду. Проводиться стеження за урядами інших країн, терористами та політичними противниками. Переманює персонал конкуруючих країн.

Джерело: сформовано автором за даними джерела [48].

У таблиці 2.1 проаналізовано досвід США, Великої Британії, Ізраїлю та Об'єднаних Арабських Еміратах щодо організації розвідувальної діяльності. У всіх країнах набувають розповсюдження приватні розвідувальні компанії. Високий професіоналізм забезпечує їх «непомітність» під час виконання робочих обов'язків. Українській розвідці варто запозичити досвід зарубіжних партнерів.

РОЗДІЛ 3
УДОСКОНАЛЕННЯ ОРГАНІЗАЦІЇ ЦИФРОВОЇ РОЗВІДКИ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ З РОСІЙСЬКОЮ ФЕДЕРАЦІЄЮ

3.1. Виклики Російсько-Української інформаційної війни

До того як почалася гібридна російська агресія проти української державності здійснювалася масштабна інформаційна кампанія. В. Задірака [33] наголошує на тому, що «Росія використовує інформацію в якості головного ресурсу сучасного суспільства, зброї масового ураження. Головна мета – змінити внутрішні установки, ідеали, поведінку, думки населення в тому напрямку, який потрібен агресору. У подальшому використати ця частина населення може бути використана як елемент».

Під час підготовки до вторгнення застосовувався увесь наявний арсенал засобів масової інформації. Використовувалися зовнішні сили разом с російськими мас-медіа, а також внутрішні інформаційні ресурси, лідери громадської думки, проросійські громадські об’єднання та політичні сили. Б. Кормич [35] підкреслює, що Російська Федерація протягом довгого періоду часу використовувала інформаційний ресурс аби загострювати різноманітні суперечності в середині України: соціально-економічні, релігійні, етнічні, політичні та культурні. Це необхідно для того, аби поділити населення на протиборчі сторони та послабити суспільство внутрішньо. Інформаційні атаки спрямовані аби посилити протистояння між громадянським суспільством і органами державної влади. В український політичний простір Росія інтегрувала сили, які займаються лобіюванням ворожих інтересів для державності України. Це призвело до значного впливу російських ідей на півдні та сході України.

За твердженням І. Захарова [48], «інформаційний чинник виступає у ролі головної складової гібридної війни РФ проти України. Через недостатню оцінку цього фактору Україна виявилася неготовою до нападу з боку РФ та не змогла вчасно протистояти використовуючи ефективні методи та засобами. Саме це спричинило величезні втрати для Української держави. РФ використовує інформаційний та культурний простір, аби просувати свої інтереси та культурні цінності, які є шкідливими для державності України. Технології маніпуляції та пропаганди є основними складовими російської інформаційної компанії. Росія підключила медійний та політичний ресурс, аби поступово розділити українське суспільство на дві протиборчі табори – Схід та Захід. Для цього Росія залучає релігійні, культурні, етнічні, соціальні, протиріччя між жителями різних регіонів, підсилюючи їх конфронтацію між собою. Українська політична еліта за багато років на жаль не приділила великої уваги цим передумовам, що вказували на подальшу гібридну агресію. Це розв'язало руки проросійським силам і дозволило вільно інтегрувати в Україні свої інформаційні продукти».

Сьогодні Україна протистоїть агресору як зброєю, так і на інформаційному фронті. Перед нашої державою постає важливе завдання – виробити ефективні засоби протидії інформаційному впливу та атакам на український інформаційний простір зсередини. Доцільно вести альтернативну інформаційну компанію щоб протидіяти деструктивному російському впливу, як усередині країни, так і на міжнародному рівні.

Є. Стратегополус [51] провівши наукову розвідку з цього питання стверджує, що « РФ аби зміцнити свої позиції у Європі вдається до використання «інформаційної зброї», намагається здійснювати вплив на внутрішньополітичну ситуацію у європейських державах. Разом з тим підживлює конфліктні ситуації, до створення яких сама і причетна. Аби відновити свій вплив в Україні Російська Федерація не зупиняє гібридну війну, використовуючи засоби політичного, економічного, інформаційно-психологічного характеру». Її деструктивна пропаганда покликана

розпалювати ворожнечу, провокувати міжнаціональні та міжконфесійні конфлікти, підривати суспільну єдність.

Варто виокремити наступну думку В. Голоти [50] «духовна атмосфера суспільства Росії знаходиться під повним контролем пропаганди Кремля. Матеріальна база суспільства поступово розвивається під тиском інновацій інформаційної цивілізації. Через механізми самоорганізації соціального світу вона виходить назовні. Саме через це в Росії є Інтернет, Facebook та інші світові мережі. Адже на цьому етапі саморозгортання соціального світу розвиток суспільства відбувається швидше, ніж зміни у мисленні людини». Державне керівництво РФ базується на ідеологемах попередніх етапів життєвого циклу індустріальної цивілізації.

Варто звернути увагу на те, що у своїх промовах президент РФ критикує Володимира Леніна, Микиту Хрущова, але захоплюється стратегією Йосипа Сталіна. Тому в регіонах Росії відновлюються пам'ятники Й. Сталіну. Це з одного боку, а з іншого – можна простежити, що російське керівництво не надто добре сприймає реалії інформаційної доби. Через це вони намагаються заборонити в країні соціальні мережі, та інші нові комунікативні можливості через які громадяни спілкуються між собою і зі світом. Керівництво РФ керується страхом, що поведінка людей може вийти поза межі контролю силового блоку держави.

П. Хамула [28] застерігає, що «керівництвом РФ робляться спроби використати технічні можливості інформаційної цивілізації аби наростити військову потужність. У сфері пропаганди вони намагаються контролювати свідомість пересічних громадянин країни. А також витрачає великі кошти аби підтримувати пропагандистські канали. Наприклад канал Russia Today, який спрямований на зарубіжну аудиторію. Поведінку сучасного державного керівництва РФ можна назвати гібридною через те, що духовний елемент, який вони беруть за основу, напрацьований ще за індустріальної доби. Росія запозичує технологічні можливості для ведення агресивної політики і гібридної війни з інформаційної цивілізацією. Інформаційне забезпечення -

головний етап російської наступальної кампанії. Через поширення інформації із закодованим повідомленням представляється можливість підготувати наступ, збурити громадян виступати проти власної держави. За допомогою використання викривленої, маніпулятивної інформації, агресор із залученням ярликів, стереотипів, міфів та страхів в певній частині суспільства прагнув спонукати громадян на дії. Все це комплексно суттєво послаблювало внутрішньодержавні позиції політичної влади Україні». Війна здійснюється із залученням накопичених медіаресурсів, що має агресор. Як окремій людині захиститися від агресивного впливу ЗМІ. Лише формуючі у собі високу політичну культуру та самосвідомість.

О. Рєзнік [31] у своїх наукових дослідженнях наголошує, що «якщо проаналізувати події з початку загострення відносин між Україною та Російською Федерацією можна простежити наскільки неефективною була інформаційна політика, нескоординована діяльність різних суб'єктів забезпечення інформаційної безпеки держави, слабка присутність України на теренах світового інформаційного простору. Вище воєнно-політичне керівництво зазначає як пріоритетні проблеми забезпечення інформаційної безпеки держави та проведення дієвого комплексу заходів контрпропаганди, реалізацію інформаційної політики, спрямованої на консолідацію українського суспільства та міжнародної спільноти з метою стримування збройної агресії. Україна не може адекватно реагувати на виклики та ризики у воєнній сфері через внутрішні та зовнішні фактори. Тому виникає потреба у тому, щоб розробити систему поглядів та визначити дії воєнно-політичного керівництва України. Все це дуже потрібно аби реалізувати державну інформаційну політику та забезпечити інформаційну безпеку України». На нашу думку головна проблема реалізації державної інформаційної політики та забезпечення інформаційної безпеки України полягає у відсутності злагодженості діяльності всіх державних інституцій в інформаційному просторі, а також конкуренція між ними. Також значна частина інформаційних

заходів спрямована аби створити імідж кожної окремої інституції, а не досягати загальні цілі держави.

В. Варенко [46] підкреслює, що не вирішення зазначених проблем стає причиною наступного:

- неоднозначного розуміння аспектів державної інформаційної політики різними верствами населення України, населенням тимчасово окупованих територій, керівництвом та населенням країни-агресора РФ, міжнародної спільноти;
- функції моніторингу інформаційного простору дублюються;
- загрози інформаційної безпеки виявляються несвоєчасно, прогнозування наслідків загроз інформаційній безпеці України здійснюється не точно;
- між державними інституціями процес обміну інформацією досить складний.

На думку О. Левченко [44] «реалізацію державної інформаційної політики України необхідно робити щоб забезпечити єдине розуміння офіційної позиції України. Варто окреслити події та процеси, які відбуваються в Україні, чітко зазначити позицію України в світі; задовольнити національні інтереси держави». За умов конфлікту з РФ державну інформаційну політику України необхідно спрямувати на відновлення суверенітету та територіальної цілісності України. І звичайно ж завершити конфлікт та стабілізувати постконфліктну суспільно-політичну ситуацію.

Аби забезпечити інформаційну безпеку та створити відповідні умови, на думку В. Задіраки [33], необхідно окреслити основні завдання, які дуже потрібні для реалізації державної інформаційної безпеки України:

– забезпечити постійний моніторинг інформаційного простору (внутрішнього та зовнішнього), а також систематично аналізувати результати моніторингу;

– чітко визначити загальнодержавний стратегічний наратив та особливості його трактування різними українськими державними інституціями;

– створити механізми, які дозволять унеможливити відхилення від наративу при проведенні інформаційної діяльності різними державними інституціями; скоординувати роботу державних інституцій в інформаційному просторі;

– реалізувати принципи та методи стратегічних комунікацій всіма державними інституціями, які займаються інформаційною діяльністю;

– виявити, оцінити та дати прогноз наслідкам загроз національним інтересам та нацбезпеці України в інформаційній сфері;

– протидіяти інформаційним впливам зовні на населення України: на воєнно-політичне керівництво, особовий склад всіх складових Сектору безпеки і оборони України;

– захистити об'єкти української критичної інформаційної інфраструктури.

Згідно висновків О. Рєзніка [40] мережева війна має два аспекти:

– 1. Технологічний. Це війна нових можливостей. Мережа постає у ролі механізму. Найбільше поширення в сучасній мережевій комунікації мають кібератаки на державні установи, оборонні та високотехнологічні компанії, а також кіберзлочини, що несуть фінансовий збиток.

– 2. Соціальний. Цей аспект вирізняється формуванням нових груп, кібернайманців. Саме вони роблять різноманітні напади. Кібернайманці – це організовані групи хакерів, що мають високий рівень підготовки. Їх наймають уряди та приватні компанії, аби організувати та провести складні цільові атаки на державні структури та установи, приватні компанії. Все робиться аби потрапити в бази даних, викрасти інформацію, знищити дані чи навіть інфраструктуру тощо.

Отже, мережева війна – «це війна нового покоління, кардинально новий рівень протиборства між державами. Це воєнне мистецтво та разом з тим форма геополітичного насильства, для якої залучається велика кількість суб'єктів» [40].

На думку Н. Рибалки [29] «забезпечити кібербезпеку України можна через комплексне застосування заходів правового, організаційного, інформаційного напряму. Проаналізувавши дані можна прослідкувати наявність прогалин у правовому полі та колізій законодавчих та інших правових актів. На останні покладена регламентація контррозвідувальної та оперативно-розшукової діяльності, охорона державної таємниці. Все це підкреслює, що потрібно займатися вдосконаленням правових і організаційних засад забезпечення конфіденційності відносин з особами, які допомагають СБУ».

Автор російської концепції «гібридної війни», начальник Генштабу РФ генерал В. Герасимов, виступаючи на зборах Академії військових наук у 2013 році, охарактеризував її так: «Акцент використовуваних методів протиборства зміщується в бік широкого застосування політичних, економічних, інформаційних, гуманітарних та інших невійськових заходів, реалізовуваних із задіянням протестного потенціалу населення». Все це доповнюється воєнними заходами прихованого характеру, в тому числі реалізацією заходів інформаційного протиборства і діями сил спеціальних операцій. До відкритого застосування сили – часто під виглядом миротворчої діяльності та кризового реагування – переходять тільки на якомусь етапі, в основному для досягнення остаточного успіху в конфлікті [40].

У цих розробках Генштабу Росії були використані теоретизування колишнього білоемігранта Є. Месснера, праці якого в Росії стали поширюватися з 2006 року. Це не «класична війна», а новий тип «спецоперації». Дослідник Месснер розробив концепцію, згідно з якою війни будуть точитися не за території та ресурси, а «за душі націй», то будуть бунтівні війни – «заколот-війни». Тобто це будуть такі конфлікти, в яких

матеріалом є національні та соціальні чвари й дезінформація, вони, по суті, є війнами передусім психологічними. Це провокування жорсткої напруженості. У «війнах» такого плану найбільша користь від спецназу. На полі бою результат таких воєн простежити неможливо.

Не оминув цей теоретик війни і моральний аспект таких дій та їх глобальне призначення, яке нам – українським та російським інтелектуалам – треба знати, щоб розуміти сутність так званої «української кризи»: «Треба припинити думати, що війна – це коли воюють, а мир – коли не воюють. «Заколот-війна» є розбій, жахливий, різноманітний, для совісті неприйнятний, але для безсовісного розуму зрозумілий і потрібний, як руйнування Світової структури, ймовірно не придатної для перенаселеного Світу». Тобто Кремль використовує той набір сил, засобів, способів та сценаріїв їх застосування, який він вважає достатнім для досягнення своїх цілей у протистоянні із заздалегідь і цілеспрямовано зруйнованим сектором безпеки України. У міжнародній практиці конфлікт такого типу визначають як «війна чужими руками». Росія готувалася сама та підготовлювала світ до цього конфлікту щонайменше сім років – від промови президента Росії Путіна в лютому 2007 року на конференції з безпеки в Мюнхені. Окрім класичних воєнних методів, Росія в рамках «гібридної війни» застосувала концепцію «війни трьох кварталів».

Суть зазначеної концепції, за визначенням Р.Тевліна [25] полягає в тому, що «від сучасного воїна вимагається готовність в одному кварталі вести загальновоєнний бій, у другому – вже виконувати поліцейські функції, а вже в третьому – брати на себе гуманітарні місії». Метою Російської Федерації є через успіхи у локальних конфліктах продемонструвати можливість вирішувати тактичні завдання, підвердитиглобальне лідерство на основі «особливої моделі» відносин із навколишнім світом. Москва через визнання незалежності Південної Осетії й Абхазії, анексії та включення до свого складу Криму відповіла на «прецедент Косово». Росія хоче мати великий вплив завдяки створенню «зони привілейованих інтересів» по периметру власних

кордонів і підвести світ до визнання свого права втручатися у внутрішні справи інших суверенних держав. Подібна поведінка Російської Федерації виступає викликом для ЄС і США. Очікувальна стратегія чи позиція м'якої сили можуть не мати жодної ефективності у боротьбі з Росією.

Парадигма сучасної війни змінюється через залучення невоєнних структур. Про це говорить і Ф. ван Каппен [33]: «Гібридна війна» об'єднує у собі класичний тип війни, до якого включається використання нерегулярних військових формувань. Держава, яка проводить гібридну війну, оформлює договір з недержавними виконавцями. Це можуть бути бойовики, терористи, групи місцевого населення, організації. Зивчайно зв'язок з якими повністю заперечується. Ці виконавці можуть роботи певні дії, які сама держава виконувати не може. Таким чином «брудну роботу» можуть брати на себе саме недержавні формування».

Концепція «війни трьох кварталів», яку реалізує Росія на території України, пітверджує реальність зазначених міркувань. Особливо це стало очевидним під час анексії Криму. Проте зазначена концепція була реалізована не в «просторовому», а в «часовому», до того ж «зворотному» її вимірі. Спочатку «зелені чоловічки» з'явилися в Криму як виконавці квазігуманітарної місії із забезпечення «прав російськомовного населення». Однак поступово почали виконувати функцію поліцейских аби забезпечити потрібне Москві проведення «референдуму». Незабаром вони вже виконували і квазівоєнні функції щодо силового нав'язування виконання результатів «референдуму».

Як зазначає В. Бойко [23] «на регіональному рівні спостерігаємо двосторонній конфлікт між Україною та Росією. Одна з його причин полягає в тому, що було зруйновано пострадянську систему відносин. Разом з тим Росії виявила бажання відновити «історичну справедливість». Поставила собі мету повернути свої втрачені позиції у регіоні, який постає для неї власною сферою впливу. Цілеспрямовано йде того, аби забезпечити собі належне місце у архітектурі безпеки та співробітництва світового рівня». Росія розглядає

Україну насамперед як предмет свого впливу та ключову складову пострадянських інтеграційних процесів. Відтак сьогодні постає нагальна потреба у розробці сценаріїв врегулювання конфлікту на сході. Від українсько-російського врегулювання та способу примирення буде залежати мир, стабільність та добробут не лише обох країн, але й інших країн регіону Східної Європи, Південного Кавказу та Центральної Азії.

Наразі з 24 лютого 2022 року відбувається повномасштабне військове вторгнення. Російська Федерація збройним шляхом захопила частиною території України. Разом з тим активно проводить активну інформаційну війну, залучаючи усі можливі методи та засоби.

Яким чином надалі Росія може впливати на Україну в рамках інформаційної війни? Створимо певний прогноз.

– Шантаж. Різнопланові елементи шантажу України та світу: застосування ядерної зброї, підрив Запорізької АЕС, руйнування Каховської ГЕС. Примус до того, аби прийняти умови РФ. Зокрема Росія таким чином може активно схиляти до переговорного процесу.

– Знищення об'єктів інфраструктури. Залякування, терор цивільного населення. Серйозні удари по економіці країни, аби спровокувати глобальну кризу, позбавити населення усіх необхідних ресурсів.

– Випуск фейкових даних в український інформаційний простір. Аби створити інший негативний образ України.

– Дискредитація українських військових. Підробні відео та фото матеріали, провокативні заяви та звинувачення. Зображення українських військових у негативному світлі.

– Підрив довіри до української влади. За рахунок «зливу» неоднозначної інформації, аби розхитати обстановку в середині країни. Активне застосування російської пропаганди для цього.

– Прийняття документів. Референдуми, приєднання територій, мобілізація, видання нелегітимних законів.

– Кібератаки на банківські установки, бази даних, державі установи, сайти та можливе оприлюднення конфіденційних даних. Бажання паралізувати фінансову систему України.

На мою думку, українська цифрова розвідка має великий потенціал, який можливо реалізувати. Але для цього необхідно вжити певні заходи. Було проведено SWOT аналіз цифрової розвідки в Україні, який представлено у таблиці нижче.

Таблиця 3.1 – SWOT аналіз цифрової розвідки в України

			Чинники зовнішнього середовища	
			Можливості	**Загрози**
			1. Залучення технічної, інформаційної допомоги від інших країн. 2. Перейняття досвіду від зарубіжних колег. 3. Гранти від міжнародних організацій та компаній.	1. Активізація військової агресії з боку РФ. 2. Міграція кваліфікованих кадрів. 3. Кібератаки, злив конфіденційної інформації. 4. Посилення інформаційної війни. 5. Дискредитація українських військових.
Чинники внутрішнього середовища	**Сильні сторони**	1. Кадровий потенціал. 2. Вмотивованість. 3. Великі перспективи становлення та інтеграції у європейський простір.	Кошти, надані партнерами необхідно залучати разом з тим на стимулювання розвитку розвідувальної діяльності в Україні. Оновлювати устаткування, орієнтуватися на сучасні технології отримання інформації.	Аби знизити дію загроз на українську розвідку необхідно працювати над її підсиленням. Розширювати розвідувальну мережу. Підвищувати кваліфікацію працівників.
	Слабкі сторони	1. Корупція та недостатнє фінансування з бюджету. 2. Застаріле устаткування та технології радянського зразка. 3. Відсутність комплексного управління та контролю.	В умовах повномасштабної війни безумовно важко розвивати роботу розвідки в Україні. Українська розвідка зазнає сильного тиску з боку РФ і працює у важких умовах.	Мінімізувати слабкі сторони можливо якщо провести комплексне оновлення української розвідки: від управління до технічного забезпечення. Проаналізувати досвід розвідок різних країни та запозичити ключові, ефективні моменти їх роботи.

Джерело: розроблено автором.

Аби звести до мінімуму вплив, який може здійснити російська розвідка необхідно активно укріплювати українську розвідку. Стіни повинні будуватися не тільки на державних кордонах, а і у інформаційні та цифровій сферах.

3.2 Перспективні напрямки удосконалення нормативно-правового забезпечення цифрової розвідки органів державної влади в Україні

А. Лапкін [24] у наукових розвідках звернув увагу на створення «Військового університету технологій як виступив у якості інтегрованої загальнодержавної структури. Він необхідний для здійснення наукових досліджень, підготовки кадрів різного рівня». Також дозволяє зосередитися на пріоритетних високотехнологічних напрямах з інформаційної та кібербезпеки, інформаційних технологіях, технічних видах розвідки. Не останнє місце у цьому питанні займає радіоелектронна боротьба, технічний захист інформації та криптології, космічні системи та геоінформаційне забезпечення. Дорого вартісні, але дуже потрібні технології автоматизованої обробки інформації, інформаційно-аналітичної роботи, інформаційно-психологічних дій, інформаційно-телекомунікаційних систем, спеціального зв'язку, експлуатації та застосування робототехнічних комплексів і систем боротьби з ними. Виключити однотипну підготовку фахівців дозволить впровадження нанотехнологій у військовій сфері та зброї, побудованої на нетрадиційних і новітніх принципах. Військовий університет відповідає за те, аби забезпечити раціональне використання ресурсів, насамперед фінансових та кадрових. Працює над підвищенням якості підготовки фахівців з високотехнологічних напрямків для всіх видів збройних сил і інших міністерств і відомств сектора безпеки і оборони держави. Стимулює ефективність досліджень, розробку, створення, випробування і застосування інноваційних технологій у озброєнні.

Аби розвідувальна діяльність була успішною необхідно виконати певні вимоги, які розгорнуто представлені у таблиці.

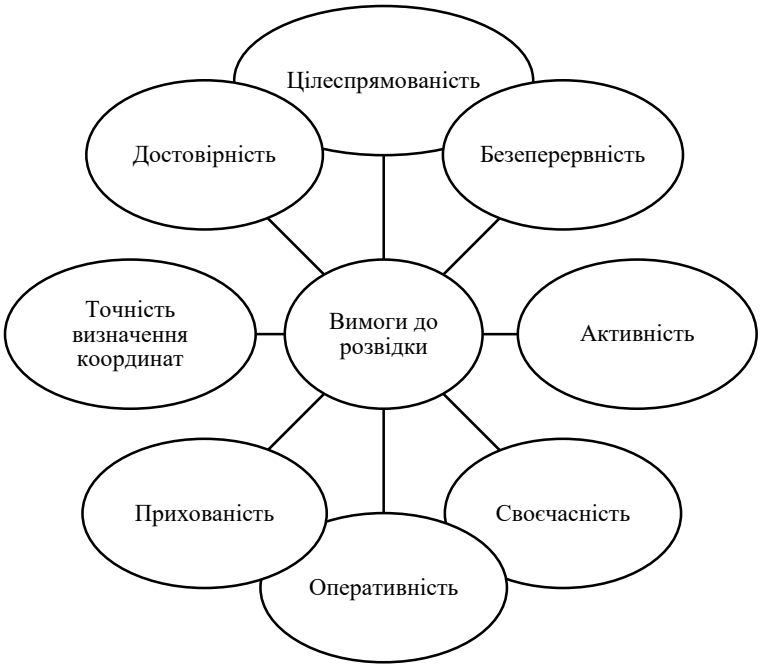


Рисунок 3.1 – Вимоги до організації розвідувальної діяльності

Джерело: створено автором за джерелом [25].

Розглянемо кожен з пунктів вимог до організації розвідувальної діяльності більше детально:

– Безперервність. Розвідка треба проводити постійно незалежно від пори року і доби, за будь-якої погоди, за будь-яких умов й у всіх видах бойової діяльності військ. І здійснювати розвідку поки не відбудеться повний розгром противника.

– Активність. За рівних умов успіх в розвідці чи бою, приходить до того, хто вдається до більш активних і рішучих дій. Командири і штаби, що займаються організацією розвідки, повинні підтримувати активний темп діяльності. Активності у розвідці можна досягти завдяки умілому використанню різних сил і засобів, ініціативністю, рішучими діями підрозділів, які відправили у розвідку.

– Цілеспрямованість. Кожна розвідка потребує цілеспрямованої організації. Тобто зусилля і засоби розвідки повинні бути зосереджені на головному напрямку і на виявленні найважливіших об'єктів. Варто спрямувати діяльність розвідувальних органів на те, аби своєчасно доправити командиру точні розвідувальні дані, які дуже необхідні для виконання поставленого завдання під час бою.

– Своєчасність і оперативність. Добувати необхідну розвідувальну інформацію необхідно до встановленого терміну. Це важливо, аби командири могли спрогнозувати майбутні дії противника, вчасно прийняти рішення й ефективно користуватися вогневими засобами. Цінність відомостей знижується, якщо командир одержить їх запізно.

– Прихованість. Суворе збереження у таємниці всіх заходів щодо організації і ведення розвідки. Але прихованість не повинна впливати на повноту отримання розвідувальних даних виконавцями.

– Достовірність розвідувальних даних і точність визначення координат об'єктів. Достовірність – один з найбільш важливих показників розвідки. Достовірні дані дають можливість прийняти правильне рішення, що приводить до успіху на полі бою. Аби ефективно використовувати наявні засоби ураження потрібно мати точні дані про координати об'єктів противника на всю глибину досяжності цих засобів. За відсутності такої інформації вогневі удари будуть не точними. Поява нових засобів збройної боротьби і зміна характеру ведення бойових дій висуває до розвідки підвищені вимоги. Умови ведення розвідки стають більш складними і потребують залучення різних сил та засобів для вирішення поставлених завдань.

З розвитком технологій людство в цілому й окремі держави, зокрема, займають нові простори для діяльності. Раніше це проявлялось у географічному аспекті, однак, наразі важливу роль відіграють нові сфери, на які покладаються певні функції. Одним із таких новоутворень, що відрізняється своїми специфічними рисами, є цифрова розвідка. Водночас, новітні простори передбачають й появу нових загроз, а, відповідно, й пошук

шляхів, способів їх попередження та усунення. Природно, що з початком повноцінної функціонування цифрової розвідки, уразливішими стали традиційні складові національної безпеки, зокрема об’єкти критичної інфраструктури.

Однак на сьогодні, незважаючи на прийняття ряду нормативно-правових актів, що регулюють цю сферу, вирішення питання взаємодії державного та приватного секторів з метою забезпечення кібербезпеки потребує подальшого удосконалення. Особливо гостро це виявляється під час захисту об’єктів критичної інфраструктури.

Чинним законодавством термін, цифрова розвідка визначається як «знаходження під захистом життєво важливих інтересів людини і громадянина, суспільства та держави під час задіювання кіберпростору, забезпечення сталого розвитку інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України» [35].

Враховуючи комплексність і відносну новизну діяльності щодо забезпечення кібербезпеки, вона потребує застосування всіх наявних засобів та залучення усіх доступних сил. Це відобразилось й у принципах, закріплених на законодавчому рівні: державно-приватної взаємодії, співпраці з суспільством у сфері кібербезпеки та кіберзахисту, зокрема, обмін інформацією про інциденти кібербезпеки, реалізація спільних наукових та дослідницьких проєктів, навчання та підвищення кваліфікації кадрів у цій сфері.

Однак, поряд з нормативно-правовим регулюванням не менш актуальним є питання практичної реалізації заходів, які спрямовані аби захищати об’єктів критичної інфраструктури у кіберпросторі. Об’єкти критичної інфраструктури мають вагоме значення для економіки та промисловості, комфортного життя суспільства та безпеки населення, а тому забезпечують складові її безпеки, зокрема й у кіберпросторі, однаково важливі

як для приватного так і для державного сектору. Така взаємодія двох вказаних секторів зумовлена демократичними засадами вітчизняного державотворення, адже під безпосереднім контролем держави перебуває лише частина об'єктів критичної інфраструктури [3, с. 52]. Незважаючи на визначення форм, у яких повинна реалізовуватись державно-приватна взаємодія у сфері забезпечення кібербезпеки, її практична реалізація потребує удосконалення.

Перш за все, досі чітко не визначено характер такої взаємодії, як вона співвідноситься з державно-приватним партнерством. По-друге, наразі не встановлено мінімальну частку участі у проєкті забезпечення кібербезпеки приватного суб'єкта. Це дозволяє приватним партнерам перекладати більшу частину відповідальності та зусиль на державний сектор. Варто додати, що великі ризики для іноземних інвесторів в Україні також не сприяють як державно-приватній взаємодії у вказаній сфері, так й міжнародному співробітництву у цілому.

Також, належним чином не вирішено питання координації та управління в рамках державно-приватної взаємодії, зокрема, який з секторів, не говорячи вже про конкретний орган, може приймати управлінські рішення, який їх статус для суб'єктів взаємодії.

Отже, на сьогодні стан нормативно-правового забезпечення цифрової розвідки кращий ніж декілька років тому, хоча і потребує подальшого вдосконалення. Водночас, у контексті забезпечення безпеки людини, суспільства, держави особливої актуальності набуває питання реалізації вже закріплених норм. Наявні проблеми повинні бути вирішені з урахуванням як вітчизняної досвіду практичного діяльності у цій сфері так і позитивних здобутків інших держав.

Необхідність у створенні спеціальних інформаційних систем виникає через збільшення смуги застосування військ та швидкого розгортання операцій, набуття ними міжвидового високоманевровного характеру. Для вдосконалення інформаційного забезпечення збройних сил України важливо використовувати засоби обробки цифрової інформації про місцевість і

поєднувати їх з різноманітними даними про противника та свої війська. Без застосування космічних систем (апаратів дистанційного зондування Землі) не можливе успішне виконання завдань своїми військами.

Концепція реалізації державної політики у сфері космічної діяльності на період до 2032 року в Україні вказує на те, що передбачено підвищення вимог до інформаційного забезпечення збройних сил, а також інших завдань. Все відбувається за рахунок створення угруповання високого розрізнення подвійного призначення, в інтересах національної безпеки й оборони» [18].

Видається можливим простежити загальну тенденцію, яка включає в себе використання комплексованих систем високої, середньої та низької просторової розрізненості інших країн. Системи середньої розрізненості з відкритими кодами передачі даних швидко визначають зміни в обстановці, і завдяки системам високої розрізненості швидко деталізують їх.

Завдяки багатоспектральному космічному зніманню апаратами розширюється науково-методичний апарат дистанційного зондування. Отримавши дані про неоднозначні спектральні яскравості ландшафтних об’єктів, їх можна застосовувати у якості спеціальних ознак, крім традиційної щільності тону, а також отримувати так звані «спектральні образи” шляхом інтегрування серії багатоспектральних знімків тієї самої ділянки спостереження.

Як стверджував Вінстон Черчилль [35], «...Держава має є два найбільш обов'язки, обидва однаково важливі. Перший – попередити війну. Другий – бути готовим до війни, якщо вона почнеться». Виконати ці зобов'язання допомагає у певній мірі розвідка. Розвідка – є тим самим важелем, завдяки якому споживачі розвідувальних даних можуть знати та передбачити ситуацію.

Розвідка, незважаючи на тисячолітню історію, не має чітких форм, хоч для реалізації завдань керується сучасними досягненнями науки і техніки. Проте загальні вимоги щодо її побудови та ведення все ж наявні, та з незначними кореляціями їх беруть до уваги усі розвідувальні служби світу.

Основні принципи функціонування цифрової розвідки:

1. Збір даних.

2. Обробка даних.

3. Оцінка інформації.

4. Надання споживачам інформації.

5. Отримання висновків, рекомендацій.

6. Планування і націлювання.

В. Окіпнюк [15] вважає доцільним зазначити, що «важливий елемент оцінювання ризиків і загроз, який властивий обом країнам – це окреслення я типових загроз і їх наслідків. На основі проведеного аналізу проводиться розробка універсальних протоколів узгоджених дій, які визначають як реагувати на загрози, надзвичайні та кризові ситуації на різних етапах їх реалізації».

На сьогодні світовий геополітичний простір та внутрішньодержавні відносини формуються за умов інформаційного протиборства. Для України ця проблема є актуальною через невизначеність геополітичного статусу, нестабільність у політиці, нестійкість інформаційного простору вітчизняного зразка. Україна вже довгий час перебуває під систематичним тиском інформації. В умовах впливу Росії на Україну, підбурювання, організації та всебічного забезпечення війни на сході та півдні нашої держави, проявляється нова тенденція ведення Росією воєнних дій. Водночас всі ці заходи супроводжуються цілеспрямованою потужною інформаційною кампанією.

М. Мельник [20] вказує на те, що «інтенсивний розвиток інформаційних технологій, наявність глобальних інформаційних мереж і засобів масової інформації, у гібридних війнах має вагому вирішальну роль». У цих умовах гостро постає проблема захисту національного інформаційного простору.

Враховуючи викладене, пошук шляхів надійного виявлення, аналізу та оцінюванню інформаційних загроз та протидії їм є актуальним науковим та практичним завданням. Комплексна методика оцінювання інформаційних

загроз державі у воєнній сфері базується на показниках, які характеризують інформаційний вплив для кожного напряму, якими є: рівень інтенсивності негативного інформаційного впливу; тривалість негативного інформаційного впливу; поширеність джерел інформаційного впливу; масштаб об'єктів інформаційного впливу. Зазначені показники враховують комплекс завдань - від виявлення ознак негативного інформаційного виливу до визначення переліку конкретних заходів негативного інформаційного впливу. Удосконалена методика дає змогу виробити шляхи зниження рівня загрози держави у воєнній сфері та практично застосувати їх, а саме: в органах військового управління та органах державної влади, на які покладено завдання виявлення, аналізу та оцінювання інформаційних загроз національній безпеці України, зокрема для розробки та супроводження паспортів воєнних загроз національній безпеці.

Необхідність в комплексному та ефективному підході до процесу забезпечення безпеки національного інформаційного простору постійно зростає. Актуальним на сьогодні залишається визначення чітких завдань та відповідальних суб'єктів за інформаційну безпеку. Визначаючи цілі, принципи, правові складові, Доктрина має стати основою для розробки проєктів, концепцій, стратегій, цільових програм і планів дій із забезпечення інформаційної безпеки України; базою для удосконалення норм та юридичних механізмів системи захисту інформації в державі.

Органи державної влади повинні спрямувати свою діяльність на виконання конкретних завдань у цій сфері. А также об'єднуватися для того, аби надавати належні умови для гарантування інформаційної безпеки України. Узгоджена діяльність по забезпеченню інформаційної безпеки на основі єдиних правових норм сприятиме ефективному протистоянню інформаційним загрозам.

Отже, зазначена система розвідувальних, органів та розшукових підрозділів підводить до того, що необхідно розроблювати єдиний загальний законодавчий акт про «спеціальну Державну розвідувальну,

контррозвідувальну та розшукові діяльність» зазначені державними структур. Також доцільно здійснювати приватну детективну діяльність в Україні. Розвідувальні служби, на наш погляд, повинні мати спеціальні повноваження, якими вони повинні наділятися при забезпеченні чітких процедур отримання дозволів, збирати інформацію, отримати право перехоплювати повідомлення, проводити негласне спостереження, використовувати джерела інформації, заходити на територію приватної власності як гласно, так і негласно на підставі спеціальних розвідувальних процедур та правил.

На мою думку, необхідно працювати над удосконаленням діяльності розвідувальних органів у контексті пристосування до різних форм ведення воєнних дій на фоні здійснення необхідних структурних трансформацій щодо забезпечення дієвості розвідки в Україні в сучасних умовах. Повномасштабне вторгнення Росії спонукає розвідку до більш активних дій, з чітким і агресивним добуванням та компілюванням отриманої інформації. Важливо, аби інформація могла працювати на випередження.

До того вважаю за потрібне сконцентруватися на боротьбі зі зрадниками і шпигунами, які звичайно присутні у лавах розвідки України. Варто проводити детальні перевірки штату, аби бути впевненими у їх відданості присязі та роботі загалом.

Необхідно активізувати інформаційну роботу, яка буде протидіяти «російській машині пропаганди» та дезінформації. Дотримуватися правил інформаційної гігієни та працювати над розповсюдженням виключно правдивих та перевірених даних.

У планах національних заходів, що спрямовані на протидію та попередження зовнішньої військової агресії, а також внутрішнього сепаратизму, важливо розуміти цілі противника. Саме для цього застосовуються усі наявні види військової розвідки. Все це підводить до ключової думки, що важливим завданням розвідувальної діяльності України є пошук, збір та аналіз інформації. Це дозволить сформувати доказову базу щодо російської агресії та злочинів на території України.

3.3 Методи та ресурсне забезпечення удосконалення цифрової розвідки органів державної влади в Україні

Від роботи розвідки, залежить життєдіяльність всього механізму держави і взагалі існування держави як такої. Від ефективного управління розвідкою залежить якість їх роботи.

Революція Гідності і відразу ж підступно розв'язана Російською Федерацією гібридна війна проти України висвітлили багато проблем. Стало очевидним, що загальнодержавна політика позаблоковості і багатовекторності призвела до розпорошення ресурсів розвідки, а дружба і стратегічне партнерство з Росією сприяли ослабленню силі засобів розвідки на найбільш загрозливому, як з'ясувалося, напрямі. До зазначених подій Російська Федерація навіть гіпотетично не розглядалася як потенційний ворог. Розвідувальна робота на «східному» напрямку практично не велася.

А. Куліш [26] констатує, що «наша країна не повністю усвідомлює небезпеку, яка може надходити з інформаційної сфери. В Україні відсутні штатні спеціалісти з інформаційної безпеки в органах державного управління. Підготовка фахівців здійснюється не на належному рівні. Варто наголосити на важливості застосування аналітичних методів пізнання. Необхідно досліджувати стан суспільної свідомості у сфері інформаційної безпеки».

За ствердженням українських науковців, серед яких П. Хамула [28] «важлива умова забезпечення інформаційної безпеки полягає не тільки у секретності, конфіденційності інформації, скільки у її доступності, цілісності, захисту від різних загроз». Тому система має належним чином реагувати і виступати гарантом ефективної діяльності у цьому напрямі. Інше завдання захисту – це забезпечити незмінність інформації в процесі її зберігання або передачі, тобто гарантувати її цілісності. Все це підводить до висновку, що конфіденційність інформації, забезпечення якої відбувається за допомогою криптографічних методів, немає вагоме значення при проектуванні систем захисту інформації.

Дослідження Б. Кормич [35] вказують на те, що «принцип доступності та безпеки повинен бути одним з головних в процесі управління в сфері інформаційної безпеки. Система забезпечення інформаційної безпеки повинна гарантувати: доступність, цілісність, конфіденційність інформації. Аби протидіяти загрозам інформаційної безпеки проводяться необхідні заходи для здійснення певного впливу на джерело загрози та зміцнення об'єкта безпеки. Виокремлюють дві предметні сфери протидії. Одна з них утворюється сукупністю джерел загроз, а інша – комплекс дій щодо забезпечення інформаційної безпеки об'єкта».

Водночас розвідка України у різні роки мала інформацію про те,що керівництво РФ проводить стосовно України послідовну агресивну політику, спрямовану на дестабілізацію ситуації всередині держави, вчинення політичного й економічного тиску, негативного впливу на представників національних меншин у місцях. Їх компактного проживання, поширення в їхньому середовищі антиукраїнських і сепаратистських настроїв, використання російською стороною релігійного фактора, проведення антиукраїнських акцій. Про таку недружню політику Росії інформаційно-аналітичні підрозділи розвідки України готували відповідні документи для вищого керівництва держави, але ці інформації не надавалося належної уваги. Все це мало катастрофічні наслідки Україна виявилася не готовою до самозахисту на початковому етапі відкритої російської агреси, посягання на територіальну цілісність України в Криму і Донбасі.

Варто підкреслити, що у спецслужбах нашої держави за останній період приділяється вагома увага оновленню систем і комплексів технічної розвідки, активно нарощуються їх можливостей щодо несанкціонованого доступу до об'єктів критичної інфраструктури інших країн, проводяться спеціальні інформаційні операції. Беручи до уваги подібні обставини С. Балабан [29] зазначає, що особливого значення набувають питання модернізації систем забезпечення інформаційної безпеки силових органів державної влади України. Передусім це стосується розвідувальних органів, які

використовують значний обсяг цінної конфіденційної інформації, створюються необхідні умов їх роботи за нових реалій геополітичної обстановки. Аби вирішити це завдання необхідно створити максимально надійну систему забезпечення інформаційної безпеки, яка буде побудована на основі сучасних організаційних і технологічних розробках, результатах наукових досліджень. Обов'язково з урахуванням специфічних вимог до захисту інформації, які характеризуються конкретними потребами сфери розвідувальної діяльності.

Головне завдання щодо створення такої системи – це досягнення високої ефективності захисту інформаційних ресурсів розвідувального органу на основі комплексного застосування необхідних методів і засобів, що виключають несанкціонований доступ до конфіденційної і таємної інформації. Аби створити таку систему варто прийняти оптимальне рішення. Важливе питання полягає у забезпечені максимально надійного захисту інформації. Аби виключити випадкові чи навмисні доступу до інформаційних ресурсів сторонніх осіб. Необхідно розділити доступ до пристроїв системи всіх користувачів. Разом з тим система система не повинна створювати незручності користувачам під час взаємодії з ресурсами. Досягнути високого рівня захисту можна завдяки об’єднанню в цілісну систему, що складається з організаційних і технологічних прийомів, розробивши комплекс спеціальних засобів і методів захисту інформації. Вважаємо доцільним наголосити на будові системи організаційно-технологічного типу. У ній керівництво буде забезпечувати загальну організацію захисту та виконання поставлених завдань. Захист інформації відбувається разом з технологічними процесами її обробки. Під час побудови такої системи необхідно брати до уваги особливості об’єкта впроваджуваної системи, чітко оцінювати ймовірні загрози безпеці об’єкта, аналізувати способи та засоби якими необхідно оперувати, створюючи систему, оцінку економічної доцільності її створення, співвідношення внутрішніх і зовнішніх загроз та можливість внесення необхідних змін у процесі функціонування системи.

Ключовий пункт у розробці системи інформаційної безпеки (СЗІБ) – це визначення можливих джерел появи загроз безпеці інформації розвідувального органу. Джерела виокремлюються як комплекс явищ, факторів та умов, що можуть призводити до витоку інформації з відміткою «секретно».

Вважаємо доцільним впроваджувати заходи зі створення системи інформаційної безпеки за трьома напрямами:

1. Адміністративний напрям. Керівництво розвідувального органу Передбачає формулює мету та програму виконуваних робіт щодо створення системи забезпечення безпеки інформаційного ресурсу. Постає питання планування необхідного фінансового та матеріального забезпечення, а також контроль за виконанням запланованих заходів.

2. Організаційний напрям. Вирішуються питання щодо створення умов для ефективної роботи служби, яка відповідальна за режим захисту інформаційного ресурсу, проведення заходів профілактичного характеру.

3. Програмно-технічний напрям. Програмно-технічні засоби, що реалізують вказані вимоги.

На державному рівні органи влади та державні інституції, зобов'язані створити найбільш ефективне сприяння розвідувальним служби при виконанні ними своїх повноважень та забезпечити дієвий парламентський контроль за діяльністю розвідувальних служб із залучення широкого кола членів громадянського суспільства. Держава повинна продемонструвати свою зацікавленість у розвитку розвідувальної діяльності в нашій країні.

Які ресурси потрібні для вдосконалення цифрової розвідки в Україні:

– кадрові;
– фінансові;
– технічні;
– матеріальні;
– інформаційні.

На нашу думку модернізацію цифрової розвідки в України варто почати з керівництва. Доцільно створити Комітет з питань розвідки при Президентові України. Зараз відповідно до законодавства існує Об’єднаний комітет з питань розвідувальної діяльності при Президентові України. Але краще, якби Комітет існував у якості суб'єкту закону України. Така організація могла б покращити координування українською розвідкою.

Безумовно для кращої та ефективної роботи розвідка України потребує більш повного фінансування. Видатки на цю галузь варто закріпити у Державному бюджеті на постійні основі. Для фінансування розвідувальної діяльності України також можна залучати кошти міжнародних партнерів. З цією метою доцільно провести переговори, зустрічі з потенційними спонсорами. Безумовно важливим є контроль за доцільним використанням отриманих коштів. Грошові ресурси – це корисна інвестиція у міцну та надійну розвідку, що зможе захистити країну від різноманітних атак та загроз.

Варто приділити увагу кадровому зміцненню розвідки. Розвиток цієї сфери національної безпеки можливий лише при залученні кваліфікованих та досвічених кадрів. Можна залучати нових працівників, підвищувати кваліфікацію тих, хто вже працює в цій галузі. Було б корисно залучати міжнародних спеціалістів для обміну досвідом. Українським розвідникам дійсно є чому повчитися у зарубіжних колег.

Не останнє місце займає технічне забезпечення української розвідки. Країна продовжує використовувати розвідувальну техніку радянського зразка. Кількість нового устаткування мінімальна. Оновлення технічного устаткування розвідки України могло б стати потужним поштовхом для її розвитку у майбутньому. Також варто приділити увагу оновленню програмного забезпечення української розвідки. Ефективно працювати та оберігати національну безпеку можливо лише за умови залучення сучасних версій програм.

Важливо працювати на розширенням інформаційних ресурсів. Використовувати усі можливі бази даних, архіви, документи, детально

опрацьовувати усю інформацію, яка потрапляє до рук розвідки. Задіяти сучасні канали отримання даних. Розширювати власну мережу джерел отримання інформації. Залучати до власної роботи дані від розвідок інших країн.

Якісне ресурсне забезпечення дозволить розвідці України активно розвиватися та поліпшувати рівень захисту національної безпеки нашої країни. За комплексно реформування та оновлення українська розвідка має великий потенціал та високі шанси стати однією з кращих в Європі.

ВИСНОВКИ

У кваліфікаційній магістерській роботі здійснено обґрунтування шляхів удосконалення цифрової розвідки в умовах інформаційної війни в Україні. Основні результати дослідження знайшли відображення у висновках і пропозиціях в контексті визначених у роботі мети і завдань:

1. Дослідження сутності цифрової розвідки та особливостей її реалізації показало, що сутність розвідувальної діяльності органів влади - це збір інформації різноманітного характеру: політичного, економічного, науково-технічного про обстановку в окремих країнах чи коаліціях країн для гарантування безпеки та отримання ключових позицій в області збройних сил, військових дій, політики або економіки. Основними видами цифрової розвідки є стратегічна, тактична, оперативна.

2. Дослідження нормативно-правової бази цифрової розвідки вказують на те, що організаційний аспект та особливості проведення сучасних бойових дій вимагають від угруповань військ кардинально іншого інформаційного забезпечення цифрової розвідки України. В країні впроваджені та працюють закони «Про національну безпеку України», «Про Стратегію інформаційної безпеки», «Про розвідувальні органи України». Вони визначають правові засади функціонування розвідки, забезпечують комплексний підхід до виконання поставлених завдань.

3. Аналіз світового досвіду реалізації цифрової розвідки в умовах інформаційних війн свідчить про те, що в різних країнах активно розвивається розвідувальна діяльність. Засновуються компанії, які на замовлення державних органів здійснюють розвідку з приводу різних питань. До прикладу США займається створенням агентурної мережі. Ізраїль займається проникненням в цільову аудиторію, дискредитацію політичних опонентів через поширення оманливої інформації. Британія ж є одним з лідерів у наданні приватних розвідувальних послуг.

4. Аналіз практики реалізації цифрової розвідки в умовах інформаційної війни в Україні показує, що розвідка в України потребує переформатування задля ефективної роботи. Розвідка в Україні вирізняється добування розвідувальних відомостей з комп'ютерних систем або інформаційних мереж та їх обробкою за допомогою апаратно програмних засобів. Також вона включає в себе добування і систематизацію даних про потенційні джерела кіберзагроз за допомогою різних методів. Потрібно приділити уваги укомплектуванню кадрами, повному сучасному технічному забезпеченню, провести реорганізацію на державному рівні.

5. При обґрунтуванні пріоритетів щодо удосконалення цифрової розвідки в умовах інформаційної війни в України нами визначено, що головна мета, яка допомагає удосконаленню цифрової розвідки, саме розвідувальні служби повинні мати спеціальні повноваження, якими вони повинні наділятися при забезпеченні чітких процедур отримання дозволів, збирати інформацію. На державному рівні органи влади та державні інституції, зобов'язані створити найбільш ефективне сприяння розвідувальним служби при виконанні ними своїх повноважень та забезпечити дієвий парламентський контроль за діяльністю розвідувальних служб із залучення широкого кола членів громадянського суспільства. Були запропоновані удосконалені методики, які покращають цифрову розвідку нашої держави. Після проведеного аналізу серед різноманітних методик оптимальною для цифрової розвідки є циклічна розвідувальна діяльність, яка заснована на передових технологіях. Всередині цієї системи набуває розвитку концептуальна модель інформаційної і аналітичної підтримки прийняття рішень. Це в свою чергу дозволяє забезпечити певний рівень інформаційної безпеки у межах системного моніторингу різних джерел. Останній бере за основу комплексне інформаційне оброблення нормативно-довідкових, аналітичних, експертних, статистичних даних, які надає розвідка.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Басай В. Судові, правоохоронні та правозахисні органи України: підруч. Коломия: Видавничо-поліграфічне товариство «Вік», 2006. 972 с.
2. Бойко В.П. Российская юридическая энциклопедия. М.: ИНФРА М, 1999. 1100 с.
3. Бойовий статут механізованих і танкових військ Сухопутних військ Збройних Сил України. Ч. III (взвод, відділення, екіпаж)/ затверджений наказом командувача СВ ЗС України від 25.05.2016 No 238. 296 с.
4. Варенко В. М. Інформаційно-аналітична діяльність : навчальний посібник. К. : Університет «Україна», 2014. 417 с.
5. Вертузаєв М.С. Проблеми контррозвідувального захисту економічної інформації як об'єкту промислової власності. *Право і безпека.* 2006. № 5. С. 7 9.
6. Військовий стандарт 01.101.001. Видання 2. *Воєнна розвідка. Терміни та визначення.* К. : Міністерство оборони України, 2011. 24 с.
7. Військовий стандарт 01.101.004. Видання 2. Воєнна розвідка. Розвідувально-інформаційна діяльність. Терміни та визначення. К. : Міністерство оборони України, 2015. 26 с.
8. Голота В. В., Тимкован В. І. Конкурентна розвідка як елемент фінансово-економічної безпеки підприємства. *Міжнародний науковий журнал «Інтернаука».* 2017. № 16 (1). С. 56 59.
9. Гур'єв В.І. Інформаційна безпека держави. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://ir.stu.cn.ua/bitstream/handle/123456789/19246/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC.%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%B4%D0%B5%D1%80%D0%B6.%20New%20booklet%201.pdf?sequence=1&isAllowed=y (Дата звернення: 24.11.2022)
10. Доктрина інформаційної безпеки України. Указ Президента України від 27 лютого 2017 р. № 47/2017. URL:

https://zakon.rada.gov.ua/laws/show/47/2017#n12 (Дата звернення: 24.11.2022)

11. Задірака В.К. Сучасні методи розв'язання задач інформаційної безпеки. *Вісник НАН України*. 2014. № 5. С. 65 69.
12. Захарова І. В. Основи інформаційно-аналітичної діяльності : навчальний посібник. К. : «Видавництво «Центр учбової літератури», 2013. 336 с.
13. Золотар О.О. Інформаційна безпека людини: теорія і практика : монографія. Київ :ТОВ «Видавничий дім «АртЕк», 2018. 446 с.
14. Історія становлення Національного антикорупційного бюро: Офіційний сайт НАБУ: URL: https://nabu.gov.ua/istoriya stanovlennya (Дата звернення: 24.11.2022)
15. Конституція України. Київ : Інститут законодавства Верховної Ради України, 1996. 376 с.
16. Кормич Б. А. Інформаційне право. Підручник. Харків: БУРУН і К., 2011. 334 с.
17. Куліш А. М. Правоохоронна система України: адміністративно правові засади організації та функціонування. Х.: 2009. 432 с.
18. Лапкін А. В.Організація судових та правоохоронних органів України : навч. посіб. у схемах. Вид. 6 те, змін. і допов. Харків : Право, 2017. 168 с.
19. Левченко О. В. Методика оцінки противника у бою : навчальний посібник/ О. В. Левченко. К. : НАОУ, 2001. 76 с.
20. Мельник С.І. Правові засади організації та функціонування розвідки: деякі напрями вдосконалення. *Підприємництво, господарство і право.* 2021. № 2. С.110.
21. Мельник М.І. Правоохоронні органи та правоохоронна діяльність: навч. посібник. М.І. Мельник, М.І. Хавронюк. К.: Атіка, 2002. 576 с.
22. Методичні рекомендації з розробки розвідувальних оцінок (за стандартами провідних країн-членів НАТО). К. : ГУР МО України, 2018. 118 с.

23. Настанова з тактичної розвідки/ Командування СВ ЗС України. Київ :МОУ, 2017. 127 с.
24. Окіпнюк В.Т. Комітет державної безпеки СРСР та Комітет державної безпеки УРСР II Енциклопедія історії України : у 10 т. редкой.: В.А. Смолій (голова) та ін.; Інститут історії України НАН України. Київ: Наукова думка, 2007. Т.4:Ка Ком. С. 479.
25. Парламентський нагляд. URL: https://securitysectorintegrity.com/uk/ (Дата звернення: 24.11.2022)
26. Основи розвідувально-інформаційної діяльності: настанова Штабу розвідки Міністерства оборони Великобританії. К. : ГУР МО України, 2015. 51 с.
27. Про національну безпеку України : Закон України. *Відомості Верховної Ради України.* 2018. № 31. 241 с.
28. Про Службу зовнішньої розвідки України : Закон України. *Відомості Верховної Ради України.* 2006. № 8. 94 с.
29. Про оборону України : Закон України. *Відомості Верховної Ради України*. 1992. № 9. 106 с.
30. Про розвідку : Закон України. *Відомості Верховної Ради України.* 2020. № 86. 2761 с.
31. Про Державну прикордонну службу України : Закон України. *Відомості Верховної Ради України*. 2003. № 27. 208 с.
32. Про Національну поліцію : Закон України. *Відомості Верховної Ради України.* 2015. № 40-41. 379 с.
33. Про оперативно-розшукову діяльність : Закон України. *Відомості Верховної Ради України.* 1992. № 22. 303 с.
34. Про Раду національної безпеки і оборони України : Закон України. *Відомості Верховної Ради України*. 1998. № 35. С. 237.
35. Про Службу безпеки України : Закон України. *Відомості Верховної Ради України*. 1992. № 27. С. 382.

36. Про внесення змін до Податкового кодексу України щодо покращення інвестиційного клімату в Україні: Закон України від 21 грудня 2016 року № 1797 VIII: URL: http://zakon3.rada.gov.ua/l aws/show/1797$19/page (Дата звернення: 24.11.2022)
37. Про національну безпеку України: Закон України від 21.06.2018 № 2469 VII. URL: http://zakon.rada.gov.ua/laws/show/2469 1920. (Дата звернення: 24.11.2022)
38. Про Службу безпеки України: Закон України від 25 березня 1992 р. *Відомості Верховної Ради України*. 1992. № 27. С. 382.
39. Про Військову службу правопорядку у Збройних Силах України від 7 березня 2002 р. *Відомості Верховної Ради України.* 2002. № 32. С. 225.
40. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 2015 рр. : Закон України від 09 січня 2007 р. № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text. 325 (Дата звернення: 24.11.2022)
41. Приватні розвідувальні компанії: іноземний досвід залучення приватного сектору до виконання завдань розвідки. URL: https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/pryvatni-rozviduvalni-kompaniyi-inozemnyy-dosvid-zaluchennya (Дата звернення: 24.11.2022)
42. Процеси розвідувальної діяльності. Стандарт НАТО. Союзницька об'єднана настанова AJP 2.1 (видання B, варіант 1). Управління стандартизації НАТО, 2016. 80 с.
43. Розвідувальні органи України: класифікація, характеристика, особливості діяльності. URL: https://bintel.org.ua/nukma/rozviduvalni-organi-ukra%D1%97ni/ (Дата звернення: 24.11.2022)
44. Рєзнік, О.М. Мета, завдання та функції правоохоронних органів, які забезпечують фінансово економічну безпеку України. *Порівняльно аналітичне право.* 2018. № 1. С. 208 211.

45. Рєзнік, О.М. Адміністративно правове регулювання діяльності правоохоронних органів із забезпечення фінансово економічної безпеки України. *Вчені записки Таврійського національного університету імені В.І. Вернадського.* Серія: Юридичні науки. 2018. Т. 29 (68). № 2. С. 88 94.
46. Рибалка Н., Балабан С. Концептуальні засади визначення ефективності адміністративно правового регулювання: міждисциплінарний підхід. *Науковий часопис Національної академії прокуратури України.* 2014. № 1. С. 147 159.
47. Стратегія національної безпеки України. Безпека людини безпека країни: Указ Президента України від 14 вересня 2020 року № 392/2020. Офіційний вісник Президента України. 2020. № 19. С. 926.
48. Стратегопулос Є. Ю. Зміст і основні завдання конкурентної розвідки на підприємстві. *Збірник наукових праць здобувачів другого (магістерського) рівня вищої освіти кафедри економічної кібернетики та управління економічною безпекою за ред. Т. В. Полозової та ін.* Харків: Харківський національний університет радіоелектроніки, 2019. С. 113117.
49. Тактична розвідка в бойових прикладах за досвідом проведення АТО :посібник. Київ : МОУ ГУР, 2017. 160 с.
50. Тактика в бойових прикладах (з досвіду антитерористичної операції): навч.-метод. посіб./колектив авторів; за заг. ред. А. М. Сиротенка. К. : НУОУ ім. І. Черняховського, 2017. 140 с
51. Тевлін Р. Про поняття «правоохоронні органи» у вузькому та широкому розумінні. Радянське право. 1985. № 7.
52. Форми, методи і засоби розвідувальної діяльності. URL: https://bintel.org.ua/nukma/formi-metodi-i-zasobi-rozviduvalno%D1%97-diyalnosti/ (Дата звернення: 24.11.2022)
53. Хамула П.І. Правоохоронні органи в системі органів державної влади: дне.канд. юрид. наук: 12.00.01. Харків, 2015. 235 с.

54. Шевчук О. Д. Про проблеми та перспективи реорганізації податкової міліції. О. Д. Шевчук. Агросвіт. 2017. № 11. С. 34 39.

55. Шай Р. Я. Роль і місце правоохоронних органів у правовій державі. *Науковий вісник Львівського державного університету внутрішніх справ.* 2011. Вип. 2. С. 496-508.

56. Рєпко А. С. Цифрова розвідка в умовах інформаційних війн. *Публічне управління та кібербезпека: теорія та практика: теорія та практика*: зб. матеріалів наук.-практ. конф., м. Київ, 15 вересня 2022 р. Київ, 2022. С. 73-76.

ДОДАТКИ

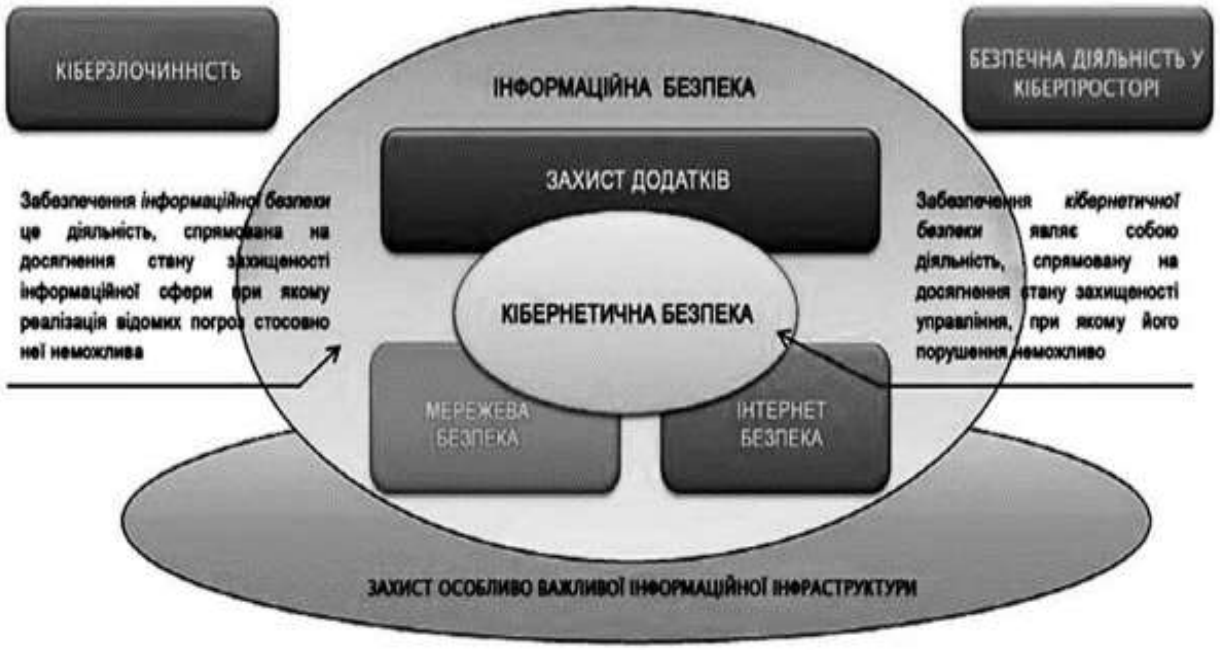
Додаток А

Взаємозв’язок понять безпека, інформаційний та кібернетичний простори

Джерело: [9].

Додаток Б

Прикладна галузь інформаційної та кібербезпек



Джерело: [9].

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Рєпко Артем Сергійович

Назва: КМР Рєпко ЦВ-601_30.11.2022_на плагіат.docx

Координатор: Федірко Наталія Вікторівна

Підрозділ: кафедра національної економіки та публічного управління

Коефіцієнт подібності 1:9.9

Коефіцієнт подібності 2:2.8

Тривога: 540

Після аналізу Звіту подібності констатую наступне:

☐ виявлені в роботі запозичення є сумлінними і не мають ознак плагіату. Тому робота визнається самостійною і допускається до захисту;

☐ виявлені в роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і самостійності її автора. Роботу направити на доопрацювання;

☐ виявлені в роботі запозичення є недобросовісними і мають ознаки плагіату або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень. У зв'язку з чим, робота не допускається до захисту.

Обгрунтування:

…….....
…….....
…….....
…….....
…….....

…… ……

Дата *Підпис Наукового керівника*

«ОФІС ЦИФРОВОГО ВРЯДУВАННЯ»

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

ПУБЛІЧНЕ УПРАВЛІННЯ ТА КІБЕРБЕЗПЕКА: теорія та практика

Збірник матеріалів
науково-практичної конференції
(Київ. 15 вересня 2022)

Електронне видання

КИЇВ - 2022

УДК 351/004.056

Рекомендовано до друку Вченою Радою Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського" (протокол №4 від 22 жовтня 2022 року)

Публічне управління та кібербезпека: теорія та практика зб. матеріалів наук.-практ. конф.. (Київ, 15 вересня 2022 р.). [Електронне видання]. – Київ : «ОФІС ЦИФРОВОГО ВРЯДУВАННЯ», 2022. – 111 с.

У збірнику висвітлено результати наукових досліджень науково-педагогічних працівників, студентів та аспірантів щодо підвищення якості підготовки здобувачів вищої освіти за спеціальністю 281 «Публічне управління та адміністрування», удосконалення компетентностей посадових осіб органів публічної влади, законодавчих ініціатив з питань освіти державних службовців, забезпечення національної безпеки держави, інвестиційно-інноваційного розвитку, організації діяльності публічних службовців, цифровізації публічних послуг, інструментів регулювання інформаційного простору та протидії дезінформації в умовах воєнного стану, механізмів взаємодії влади з представниками бізнесу та громадськості у процесі реалізації реформи децентралізації та ін.

Тези публікуються в авторській редакції.
Організаційний комітет залишає за собою право не поділяти думку авторів.

УДК 351/004.056

У дослідженні Українського інституту майбутнього передбачено два сценарії розвитку цифрової економіки в Україні: еволюційний та форсований. Наведені розрахунки відповідають еволюційному сценарію розвитку цифрової економіки, який наразі і має місце в Україні. За умови реалізації форсованого сценарію розвитку цифрової економіки її частка у ВВП до 2030 р. складатиме 65 % у ВВП. Водночас за умови реалізації будь-якого сценарію розвитку цифрової економіки у трудовій сфері відбуваються незворотні процеси, які зумовлюють скорочення наявних робочих місць та появу нових, які потребують цифрових навичок. Згідно з прогнозами Євростату, близько 50 % наявних робочих місць у всьому світі можна автоматизувати. Під автоматизацію підпадуть до 60 % професій та щонайменше 30 % видів діяльності до 2030 р. Це дозволить звільнити 40 % робочого часу для постійного навчання та виявлення творчості.

Швидкий розвиток та впровадження цифрових технологій у бізнес-процеси зумовлюють докорінні зміни у сфері праці та соціально-трудових відносин. Відбувається формування нового виду зайнятості – цифрового, який поширюється у глобальному вимірі. Державна служба зайнятості, як орган що реалізує політику у сфері зайнятості населення значно відстає за темпами діджиталізації економіки в Україні. А враховуючи що цифрова зайнятість має глобальний характер, і уже є невід'ємною складовою суспільства у всьому світі це зумовлює потребу у моніторингу такої зайнятості та адаптації національних інструментів надання послуг у сфері зайнятості населення.

Рєпко Артем Сергійович
Київський національний економічний університет
імені Вадима Гетьмана

ЦИФРОВА РОЗВІДКА В УМОВАХ ІНФОРМАЦІЙНИХ ВІЙН

У період війни в країні, забезпечення безпеки всіх громадян та збереження територіальної цілісності і єдності держави є пріоритетом для всіх органів державного управління. Зокрема й підтримка інформаційної безпеки в країні та протистояння пропаганді, маніпуляціям, дезінформації населення, впливу на масову свідомість суспільства. Цифрова розвідка сприяє збереженню інформаційної безпеки держави, а також контролює появу і вплив зовнішніх чинників, які можуть похитнути ситуацію в середині країни й у медійному

просторі зокрема. Вона має на меті не лише протистояти загрозам, що вже існують, а й запобігти виникненню таких агресивних дій. Тобто цифрова розвідка є превентивним механізмом у протидії ворогу. Ми можемо спостерігати це під час війни, яку розв'язала росія на території України.

Щодня в медіапросторі з'являються нові фейки, інформаційні вкиди щодо можливих ракетних ударів, вибухів бомб на території України та Придністров'я. Їх навмисно розповсюджує керівництво рф задля звинувачення України, нібито у розв'язанні громадянської війни та веденні терористичної діяльності, а також це робиться для дезінформації власного населення росії. Вагому роль у протидії ворогу займає діяльність Служби безпеки України. Однією зі сфер впливу якої є цифрова розвідка. Спеціалісти щодня фіксують спроби розхитати інформаційну та кібербезпеку України. Наразі країни борються за чистоту, достовірність та правдивість інформації, яка під час війни є потужним засобом впливу на велику кількість населення.

Цифрова розвідка допомагає оперативно здобути будь-які дані з різних видів джерел, що у свою чергу впливає на хід війни, і не лише інформаційної, а й геополітичної. Актуальність обраного напряму дослідження пов'язана з високим рівнем важливості та значущості у протидії фейкам та дезінформації, в отриманні оперативної інформації про дії ворога. Тема має глобальне значення для кожного українця, адже постійний розвиток, вдосконалення цифрової розвідки може допомогти припинити війну на території України. Одним із чудових прикладів роботи цифрової розвідки, яка реалізується Службою безпеки України, є відстежування переміщень ворога за допомогою чат-ботів у соціальних мережах. Будь-який користувач Телеграму може оперативно повідомити надважливу інформацію - і цим врятувати життя багатьом людям. Окрім цього, як зазначається на офіційному сайті Служби безпеки України: "На базі Ситуаційного центру забезпечення кібербезпеки СБУ функціонує система управління подіями інформаційної безпеки (SIEM), яка моніторить події в режимі реального часу та дозволяє аналізувати стан інформаційної безпеки. Потенційно критичні події безпосередньо обробляються аналітиками безпеки, що дає змогу оперативно виявляти, реагувати та попереджувати загрози в національному кіберпросторі". Під час вивчення особливостей та розвитку цифрової розвідки в Україні, важливо також звернути увагу на міжнародний досвід у веденні інформаційної війни, зокрема на дії Великої Британії, Сполучених Штатів Америки. Вони завжди дуже оперативно отримують дані та ретельно перевіряють їх, що неодноразово допомагало Україні в

боротьбі з агресором. Запозичення та реалізація успішного досвіду інших країн може сприяти зміцненню цифрової розвідки в органах державного управління України.

Цифрова розвідка в умовах інформаційних війн має швидко трансформуватися відповідно до викликів. Адже інформаційна пропаганда та дезінформація суспільства, до яких щодня вдається росія, стають усе агресивнішими та абсурднішими, проте не менш впливовими на населення. Те, що насаджувалося роками російською федерацією через різні засоби впливу: ЗМІ, релігійні інституції, політичні партії, залучення ворожих агентів та диверсійних груп для дестабілізації ситуації в Україні, - не може зникнути миттєво. А тому діяльність органів влади, котрі забезпечують виконання основних завдань цифрової розвідки зараз має бути одним із пріоритетів. У статті 17 Конституції України наголошується: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу».

Про особливості інформаційної війни рф у своїх дослідженнях часто згадують українські науковці. Так, наприклад, І. В. Слюсарчук і Н. Я. Пічак у праці «Антиукраїнська інформаційна війна російської федерації» детально описують причини, етапи та методи, до яких вдається рф у реалізації своїх планів на інформаційному агресивному фронті. Дослідниці також зазначають, як наша країна може протидіяти державі-агресору. Вони сформували такі рекомендації: «створення спеціалізованого центру із забезпечення інформаційно-психологічної безпеки; вироблення механізмів взаємодії між міністерствами і відомствами України з питань інформаційної боротьби; внесення суттєвих змін до законодавства (воно має бути спрямоване на обмеження російського інформаційного впливу на півдні та сході України, захист українського інформаційного простору від розповсюдження інформаційної продукції антиукраїнського змісту; на удосконалення діяльності ЗМІ); формування спеціальних норм журналістської етики під час воєнного, надзвичайного стану або особливого періоду чи в бойовій обстановці; підвищення професійного рівня вітчизняної журналістики; налагодження дієвого внутрішнього та зовнішнього державного інформування, а також чіткої зовнішньої й внутрішньої іміджевої політики; заходи патріотичного виховання; розроблення та реалізація власних спеціальних інформаційних операцій». Усі ці рекомендації залишаються важливими й зараз, проте їх реалізація в умовах повномасштабної війни повинна мати комплексний та оперативний характер.

Дослідниця М. А. Зубарєва також проаналізувала особливості інформаційної війни між росією та Україною. Авторка зосереджує увагу на засобах за допомогою яких вона реалізується. До них належать: “маніпуляція, порушення інформаційного обміну, руйнування інформаційного простору країни або його використання з антидержавною метою, інформаційний тероризм”. У своїй праці вона наводить результати соціологічних опитувань та дає рекомендації щодо запобігання масштабній інформаційній війні. Тобто, як ми можемо простежити, дослідження українських науковців щодо інформаційної війни рф та розвитку цифрової розвідки України, які були зроблені до 2022 року, можуть бути фундаментом для нашої роботи. Проте у зв’язку з розгортанням повномасштабної війни на території України, з’явилися нові інформаційні виклики, загрози, які потребують ретельного опрацювання та дослідження. Це також свідчить про новизну та важливість оновлення інформації з даної теми у науковій площині.

Суєтіна Катерина Олександрівна
Київський національний економічний університет
імені Вадима Гетьмана

ЦИФРОВА ТРАНСФОРМАЦІЯ СОЦІАЛЬНОЇ СФЕРИ В УКРАЇНІ

Цифрова трансформація соціальної сфери на сьогодні є серед іншого одним з найважливіших напрямів цифрової стратегії держави. Вона, зокрема, спрямована на організацію виконання ефективної сервісної функції цифрової держави. Діджиталізація є механізмом державної цифрової стратегії, яка передбачає переведення усіх соціальних послуг з режиму роботи офлайн в онлайн.

Цифрова трансформація соціальної сфери наразі є одним з визначальних напрямів державної цифрової стратегії, спрямованої на формування ефективної сервісної цифрової держави. Парламентом та урядом прийняті необхідні законодавчі акти, які відкривають шляхи до реалізації забезпечення європейських стандартів функціонування інституцій соціального захисту, надання соціальних послуг, фінансової стабільності соціальної сфери, підвищення її прозорості та оптимізації адміністративних видатків. Зазначене надасть можливість досягти адресності державної соціальної підтримки та допомоги, мінімізувати корупційні прояви, зловживання та інші негативні явища, притаманні

ЗМІСТ

Наукове видання

збірник тез
науково-практичної конференції

ПУБЛІЧНЕ УПРАВЛІННЯ ТА КІБЕРБЕЗПЕКА: теорія та практика

Київ. Вересень 2022

Електронне видання

Авторська редакція

Упорядник
ГО «ОФІС ЦИФРОВОГО ВРЯДУВАННЯ»
digital.gov.office@gmail.com