Київський національний торговельно-економічний університет
Кафедра публічного управління та адміністрування

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

МОНІТОРИНГ ТА ОЦІНЮВАННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Студента 2 курсу, 5мз групи, спеціальності 281 «Публічне управління та адміністрування» спеціалізації «Публічне управління та адміністрування» _____ *(підпис студента)* Фозілов Рустам Таварович

Науковий керівник Кандидат наук з державного управління _____ *(підпис керівника)* Мірко Наталія Вікторівна

Гарант освітньої програми Кандидат економічних наук, доцент _____ *(підпис гаранта)* Дьяченко Ольга Володимирівна

Київ 2021

Київський національний торговельно-економічний університет

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

Затверджую
Зав.кафедри_____

«20» січня 2021р.

Завдання
на випускну кваліфікаційну роботу (проект)
студентові
Фозілов Рустам Таварович
(прізвище, ім'я, по батькові)

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

Затверджена наказом ректоравід«28» грудня 2020 р.№3940

2. Строк здачі студентом закінченої роботи (проекту): 22.10.2021

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

Мета роботи (проекту): дослідження сучасного стану та перспектив розвитку підходів оцінки загроз інформаційної безпеки України та визначення ефективних шляхів вдосконалення системи моніторингу інформаційних загроз.

Об'єкт дослідження: процес виявлення найбільш небезпечних і значимих загроз інформаційній безпеці України.

Предмет дослідження: теоретико-методологічні та прикладні засади механізму реалізації державної політики інформаційної безпеки.

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

ВСТУП

РОЗДІЛ 1. ТЕОРЕТИКО - МЕТОДИЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

1.1. Сутність та зміст інформаційної безпеки в сучасних умовах

1.2. Методи забезпечення інформаційної безпеки в Україні

РОЗДІЛ 2. АНАЛІЗ СТАНУ МОНІТОРИНГУ ТА ОЦІНЮВАННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Діяльність Ради Національної Безпеки і Оборони України щодо моніторингу та оцінювання загроз інформаційної безпеки України

2.2. Результати діяльності Ради Національної Безпеки і Оборони України щодо протидії загрозам інформаційної безпеки України

РОЗДІЛ 3. ШЛЯХИ ВДОСКОНАЛЕННЯ СИСТЕМИ МОНІТОРИНГУ ТА ОЦІНЮВАННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

ВИСНОВКИ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

ДОДАТКИ

5. Календарний план виконання роботи(проекту)

№ пор.	Назва етапів випускної кваліфікаційної роботи (проекту)	Строк виконання етапів роботи	
		за планом	фактично
1	Визначення напряму дослідження та затвердження теми випускної кваліфікаційної роботи	до 13.11.2020	13.11.2020
2	Затвердження плану та завдання випускної кваліфікаційної роботи	до 20.01.2021	20.01.2021
3	Представлення на рецензування науковому керівнику рукопису першого розділу випускної кваліфікаційної роботи	до 16.04.2021	16.04.2021
4	Представлення на рецензування науковому керівнику рукопису другого розділу випускної кваліфікаційної роботи	до 14.06.2021	14.06.2021
5	Представлення на рецензування науковому керівнику рукопису третього розділу випускної кваліфікаційної роботи	06.09.2021	06.09.2021
6	Представлення закінченої випускної кваліфікаційної роботи на кафедру	до 22.10.2021	22.10.2021
7	Проведення попереднього захисту випускних кваліфікаційних робіт	25.10-05.11.2021	25.10-05.11.2021
8	Зовнішнє рецензування ВКР	08.11-12.11.2021	08.11-12.11.2021
9	Подача роботи завідуючому кафедри	15.11-19.11.2021	15.11-19.11.2021
10	Захист випускної кваліфікаційної роботи	За графіком	За графіком

6. Дата видачізавдання«20» січня 2021р.

7. Науковий керівник випускної кваліфікаційної роботи(проекту)
Мірко Н.В.
(прізвище, ініціали, підпис)

8. Керівник проектної групи(гарант освітньої програми) Дьяченко О.В.

9. Завдання прийняв до виконання студент Фозілов Рустам Таварович
(прізвище, ініціали, підпис)

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

Дослідження даної теми є актуальним, оскільки інтенсивний розвиток інформаційних технологій та їх інтеграція практично міститься у всіх сферах життя суспільства і держави, відкриває можливості масового доступу користувачів до інформації, що сприяє збільшенню кількості критично важливого інформаційного ресурсу.

В випускній кваліфікаційній роботі проведено дослідження та узагальнення наукових підходів до визначення сутності державної політики інформаційної безпеки та визначено пріоритетні напрями механізму її вдосконалення.

У роботі, студентом Фозіловим Р.Т. була визначена сутність та зміст інформаційної безпеки в сучасних умовах, вивчені методи її забезпечення. Охарактеризовано діяльність Ради Національної Безпеки і Оборони України щодо моніторингу та оцінювання загроз інформаційної безпеки України та їх результати. Виокремлено шляхи удосконалення системи моніторингу та оцінювання загроз інформаційної безпеки України. Сформульовано напрями поліпшення організаційної структури Ради Національної Безпеки і Оборони України з урахуванням нової концепції протидії загрозам інформаційній безпеці. Слушною, є думка про перспективи розвитку та пріоритетні напрями вдосконалення організаційної структури Ради Національної Безпеки і Оборони України з урахуванням нової концепції протидії загрозам інформаційній безпеці.

Зміст випускної кваліфікаційної роботи підпорядкований поставленій у роботі меті. Завдання поставлені в роботі виконані, що підтверджено висновками.

Випускна кваліфікаційна робота має досить логічну структуру та відповідає вимогам оформлення. Зауваження, які відмічались науковим керівником виправлені. Робота написана на достатньому науковому рівні, є самостійним дослідженням студента, розкриває обрану тему. Вважаю, що випускна кваліфікаційна робота заслуговує позитивної оцінки, а її автор Фозілов Рустам Таварович на присвоєння ступеня магістр зі спеціальності 281 «Публічне управління та адміністрування».

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

Відмітка про попередній захист Дьяченко Ольга Володимирівна_____
(підпис, дата)

11. Висновок про випускну кваліфікаційну роботу (проект):

Випускна кваліфікаційна робота (проект) студента___Фозілова Р.Т._____
(прізвище, ініціали)
може бути допущена до захисту екзаменаційній комісії.

Керівник проектної групи (гарант освітньої програми): Дьяченко О.В._____
(підпис)

Завідувач кафедри: Новікова Н.Л._____
(підпис)

«19» листопада 2021 р.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Інтенсивний розвиток інформаційних технологій та їх інтеграція практично у всі галузі життя суспільства і держави відкриває можливості масового доступу користувачів до інформації. Це сприяє збільшенню кількості критично важливого інформаційного ресурсу, який циркулює, накопичується та обробляється в інформаційно-телекомунікаційних системах, й призводить до підвищення ступеня залежності більшості важливих рішень, що приймаються на різних рівнях (від громадянина до голови держави) від якості інформації та оперативності її обробки.

Саме можливість усього суспільства і його складових інститутів збирати, накопичувати й використовувати інформаційний ресурс, забезпечувати своєчасний доступ до нього та свободу інформаційного обміну, а також захищати критично важливу інформацію загроз. Наразі проблематика інформаційної безпеки постає особливо гостро саме в українському просторі, коли спостерігаємо російську агресію, застосування інформації як зброї, що може призвести до жахливих наслідків. Намагались з’ясувати, що ж таке безпека вже декілька століть. Проте сьогодні важливо з’ясувати, яких заходів необхідно вжити, щоб інформаційний простор перебував під надійним захистои та він набув максимальної ефективності.

Метою випускної кваліфікаційної роботи є дослідження сучасного стану та перспектив розвитку підходів оцінки загроз інформаційної безпеки Україниа визначення ефективних шляхів вдосконалення системи моніторингу інформаційних загроз.

Для досягнення мети необхідно виконати такі **завдання:**

- визначити сутність інформаційної безпеки в сучасних умовах;
- проаналізувати законодавче регулювання процесу моніторингу та оцінювання загроз інформаційної безпеки;

- дослідити досвід іноземних держав щодо здійснення ними інформаційної політики та можливості його застосування в Україні;
- здійснити аналіз діяльності РНБО та визначити основні результати цієї діяльності;
- запропонувати шляхи покращення моніторингу загроз інформаційної безпеки;
- запропонувати шляхи покращення організаційної структури РНБО.

Об'єктом дослідження випускної кваліфікаційної роботи є процес виявлення найбільш небезпечних і значимих загроз інформаційній безпеці України.

Предметом дослідження є теоретико-методологічні та прикладні засади механізму реалізації державної політики інформаційної безпеки.

Методи дослідження. В випускній кваліфікаційній роботі були використані методи експертного оцінювання, метод парних порівнянь та метод анкетування, методи векторної оптимізації, теорії ймовірностей та логіко-конструктивні методи.

Обсяг і структура роботи. Випускна кваліфікаційна робота загальним обсягом 54 сторінки, з них – 46 основного тексту, складається зі вступу, трьох розділів, висновків, списку використаної літератури, який налічує 50 позицій.

Апробація результатів дослідження. За результатами дослідження була опублікована наукова стаття «Сутність категорії безпека в умовах загострення інформаційних загруз» // Публічне управління та адміністрування в умовах суспільних трансформацій : зб. наук. ст. студ. відп. ред. Р. Т.Фозілов. – К.: Київ. нац. торг.-екон. ун-т, 2021. – С. 247-251.

РОЗДІЛ 1
ТЕОРЕТИКО - МЕТОДИЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

1.1. Сутність та зміст інформаційної безпеки в сучасних умовах

Інформаційну безпеку, її сутність та зміст наразі не можна розглядати без дослідження еволюційних етапів розвитку цього поняття.

Під час здійснення аналізу відповідної літератури, яка присвячена дослідженню еволюційних аспектів категорії «безпека», зробили висновок, що більшість науковців суголосна з думкою про те, коли безпека з'являється, та загалом підтримують позицію, що вона виникає водночас з появою держави та входить до складової національних інтересів.

Виокремлюємо кілька етапів розвитку заданого поняття:

- розуміння поняття «безпека» звужено, як індивідуальну приналежність;
- осмислення безпеки більш розширено, як загального блага і мети держави (такою була функція в XVII-XVIII ст. у країнах Західної Європи);
- усвідомлення поняття безпеки глобально, як категорія суспільства загалом та держави після трагічних війн та революцій в Європі в XIX-XX ст. [2, 7].

Сьогодні поняття «безпека» є комплексним та включає різні характеристики. До того ж, супроводжується дискусіями між різними вченими

щодо наповненості дефініції. Сучасні погляди на сутність поняття «безпека» наведено в таблиці 1.1.

Таблиця 1.1

Сучасні погляди на сутність поняття «безпека»

Джерело	Визначення
Чуваков О.А. [3]	визначає безпеку як багатофункціональне явище, під яким передусім розуміємо діяльність певної групи різних суб'єктів, проте з іншого боку трактує це явище як соціальну потребу, обґрунтовуючи цілеспрямований результат певної діяльності
Краснокутська Н. С., Коптєва Г. М. [5]	трактують безпеку як стан захищеності, що сформувався в результаті протистояння «мозаїці» негативних факторів
Нікіпєлова Є. М. [6]	розуміє під безпекою складне явище соціально-політичного характеру, сформоване у результаті поєднання елементів в системі «природа - людина - суспільство». Вчений наголошує, що ця категорія має відносний характер, адже набуває значення лише в конкретній ситуації
Ситник Г.П. [8]	трактує безпеку як систему, однак, в умовах такого стану, що вона залишається цілісною, стійкою, ефективною та перспективною, а, отже, здатна захистити свої підсистеми від руйнівного впливу негативних факторів
Антонов В. О. [8]	трактує безпеку як стан захищеності й інтересів індивіда (у вузькому значенні), суспільства і держави (у широкому), що виявляються найважливішими у певній ситуації та певних умовах від різноманіття існуючих загроз
Корнієнко Т.О. [9]	визначає безпеку також як стан захищеності «мозаїки» інтересів від різноманітних загроз (береться до уваги, які інтереси виступають першочерговими)

Джерело: Узагальнено автором на основі [5, 6, 8, 9].

Так, є різні бачення категорії та поняття «безпека», які узагальнюємо певним чином як:

- провідну діяльність суб’єктів;
- оцінка рівня захищеності;
- підсумки мети провадження діяльності.

Перший підхід, згідно якого безпека визначається як діяльність суб’єктів, у певному сенсі звужує зміст цієї категорії через те, що висвітлює лише одну змістову характеристику безпеки, а саме той факт, що безпека стосується лише певного кола людей.

Необхідно звернути увагу на другий підхід, як робить акцент на безпеці як стані захищеності. І справді поняття «безпека» та «захищеність» знаходяться на одній паралельній прямій. Однак стан захищеності не є основною змістовою характеристикою. Його слід визначати, як проміжна ціль чи ключове завдання.

Не можна трактувати безпеку лише як результат діяльності. Цей підхід спрямований лише на кінцевий результат. Але чи можемо ми говорити про безпеку як стале поняття, адже треба постійно підтримувати цей результат, завжди здійснювати необхідні дії, процеси. Даний підхід відіграє суттєву роль, однак не відображає характерних ознак такої багатогранноїскладової, а лише підкреслює результативність діяльності як процесу із забезпечення безпеки.

Під час формулювання дефініції категорії «безпека» необхідно акцентувати увагу на змістовій ознаці, однак, не уникати й інших бачень категорії, що апелюють до суб’єкта, об’єкта, мети та результату. Тобто в основі має бути принцип комплексності.

Отож запропонуємо таке визначення поняття «безпеки» з урахуванням комплексності цієї категорії. Безпека як категорія – це відносини між суб’єктами певної діяльності, яка направлена на захист інтересів особи,

суспільства та держави з метою протистояння аномаліям зовнішнього та внутрішнього характеру. Ця дефініція є відмінною від підходів, що запропоновані вище, адже визначає безпеку саме як категорію, враховує комплексний підхід та є універсальним визначенням (можна пристосовувати до будь-якої конкретної ситуації): конкретизація виду загроз дозволить адаптувати запропоноване визначення до трактування будь-якого виду безпеки.

Також в контексті нашого дослідження необхідно конкретизувати зміст безпеки шляхом уточнення його складових. Існує певна плутанина в теоретичному аспекті, немає сталої класифікація видів та форм безпеки. У результаті аналізу наукових джерел робимо висновок, що в літературі зустрічається низка форм та видів безпеки, але які не є систематизованими: економічна, фінансова, продовольча, інформаційна, медична, міжнародна, національна, екологічна, особиста та багато інших.

Для того, щоб уникнути такої плутанини, потрібно види безпеки доцільно класифікувати залежно від загроз.

Під загрозою чи ризиком в найбільш загальному розуміють явище або чинник, що може активізувати небезпеку. Небезпека, у свою чергу, це деструктивне, руйнівне явище, що може привести до негативних наслідків, часом руйнівних [4].

Найчастіше науковці сходяться на думці, що ризики небезпеки доцільно класифікувати залежно від суб’єкта, що створює цю небезпеку.

Отже, загрози найчастіше поділяють на:

- природні – загрози з боку природного середовища;

- інформаційні – загрози з боку засобів зберігання та передачі інформації,

пов’язані із накопиченням інформації у осіб, які можуть її використати з негативною метою;

- соціальні – загрози, які утворюються як результат соціальних конфліктів.

З урахуванням зазначеного пропонується безпеку поділяти на соціальну, природну та інформаційну. Акцентуємо на тому, що саме інформаційна безпека насьогодні має найважливіше значення. Таке твердження ґрунтується на тому, що саме інформаційні загрози в умовах сьогодення набувають обертів, а через постійну модернізацію потенційно небезпечних з інформаційної точки зору об’єктів, існує постійна потреба в оновленні способів забезпечення даного виду безпеки.

Загрози можуть бути активні та пасивні.

1. Пасивні загрози інформаційній безпеці передбачають незаконне використання інформаційних ресурсів і не спрямовані на порушення функціонування певної інформаційної системи. До пасивних загроз інформаційній безпеці можна віднести, наприклад, незаконний доступ до окремих баз даних або використання методів прослуховування каналів передачі інформації.

2. Активні загрози інформаційній безпеці спрямовані на порушення функціонування діючої інформаційної системи шляхом цілеспрямованої атаки на окремі її компоненти [4].

На думку автора, інформаційну безпеку доцільно трактувати як відносини з приводу захисту суспільства та держави від інформаційних загроз, пов’язаних із накопиченням інформації у осіб, які можуть її використати з негативною метою.

При цьому інформаційна безпека може мати прояв в різних формах, до яких

слід віднести інформаційну безпеку особистості, інформаційну безпеку бізнесу, інформаційну безпеку держави. Такі форми інформаційної безпеки доцільно виділяти з огляду на виокремлення суб'єкта, на який може бути спрямована загроза порушення інформаційної безпеки.

З урахуванням зазначеного можна надати авторське бачення співвідношень базових понять даного дослідження (рис. 1.1).

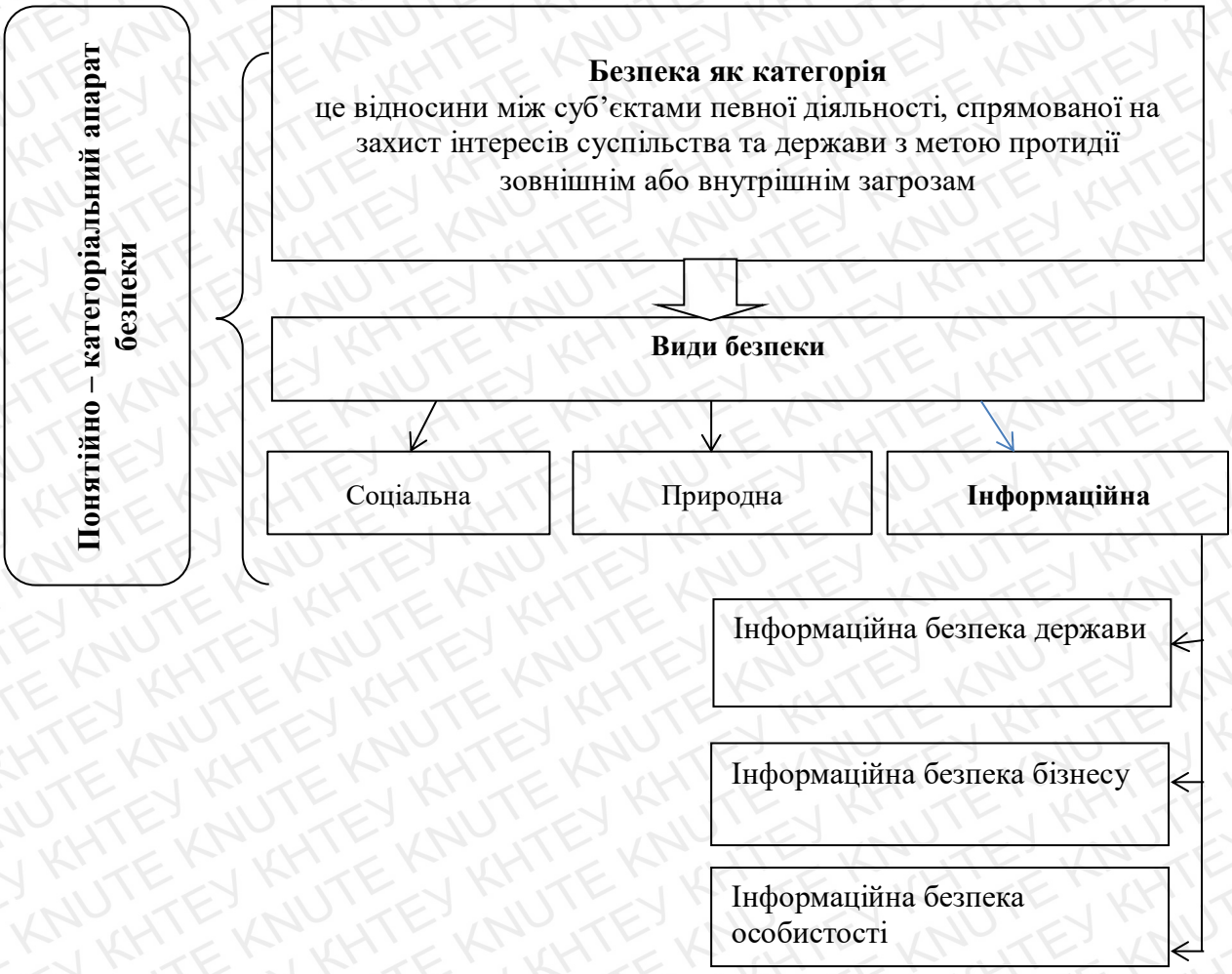

Рис. 1.1. Співвідношення базових понять даного дослідження.

На даному рисунку простежується зв'язок базових понять: безпека як

категорія має власні види, чільне місце серед яких займає інформаційна безпека, яка в свою чергу поділяється на безпеку індивіда, безпеку бізнесу та безпеку держави.

Окреслені форми інформаційної безпеки пов’язує спільна ознака: вони спрямовані на протидію загрозам, що виникають внаслідок накопичення інформації у осіб, які можуть її використати з негативною метою.

Таким чином, безпека виступає важливішою складовою сучасної наукового світу та здійснює впровадження відносин між окремими суб’єктами, діяльність яких спрямована на захист суспільних інтересів, маючи на меті протидію зовнішнім або внутрішнім загрозам. Безпека прийнято поділяти на наступні види: соціальна, природна та інформаційна. З огляду на стрімкий розвиток існуючої інфраструктури та враховуючидієвий процес втілення технічної революції, саме інформаційна безпека набуває суттєвого значення. Отже, розділяють такі форми інформаційної безпеки, якій властиві наступні ознаки: вони мають спрямування на надання протидії загрозам, що утворюютьсяна підставі збирання інформації у завідомо підозрілих осіб, а розрізняє суб’єкт, на які поширюються загрози використання інформації маючи негативні спрямування.

1.2. Методи забезпечення інформаційної безпеки в Україні

Інформаційний простір вимагає захисту виважених дій. Тому основною метою є досягнення високої результативності з приводу реалізації інформаційної безпеки шляхом практичного використання певних методів, прийомів, підходів, засобів, ресурсів, що допоможуть захистити від чужорідного втручання в інформаційне тло як персональне, так і державне.

Характер систематичного інформаційногозахисту слід назвати організоційно-технологічний. Тобто головними суб'єктами, що здатні захистити від небезпечних аномальних явищ. Так, організаційними питання займаються люди (а також приймають важливі рішення), проте без інформаційних технологій не обійтись, які миттєво здатні виявити ризики та мінімізувати їх[8].

Наразі інформаційнийзахист безпеки має такі особливості:

- Комплексний характер процедури захисту;
- У цей час дуже актуальним стало питання забезпечення іфнормаційної безпеки як серед окремих громадян, так і серед усієї держави;
- Потребує захист інформаційного простору не лише воєнна сфера, але й такі як корупційна, економічна, промислова, екологічна і т.ін.)

Здійснити успішні кроки в реалізації захисного механізму інформаційної безпеки можливо лише шляхом теоретичного обдумування інструментарію у вигляді методів, ресурсів, засобів. І згодом його практичного втілення. Отож мають бути розвинені науково-методологічні основи реалізації інформаційної безпеки.

Необхідно запропонувати таку дефініцію поняття «науково-методологічні основи», які допоможуть захистити інформаційний простір. Отож науково-методологічні основи – це сукупність таких складових частин, як принципи, підходи та методи, які необхідні для здійснення коректного дослідження, аналізу мінімізації ризиків[2].

Так, основними складовими частинами є принципи, підходи та методи. Саме в такому порядку їх слід розглядати. Так, принципи – це вихідний пункт, початкова точка якоїсь теорії, вчення, науки. Підхід – це різноманітні способи

вивчення на вибір найефективнішого з них. Кінцевим результатом є метод, який саме спрямований на застосування того способу, що є найбільш результативним. Наприклад, при реалізації принципу розмежування доступу в якості підходу можна вибрати моделювання, а в якості методу реалізації - побудова матриці доступу. Загальне призначення методологічного базису процесу проектування системи захисту інформації полягає в [11]:

- формуванні узагальненого погляду на організацію та управління КСЗІ, що відображає найбільш істотні аспекти проблеми;
- формуванні повної системи принципів, дотримання яких забезпечує найбільш повне рішення основних завдань;
- формуванні сукупності методів, необхідних і достатніх для вирішення всієї сукупності завдань управління.

Під час формування складу науково-методологічних основ необхідно враховувати такі положення:

- слід застосовувати такі загальні методи, що сприятимуть покращенню організаційної структури та правильній побудові системи захисту інформаційного простору;
- також в основі науоково-методичної складової мають бути закони кібернетики, адже мова йде про ефективне управління;
- складовими методологічних основ мають бути такі принципи, підходи та методи, що будуть спрямовані на моделювання великих систем.

Отже, коли будується певна система, то необхідно звертати увагу саме на науково-методологічну базу, на принципи, підходи та прийоми, які влучно застосовувати.

Систематичний інформаційний захист потребує значних витрат як матеріальних, так і ресурсних, проте результативність цієї системи важко передбачити, адже не знаєш наперед, на яких масштабів ризики необхідно чекати. Ми можемо тільки теоретично передбачити та запропонувати принципи захисту інформації, з якими пов'язані також і підходи. (табл.1.2).

Таблиця 1.2.

Принципи системи захисту інформації [7]

Принцип	Характеристика
Принцип законності	Різні рішення мають бути закріплені законодавчо, щоб набути своєї вагомості
Принцип обґрунтованості	Необхідно з'ясувати, витік якої інформації становитиме загрозу для людини, суспільства чи держави. Щоб доцільно витрачати ресурси згідно з цим принципом з'ясовуємо, чи має та чи інша інформація носити засекречений характер. Та передбачити, якими будуть наслідки після спливання цієї інформації.
Принцип створення спеціалізованих підрозділів	Здійснювати захист інформації мають експерти, люди, які в цьому спеціалізуються. Тому значної уваги слід привернути й організаційному питанню, формування складу певних підрозділів, що слідкуватимуть за інформаційним простором та здійснюватимуть відповідну політику.
Принцип участі в захисті інформації всіх дотичних осіб	Важливість захисту інформації мають розуміти усі особи, що дотичні до інформаційного простору будь-яким чином. Так, шляхом спільного зусилля можна надіятись на позитивний результат.
Принцип персональної відповідальності за захист інформації	Важлива інформація має носити конфіденційний характер, а в разі витоку інформації необхідно притягувати до кримінальної, адміністративної або іншої відповідальності.
Принцип наявності та використання всіх необхідних сил	Як ми вже з'ясували система захисту інформації повинна втілювати системний характер. Так, необхідно враховувати ефективність усіх складових цієї системи та застосовувати певні

і засобів для захисту	дії для покращення результативності. Отож важливою є організаційна функція, що полягає в адекватному формування складу відповідних органів, що відповідають за інформаційну безпеку. Також слід враховувати, наскільки ефективною є науково-методологічна база. Отже, потрібна наявність правильних людей, ефективних способів здійснення інформаційної політики, а ще, що є не менш важливим, наявність матеріальних ресурсів, що допоможуть під час нівелювання ризиків.
Принцип превентивності прийнятих заходів щодо захисту інформації	припускає апріорне випереджувальний завчасне вжиття заходів щодо захисту до початку розробки або отримання інформації. З цього принципу випливає, зокрема, необхідність розробки захищених інформаційних технологій

Джерело: Узагальнено автором на основі [7].

Знову нагадаємо, що систематичний захист інформації відзначається системним характером і кожна із її складових частин, кожен із принципів та методів є важливим та обов’язком для використання, не можна упускати будь-який з них.Коли формуємо цю систему потрібно здійснити такі заходи у встановленому порядку [3]:

1. Обстеження інформаційно-комунікаційної системи, розподіл інформаційних ресурсів та розробка концепції інформаційної безпеки. Тобто необхідний глибокий і детальний аналіз структури об'єкта захисту та умов його функціонування, а також категорії оброблюваної інформації. На цьому етапі вивчається технологія обробки даних, прийнята в організації і розробляються документи, необхідні для регламентації процесу роботи користувача в системі захисту інформації, в яких представляється: опис технології обробки даних, опис загроз з оцінкою ймовірності їх появи та можливої, порядок взаємодії підрозділів організації для забезпечення безпеки, рекомендації щодо вдосконалення системи захисту, організаційно-розпорядчі документи, які регламентують діяльність користувачів і обслуговуючого персоналу.

2. За результатами обстеження розробляється концепція інформаційної безпеки. Даний документ визначає загальну систему поглядів в організації на проблему захисту інформації та шляхи вирішення цієї проблеми з урахуванням накопиченого досвіду і сучасних тенденцій розвитку засобів і способів захисту.

3. Створення служби захисту інформації. Служба захисту інформації в структурі організації функціонує як спеціально створений підрозділ, який займається розробкою правил експлуатації, затвердженням повноважень користувачам щодо доступу до ресурсної системи, котра займається адміністративною підтримкою систематичного захисту інформації (настройку, контроль і оперативне реагування на сигнали про порушення правил доступу, аналіз журналів реєстрації подій і т.д.

4. Формування політики безпеки та розробка організаційно-розпорядчих документів. Політика безпеки є складовою часткою політики безпеки. Для кожної системи політика безпеки інформації є унікальною. Вона повинна містити такі положення: організаційні методивтілення безпеки; класифікація і принципи управління інформаційними ресурсами; безпеку персоналу; фізична безпека; перелік складових інформаційної безпеки; управління комунікаціями і процесами; контроль доступу; розробка та технічна підтримка обчислювальних систем.

5. Розробка технології захисту і визначення вимог до складу засобів захисту. На цьому етапі проводиться:

- інтеграція в єдиний комплекс різнорідних засобів і механізмів захисту та централізоване адміністрування механізмів захисту;
- визначення рівнів доступу об'єктів, прав доступу користувачів до об'єктів системи і правил розмежування доступу;

- формування правил реагування на загрози інформаційних ресурсів;
- оперативне оповіщення адміністратора безпеки про спроби порушення політики безпеки;
- реєстрація дій користувачів в захищених журналах для аналізу;
- моніторинг стану захищеності інформаційних ресурсів;
- контроль цілісності програмно-технічного середовища .

6. Вибір, придбання, встановлення та налаштування засобів захисту.

7. Навчання персоналу роботі із засобами захисту і правилам організаційного забезпечення безпеки .

8. Експлуатація системи .

9. Постійний моніторинг стану захисту ресурсів і вироблення пропозицій щодо її вдосконалення. Мається на увазі періодичний перегляд наступних положення політики безпеки: ефективність політики, який визначається за характером, кількістю і впливу зареєстрованих інцидентів, що стосуються безпеки; вартості засобів забезпечення безпеки на показники ефективності функціонування системи; вплив змін на безпеку технології.

Отже, вирішення питань захисту даних у сучасних інформаційних системах буде успішним лише за умови використання комплексного підходу до побудови системи забезпечення безпеки інформації.

РОЗДІЛ 2
АНАЛІЗ СТАНУ МОНІТОРИНГУ ТА ОЦІНЮВАННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Діяльність Ради Національної Безпеки і Оборони України щодо моніторингу та оцінювання загроз інформаційної безпеки України

Відповідно до положень Конституції України однією з найважливіших ланок державного управління і діяльністю усьогоукраїнського народу є України інформаційна безпека.

Рішення Ради національної безпеки і оборони України(далі – РНБО) «Про невідкладні заходи щодо забезпечення інформаційної безпеки України» була затвердженаУказом Президента України від 23 квітня 2008 року № 37 (скасовано 28 квітня 2014 року). Натомість Доктрину інформаційної безпеки (далі – Доктрина) булаприйнята після указу Президента України від 08 липня 2009 року № 514.

Як зазначено в Доктрині інформаційної безпеки України (далі – Доктрина), інформаційна політика– це самостійна ланка, що забезпечує національну безпеку нашого народу, але водночас є і складовою частиною кожної із її сфер.

У Доктрині вказано, що основною метою є створення в Україні розвиненого національного інформаційного простору і захист державного інформаційного суверенітету [11].

В інформаційній сфері України (згідно з Доктриною) життєво необхідними є інтереси як і окремої особистості, так і всього суспільства. А забезпеченню цих інтересів сприяє РНБО:

- інтереси особистості: дотриманнягарантованих Конституцією прав і

свобод людини на збирання, зберігання, використання та поширення інформації; недопущення незаконного втручання у зміст, процедури оброблення, передання і використання особистих даних; захист від антипозитивного інформаційно-психологічного впливу зовні;

- інтереси суспільства: підтримання і збільшення духовних, культурних і моральних цінностей національного народу; утворення і генезис демократичних інститутів суспільства;
- інтереси держави: неможливість інформаційної залежності, інформаційної блокади України, експансії у інформаційній галузі інших держав та міжнародних структур; дієву сумісну співпрацю органів державної влади та інститутів громадянського суспільства щодо реалізації державної політики угалузі інформаційного забезпечення; стрімке розвинення інформаційного суспільства та ін.

Також у Доктрині є перелік принципів, за якими має здійснюватися дотримання інформаційної безпеки України й запобігання ризикам [10]:

- вільний доступ до недоторканності оброблення інформації;
- правдивість, змістовністьта неупередженість інформації;
- забезпечення обмеженого доступу до інформації відповідно до чинного законодавства;
- налагодженнявзаємодії усіх різновидів інтересів;
- недопущення вчинення порушень у інформаційній галузі;
- економічна відповідність;
- відповідністьта однотипність законодавства України з міжнародним у інформаційній галузі;
- надання переваги національній інформаційній продукції.

Доктрина 2009 року, але і наразі важливим є останній принцип, але для його здійснення мають бути створені передумови, зокрема нормативно-правові, фінансові, фіскальні, що сприятимуть підвищенню конкурентоспроможності на світовому і національному ринках інформаційних та телекомунікаційних послуг національних телекомунікацій, вітчизняного виробника нашої інформаційної продукції.

Доктрину інформаційної безпеки від 2009 року також було скасовано в червні 2014 року Указ Президента України.

Скасовує Укази Президента 6 червня 2014 року №504, що втратили свою чинність, серед яких і Указ, що стосувався прийняття Доктрини, виконуючий обов'язки голови держави. А вже 7 червня Президентом України був обраний новий президент.

Нова редакція Доктрини набула чинності лише 29 грудня 2016 року, що була розроблена Міністерством інформаційної політики України.

Ця Доктрина, як і попередня, окреслюєзацікавленість нації в інформаційній сфері, та одночасно мету, завдання, принципи та механізми формування і забезпечення на території України інформаційної політики.

Так, пріоритетами української державної політики у вищезазначеній сфері є (порівняймо з попередньою Доктриною) [11]:

- побудова та розвиток структур, відповідальних за інформаційно-психологічну безпеку;
- розвиток і збереження технологічної інфраструктури підтримання інформаційної безпеки на території України;
- підтримання повноцінногозанурення України цифровою мовою, перш за все прикордонних і тимчасово окупованих територій.

Згідно з новою Доктриною, РНБО та інші державні структури має докласти багато зусиль для захисту інформаційного простору держави, адже фальсифікації, дезінформація має негативний вплив та наслідки, що можуть спричинити розкол українського народу, адже така політика є більш небезпечною за будь-яку іншу зброю.

Усі суб'єкти, що сприяють стабільності у галузі національної безпеки, їхню компетенцію та завдання прописано та закріплено у Законі, що має назву «Про основи національної безпеки України» від 19 червня 2003 року № 964-IV.

Цей Закон згідно з Конституції України окреслює найважливіші засади державної політики, метою якої є забезпечення захисту національних інтересів і гарантування безпеки кожної особистості, суспільства і держави в цілому від загроз і зовнішнього, і внутрішнього характеру у всіх сферах життєдіяльності, зокрема і в інформаційній.

Апелюючи до Закону № 964-IV, зазначаємо, що об'єкти національної безпеки, і в інформаційній сфері є:

- людина і громадянин – забезпечення прав і свобод, передбачених Конституцією;
- суспільство –підтримання духовних, морально-етичних, культурних, історичних, інтелектуальних та матеріальних цінностей, інформаційного і навколишнього природного середовища і втілення природних ресурсів;
- держава –забезпечення конституційного ладу, суверенітету, територіальної цілісності і недоторканості.

А основними принципами, що спрямовані на захист безпеки нації, у тому числі й інформаційної є:

- надання переваги правам і свободам фізичним особам;
- здійснення та дотримання на верховенство права;
- надання переваги договірнимшляхам розв’язання конфліктних ситуацій;
- особистість і реальність втілення методів, спрямованих на національні інтересидійсним і можливим чинникам загрози;
- диференціація компетентностііспівпраця органів державної влади щодо втілення національної безпеки;
- вільний цивільно – правовий контроль Воєнної організації держави з іншими органами усфері національної безпеки;
- здійснення в інтересах держави міждержавних систем та засобів міжнародної колективної безпеки.

Натомість суб’єктами, які здатні забезпечити національну безпеку, зокрема й інформаційну, згідно з Законом № 964-IV, є [14]:

- Президент України;
- РНБО;
- ВРУ;
- КМУ;
- центральні органи виконавчої влади;
- НБУ;
- загальні суди;
- прокуратура;
- НАБУ;
- державні адміністрації та органи місцевого самоврядування;
- ЗСУ, СБУ, СЗР України, Держприкордонслужба та інші.

Компетенція, якою наділені суб'єкти здійснення національної безпеки визначені

цим же Законом України, а також у відповідних профільних законах і положеннях, предметно регулюють правовий статус кожного з них.

Національна безпека Українизідійснюється за допомогою дієвої державної політики, яка базується на загально прийнятих доктринах, концепціях, стратегіях і програмах.

Обрання або надання переваги певним методам та напрямам здійснення національної безпеки України в даній сфері характеризується наявністю вчасного затвердження необхідних заходів, певному характеру і глобальністю загроз національним інтересам.

Головними різновидами державної політики, що стосується національної безпеки слід виокремити [14]:

- підтримання інформаційного суверенітету держави;
- поліпшення державного врегулювання розвитку даної галузі, що визначається прийняттям нормативно-правових актів та наявністю економічних чинників для забезпечення розвитку національної інформаційної інфраструктури та ресурсів, втілення сучасних технологій, заповнення усього масштабу інформаційного простору перевіреною та правдивою інформацією, що стосується держави;
- стрімке звернення уваги засобами масової інформації до протистояння корупції, перевищення службових повноважень та іншими загрожуючими державі явищами;
- підтримання безперешкодного втілення та реалізації Конституції щодо забезпечення прав і свобод громадян, доступу до інформації, вчинення перешкоджуючих дій органами державної влади, місцевого самоврядування, ЗМІ;
- прийняття певних шляхів, спрямованих на захист національного

інформаційного простору та протидії монополізації інформаційної сфери України.

РНБО України здійснює координацію і контроль діяльності суб'єктів сектора безпеки і оборони, які забезпечують кібербезпеку України.

Структура Національної системи кібербезпеки [14]:

- Міноборони
- СБУ
- Нацполіція
- НБУ
- Органи, які здійснюють розвідувальні заходи

Переважна увага Стратегії кібербезпеки України спрямована на:

- забезпеченняприятливих умов для привертання уваги нових підприємств, усіх форм власності, які задіяні у сфері електронних комунікацій, захисту інформації та / або які є власниками (розпорядниками) об'єктів критичної інфраструктури;
- вирішення завданнянеобхідності забезпечення заходів, спрямованих на захист інформації та кіберзахисту згідно з діючими нормами законодавства та взаємодія між державними органамипри досягненні мети.

Окрім державних органів управління, виконавчої та законодавчої влади, треба залучати громадське суспільство, зокрема науковців, навчальні заклади, різноманітні громадські організації та об’єднання, що допомагатимуть у розробці та реалізації заходів, що забезпечуватимуть кібербезпеку та кіберзахист.

Стратегія кібербезпеки України перераховує цілий комплекс заходів, пріоритетів і напрямів, що здатні забезпечити кібербезпеку України, зокрема [13]:

- будова і реалізація державної політики, яка має на меті стрімкий розвиток кіберпростору і відповідність нормам ЄС і НАТО;
- наявність конкурентного ринку та обслуговування у сфері кіберзахисту та електронних комунікацій;
- втілення та реалізація потенціалів установ, об'єднань підготовки певних проектів та суттєвих концептуальних документів у сфері кібербезпеки;
- проведення навчань з надзвичайних ситуацій та інцидентів в кіберпросторі;
- зростаннякультури безпеки поведінки в кіберпросторі та цифрової грамотності громадян;
- розширення масштабів співробітництва на міжнародній арені й надання переваги міжнародним ініціативам кібербезпеки, враховуючи співпрацю України разом із ЄС та НАТО.

У Стратегії кібербезпеки України зазначено, що робочим органом РНБОУ має стати Національний координаційний центр кібербезпеки,який необхідно створити. І сьогодні Національний координаційний центр кібербезпеки є постійно діючим, прауюючим органом РНБО України.

Апарат Національного координаційного центру складається з [14]:

- Керівника, яким є Секретар РНБО України
- Секретар – керівник структурного підрозділу Апарату РНБО України, який займається питаннями кібербезпеки

- Члени Центру – представники суб'єктів сектора безпеки і оборони України у сфері кібербезпеки

Також до складу Національного координаційного центру входять суб'єкти, відповідальні за безпеку і оборону України у сфері кібербезпеки: заступники Міноборони України, начальника Генерального штабу ЗСУ, Голови СБУ, Голови Служби зовнішньої розвідки України, Голови Нацполіції України, Голови НБУ, до відання яких належать питання кібербезпеки, начальник Головного управління розвідки Міноборони України, начальник управління розвідки Адміністрації Державної прикордонної служби України та Голова Держслужби спеціального зв'язку та захисту інформації України.

Завданнями Національного координаційного центру є:

- проведення аналізуючої діяльності:
- рівень кібербезпеки;
- надання оцінки національної системи кібербезпеки;
- можливість суб'єктів реалізаці кібербезпеки до вчинення професійних обов’язків;
- забезпечення втілення законодавства у даній сфері;
- даних про кіберінцідентах щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;
- надання прогнозів і можливість прояву загроз;
- узагальнення міжнародного досвіду у даній сфері;
- стрімке, інформаційно-аналітичне забезпечення РНБО;
- прийняття участіуреалізації і втіленні національних і міжнароднихвчень, методичне розроблення певних документів і порад.

Національний координаційний центр виконує важливу функцію у забезпеченні інформаційної безпеки України. Тому він має доступ до інформаційний баз даних різних державних систем, доступ до державних, зокрема й урядових, систем зв'язку та комунікації, до мереж спеціального зв'язку. Центр має право також в установленому порядку запитувати та отримувати дані, інформацію матеріали довідкового характеру від органів виконавчої влади, органів місцевого самоврядування, підприємств, установ і організацій.

2.2. Результати діяльності Діяльність Ради Національної Безпеки і Оборони України щодо протидії загрозам інформаційної безпеки України

Початок 2021 року асоціюється із важливими кроками, які здійснило керівництво. Заблокування проросійських каналів з «пулу Медведчука» – це крок до патріотизму, до видалення небажаних елементів, що спотворюють інформацію. Згодом були введені санкції і проти самого кума Путіна, і проти його дружини.

Президент лише ухвалив це рішення, проте вагома роль належить саме Раді національної безпеки та оборони України. Це чудовий результат для діяльності органу, дії якого спрямовані на забезпечення безпечного стану в державі.

Отже, РНБОУ –це координаційний орган, що спрямований на розробку, вирішення та реалізацію питань національної безпеки і оборони. Розберемось із словом координаціний, координує. Це означає впорядковує. Але що саме? Діяльність інших органів державної влади, інформаційна галузь для яких є профільною.

Верховним головнокомандувачем, тим, хто регулює діяльність самої РНБОУ є не секретар цього органу (ця думка є поширеною), а Президент, що ухвалює рішення, після їх скрупульозного перегляду.

СтруктураРНБОскладається з: прем'єр-міністра, міністра оборони, голови СБУ, міністра внутрішніх і закордонних справ. Однак формує апарат РНБО саме голова країни, і він може включити туди «керівників інших центральних органів виконавчої влади» та «інших осіб» – тобто різних осіб на власний розсуд, але які будуть спеціалізуватися на питаннях національної безпеки.

Не менш важливу функцію виконує і секретар Ради, що корегує організаційну структуру, готує проєкти указів Президента, що мають вступити в дію, а також здійснює контроль над органами влади, а саме як вони виконують свої обов'язки [12].

У документі, що стосується координаційного органу (РНБОУ) розписано багато положень про його функції та компетенції. Наприклад, таких як: «розробляє і розглядає питання, що належать до сфери національної безпеки і оборони» або «приймає рішення щодо визначення стратегічних національних інтересів України».

Ще, як ми вже з'ясували, РНБО здійснює контроль та координує діяльність інших органів влади, готує проєкти указів президента і інших нормативних актів (зокрема секретар), що розглядають питання національної безпеки. Склад РНБО має миттєво реагувати на ризики, аномалії, атаки, що здатні призвести до негативних наслідків. РНБО має право вводити надзвичайний та воєнний стан у країні.

Проте випадків введення воєнного стану за всю історію незалежності України, на щастя, не так і багато. Лише один, який був за головування Петра Порошенка у листопаді-грудні 2018 року.

Коли розпочалась війна на сході України, коли посягнули на територіальну цілісність держави та ведуть нечесну боротьбу, де інформація є потужною

зброєю, то тема національної безпеки, кібербезпеки стала настільки актуальною, як ніколи раніше.

Отже, організаційна структура РНБО та її роль не буде завжди стабільною, бо багато залежить від того, хто стоїть на чолі держави та наскільки ця особа зацікавлена питаннями нацбезпеки.

Зростає роль РНБО з початком війни, коли на порядку денному питання безпеки стало найголовнішим. Порошенко і Зеленський не лише застосовують інший інструментарій. Під час їхнього керування державою здійснено низку рішень, що сприяли покращенню діяльності органу.

Так, у 2014 році РНБО здобула більше повноважень, адже відтепер усі рішення, що ухвалив Президент, є обов'язковими для виконання. Також деякі зміни відбулись і в організаційній структурі, бо до складу РНБО можуть входити «інші особи», яких призначить Президент.

Найбільше обговорення викликав Закон про санкції, що набув чинності у серпні 2014 року. Тоді, завдяки цьому рішенню, вдалося заблокувати такі популярні в Україні російські соціальні мережі, як «ВКонтакте», «Одноклассники» та низку інших російських сайтів.

Цей закон сприяє більшій відповідальності громадян, проти яких можуть вводитися обмежувальні заходи, якщо будь-хто із громадян здійснює терористичну операції. Такі заходи були вжиті щодо депутатів Тараса Козака та Віктора Медведчука.

Коли санкції вводяться проти конкретної фізичної та юридичної особи, то рішення приймає сам орган на чолі з президентом. Проте якщо обмежувальні заходи стосуються іншої країни, то залучається також законодавча влада – парламент.

Складним та дискусійним питанням і досі є введення санкції проти конкретних громадян. Так, чи можна вважати їх винними, якщо вони не є засудженими, чи можна без судового процесу обмежити їхні права? Проте РНБО можна виправдати, якщо враховувати мету органу – ліквідація загрози, що має згубні наслідки для інформаційного простору України.

Наступне питання, яке потребує обговорення: чи правильно, що головою РНБО є президент? Чи не призведе це до узурпації влади? Функція Президента – координувати та ухваляти, проте не нав'язувати тільки свою думку без узгодження членів РНБО. Проблемою є те, чи добросовісно він поставиться до формування апарату Ради, чи призначить «своїх» людей [13].

Наразі виникла тенденція – забезпечувати вплив РНБО в інших сферах. Так, до конкурсної комісії РНБО із дев'яти членів відправлятиме трьох. Завдання комісії: обрати директора Бюро економічної безпеки. А законопроект про Національне антикорупційне бюро передбачає той же і щодо комісії, яка обиратиме його керівника.

Повернімося до Закону про санкції та рішень, які були прийняті після набуття його чинності. Окрім санкцій проти Медведчука та Козака, РНБО доручає органу виконавчої влади повернути державне майно (як зазначив Олексій Данилов – секретар РНБО) – нафтопродуктопровід«Самара – Західний напрямок».

РНБО може стати як рятівним жилетом, якщо вдосконалювати його організаційну структуру та інструментарій, але може стати і якорем, якщо голова держави буде зловживати своїми повноваженнями (без вердикту суду!) У такому разі не уникнути «ящика Пандори» та усіх бід, що чекатимуть на державу в цілому.

РНБО – це або чарівна паличка, або небезпечна зброя в руках президента. Проте склад РНБО має направляти голову у правильне русло та не дозволяти зловживати своїми повноваженнями.

Покращити діяльність РНБО можливо, проте чи буде та стабільність завжди, якщо змінюються президенти. Україна потребує впорядкованого, організованого, координаційного органу, що зможе захистити національні інтереси усієї держави.

Отже, різні небезпечні виклики в галузі національної безпеки «пробудили» РНБО. Наш інформаційний простір потребує захисту та конфіденційності, а особливо в умовах російської агресії. Члени РНБО передусім мають піклуватися не про власні інтереси, а про інтереси особи, суспільства та держави.

Одним з головних та передбачених законодавством завдань, що належить до державної політики держави є забезпечення та підтримання національної безпеки, однак слід звернути увагу, що на першочергових етапах забезпечення державної політики розуміється як підтримання та сприяння військовій безпеці, яка згодом була а поширена на національну безпеку.

А механізм української державної політики спрямований на досягнення мети національної безпеки, провідним завданням якої є підтримання вже існуючого рівня заінтересованості суспільства і країни, за допомогою ведення моніторингу, своєчасне виявлення та попередження вчинення загроз внутрішніх і зовнішніх чинників.

Ефективність такої політики потребує суттєвої зміни, оскільки необхідно Створити модель її функціонування та запровадити комплексну систему нормативно-правових актів у галузі національної безпеки [26].

До провідних функції державної політики відносять такі дії суб'єктів

державного управління, які є чітко визначеними, організованими різновидами управління у сфері національної безпеки, за допомогою яких відбувається здійснення а втілення національних інтересів суспільства, тим не менш, здійснюється координування усіх галузей життєвої діяльності як держави так і суспільства в цілому.

Тож, існування цілеспрямованості, полягає у здійсненні відповідних умов для розвитку людства, стрімкий розвиток одночасно держави і суспільства та подолання можливих. негативних чинників, які можуть знизити спроможність держави на втілення національних інтересів на світовому ринку.

Особливість таких чинників має втілення у аналізуванні та подоланні негативних чинників, за допомогою національних інтересів здійснюється ЗСУ та іншими органами [27].

Та зокрема, Провідною метою дослідження таких механізмів, за допомогою яких здійснюється державна політика у галузі інформаційної безпеки є сприяння та підтримання інформаційного суверенітету та затвердження підходів, що спрямовані на розвиток та захист інформаційного простору держави задля повного та грунтовного інформаційного забезпечення суспільства України.

Інформаційна безпека визначає рівень захисту суспільно важливих життєвих інтересів людини, і держави в цілому. У зв'язку із неповним, несвоєчасним, недостовірним поширеннямінформації відбувається виникнення загрози доступу до такої інформації, її незаконний обіг, що має обмежений доступ у зв'язку із розповсюдженням інформаційного і психологічного впливу, який носить негативний характер та цілеспрямоване спричинення антипозитивнихнаслідків використання технології у сфері інформації.

Інформаційна безпека та здійснення державної політики у даній галузі передбачає цілеспрямовану діяльність, яка спрямована на здійснення захисту

потреб та інтересів суспільства у зазначеній галузі, розвиток стратегічного напрямку держави та суспільної інформації, існування та захист від тебе кібернетичних, комп'ютерних та інших систем, які здійснюють утворення та побудову інфраструктурної основни державного простору у галузі інформації [28].

РОЗДІЛ 3

ШЛЯХИ ВДОСКОНАЛЕННЯ СИСТЕМИ МОНІТОРИНГУ ТА ОЦІНЮВАННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Удосконалена процедура моніторингу загроз інформаційної безпеки України

В умовах глобалізації інформаційний простір будь-якої країни перебуває під загрозою. Україна є вкрай вразливою до політичних зазіхань з боку як країни-агресора, так і західних популістів. Так, коли в країні гібридна війна, то великого значення необхідно надавати саме інформаційній безпеці, що перебуває під загрозою, є ареною зазіхань на інформаційний потік іншої держави. Зазіхання на безпеку цього виду з боку Російської Федерації є дуже потужною зброєю як проти України, так і проти її громадян. Це маніпулювання їхньою свідомістю, коли метою є викликати зміну , що негативно вплине на перебіг подій соціально-політичного характеру в Україні. Отож країна-агресор застосовує дієві та сучасні інформаційні технології, за допомогою яких відбувається вплив на свідомість громадян та здійснюється цілеспрямоване розпалювання одночасно агресивногонаціональногота релігійного ворожого ставлення, підбурювання до війни, внесення змін та доповнень до

конституційного ладу із застосуванням насиллячируйнування суверенітету та територіальної єдності України.

Щоб захистити державу від кібератак, необхідно звернути увагу на те, які інноваційні підходи допоможуть захистити інформаційну систему та вплинути на розвиток інформаційного простору в умовах вільного обігу інформації.

Оскільки в сучасному світі будь-які контакти відбуваються переважно через мережу Інтернет, то надважливою ланкою є кібербезпека. Відомим фактом є моніторинг соціальних мереж з боку спецслужб задля вияву небажаних проявів користувачів, що становлять певну загрозу для суверенітету нашої країни. Проте інформаційний потік відбувається не лише в листуванні чи в постах/репостах. Основне його відгалуження це різноманітні сайти, левова частка яких є ще й приватними, такими, що мають на меті приховати, будь-якими способами перекодувати інформацію, деколи спотворюючи основний зміст. Моніторинг загроз, на нашу думку, варто розпочинати саме з перевірки функціонування таких сайтів.

У цьому разі слід акцентувати увагу на такому інноваційному підході, що виявляє відхилення в інформаційній безпеці (мережевій) - Network behavior anomaly detection або ж знакодженні відхилень у поведінці в мережі. Слід також наголосити, що він достатньо часто може бути використаний як антивірусне та антишпигунське програмні. У випадках, коли відхилення виявлені вчасно слід проводити терміновий моніторинг мережі на відсутність чи наявність нестандартних подій або тенденцій.

Відхилення виявляються за допомогою цілісного комплексу систем у мережевій поведінці, які надають можливість ідентифікувати загрози, у випадках коли сигнатурний аналіз не надає жодних результатів, тобто:

- при загрозах нульового дня;
- при зашифровані трафіку при переданні даних на командний сервер у ботнетах.

Тобто надає можливість ідентифікувати критичні характеристики мережі у реальному часі і надсилає тривожний сигнал при будь-якому прояві підозрілою загрози. Дані характеристики містять у собі обсяг трафіку, забезпечення смуги пропускання та використання протоколів.

Дані системи також мають можливість слідкувати за поведінкою вузлів мережі, виявлення аномалій є дієвим у випадку, коли звичайно поведінка у мережі є незмінною тривалий час, тобто стала поведінка —норма, а будь-які відхилення від норми – аномалія.

На нашу думку, системи, які виявляють аномалії мають бути використані сумісно із звичайними мережевими екранами та усіма застосунками, за допомогою яких здійснюється виявлення загрожуючих програм, однак деякі виробники зазначають, що використання таких систем є їх власним рішенням щодо мережевої безпеки для подолання негативних проявів та одночасного їх дешифрування.

Якщо розглядати соціальні мережі, то достатньо вірним є рішення щодо блокування російських сайтів, що позитивно зазначається на безпеці українського інформаційного простору, наприклад, Вконтакті, який є інтелектуальний власністю Російської Федерації, у зв'язку з чим ускладнюється всебічний контроль за обсягом інформації у мережах України та Російської Федерації.

Відтак, постає проблема моніторингу інших російських додатків, які зараз є в активному користуванні українців (наприклад, Telegram). Відомою є їхня політика конфіденційності, однак це може служити і недоліком з точки зору інформаційної безпеки України.

Незабаром має з’явитись нова функція у системі Google, про що повідомляє The Indian Express. Ця можливість допоможе краще захистити персональні дані, аніж це було раніше. Так, відтепер користувачі зможуть встановити опцію, щоб

кожні 15 хвилин історія видалялась автоматично. У такому разі сторонні особи не зможуть переглянути, що цікавило користувача, яку інформацію він шукав.

Отож якщо ми говоримо про моніторинг та оцінку інформаційної безпеки, то необхідно звернути увагу не на кількісний чинник (тобто запропонувати велику кількість шляхів уникнення загроз), а на якісний (запропонувати небагато способів, але ефективних). Потрібно слідкувати за змінами, вміти виявити аномалії вчасно, мінімізувати ризик до мінімуму, щоб не відбулося просочення (витоку) інформації, зокрема державного масштабу.

Етапи процесу управління загрозами інформаційної системи запропоновано у статті «Організація інформаційної безпеки ресурсів на базі системи оцінки ризиків». Серед них:

1. **Оцінка ризику.** На цьому етапі відбувається збір даних: класифікація компонентів інформаційної системи та класифікація ризиків, послідовне розміщення джерел загроз, розміщення ризиків згідно з пріоритетом.
2. **Підтримка ухвалення рішень.** Етап, на якому вже починають діяти: вибір можливих рішень для моніторингу, оцінка цього рішення, чи допоможе воно знизити ризик та згодом нейтралізувати його.
3. **Реалізація контролю.** Етап, коли здійснюється моніторинг шляхом застосування цілісного підходу.
4. **Оцінка ефективності.** Етап, коли перевіряють, наскільки ефективною є та програма, яку розробили для контролю та усунення загроз [15,с.103].

Також автор статті пропонує узагальнену процедуру управління загрозами інформаційної системи:

«1. Детальна класифікації інформаційних ресурсів.

2. Перелік всіх уразливостей та загроз по відношенню до інформації, які стали причиною отриманого значення ризику.

3. Визначення ризику для кожного цінного ресурсу організації.

4. Визначення ризику для ресурсів після вжиття контрзаходів (залишковий ризик).

5. Оцінка ефективності використаних контрзаходів з ціллю мінімізації ризику.

6. Моніторинг та переоцінка ризику інформаційної безпеки»[15, с.103-104].

Сьогодні під загрозою перебуває економіка держав, тому людство намагається надати захист, створюючи різні системи, які здатні надати інформаційну безпеку. Кожна із установ повинна передусім мати міжмережевий екран, система виявлення вторгнення та антивірусне рішення. Але це лише необхідний мінімум. Забезпечують захист від атак SIEM-системи, які мають такі можливості:

- збір даних про події з різних пристроїв;
- показ подій у реальному часі;
- підтримка і сигнатурних, і поведінкових методів виявлення загроз;
- можливість заблокувати шкідливий трафік на мережевих пристроях;
- можливість спрогнозувати, якими ж будуть результати атаки.

Серед таких SIEM-систем популярними є:

- Solarwinds;
- Netwrix;
- Rapid7;
- MicroFocus.

Проте програмне забезпечення SolarWinds вдалося зламати хакерам у 2020 році та отримати доступ до дев’яти державних відомств США та сотні приватних компаній. Цю атаку визнано одним з найнебезпечніших втручань

в інформаційний потік держави. Найгірше те, що про дії хакерів не мали уявлення декілька місяців, адже система не змогла визначити загрозу.

У праці Є.Насвіта виділено основні процеси системи управління інформаційною безпекою (на основі перерахованих вище дій та етапів), адже безпека не є сталим поняттям та кінцевим результатом (безпека –це процеси, метою яких є захистити):

- Процес оцінки ризиків інформаційної безпеки;
- Процес усунення ризиків інформаційної безпеки
- Процес управління ресурсами
- Процес забезпечення обізнаності та компетентності
- Процес зв'язку
- Процес контролю документації та записів
- Процес управління вимогами
- Процес управління змінами інформаційної безпеки
- Процес управління зовнішніми процесами
- Процес оцінки продуктивності
- Процес внутрішнього аудиту
- Процес управління інцидентами інформаційної безпеки
- Процес вдосконалення інформаційної безпеки
- Процес управління відносинами і споживачем інформаційної безпеки
- Процес управління конфігураціями

Повернімося до інформаційної безпеки України. Найбільшою загрозою для українських користувачів є спілкування через месенджери, адже наша держава не має важелів впливу на відповідні програми для швидкого обміну повідомленнями. Наприклад, Telegram – це не тільки обмін повідомленнями (перевагою є створення секретних чатів, повідомлення з яких видаляються автоматично через певний проміжок часу), а й також низка каналів, які можуть

носити неприйнятний характер та поширювати пропаганду (зокрема російську). Наскільки цей месенджер є безпечним з'ясувати неможливо, адже немає достовірної інформації щодо офісу та самих розробників. Вседовзволеність Телеграму є небезпечною не тільки для України (витік важливої інформації), а й взагалі для людства, адже цей додаток відкриває простір для небезпечних терористичних організацій.

Інформаційна війна проти українського народу є небезпечним явищем, це зброя, адже загрози в інформаційному просторі, пропагандистські операції впливають на психіку окупованого народу, на його рішення та здійснюють розкол між захисниками та мирним населенням, між окупованим населенням та українцями по ту сторону барикад. Метою є протистояння гібридній війні та забезпечення кібербезпеки. Для цього необхідно вжити заходів задля уникнення аномалій та атак на інформаційну систему з боку держави-сусіда, щоб зберегти суспільні цінності та уникнути розколу нації.

Конкурентноспроможним український інформаційний простір буде тоді, коли держава зможе забезпечити його зовнішній розвиток, тобто шляхом інтеграції до структур глобальної інформаційної системи. Покращити інформаційну систему необхідно у всіх галузях: внутрішніх та міжнародних відносинах, енергетики, транспорту, державного управління, фінансової сфери.

Щоб вдосконалити систему управління інформаційною безпекою, необхідно змінити правові та організаційні механізми, покращити інтелектуально-кадрове та ресурсне забезпечення, зокрема треба підвищити ефективність шляхом впровадження змін у законодавстві з питань національної безпеки та втілити це потім на практиці. Отже, передусім треба вдосконалити законодавство шляхом:

– розвитку правових засад управління національною безпекою за допомогою розроблення та прийняття певних нормативно-правових актів, стратегій, Національної програми протидії тероризму та екстремізму, Концепції розвитку Воєнної організації держави, Національної стратегії формування

інформаційного суспільства, Доктрини інноваційного та науково-технологічного розвитку тощо;

– прийняття та втілення національних стандартів та технічних регламентів використання інформаційних комунікаційних технологій, які відповідають міжнародним стандартам, а також є ратифікованими Верховною Радою України Конвенції про кіберзлочинність;

– застосування міжнародних стандартів на національному рівні щодо питань охорони державної таємниці;

– прийняття та втілення загальнодержавної системи проведення моніторингу показників, що визначають рівень захисту національних інтересів у різноманітних сферах діяльності суспільства та появу дійсних загроз національній безпеці [17, с.19].

Вживати заходів щодо інфо-роззброєння мають і національні уряди, і виконавча влада, і громадянське населення, а також міжнародні спільноти та інституції ЄС.

Обов'язки парламенту та виконавчої влади:

- Нагадати українським медіа (зокрема онлайн-медіа), що вони мають не тільки права та свободу слова, але й також несуть відповідальність за оголошену інформацію. Законопроєкт «Про медіа» намагаються вдосконалити і досі, адже щодня відбуваються певні зміни, до яких треба пристосовуватися. Потребують змін також і закони «Про Національну раду України з питань телебачення і радіомовлення», «Про телебачення і радіомовлення».

- Забезпечити прозорість не тільки онлайн-медіа, а також і політичних та інформаційних кампаній.

- Треба протистояти поширенню дезінформації та різноманітних маніпуляцій шляхом законодавчої боротьби.

- Забезпечити зміну мовної політики; підвищити рівень законодавчої боротьби проти мови ненависті та ворожнечі.

- Накладати санкції на тих, хто здійснює кібератаки та на російські «медіа»-компанії, які порушують попередні санкційні режими.
- Найголовніше – розвивати медіаграмотність не тільки на формальному рівні, але й на неформальному та позаформальному.

Щоб здійснити ці заходи національні уряди повинні виконувати «Доктрину інформаційної безпеки» України, створити урядовий центр, з метою моніторингу, оцінки та уникнення ризиків; покращити кадровий та ресурсний потенціал інституцій, що займаються питаннями інформаційної безпеки; моніторити ефективність тих кроків, які були здійснені, щоб і надалі крокувати в правильному напрямку; співпрацювати з такими гігантами, як Google, Facebook; співпрацювати з міжнародними медіа, щоб уникнути викривлення інформації.

Від громадянського суспільства та медіа потребуємо:

- реалізувати проєкти, які характеризують постійних аґентів інформаційного впливу;
- плідно опрацьовувати шляхи покращення певних демократичних наративів;
- підвищити ступінь саморегуляції та співрегуляції, задля можливості уряду для ухвалення ініціативи, яка спрямована від певної галузі;
- збільшити масштаб практики і навиків фактчекінґу у медіа та суспільствівцілому.

Отже, ми намагалися з’ясувати, як удосконалити систему управління

інформаційною безпекою, яких заходів вжити з боку національних урядів та громадянського суспільства. І це з метою інфо-роззброєння треба здійснювати процеси, що зможуть зменшити ризик проникнення чужорідних елементів в інформаційну систему держави та нівелювати аномальні явища.

Напрями удосконалення організаційної структури Ради Національної Безпеки і Оборони України з урахуванням нової концепції протидії загрозам інформаційній безпеці

14 вересня 2020 року указом Президента України було затверджено «Стратегію національної безпеки України». Згідно з цим указом забезпечити безпеку всієї країни зможемо шляхом застосування дедуктивного методу. Тобто від безпеки кожної особистості залежить безпека країни, а людина та її безпека відповідно до чинного законодавства вважається найвищою соціальною цінністюна території України, дане положення є головноюметою державної політики національної безпеки згідно Конституції України [18].

Базується нова стратегія, як ми вважаємо, на ретельно прописаних засадах, а саме: стримування, стійкість та взаємодія. Стримування – засада, що передусім стосується організації воєнної безпеки України. У наш час національна та воєнна безпеки тісно переплетені. Так, потребують удосконалення та розвитку оборонні спроможності, щоб запобігти збройній агресії проти України.

Наступна засада – стійкість. Полягає у стабільному функціонуванні безпечного стану та можливості швидко адаптуватися до змін, з метою мінімізувати ризики та аномалії. У стабільності та організованості закладено успіх усіх державних структур, що забезпечують безпеку країни. Натомість хаос та дезорганізації

здатні призвести до руйнівних наслідків. Система управління має бути правильно організовано, але і цього замало. Апарат РНБО має ухвалити низку законопроєктів, що сприятимуть захисту від наслідків кібер-, інформаційних, терористичних атак, від ворожих впливів ззовні.

Ще одна важлива засада, на яка задіянапобудова стратегії національної безпеки України – це плідна взаємодія. Національну безпеку можна забезпечити вповні шляхом взаємозв'язку із зовнішнім світом (але не слід забувати про національні інтереси). Стабільність та стійкість національної безпеки – це не тільки покращення організаційної та правової структури; це також залучення іноземних партнерів до співробітництва: Європейського Союзу, НАТО, США та інших країн.

Отже, протидіяти загрозам інформаційної безпеки можна шляхом забезпечення безперервності управління держави, а також шляхом інтеграції в європейський простір. Необхідно не забувати, що значну увагу слід приділяти розписування тих документів, що будуть забезпечувати національну безпеку в країні. Для нашого народу – це вищезгадана «Стратегія національної безпеки України», для США – «Стратегія національної безпеки США», для Німеччини – «Біла книга» і т.ін.

У документі, що регулює державну безпеку в Україні, постійні інтереси та пріоритети, які мають значення на цей момент, розписані під одним підрозділом. Серед них такі:

«боротьба за незалежність державного суверенітету;

Побудова єдиного територіального округу у межах визначеного на міжнародній арені державного кордону країни;

суспільний розвиток;

захист прав, свобод і законних інтересів громадян України;

євроатлантична і європейська інтеграція» [18].

В американській системі безпеки також відбуваються зміни та реформування, але здебільшого вона зберегла свою спадкоємність і навіть базується ще на Законі «Про національну безпеку США» від 1947 року.

Чи могла б система безпеки України зберегти свою спадкоємність? Чи можна було б не змінювати організаційну структуру РНБО та не прописувати нові стратегії? Чи можливо тому, що ми громадяни України, помічаємо разючі зміни у різних сферах життя, зокрема і тієї, що стосується інформаційної безпеки. Тому система безпеки потребує вдосконалення та стабільності, враховуючи сьогоднішні події, а саме агресивні дії сусідньої держави.

У «Стратегії» прописані напрями, що допоможуть реалізувати пріоритети. І ці напрями передусім стосуються відновленню територіальної цілісності та миру на тимчасово окупованих територіях та різних заходів, що допоможуть мінімізувати та нівелювати російську агресію (це стосується і кібербезпеки).

У чому недолік «Стратегії національної безпеки України»? Так, у документі добре прописано плани на майбутнє, враховано різні сфери, які потребують вдосконалення, але хто виконуватиме низку тих завдань, які потребують виконання? Немає чіткої структури, за ким певні обов’язки закріплені, усю вагу відповідальності перекинути на плечі України.

І незрозуміло, яка роль Президента, яка роль РНБО, яка роль інших структур. Без чіткого розподілу існує загроза хаосу та неможливості запобігти ризикам, зокрема інформаційним.

РНБО України повинна не лише приймати стратегічні рішення, але й також здійснювати модернізацію структур апарату національної безпеки. Важливим є те, щоб дії тих, кому належить влада у державі, не мали закритий характер. Необхідно звертати увагу на зв'язок з громадськістю. Наприклад, рекомендації, що обговорюються на засіданнях, повинні виноситись на розгляд громадськості.

Апарат РНБО вимагає зміни та розвитку, адже наразі не достатньо ефективно виконує свої функції у прийнятті важливих рішень, що стосуватимуться сфери національної безпеки і оборони, а також координації та контролю діяльності визначених державних органів у цій сфері. До роботи у цьому форматі мають залучатися не лише працівники апарату та спецслужб, а визнані науковці, політологи, громадські діячі тощо. Слід звернути увагу і на необхідність підвищення рівня виконання рішень РНБОУ, посилення відповідальності за їх невиконання.

ВИСНОВКИ

Програмою-максимум для нас було з’ясувати, які найбільш ефективні шляхи вдосконалення системи моніторингу та оцінювання інформаційних загроз. Ми намагалися вповні дослідити цю проблему шляхом теоретичного обґрунтування та практичних рекомендацій.

Так, у першому розділі ми закцентували увагу на теоретичній базі, щоб визначити для себе, що таке безпека, а саме інформаційна її складова на сучасному етапі (шляхом аналізу різноманітних поглядів на цю проблему). У першому розділі ми з’ясували, що безпека виступає важливішою категорією сучасної науки та передбачаєвідносини між суб’єктами певної діяльності, спрямованої на захист інтересів суспільства та держави з метою протидії зовнішнім або внутрішнім загрозам. Безпека в найбільш загальному поділяється на такі види: соціальна, природна та інформаційна. При цьому з погляду особливостей розвитку сучасної інфраструктури та з огляду на стрімкий процес протікання четвертої технічної революції, саме інформаційна безпека набуває першочергового значення. Отже, виокремлені форми інформаційної безпеки пов’язує спільна ознака: вони спрямовані на протидію загрозам, що виникають внаслідок накопичення інформації у потенційно небезпечних осіб, а відрізняє суб’єкт, на якого спрямовані загрози використання інформації у небажаних цілях.

У теоретичному розділі звернено увагу і на методологічну основу, яка необхідна для захисту інформації, на ефективні принципи, що потрібні для реалізації функції захисту. Такими важливими принципами є: принцип законності, обґрунтованості, створення спеціалізованих підрозділів, участі в захисті інформації всіх дотичних осіб, персональної відповідальності за захист інформації, наявності та використання всіх необхідних сил і засобів для захисту, превентивності прийнятих заходів щодо захисту інформації.

У другому розділі ми здійснюємо аналіз діяльності РНБО та з'ясовуємо, якими є результати цієї діяльності. Так, ми дійшли до таких висновків:

РНБО може стати як рятівним жилетом, якщо вдосконалювати його організаційну структуру та інструментарій, але може стати і якорем, якщо голова держави буде зловживати своїми повноваженнями (без вердикту суду!) У такому разі не уникнути «ящика Пандори» та усіх бід, що чекатимуть на державу в цілому.

РНБО – це або чарівна паличка, або небезпечна зброя в руках президента. Проте склад РНБО має направляти голову у правильне русло та не дозволяти зловживати своїми повноваженнями.

Покращити діяльність РНБО можливо, проте чи буде та стабільність завжди, якщо змінюються президенти. Україна потребує впорядкованого, організованого, координаційного органу, що зможе захистити національні інтереси усієї держави.

Третій розділ є найбільш творчим. Тут ми намагаємось запропонувати шляхи вдосконалення моніторингу інформаційних загроз та покращення роботи координаційного органу – РНБО.

Отже, ми намагалися з'ясувати, як удосконалити управлінську систему, яка забезпечує інформаційну безпеку, яких заходів вжити з боку національних урядів та суспільства. І це з метою інфо-роззброєння треба здійснювати процеси, що зможуть зменшити ризик проникнення чужорідних елементів в інформаційну систему держави та нівелювати аномальні явища.

Протидіяти загрозам інформаційної безпеки можна шляхом забезпечення безперервності управління держави, а також шляхом інтеграції в європейський простір. Необхідно не забувати, що значну увагу слід приділяти розписування

тих документів, що будуть забезпечувати національну безпеку в країні. Для нашого народу – це «Стратегія національної безпеки України».

РНБО України повинна не лише приймати стратегічні рішення, але й також здійснювати модернізацію структур апарату національної безпеки. Важливим є те, щоб дії тих, кому належить влада у державі, не мали закритий характер. Необхідно звертати увагу на зв'язок з громадськістю. Наприклад, рекомендації, що обговорюються на засіданнях, повинні виноситись на розгляд громадськості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Яницкий О. Н. Четвёртая научно-техническая революция и глубинные изменения процессов глобализации // Вестник Института социологии. 2017. - № 21. - С. 12-34. Режим доступу: https://doi.org/10.19181/vis.2017.21.2.452(дата звернення 03.02.2021). – Назва з екрана.

2. Шкарлет С. М. Еволюція категорії «безпека» в науко- вому та економічному середовищі / С. М. Шкарлет // Формування ринкових відносин. – 2007. – № 6. – С. 7−12.

3. Чуваков О.А. Безпека: соціально-політична сутність поняття \\ Правова держава, №18. – 2014. - Режим доступу: file:///C:/Users/user8/Downloads/Prav_2014_18_24.pdf(дата звернення 03.02.2021). – Назва з екрана.

4. Утенкова К. О. Дестабілізуючі чинники зовнішнього і внутрішнього середовища підприємства та їх вплив на економічну безпеку \\ Економіка та держава № 8. - 2019 - Режим доступу: http://www.economy.in.ua/pdf/8_2019/10.pdf(дата звернення 03.02.2021). – Назва з екрана.

5. Краснокутська Н. С., Коптєва Г. М. Дефініція поняття «фінансова безпека підприємства»: основні підходи та особливості. Бізнес Інформ. 2019. - №7. - С. 14–19 Режим доступу: https://doi.org/10.32983/2222-4459-2019-7-14-19(дата звернення 03.02.2021). – Назва з екрана.

6. Нікіпєлова Є. М. Сутність поняття “безпека” та його використання у системі державного управління й міжнародних відносин // Міжнародний науковий журнал "Інтернаука". — 2018. — №10. – С. 9 – 12

7. Горбатюк С. Є. Еволюція феномену безпеки: від стародавніх

політико-правових учень – до сучасної наукової думки \\ Вісник НАДУ при Президентові України № 2. - 2016. - Режим доступу: http://visnyk.academy.gov.ua/pages/dop/54/files/b7db0973-cf43-4ebc-bf58-05d250f71603.pdf(дата звернення 03.02.2021). – Назва з екрана.

8. Антонов В. О. Конституційна безпека країни: монографія / В. О. Антонов; наук. ред. Ю.С. Шемшученко. Київ: ТАЛКОМ, 2017. - 576 с.

9. Корнієнко Т.О. Сутність та еволюція поняття «економічна безпека» \\ Економічні горизонти, № 1 (4). - 2018 . - Режим доступу: http://eh.udpu.edu.ua/article/view/113118/128930(дата звернення 03.02.2021). – Назва з екрана.

10. Вишневська, І.А. Деякі аспекти діяльності ради національної безпеки та оборони України в протидії злочинам проти основ національної безпеки [Текст] / І.А. Вишневська, О.Ю. Дудченко // Діяльність органів публічної влади щодо забезпечення стабільності та безпеки суспільства : матеріали Міжнародної науково-практичної конференції, м. Суми, 21-22 травня 2015 р. / За ред.: А.М. Куліша, М.М. Бурбики, О.М. Рєзніка. — Суми : СумДУ, 2015. — С. 238-241.

11. Петрів І.М. Рада національної безпеки і оборони України: правові основи становлення та розвитку : монографія. Харків : Право, 2016. 202 с.

12. Федоренко В.Л. Конституційно-правовий статус Ради національної безпеки і оборони України. Бюлетень Міністерства юстиції України. 2010. № 12. С. 32–39.

13. Ситник Г.П. Концептуальні засади забезпечення національної безпеки України : навчальний посібник. Ч. 3. Київ : НАДУ, 2017. 314 с.

14. Цоклан В.І. Структура Ради національної безпеки і оборони України як важливий елемент її конституційно-правового статусу. Часопис Київського університету права. 2011. № 2. С. 90–93.

15. Чунарьова А. Організація інформаційної безпеки ресурсів на базі

системи оцінки ризиків // Режим доступу: https://www.researchgate.net/publication/328828485_ORGANIZACIA_INFORMACIJNOI_BEZPEKI_RESURSIV_NA_BAZI_SISTEMI_OCINKI_RIZIKIV

16. Насвіт Є. Фреймворк управління процесами забезпечення інформаційної безпеки в SOC // Режим доступу: https://ela.kpi.ua/bitstream/123456789/31418/1/Nasvit_magistr.pdf

17. Малик Я. Й. Інформаційна безпека України: стан та перспективи розвитку / Я. Й. Малик // Ефективність державного управління. - 2015. - Вип. 44(1). - С. 13-20. - Режим доступу: http://nbuv.gov.ua/UJRN/efdu_2015_44(1)__3.

18. Стратегія національної безпеки України (рішення від 14 вересня 2020 року) // Режим доступу: https://www.president.gov.ua/documents/3922020-35037

19. Рада національної безпеки і оборони України // Режим доступу: https://rnbo.gov.ua/?fbclid=IwAR0OPdzp0NjXpUh1B7FM7-e3qM4QM-ayCCynGFo_Yw_sFlk_XTPNsZ8B6HI

20.Федоренко Р. Контент-моніторинг інформаційного простору як чинник забезпечення інформаційної безпеки держави у воєнній сфері // Режим доступу: http://journals.dut.edu.ua/index.php/dataprotect/article/view/332

21. Закон України «Про Раду національної безпеки і оборони України» // Режим доступу: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text

22. Кацалап В. Метод моніторингу інформаційного простору воєнної сфери в інтересах забезпечення дій військ (сил) // Режим доступу: http://sit.nuou.org.ua/article/view/207647/213293

23. Стецюк С. Напрями оптимізації організаційної структури Міністерства оборони України відповідно до стандартів і принципів НАТО // Режим доступу: http://lsej.org.ua/3_2020/67.pdf

24. Апарат Ради національної безпеки і оборони України / Рада національної безпеки і оборони України. – Режим доступу:

https://www.rnbo.gov.ua/ua/Aparat-Rady-natsionalnoi-bezpeky-i-oborony-Ukrainy.html

25. Аналіз державної політики у сфері національної безпеки і оборони України // Режим доступу: https://rpr.org.ua/wp-content/uploads/2018/02/Analiz-polityky-NB-pravl-final.pdf

26. Криштанович М. Ф. Механізми державної політики України щодо забезпечення національної безпеки / М. Ф. Криштанович // Публічне управління та митне адміністрування. – 2019. - № 3 (22). – С. 248 – 253

27. Ситник Г.П. Концептуальні засади забезпечення національної безпеки України : навч. посібник. Київ : НАДУ, 2010. 208 с 3. Телявский Д. Политическая б

28. Почапцов Г.Г. Информация & дезинформация. – К.: Эльга, 2001. – 256с.

29. Пожуєв В.І. Формування державної інформаційної політики в умовах глобалізації / В.І. Пожуєв // Гуманітарний вісник Запорізької державної інженерної академії. – 2010. – Вип. 43. – С. 4–12.

30. Токар О. Державна інформаційна політика: проблеми визначення концепту / О. Токар // Політичний менеджер. – 2009. – № 5. – С.131–141.

31. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти : монографія / І.В. Арістова; за загальною редакцією д-ра юрид.

наук, проф. Бандурки О.М.. – Харків: Вид-во Ун-ту внутр. Справ, 2000. – 368 с.

32. Коментар до проекту Доктрини інформаційної безпеки України [Електронний ресурс]. – Режим доступу: http://www.rainbow.gov.ua/news/942.html

33. Чукут С.А. Роль сучасних засобів масової інформації в процесах державотворення (окремі аспекти) // Вісник УАДУ. – 1999. - № 3. – С. 158-167.

34. Телявский Д. Политическая безопасность. URL:

www.myshared.ru/slide/1282428.

35. Домбровська С.М. Механізм забезпечення державної соціальної безпеки в Україні. Наукові праці: Науково-методичний журнал. Державне управління. Миколаїв : Вид. ЧДУ ім. Петра Могили, 2015. Вип. 242. Т. 254. С. 28−32.

36. Якібчук О.В. Особливості екологічної безпеки України в системі національної безпеки. Вісник Київського національного університету ім. Т. Шевченка / Київ. нац. ун-т ім. Т. Шевченка. Київ, 2014. Вип. 1. Державне управління. С. 100−104.

37. Красноступ Г.М. Основні напрями правового забезпечення державної інформаційної політики / Г.М. Красноступ // Офіційний веб-сайт Міністерства юстиції України [Електронний ресурс]. – Режим доступу : http://old.minjust.gov.ua/30768

38. Коротич О. Б. Державне управління регіональним розвитком 29 України : монографія / О. Б. Коротич. – Х. : «Магістр», 2006. – 220 с.

39. Брижко В. М. Інформаційне суспільство. Дефініції / В. М. Брижко, О. М. Гальченко, В. С. Цимбалюк, О. А. Орєхов, А. М. Чорнобров. – К., 2002. – 220 с.

40. Тодика Ю.М. Конституційні права, свободи та обов’язки людини і громадянина: Підручник «Конституційне право України» / За ред. Ю. М. Тодики, В.С. Журавського. – К.: Видавничий Дім «Ін Юре», 2002. – 544 с.

41. Ємельянов С.Л. Основи інформаційної безпеки. – Одеса: Фенікс, 2014.– 357 с.

42. Белов Е.Б. Основы информационной безопасности / Е.Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов.. – М.: Горячая линия - Телеком, 2006. – 544 с.

43. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с

44. Бондарев В.В.. Введение в информационную безопасность автоматизированных систем. – М.: ГТУ им. Н.Э. Баумана, 2016. – 252 с.

45. Заплотинський Б.А. Основи інформаційної безпеки.Конспект лекцій. – КІІВіП НУ “ОЮА”, кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. – 128 с.

46. Жарков Я.М., Дзюба М.Т., Замаруєва І.В., ін. Інформаційна безпека особистості, суспільства, держави: Підручник. – К.: Видавничо-поліграфічний центр “Київський університет”, 2008. – 274 с.

47. Кавун С. В. Інформаційна безпека. Навчальний посібник. Ч. 2 / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 196 с.

48. Сидорчук О. Г. Соціальна безпека: державне регулювання та організаційно-економічне забезпечення [Текст] : монографія / О. Г. Сидорчук. — Львів : ЛРІДУ НАДУ, 2018. — 492 с.

49. Державна політика забезпечення національної безпеки України: основні напрямки та особливості здійснення. : монографія / Криштанович М.Ф., Пушак Я.Я., Флейчук М.І., Франчук В.І. – Львів : Сполом, 2020. – 418 с.

50. Нікітін Ю. В. Протидія злочинності в системі забезпечення внутрішньої безпеки українського суспільства: Монографія. – К.: ВНЗ «Національна академія управління», 2009. – 373 с.

Київський національний торговельно-економічний університет
Кафедра публічного управління та адміністрування

РЕФЕРАТ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на тему:

МОНІТОРИНГ ТА ОЦІНЮВАННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Студента 2 курсу, 5 мз групи,
спеціальності 281 «Публічне
управління та адміністрування»
спеціалізації «Публічне
управління та адміністрування» Фозілова
Рустама
Таваровича

_____
(підпис студента)

Науковий керівник
Кандиадт наук з державного
управління Мірко
Наталія
Вікторівна

_____
(підпис керівника)

Гарант освітньої програми
Кандидат економічних наук,
доцент Дьяченко
Ольга
Володимирівна

_____
(підпис гаранта)

Київ 2020

Випускна кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел (50 найменувань). Основний зміст роботи викладено на 46 сторінках комп'ютерного тексту. Робота містить 1 рисунок, 2 таблиці.

Метою роботи є дослідження моніторинг та оцінювання загроз інформаційної безпеки України в економічній структурі сучасного суспільства і запропоновані напрями удосконалення організаційної структури Ради Національної Безпеки і Оборони України з урахуванням нової концепції протидії загрозам інформаційній безпеці

Поставлена мета зумовила необхідність вирішення таких дослідницьких завдань:

- визначити сутність інформаційної безпеки в сучасних умовах;
- проаналізувати законодавче регулювання процесу моніторингу та оцінювання загроз інформаційної безпеки;
- дослідити досвід іноземних держав щодо здійснення ними інформаційної політики та можливості його застосування в Україні;
- здійснити аналіз діяльності РНБО та визначити основні результати цієї діяльності;
- запропонувати шляхи покращення моніторингу загроз інформаційної безпеки;
- запропонувати шляхи покращення організаційної структури РНБО.

Об'єктом дослідження випускної кваліфікаційної роботи є процес виявлення найбільш небезпечних і значимих загроз інформаційній безпеці України.

Предметом дослідження є теоретико-методологічні та прикладні засади механізму реалізації державної політики інформаційної безпеки.

Аналіз проблем забезпечення інформаційної безпеки в Україні базується на фундаментальних положеннях економічної теорії, діяльності Ради Національної Безпеки і Оборони України щодо протидії загрозам інформаційної безпеки України.

У роботі використовуються методи експертного оцінювання, метод парних порівнянь та метод анкетування, методи векторної оптимізації, теорії ймовірностей та логіко-конструктивні.

У першому розділі розкриваються теоретико-методологічні основи інформаційної безпеки в Україні.

У другому розділі здійснюється дослідження діяльності Ради Національної Безпеки і Оборони України щодо моніторингу та оцінювання загроз інформаційної безпеки України та результати її діяльності.

У третьому розділі оцінюються перспективи розвитку та пріоритетні напрями вдосконалення організаційної структури Ради Національної Безпеки і

Оборони України з урахуванням нової концепції протидії загрозам інформаційній безпеці.

Практичне значення одержаних результатів полягає у подальшому розвитку процедуру моніторингу загроз інформаційної безпеки України, а також у практиці впровадженняорганізаційної структури Ради Національної Безпеки і Оборони України з урахуванням нової концепції протидії загрозам інформаційній безпеці.

Анотація

У ході проведеного дослідження було визначена сутність та зміст інформаційної безпеки в сучасних умовах, вивчені методи її забезпечення. Охарактеризовано діяльність Ради Національної Безпеки і Оборони України щодо моніторингу та оцінювання загроз інформаційної безпеки України та їх результати. Виокремлено шляхи удосконалення системи моніторингу та оцінювання загроз інформаційної безпеки України. Сформульовано напрями поліпшення організаційної структури Ради Національної Безпеки і Оборони України з урахуванням нової концепції протидії загрозам інформаційній безпеці.

Ключові слова:моніторинг, оцінювання загроз, інформаційна безпека України, Рада Національної Безпеки і Оборони України, процедура моніторингу загроз, нова концепція протидії.

Abstract

In the course of the research the essence and content of information security in modern conditions were determined, the methods of its provision were studied. The activity of the National Security and Defense Council of Ukraine on monitoring and assessment of information security threats of Ukraine and their results is described. Ways to improve the system of monitoring and assessing information security threats in Ukraine are identified. Recommendations for improving the organizational structure of the National Security and Defense Council of Ukraine have been formulated, taking into account the new concept of counteracting information security threats.

Key words: monitoring, threat assessment, information security of Ukraine, National Security and Defense Council of Ukraine, threat monitoring procedure, new concept of counteraction.

РЕЦЕНЗІЯ

на випускну кваліфікаційну роботу
студента Фозілова Рустама Таваровича
2 курсу 5М групи заочної форми навчання
спеціальності 281 «Публічне управління та адміністрування»
на тему «**Моніторинг та оцінювання загроз інформаційної безпеки України**»
(за матеріалами Ради національної безпеки і оборони України)

Випускна кваліфікаційна робота виконана на тему, яка є актуальною для сфери публічного управління у сучасних умовах відбувається стрімкий розвиток інформаційних технологій, які впроваджуються у життя користувачів, саме це й забезпечує інформаційний ресурс та збільшує попит на якісну інформацію та оперативність її обробки. Виконана робота за змістом відповідає завданню в повному обсязі. Студент продемонструвала достатній рівень володіння теоретичним матеріалом щодо обґрунтування особливостей забезпечення інформаційної безпеки в Україні.

Робота розкриває сучасний стан інформаційної безпеки в Україні. В роботі проаналізовано сутність та зміст інформаційної безпеки в сучасних умовах, охарактеризовано методи її забезпечення, досліджено діяльність Ради Національної Безпеки і Оборони України щодо моніторингу та оцінювання загроз інформаційної безпеки України та визначено результати діяльності Діяльність Ради Національної Безпеки і Оборони України щодо протидії загрозам інформаційної безпеки України. Виявлені шляхи удосконалення системи моніторингу та оцінювання загроз інформаційної безпеки України. та розроблено напрями поліпшення організаційної структури Ради Національної Безпеки і Оборони України з урахуванням нової концепції протидії загрозам інформаційній безпеці.

Якість оформлення випускної кваліфікаційної роботи можна вважати задовільною. Основні вимоги щодо оформлення матеріалу враховані. Слід відзначити деякі несуттєві порушення стилю викладення матеріалу, який в окремих місцях роботи є ненауковим. В цілому матеріал роботи викладено послідовно і логічно.

Випускна кваліфікаційна робота рекомендується до захисту.

Рецензент
Заступник директора
Департаменту суспільних комунікацій
Київської міської державної адміністрації О.В. Деніс

Заява

Я, Фозілов Рустам Таварович повідомляю, що за результатами здійснення самостійної перевірки з використанням програмно-технічних засобів у наданій випускній кваліфікаційній роботі на тему: «МОНІТОРИНГ ТА ОЦІНЮВАННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ» не міститься елементів академічного плагіату. У випадках використання прямих запозичень з друкованих та електронних джерел, вказані відповідні посилання.

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

« 20 » листопада 2021 року _____ (підпис)

Згода

Я, Фозілов Рустам Таварович,

цим засвідчую, що є автором випускної кваліфікаційної роботи на тему: "МОНІТОРИНГ ТА ОЦІНЮВАННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ" несу повну відповідальність за достовірність, точність та повноту поданої у роботі інформації, жодна частина роботи не була скопійована, за винятком випадків, коли робиться належне підтвердження в присвоєнні. Я підтверджую, що у роботі не міститься державної таємниці або інформації для службового користування.

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

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

« 20 » листопада 2021 року _____ (Фозілов Р.Т.)

Підпис *Прізвище, ініціали*