НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Факультет соціології і права
Кафедра теорії та практики управління

«На правах рукопису»
УДК 351.751:351.86:004.056(477)

До захисту допущено:
В. о. завідувача кафедри
_____ Ростислав ПАШОВ
«___»_____20__ р.

Магістерська дисертація

на здобуття ступеня магістра
за освітньо-професійною програмою «Публічне адміністрування та електронне урядування»
зі спеціальності 281 «Публічне управління та адміністрування»
на тему: «Діяльність органів публічної влади в системі забезпечення інформаційної безпеки України»

Виконала:
студентка VI курсу, групи ПУ-з21мп
Панченко Дарія Дмитрівна

_____

Науковий керівник:
викладач кафедри теорії та практики управління, к. юрид. н.,
Черниш Вадим Олегович

_____

Рецензент:
доцент кафедри соціології, к. політ. н., доцент,
Багінський Андрій Владиславович

_____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студентка _____

Київ – 2023 року

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Сьогодні Україна переживає надскладні часи через неспровоковану повномасштабну агресію Російської Федерації проти нашої держави. У таких умовах інформаційна безпека набуває ще більшої актуальності та важливості як один з основних складників національної безпеки.

Як наголошують Ліпкан В., Максименко Ю. та Желіховський В. [1], становлення інформаційної цивілізації потребує докорінної зміни ставлення не лише до формування інформаційної політики, а і в її межах політики інформаційної безпеки, що містить вивчення та опанування теоретичних підвалин даних процесів. Тому важливого значення у процесі становлення інформаційного суспільства в Україні набувають питання формування національно орієнтованої інформаційної політики.

Ці питання є основою відання ряду органів публічної влади України. Виклики, які постали перед цими органами в умовах повномасштабного вторгнення Російської Федерації, набули ще більшого значення, а з тим і докладнішого опрацювання та потреби вдосконалення. У зазначеному аспекті гібридної війни значимою є і роль державних органів, зокрема, і єдиного законодавчого органу країни — Верховної Ради України.

Підрозділом у складі Парламенту України, який безпосередньо відповідає за інформування української та міжнародної аудиторії про події в Україні та діяльність Верховної Ради України, функціонування, адміністративний та інформаційний супровід в умовах повномасштабного вторгнення Російської Федерації в Україну, є Прес-служба Верховної Ради України. У відповідних умовах публічна довіра до державних інституцій, належне й об'єктивне інформування, а також потужні відповіді на внутрішні та зовнішні загрози є критично важливими задля забезпечення функціонування держави загалом.

Зв'язок роботи з науковими програмами, планами, темами. Робота виконана у межах ініціативної теми кафедри теорії та практики управління «Цифрова трансформація державного управління та місцевого самоврядування:

виклики та можливості для досягнення цілей сталого розвитку» (Державний реєстраційний номер: 0123U101483), у межах якої досліджено ряд цілей, зокрема, створення стійкої інфраструктури через сприяння інноваціям (Ціль 9), а також сприяння розбудові всеохопливого суспільства задля сталого розвитку, створення ефективних, підзвітних та інклюзивних інституцій на всіх рівнях (Ціль 16) [2].

Стан наукової розробки проблеми. Зазначену тему, а також дотичні до неї, досліджували такі українські та зарубіжні вчені як: О. Комарчук, І. Поліщук, С. Ховрич, С. Родіонов, Л. Гервіц, М. Забурмеха, Н. Васильєва, О. Мальцева, О. Матичак, І. Драпп, С. Возняк, А. Іващенко, Л. Голопатюк, Н. Марцінко. Під час роботи над магістерською дисертацією було проаналізовано ряд робіт вітчизняних та іноземних експертів. Зокрема, О. Юдіна та В. Богуша про місце інформаційної безпеки у державі та шляхи її забезпечення, її місце у загальній системі національної безпеки, а також вплив різних дестабілізаційних факторів [3]; Є. Архипової про суспільні трансформації, пов'язані з активним розвитком інформаційно-комунікаційних технологій та глобалізаційними процесами, що вимагають переосмислення уявлень про фактори безпеки та небезпеки у сучасному інформаційному суспільстві, а також забезпечення інформаційної безпеки в органах державної влади як нагальної потреби сьогодення [4]; Бурячок В., Толубко В., Хорошко В., Толюпа С. про головні принципи забезпечення інформаційної безпеки України [5]; Г. Почепцова та С. Чукут про сутність та основні складники сучасної інформаційної політики, побудову інформаційного суспільства [6]; С. Чукут та В. Яценка про комунікаційні стратегії у публічному адмініструванні [7]; Н. Ткачової, О. Іваницької та А. Похожалової щодо встановлення ефективної системи відносин між органами державної влади та суспільством на всіх рівнях влади, орієнтація на ефективний діалог із суспільством, в основі якого лежить принципи відкритості та прозорості [8].

У межах магістерської дисертації також було використано власні напрацьовані матеріали зі здобутого досвіду роботи у Прес-службі Апарату Верховної Ради України. Зокрема, матеріали з проведених для співробітників

тренінгів щодо роботи з інформацією, розпізнаванню фейків і дезінформації, боротьби з ними, основних правил роботи на інформаційних платформах Верховної Ради України у межах виконання завдань, покладених на відділ висвітлення діяльності Верховної Ради України.

Дослідження з питань реалізації інформаційної безпеки у роботі саме Верховної Ради України в умовах війни Росії проти України досі є обмеженими через закритість інформації в умовах дії правового режиму воєнного стану, так і чинності повномасштабної війни, яка досі триває.

Мета і завдання дослідження. Мета дослідження полягає у визначенні напрямів діяльності органів публічної влади у системі забезпечення інформаційної безпеки України, з огляду на теоретичну основу, роль цих органів у забезпеченні інформаційної безпеки та реалізації цих процесів у роботі Прес-служби Верховної Ради України в умовах військової агресії Російської Федерації проти України, надання рекомендацій через проведений аналіз.

Вказана мета досягається шляхом виконання ряду **завдань**, серед яких:

- дослідити теоретичні аспекти терміну «інформаційна безпека»;
- проаналізувати актуальні загрози, виклики та визначити пріоритети у сфері інформаційної безпеки в Україні;
- проаналізувати правову базу, що регулює інформаційну безпеку в Україні;
- розглянути функції та повноваження органів публічної влади, визначити їхню роль і відповідальність у забезпеченні інформаційної безпеки;
- проаналізувати досвід інших країн із розвинутою системою інформаційної безпеки;
- проаналізувати функції та завдання Прес-служби Верховної Ради України у сфері забезпечення інформаційної безпеки в умовах агресії;
- розглянути аспекти створення та оптимізації системи моніторингу та аналізу інформаційної активності у контексті взаємодії Верховної Ради України із засобами масової інформації;

- проаналізувати запроваджені варіанти навчання та підготовки персоналу Прес-служби Верховної Ради України щодо виявлення та протидії дезінформаційним кампаніям, а також надати нові рекомендації із цього питання.

Об'єктом дослідження є система забезпечення інформаційної безпеки України.

Предметом дослідження є функції та завдання органів публічної влади із забезпечення інформаційної безпеки в Україні.

Методологія дослідження. Для досягнення визначених завдань використано комплекс загальнонаукових і спеціальних методів: теоретичне узагальнення, порівняння, аналіз і синтез – для з'ясування теоретичних і методологічних основ діяльності органів публічної влади України у питанні забезпечення інформаційної безпеки в Україні; системний аналіз – для обробки тематичного українського законодавства, документів Організації Північноатлантичного договору, а також інших джерел, що стосуються роботи іноземних парламентів в умовах воєнних конфліктів; аналіз та екстраполяція – для порівняльного аналізу в аспекті інформаційної безпеки та комунікаційних стратегій європейських парламентів, здійсненої Прес-службою Апарату Верховної Ради України роботи із забезпечення інформаційної безпеки; логічне узагальнення – розроблення висновків і рекомендацій щодо забезпечення інформаційної безпеки на прикладі діяльності Прес-служби Апарату Верховної Ради України.

Емпіричною основою дослідження стали міжнародні документи, аналітичні матеріали, численні публікації та статті, внутрішні документи Прес-служби Апарату Верховної Ради України.

Наукова новизна отриманих результатів. У магістерській дисертації проаналізовано поняття «інформаційної безпеки», а також діяльність органів публічної влади в Україні щодо забезпечення інформаційної безпеки. Уперше на прикладі діяльності Прес-служби Апарату Верховної Ради України визначено, як забезпечується інформаційна безпека Парламенту України в умовах повномасштабного вторгнення Російської Федерації. З огляду на проаналізовані

аспекти, проведено аналіз ефективності вжитих заходів і запропоновано конкретні рекомендації щодо їх оптимізації. Враховано специфіку забезпечення інформаційної безпеки в Україні, а також особливості роботи державних органів, що впливає на ефективність заходів держави у цьому напрямі.

Практичне значення роботи полягає у тому, що здійснене дослідження надає конкретні рекомендації щодо підвищення ефективності діяльності органів публічної влади у забезпеченні інформаційної безпеки, що може слугувати основою для вдосконалення національної стратегії у цьому напрямі. Зокрема, результати дослідження можуть бути використані владними органами для покращення роботи у сфері інформаційної безпеки та ухвалення обґрунтованих управлінських рішень. Магістерська дисертація може слугувати основою для подальших наукових досліджень у галузі інформаційної безпеки та вдосконалення заходів захисту від сучасних і майбутніх викликів у роботі органів публічної влади в Україні.

Апробація результатів магістерської дисертації. Теоретичні положення та результати дослідження пройшли апробацію у діяльності Прес-служби Апарату Верховної Ради України. Довідка про впровадження за реєстраційним номером №10/10-2023/272150 затверджує, що результати магістерської дисертації становлять інтерес і можуть бути використані та деякі з них уже використовуються у діяльності підрозділу. Зокрема, авторкою у період із 10 по 14 квітня та з 11 по 15 вересня 2023 року проведено цикл тренінгів для працівників Прес-служби Апарату Верховної Ради України щодо роботи з інформацією, розпізнавання дезінформації та фейків, боротьби з ними, основних правил роботи на інформаційних платформах Верховної Ради України.

Публікації. Основні результати дослідження передано опубліковано у збірнику за матеріалами IV Всеукраїнської студентської наукової конференції «Науковий простір: сучасний стан, тренди та перспективи» (Івано-Франківськ, 15 грудня 2023 року) – Діяльність органів публічної влади у системі інформаційної безпеки україни. Науковий простір: аналіз, сучасний стан, тренди та перспективи : Всеукр. студент. наук. конф., м. Київ, 15 груд. 2023 р. 2023. С.

112–114. URL: https://archive.liga.science/index.php/conference-proceedings/issue/view/ukr-15.12.2023/57.

Загальний обсяг магістерської дисертації. Робота складається зі вступу, трьох розділів, восьми підрозділів, висновків і рекомендацій і списку використаних джерел. Загальний обсяг роботи становить 85 сторінок основного тексту, зокрема, список джерел на 9 сторінках, що містить 61 найменування.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Визначення поняття «інформаційна безпека»

Інформаційна безпека є важливим аспектом забезпечення стабільності, розвитку суспільства та держави. Поєднання стрімкого розвитку інформаційних технологій і зростання загроз для інформаційного простору покладає великі виклики перед поняттям «інформаційна безпека».

Для визначення основних аспектів інформаційної безпеки, насамперед варто визначити, що таке «інформація». Згідно із Законом України «Про інформацію» [9], інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Варто зауважити, що стаття 34 Конституції України стверджує, що кожен має право вільно збирати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір [10].

Водночас, відповідно до статті 20 Закону України «Про інформацію», за порядком доступу інформація поділяється на відкриту та з обмеженим доступом, а будь-яка інформація є відкритою, окрім тієї, що віднесена законом до інформації з обмеженим доступом: конфіденційна, таємна та службова. Якщо аналізувати порядок здійснення та забезпечення права кожного на доступ до інформації, варто зазначити, що публічна інформація, відповідно до Закону України «Про доступ до публічної інформації» [11], є відображеною та задокументованою будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб’єктами владних повноважень своїх обов’язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень. Така інформація є відкритою, крім окремих випадків, встановлених законом, зокрема, якщо розголошення такої інформації може завдати шкоди інтересам національної безпеки, територіальної цілісності або громадського порядку.

Відповідно до Закону України «Про державну таємницю» [12], державною таємницею (секретною інформацією) є вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України. Як стверджують Бем М., Городиський І., Саттон Г. та Родіоненко О. [13], уперше нормативне закріплення норми з правового регулювання захисту персональних даних знайшли закріплення у положеннях міжнародних договорів із прав людини, як складник права на приватність. Так, у статті 17 Міжнародного Пакту про громадянські та політичні права 1966 року закріплено, що ніхто не повинен зазнавати свавільного чи незаконного втручання у його особисте і сімейне життя, свавільних чи незаконних посягань на недоторканність його житла або таємницю його кореспонденції чи незаконних посягань на його честь і репутацію [14]. Також кожна людина має право на захист закону від такого втручання чи таких посягань». Аналогічне за змістом положення включене і до статті 16 Конвенції про права дитини 1989 року [15].

Вони також наголошують, що локомотивом розвитку законодавства у сфері захисту персональних даних є Європейський Союз. Директива 95/46/ЄС Європейського Парламенту та Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року є найбільш сучасним документом, який встановлює детальні вимоги, як має бути організована система захисту персональних даних у державі [16]. Зокрема, Закон України «Про захист персональних даних» базується фактично повністю на положеннях цієї Директиви [17]. Зазначений акт регулює правові відносини щодо захисту та обробки персональних даних, а також спрямований на захист основоположних прав і свобод людини і громадянина, зокрема, про невтручання в особисте життя.

Бем М., Городиський І., Саттон Г. та Родіоненко О. визначають безпеку як «стан, при якому кому-небудь, чому-небудь не загрожує небезпека будь-якого виду», а «національну безпеку» як «категорію політичної науки, яка

характеризує стан соціальних інститутів, що забезпечує їхню ефективну діяльність для підтримки оптимальних умов існування особистості та суспільства». Вони також стверджують, що національна безпека – це стан соціальних інститутів, який забезпечує їхню ефективну діяльність для підтримки оптимальних умов існування особистості, суспільства та держави.

Водночас Закон України «Про національну безпеку України» [18] визначає національну безпеку як захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз. Як зауважують О. Клочко та І. Семенець-Орлова [19], укріплення національної безпеки має відбуватися шляхом гарантування захисту національних інтересів та цінностей та відповідності сучасній геополітичній ситуації. Вони пропонують трактувати сутність поняття «національної безпеки» як «поєднання трьох складових частин безпеки: національні цінності-національні інтереси-національні цілі в єдину функціональну систему».

Відповідно до Стратегії інформаційної безпеки України [20], інформаційна безпека України – це складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об’єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом. Варто зауважити, що таке визначення є більш орієнтованим на стратегічні аспекти інформаційної безпеки, вказуючи на її роль у забезпеченні національної безпеки України, захисті

державного суверенітету, територіальної цілісності та демократичного конституційного ладу.

Для більшої точності, з огляду на сучасний стан загроз, інформаційною безпекою можна назвати відповідну систему тематичних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, захист інформаційно-комунікаційних систем України від незаконного доступу, використання та знищення, зокрема, й в умовах можливих і реальних загроз, до прикладу, в умовах російського повномасштабного неспровокованого вторгнення в Україну. Таке визначення можна вважати більш конкретним, зазначаючи, що надане власне визначення наголошує на захисті інформаційно-комунікаційних систем України від незаконного доступу, використання та знищення, зокрема, в умовах можливих і реальних загроз, таких як російське повномасштабне неспровоковане вторгнення в Україну. Різниця таких підходів до визначення інформаційної безпеки України, відмінного від зазначеного у нормативно-правовому акті, полягає у рівні деталізації та підходах, з огляду на сучасні виклики: перше визначення більше загальне та стратегічне, друге є конкретним та технічним.

Відповідно до статті 17 Конституції України, забезпечення інформаційної безпеки України є однією з найважливіших функцій держави, справою всього Українського народу. На думку Є. Кобко [21], інформаційна безпека є одним із найважливіших складників національної безпеки України. Зокрема, інформаційна безпека посідає особливе місце у системі національної безпеки, тому загрози інформаційного характеру можуть спрямовуватися до будь-яких складників національної безпеки, однак їхній негативний вплив завжди опосередковуватиметься завданням шкоди інформаційній безпеці держави. Також Є. Кобко наголошує, що в умовах розвитку інформаційного суспільства інформаційна безпека виступає як:

- самостійне суспільно-державне явище;

- основа для розвитку політичного, соціального, економічного, культурного складників суспільства;
- політична та економічна стабільність у державі є засобом (ресурсом) розвитку інформаційної системи суспільства, сприяє розвитку виготовлення ефективного інформаційного продукту, який першочергово зможе захистити інтереси власної країни, а також стати цікавим комерційним об'єктом для інших суб'єктів міжнародного права.

Враховуючи той факт, що інформаційна безпека у будь-якій країні має мати заходи щодо її захисту, як і у минулому, теперішньому, так і у майбутньому вимірах, поняття інформаційної безпеки можна також визначити як окремий стратегічний напрям державної політики, який є спрямованим на збереження національних інтересів, на захист усього інформаційного простору від реальних і потенційних зовнішніх та внутрішніх загроз, а також на забезпечення надійності та стійкості інформаційних ресурсів України – як державних установ, так і засобів масової інформації, до прикладу.

Як зауважує О. Степко у статті «Аналіз головних складових інформаційної безпеки держави» [22], на національному рівні інформаційна безпека держави розглядається як система заходів, спрямованих на недопущення несанкціонованого доступу до інформації, її модифікації та порушення цілісності. Вона включає:

- захист політичних, державних і громадських інтересів;
- захист моральних цінностей;
- заборону інформації, яка містить ідеї агресивної війни, насилля, дискримінації та посягання на права людини.

Забезпечення інформаційної безпеки має базуватися на повному спектрі заходів, охоплюючи не лише технічні засоби захисту, але й доволі жорсткі та чіткі організаційні заходи, законодавчі стандарти та інтенсивні освітні програми для осіб, які несуть відповідальність за безпеку інформації в Україні. Надзвичайно важливим є розробка та впровадження передових технологій і

методів виявлення та протидії потенційним атакам у сфері інформаційної безпеки, особливо в умовах гібридної російсько-української війни, коли виникають усе нові та несподівані виклики для забезпечення інформаційної безпеки.

О. Юдін та В. Богуш [23] зауважують, що на початок 21 сторіччя припадає революційна фаза розвитку суспільства, зокрема, на зміну індустріальному суспільству приходить інформаційно-індустріальне суспільство, в якому велике значення набувають системи розповсюдження, зберігання й оброблення інформації. Вони також зазначають, що «іншою стороною цих процесів є збільшення кількості цінної інформації, яка обробляється в автоматизованих системах, від якості, достовірності і оперативності одержання якої залежить більшість важливих рішень, що ухвалюються на різних рівнях — від голови держави до громадянина».

У цьому контексті також влучно зазначила В. Аніщук [24] про те, що нового звучання інформаційна безпека набула через повномасштабне вторгнення Російської Федерації в Україну. Держава-агресор проводить жорстокі підступні військові дії не лише на території нашої держави, але й в інформаційному просторі. Відповідно до Указу Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» [25], було встановлено, що інформаційна політика Російської Федерації – загроза не лише для України, але й для інших демократичних держав.

Як і наголошується у Стратегії інформаційної безпеки, «спеціальні інформаційні операції Російської Федерації спрямовуються на ключові демократичні інституції (зокрема, виборчі), а спеціальні служби держави-агресора намагаються посилити внутрішні протиріччя в Україні та інших демократичних державах». Застосовані Росією технології гібридної війни проти України, зокрема, інформаційне втручання, поширюються на інші держави, швидко адаптуючись до локальних контекстів. Санкції й ефективний механізм моніторингу й відповідальності за порушення є одним із дієвих механізмів

відповіді на дезінформаційну активність Російської Федерації як держави-терориста.

Окрім того, В. Аніщук зазначає, що, попри вищезгадане, в Україні досі триває процес становлення системи стратегічних комунікацій. Органами державної влади України здійснено ряд організаційних та практичних заходів зі зміцнення власної інституційної спроможності у сфері стратегічних комунікацій. Однак варто зазначити, що, станом на зараз, коли вже минуло майже два роки повномасштабного вторгнення Росії в Україну, органам державної влади вдалося вибудувати специфічну систему координації та взаємодії у питанні забезпечення інформаційної безпеки. Це, зокрема, й нові правила роботи для співробітників, відповідальних за захист інформації, й певні фізичні обмежувальні заходи щодо як самого плану роботи, так й умов захисту необхідної інформації. Це було передбачено та досягнуто як тренінгами всередині самих органів, так і більш глобальним аспектом, зокрема, повноцінним курсом України на набуття членства в Європейському Союзі та Організації Північноатлантичного договору, що, зі свого боку, передбачає створення дієвого механізму як усередині кожного органу окремо, так і загальної співпраці з розбудови стратегічного захисту інформаційної безпеки, реалізації у цьому плані державної політики, зокрема, контрпропаганди у відповідь на специфічні та продумані атаки Російської Федерації.

Водночас, на жаль, було утворено такий стан, коли для забезпечення ефективного захисту державного інформаційного простору з метою утвердження позитивного іміджу України та реалізації мети національної безпеки, постраждала сфера розвитку та загалом виконання своїх обов'язків представниками засобами масової інформації: як українськими, так і закордонними. Необхідно наголосити, що, попри дію правового режиму воєнного стану в Україні, в країні не було введено офіційно так званої «воєнної цензури». Натомість було встановлено кримінальну відповідальність за розповсюдження інформації військового характеру. Також було запроваджено певні правила як висвітлення самої війни, так і роботи, до прикладу, прес-служб

державних структур, відповідно до нових викликів. Зокрема, прикладом таких змін є відсутність анонсування заходів із міркувань безпеки або ж більш глобально – обмежена комунікація державних органів із медіа.

Відповідно до опитування, проведеного Фондом «Демократичні ініціативи» імені Ілька Кучеріва [26], більшість журналістів усе ж вважають, що в Україні навіть в умовах воєнного стану зберігається свобода слова. Середня оцінка свободи слова у 2023 році становить 6,4 порівняно з 2019, коли оцінка була 7,6. Водночас 44% респондентів опитування зауважили, що в Україні існують теми, про які не можна писати чи говорити: у 2019 році таких було приблизно чверть. Але водночас абсолютна більшість – 95% опитаних журналістів вважають, що в українських ЗМІ у 2023 році є цензура. З іншого боку, важливим фактором, який не можна оминати, є сама війна. Екс-заступниця Міністра оборони України Ганна Маляр під час Всеукраїнського форуму «Лідерство жінок під час війни» [27] наголосила, що українське суспільство привчилося до певної інформаційної культури, що надало владі змогу уникнути запровадження інформаційної цензури в країні в умовах війни. Також вона зауважила, що в Україні не було запроваджено інформаційну цензуру, що помітили всі партнери України, адже це є унікальним під час повномасштабної війни.

Як стверджують Виздрик В.С. та Мельник О.М. [28], інформаційна безпека є багатогранною сферою діяльності, в якій лише системний, комплексний підхід може спричинити успіх. Вони наголошують, що обсяг проблем, пов’язаних із використанням інформаційних систем, як комунікаційних систем, що забезпечують збирання, пошук, оброблення та пересилання інформації, можна розділити на наступні категорії: забезпечення доступності, цілісності та конфіденційності інформаційних ресурсів і допоміжної інфраструктури. Інформаційна безпека не обмежується захистом від несанкціонованого доступу до інформації, а є принципово широким поняттям. У контексті війни питання щодо необхідності впровадження єдиної інформаційної політики набуває надзвичайної актуальності. 19 березня 2022 року Президент України Володимир

Зеленський підписав Указ №152/2022 [29], який запровадив Рішення Ради національної безпеки і оборони України «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану». Зокрема, документом було встановлено, що в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки, забезпечення якої реалізується шляхом об'єднання усіх загальнонаціональних телеканалів, програмне наповнення яких складається переважно з інформаційних та/або інформаційно-аналітичних передач на єдиній інформаційній платформі стратегічної комунікації – цілодобовому інформаційному марафоні «Єдині новини #UAразом.

Водночас роль організаційного захисту інформації у системі заходів безпеки визначається своєчасністю та правильністю ухвалення управлінських рішень, методами захисту інформації на підставі чинних нормативних документів. Виздрик В.С. та Мельник О.М. також наголошують, що у зв'язку зі зростанням значимості інформаційно-технічного протиборства у військових діях визнається, що перевага поінформованості є основною для перемоги у повітряних, морських і сухопутних боях. З огляду на це, важливими заходами для забезпечення ефективності управління національною інформаційною безпекою є розробка показників ефективності системи захисту інформації, виявлення спалахів нестабільності та загроз, організація наукових досліджень у сфері захисту інформації та розвиток відповідної законодавчої бази.

Зазначається, що забезпечення інформаційної безпеки є критично важливою функцією держави, і для успішної реалізації політики організацій та правових механізмів у сфері інформаційної безпеки необхідно передбачити відповідні державні відомства – головна роль у цьому плані належить державним органам, які, виконуючи покладені на них завдання, забезпечують організаційне, правове, матеріально-технічне та фінансове забезпечення реалізації національної політики інформаційної безпеки. До таких органів, зокрема, належать Рада національної безпеки та оборони України, яка координує та контролює забезпечення інформаційної безпеки як складника національної, Служба безпеки

України, Міністерство внутрішніх справ України, Міністерство оборони України, Державна служба спеціального зв'язку та інформації України.

Як зазначають науковиці Плєхова Г. А. та Костікова М. В. у дослідженні актуальних проблем інформаційної безпеки [30], завдання кожної організації створити таку систему захисту, яка була б стійка до втручання сторонніх осіб. Це передбачає безпеку мереж та всієї інфраструктури, захист програмного забезпечення та баз даних, регулярний аудит інформаційних систем. Органи публічної влади в Україні поділяються на органи державної влади та органи місцевого самоврядування. По суті, це установи й структури, що здійснюють владні повноваження, надані їм законом, із метою вирішення завдань громадського управління, забезпечення законності та реалізації інтересів громадян і держави. Звужуючи специфіку зазначеного до контексту саме інформаційної безпеки, органами публічної влади у сфері інформаційної безпеки є відомства, комітети, служби, відповідальні за розробку та впровадження стратегій, стандартів і заходів щодо захисту інформації на різних рівнях державного управління. Ці органи здійснюють контроль, регулювання та координацію діяльності з інформаційної безпеки. Як наголошують Ілюшик О.М. та Дідик Н.І. [31], держава виступає основним суб'єктом забезпечення права особи на інформаційну безпеку: «Ця обставина зумовлена наявністю в компетенції відповідних прав і повноважень, спеціальних інститутів, органів і служб, що займаються забезпеченням інформаційної безпеки».

Зі свого боку, Стратегія інформаційної безпеки визначає «актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних». Її метою є «посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина».

1.2. Інформаційна безпека в Україні: загрози, виклики та пріоритети

На думку Б. Кормич [32], основні напрями забезпечення інформаційної безпеки України пов'язані з такими суб'єктами, як людина, суспільство та держава. Саме тісний зв'язок і специфіка кожного із цих суб'єктів визначається взаємодією заради суспільного блага між державою і громадянським суспільством із високим рівнем політичних, культурних і моральних рис.

Існують різні класифікації інформаційної безпеки, з огляду на види інформації, суб'єкти та об'єкти, сфери використання та забезпечення безпеки, стандарти та норми, а також загрози та ризики. Зокрема, класифікація інформаційної безпеки опирається як на теоретичне, так і на практичне значення, а розмежування її видів є важливим і необхідним для визначення джерел виникнення інформаційних загроз, для захисту інформаційної безпеки. Тому далі дослідимо деякі з наявних класифікацій. Як зауважує Б. Кормич, класифікувати інформаційну безпеку можна насамперед за її об'єктами та станом їх захищеності:

- людини та громадянина – конституційних прав і свобод;
- суспільства – його духовних, морально-етичних, культурних, історичних, інтелектуальних та матеріальних цінностей, інформаційного та навколишнього середовища;
- держави – її конституційного ладу, суверенітету, територіальної цілісності.

Варто зауважити, що саме така класифікація передбачається і Законом України «Про національну безпеку України», де людину та громадянина, суспільство й державу визначено основними об'єктами національної безпеки.

Б. Кормич також зазначає, що за об'єктною ознакою інформаційна безпека може бути класифікована у такий спосіб:

- інформаційна безпека людини;
- інформаційна безпека юридичних осіб;

- інформаційна безпека суспільства;
- інформаційна безпека держави;
- інформаційна безпека міжнародного співтовариства.

Окрім того, на його думку, інформаційну безпеку можна класифікувати за загрозами, тобто, з огляду на те, що загрози поділяють на зовнішні та внутрішні, так й інформаційну безпеку можна класифікувати як зовнішню та внутрішню.

Як зазначається у статті Ткаченко В. та Паливоди В. «Загрози інформаційній безпеці України як проблематика національної безпеки» [33], загрозами для національної безпеки України в інформаційній сфері є сукупність умов і чинників, котрі становлять небезпеку життєво важливим інтересам держави, суспільства й особи через імовірність негативного інформаційного впливу на свідомість і поведінку громадян, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру. Загрози інформаційній безпеці являють собою сукупність умов та факторів, які створюють небезпеку для життєво важливих інтересів особистості, суспільства та держави в інформаційній сфері. Ткаченко В. та Паливода В. визначають «обмеження свободи слова та доступу громадян до інформації, руйнування системи цінностей, духовного та фізичного здоров'я особи і суспільства, негативні зміни їхніх цільових настанов, маніпулювання громадською думкою з боку державної влади, фінансово-політичних кіл, низький рівень інтегрованості України у світовий інформаційний простір тощо як основні загрози інформаційній безпеці».

Проаналізувавши сучасну юридичну літературу, Паливода В. та Ткаченко В. визначили, що як певною протидією глобальним негативним інформаційним впливам, операціям і війнам, пріоритетними напрямами державної політики мають бути п'ять основних пунктів. Насамперед інтеграція України та її інформаційного простору до світового та регіонального європейського інформаційного простору, створення української національної моделі для забезпечення розвитку інформаційно обізнаного суспільства, а також – «інтеграція у міжнародні інформаційні й інформаційно-телекомунікаційні

системи та організації, упровадження нових і підвищення ефективності вже наявних інформаційно-комунікативних технологій у процеси державного управління та ефективна взаємодія органів державної влади й інститутів громадянського суспільства під час формування, реалізації та коригування державної політики в інформаційній сфері».

Водночас Стратегія інформаційної безпеки, як документ, що передбачає забезпечення інформаційної безпеки України як одну з найважливіших функцій держави, у своїй основі також визначає аналіз загроз та викликів інформаційній безпеці через наявні глобальні виклики та загрози. Одним із таких глобальних викликів, відповідно до Стратегії інформаційної безпеки, є інформаційна політика Російської Федерації, яка є загрозою не лише для України, але й для інших демократичних держав. Зокрема, спрямованість спеціальних інформаційних операцій Російської Федерації на основні демократичні інституції та виборчі процеси. Служби держави-агресора намагаються посилити внутрішні протиріччя в Україні та інших демократичних країнах. Використані технології гібридної війни проти України, включно з моделями та механізмами інформаційного втручання, розповсюджуються на інші держави, швидко адаптуючись до локальних контекстів та регуляторних політик.

Згідно зі Стратегією, запровадження обмежувальних заходів (санкцій) та ефективний механізм моніторингу й відповідальності за порушення становлять дієвий засіб відповіді на дезінформаційну активність Російської Федерації як держави-агресора. Окрім цього, повномасштабне вторгнення Росії в Україну від 24 лютого 2022 року продемонструвало міць держави-терориста та навченість у пропагандистських засобах впливу як на внутрішню, так і зовнішню аудиторії. Як стверджують Ткачова Н., Іваницька О., Похожалова А., аналізуючи стратегії розвитку комунікацій держави та суспільства під час дії правового режиму воєнного стану, інформаційна відкритість органів державної влади дає можливість громадянам отримати адекватне уявлення та сформувати критичне судження про стан суспільства та органи публічної влади, посилює дієвість та ефективність громадського контролю за діяльністю органів державної влади.

Саме тому своєрідна робота з контрпропагандою як від імені держави Україна, так і від медіа, має продовжуватися. Дієвими у цьому плані також є запроваджений ряд санкцій Європарламенту та інших країн світу до російських медійників та медіахолдингів, зокрема, й обмеження їхнього доступу до користування певними світовими відеохостингами.

Окремо у Стратегії також зазначається про інформаційний вплив Російської Федерації як держави-агресора на населення України та інформаційне домінування Російської Федерації як держави-агресора на тимчасово окупованих територіях України. Упродовж тривалого періоду спеціальні служби Російської Федерації активно впроваджують свої спеціальні інформаційні операції, більшість із яких має за мету підрив національної безпеки України, її національних інтересів, знищення української державності та української ідентичності. Ці операції спрямовані на провокування проявів екстремізму, створення панічних настроїв у суспільстві, загострення та дестабілізацію суспільно-політичної та соціально-економічної ситуації в Україні, на додаток до розпочатої у 2022 році повномасштабної агресії.

Як наголошує В. Черниш [34], дослідивши впровадження «розумної сили» проти гібридних загроз, країни зазвичай покладаються на три основні види влади. По-перше, військова сила, різновид «жорсткої сили», спрямовується через залякування, пряме використання чи загрозу застосування сили для досягнення бажаних цілей. По-друге, економічна влада, також «жорстка» влада, проста за своєю суттю, може складатися із заморожування активів, санкцій, надання економічних стимулів, преференцій і підкупу. По-третє, «м'яка» влада – це здатність впливати на дії, поведінку чи ціннісні парадигми інших опосередковано, без застосування примусу чи матеріальних стимулів, завдяки іншим типам мотивації.

Окрім того, як зауважують В. Черниш і П. Махедеван [35], із головних сильних сторін Москви є так зване «стратегічне терпіння», її активні дії – це кінцева стадія більш тривалого процесу, що може розвиватися впродовж років. Зокрема, вони дослідили, що литовська вчена Агрія Грігас поділила зазначений

процес на сім стадій, продемонструвавши, як тверда та м'яка сили можуть поєднуватися для формування «розумної сили»:

- поширення м'якої сили через такі організації, як Фонд «Русский мир»;
- адвокація російських співвітчизників, маргіналізованих у країнах, у яких вони проживають;
- політична мобілізація співвітчизників із метою посилення їхніх зв'язків із «родіной»;
- «паспортизація» співвітчизників, інколи всупереч місцевому законодавству;
- інформаційна війна або пропаганда;
- фізичний захист співвітчизників перед загрозою для них та їхнього майна;
- анексія територій.

Росія, зокрема, із 2014 року й нині продовжує застосовувати все нові прийоми та заходи щодо виправдання анексії Автономної Республіки Крим, заперечення розпочатої війни, а також посилення інформаційних та адвокаційних кампаній щодо зняття санкцій, пов'язаних із порушенням Росією суверенітету й територіальної цілісності України. Окрім того, уже після 24 лютого 2022 року Росія активно продовжує застосовувати ряд інших стратегій та заходів у межах свого повномасштабного вторгнення в Україну. Зокрема, Російська Федерація продовжує використовувати інформаційні канали для розповсюдження пропаганди, дезінформації та маніпуляції з метою впливу на громадську думку, як в Україні, так і світі; ввести наступальні дії та оборонні вже зайнятих нових від 2022 року позицій на Сході та Півдні України. Із метою отримання конфіденційної інформації, а також для впливу на роботу критичної інфраструктури в Україні Російська Федерація продовжує здійснювати кібератаки та ракетні обстріли задля дестабілізації економіки всієї країни.

Окрім того, Росія продовжує активно підтримувати будь-які рухи, зокрема, політичні, спрямовані на дестабілізацію громадських настроїв в Україну, а також підриву довіри громадськості до влади та обраного вектору руху країни. Варто наголосити, що застосування всіх можливих ресурсів Російською Федерацією у цьому процесі, включно з політичними, інформаційними, економічними, розвідувальними й іншими, становить особливо серйозний виклик для України. Зокрема, Російська Федерація досі активно розповсюджує пропаганду у своїй комунікації з країнами Глобального Півдня, спекулюючи питаннями світової продовольчої безпеки, буцімто саме Україна не відкриває зернові коридори, коли насправді всі намагання міжнародної спільноти разом з Україною постійно зриваються саме провокаціями Росії.

Ще одним не менш небезпечним викликом для України нині є ескалація конфлікту між Ізраїлем та Палестиною. Новий спалах цієї довготривалої війни відволікає увагу світу, зокрема, таких найважливіших гравців як Сполучені Штати Америки, від України та продовження надання нам військової, технічної та іншої матеріальної допомоги. Окрім того, цей конфлікт перебиває увагу світової спільноти до подій в Україні, адже багатьом політикам та державним програмам останнім часом притаманна так звана «втома» від російсько-української війни. Ці два фактори можуть негативно вплинути на якість та масштаби допомоги, яка потрібна Україні, захисникам і захисницям, для повноцінного відбиття навали ворога з повернення на кордони 1991 року, включно з Кримом, Донецькою та Луганською областей, а також частинами Харківської, Херсонської областей, які є тимчасово окупованими, унаслідок початку повномасштабного вторгнення Росії 24 лютого 2022 року.

Не менш важливим саме у питанні інформаційної безпеки є постійні кіберзагрози та хакерські напади з боку спеціальних служб Російської Федерації з метою збою роботи державних органів, витоку таємної інформації та розповсюдження пропаганди з фейками. Водночас ці атаки можуть спрямовуватися як на державні інституції, так і на громадський чи бізнес-сектор, включно з важливою критичною інфраструктурою. Саме тому для України нині

є надзвичайно важливим розвитку системи кіберзахисту від усіх імовірних зовнішніх кіберзагроз.

А втім, про загрози інформаційній безпеці варто говорити не лише під час самого воєнного повномасштабного вторгнення Російської Федерації, але й з огляду на тем, яким буде час після закінчення війни та перемоги. На думку політичного консультанта Сергія Бикова у статті для «Інтерфакс Україна» [36], на Україну чекає п’ять основних загроз інформаційній безпеці під час війни. По-перше, це стосується публічного знецінення воїнів. Станом на сьогодні, українська армія має найвищий рівень довіри серед усіх державних інститутів. Згідно з результатами січневого опитування NDI та КМІС, 98% українців вірять Збройним Силам України. Однак після закінчення війни можливо буде спостерігати зниження рівня довіри до захисників і захисниць України, а ветерани цієї війни можуть зустрітися з ворожнечею, якщо держава не забезпечить повагу до наших захисників у суспільстві. Другим фактором політконсультант називає так звану «інформаційну війну всіх проти всіх».

Зокрема, за час повномасштабного вторгнення національні телеканали й платформи соціальних мереж практично зрівнялися за популярністю як основне джерело отримання новин України та світу. У такий спосіб завдяки великому розвитку саме соціальних мереж зросла і кількість фейків та повноцінних дезінформаційних кампаній, так званих інформаційно-психологічних операцій із боку Російської Федерації.

Вельми ризикованими є анонімні платформи з «інсайдами», де перевірка інформації, яка надається, є здебільшого неможливою, і самі канали вкрай важко піддати покаранню за поширення дезінформації. Третім ризиком Сергій Биков називає реінкарнацію російських і проросійських медійників, до прикладу, яких уже було внесено до реєстру зрадників громадським рухом «Чесно», виділивши медійників (блогерів і журналістів) в окрему категорію. Четвертим ризиком, на його думку, є загроза ідентичності. Зокрема, він наголошує, що Стратегія інформаційної безпеки до 2025 року виокремлює утвердження громадянської ідентичності в окрему повноцінну ціль державної політики України. І вже

немало для її досягнення було здійснено, до прикладу, українізація культурного сферу, використання державної мови у сфері обслуговування, а також декомунізація топонімів (прийняття 21 березня 2023 року Верховною Радою України Закону України «Про засудження та заборону пропаганди російської імперської політики в Україні і деколонізацію топонімії» [37]).

Відповідний акт на рівні держави заборонив присвоювати географічним об'єктам назви, що пропагують або символізують Російську Федерацію, а також забороняє присвоювати топонімам назви, що «звеличують, увічнюють, пропагують або символізують державу-окупанта, або її визначні, пам'ятні, історичні та культурні місця, міста, дати, події, її діячів, які здійснювали військову агресію проти України та інших суверенних держав». У пояснювальній записці до законодавчого акту також ідеться про те, що за декомунізацією має бути здійснено деімперіалізацію чи деколонізацію та повне відновлення української історичної та національної топоніміки, спотвореної до невпізнаваності та стертої з мапи колишнім тоталітарним режимом. Насамкінець п'ятою можливою загрозою інформаційній безпеці він називає так звану «модель еталонного українця», тобто «спробу запакувати багатогранне українство у певну коробку з набором певних характеристик». На його думку, відновлення ідеї узагальнення українців за конкретними ознаками, що й робили російські пропагандисти впродовж багатьох років, може загрожувати спробою перенаправити процес будівництва української нації у переважно етнічні рамки із подальшим розділом на правильних та неправильних.

Варто наголосити, що аби такі загрози не справдилися, державі необхідно ретельно вивчати, аналізувати та регулювати ці питання задля забезпечення стабільності та інформаційної безпеки України як під час, так і після повномасштабного вторгнення Російської Федерації в Україну. Це може, зокрема, передбачати запровадження повноцінної політики єдиного голосу, як це було зроблено Урядом Сполученого Королівства Великої Британії та Північної Ірландії під час кризи стратегічних комунікацій усередині країни, зокрема, погодження цього плану з усіма державними структурами з

визначенням відповідальних осіб за контроль за цим процесом. Водночас необхідно й надалі стабільно працювати загалом над стратегічним комунікаціями, до прикладу, як зараз це доволі успішно робиться Міністерством закордонних справ України, яке створює щотижневу довідку зі стратегічними наративами на внутрішню та зовнішню аудиторії.

Тож, пріоритети щодо забезпечення інформаційної безпеки України можуть стосуватися подальшого прийняття відповідних законодавчих актів щодо переходу до хмарних сховищ Європейського Союзу та налагодження спільної програми кібербезпеки, у разі неможливості самостійного відбиття Україною подібних атак. У цьому контексті кібербезпека охоплюється поняттям інформаційної безпеки через тісний зв'язок між двома поняттями. Кібербезпека розглядається у контексті інформаційної безпеки, оскільки інформаційна безпека включає у себе заходи, спрямовані на захист інформації в усіх її формах та на всіх етапах обробки та передачі.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» [38], під кібербезпекою розуміється захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі, а кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем. Окрім того, в Україні функціонування національної системи кібербезпеки забезпечується шляхом вироблення і оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО, а також залучення експертного потенціалу

наукових установ, професійних та громадських об’єднань до підготовки проектів концептуальних документів у сфері кібербезпеки, проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі, функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту.

У сучасному світі значна частина інформації переходить у цифровий формат. Кібербезпека спрямована на захист цієї цифрової інформації від несанкціонованого доступу, модифікації чи знищення. Кібербезпека передбачає заходи для захисту ІТ-інфраструктуру, забезпечення безпеки цих систем є важливим для збереження конфіденційності та цілісності інформації. Тут варто зауважити, що відповідно до Стратегії кібербезпеки України [39], забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Її реалізація здійснюється шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. Зокрема, питома вага кіберзагроз зростає – і ця тенденція в міру розвитку інформаційних технологій та їхньої конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу на функціонування структур управління як національних, так і транснаціональних формує нову безпекову ситуацію.

Водночас не менш важливим є й як постійний розвиток наявних технічних засобів для забезпечення кіберзахисту, так і запровадження нових технік і засобів для інформаційної безпеки України. Загальні пріоритети включають в себе зміцнення законодавства, розвиток технічних та організаційних засобів кіберзахисту, підвищення кібергігієни суспільства та підтримку інновацій у галузі кібербезпеки. Одночасно, необхідно посилити моніторинг, аналіз та реагування на кіберзагрози, щоб забезпечити стійкість інформаційного простору України в умовах сучасних викликів.

1.3. Правова база забезпечення інформаційної безпеки в Україні

Аби докладніше здійснити аналіз поняття «інформаційна безпека» у контексті України, необхідно спочатку звернутися до більш загальних термінів і понять. Зокрема, відповідно до Закону України «Про національну безпеку України», національна безпека – це «захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз».

Водночас варто зазначити, що національними інтересами України є важливі життєві інтереси людини, суспільства й держави, які, якщо реалізовані, забезпечують державний суверенітет України, її прогресивний демократичний розвиток, а також створюють безпечні умови життєдіяльності і добробут її громадян. Насамперед правову основу державної політики у сфері національної безпеки становлять головний закон України – Конституція України. Окрім того, відповідно до Закону України «Про оборону» [40], «оборона України базується на готовності та здатності органів державної влади, усіх складових сектору безпеки і оборони України, органів місцевого самоврядування, єдиної державної системи цивільного захисту, національної економіки до переведення, при необхідності, з мирного на воєнний стан та відсічі збройній агресії, ліквідації збройного конфлікту, а також готовності населення і території держави до оборони».

Із метою запобігання ймовірній збройній агресії та збройним конфліктам, забезпечення національних інтересів та впровадження власної воєнної політики, Україна, керуючись принципами відповідальності та співробітництва, спільної поведінки у галузі безпеки, бере участь у міжнародних системах безпеки й співробітництві у питанні оборони, використовуючи основи, закладені у міжнародних договорах України та, відповідно до законодавства країни. Водночас, як наголошується у Законі України «Про оборону», «при визначенні методів забезпечення власної безпеки під час підготовки держави до оборони та

під час ведення воєнних дій, Україна дотримується принципів та норм міжнародного права, враховуючи законні інтереси безпеки інших країн».

Повертаючись до норм Закону України «Про національну безпеку», варто зазначити, що основними принципами, які визначають порядок формування державної політики у сферах національної безпеки і оборони, є верховенство права, підзвітність, законність, прозорість та дотримання засад демократичного цивільного контролю за функціонуванням сектору безпеки і оборони та застосуванням сили; дотримання норм міжнародного права, участь в інтересах України у міжнародних зусиллях з підтримання миру і безпеки, міждержавних системах та механізмах міжнародної колективної безпеки; розвиток сектору безпеки і оборони як основного інструменту реалізації державної політики у сферах національної безпеки і оборони.

Керівництво у сферах національної безпеки і оборони відповідно до Конституції України здійснює Президент України, який забезпечує державну незалежність та національну безпеку, коли водночас Рада національної безпеки та оборони здійснює у цій сфері повноцінну координацію.

Окремо у питанні забезпечення національної безпеки в Україні у контексті й інформаційного захисту варто виділити Державну службу спеціального зв’язку та захисту інформації України, яка, відповідно до Закону України «Про Державну службу спеціального зв’язку та захисту інформації України» [41], є «державним органом, призначеним для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв’язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв’язку спеціального призначення, урядового фельд’єгерського зв’язку». У такий спосіб можна вже ближче розглядати саме поняття «інформаційної безпеки» в Україні, а також умови, за яких вона має забезпечуватися, та норми закону, які мають це передбачати.

Закон України «Про інформацію» визначає основні принципи та правила збирання, обробки, зберігання, використання та поширення інформації, а також містить окремі положення щодо того, як має відбуватися захист інформації та, зокрема, забезпечуватися інформаційна безпека в Україні. Відповідно, інформація є «будь-якими відомостями та/або даними, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді», а захистом інформації, згідно із Законом України «Про інформацію», є «сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї». Стаття 3 цього ж Закону України затверджує, що одним з основних напрямів державної політики є забезпечення інформаційної безпеки України, окрім інших напрямів:

- забезпечення доступу кожного до інформації, рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; створення умов для формування в Україні інформаційного суспільства;
- забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень; створення інформаційних систем і мереж інформації, розвиток електронного урядування;
- постійне оновлення, збагачення та зберігання національних інформаційних ресурсів.

Зокрема, в умовах загрози інформаційній безпеці України з боку Російської Федерації, варто навести статтю 28 Закону України «Про інформацію», яка передбачає, що інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, скоєння терористичних актів, посягання на права і свободи людини.

Якщо Закон України «Про національну безпеку України» пояснює загальний контекст поняття «інформаційної безпеки» у межах національної безпеки і містить положення щодо захисту інформації від зовнішніх загроз, Закон України «Про основні засади забезпечення кібербезпеки України» встановлює головні принципи й заходи щодо забезпечення кібербезпеки в Україні, включно із захистом інформації від кіберзагроз в інформаційних та телекомунікаційних системах. Правову основу забезпечення кібербезпеки України, як складника загальної системи інформаційної безпеки України, становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

Стратегія інформаційної безпеки передбачає, що інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом.

Відтак, відповідно до статті 3 Закону України «Про оборону», у підготовці держави до оборони як один із пунктів має проводитися інформаційно-

аналітична діяльність в інтересах підготовки держави до оборони, а також забезпечуватися захист інформаційного простору України та її входження у світовий інформаційний простір, створюватися, попри оборонні ризики, розвинута інфраструктура в інформаційній сфері.

Отже, аналізуючи правову базу забезпечення інформаційної безпеки в Україні, можна зробити висновок, що країна розглядає це питання як пріоритетне та визнає важливість ефективного контролю та захисту інформаційних ресурсів. Національне законодавство України визначає ряд головних аспектів інформаційної безпеки: захист від кіберзагроз, протидію дезінформації та регулювання обігу конфіденційної інформації, зокрема, в умовах повномасштабного вторгнення Російської Федерації в Україну. Закони та нормативно-правові акти також передбачають відповідальність за порушення правил інформаційної безпеки. Окрім того, попри досягнуті успіхи, інформаційна безпека є динамічним полем і вимагає постійного оновлення та адаптації. Для ефективної протидії сучасним викликам та загрозам, Україна має продовжувати розширювати та вдосконалювати свою правову базу, враховуючи характер інформаційних загроз, зокрема, з боку Російської Федерації, та міжнародних стандартів.

Висновки до Розділу 1

Проаналізовано сучасний стан інформаційної безпеки в країні. Розділ охопив важливі аспекти, такі як ідентифікація загроз та викликів, які ставлять під загрозу інформаційну безпеку, а також визначено пріоритети для забезпечення ефективного захисту інформації.

Здійснений аналіз підкреслив актуальність проблеми інформаційної безпеки в Україні, зокрема, в умовах сучасних викликів. Зазначено, що інформаційна безпека є критичним елементом національної безпеки та вимагає системного підходу та посилення заходів щодо її забезпечення.

Аналіз правової бази забезпечення інформаційної безпеки в Україні включав вивчення вітчизняного законодавства, спрямованого на регулювання цієї сфери. Зроблено висновок про необхідність постійного вдосконалення нормативно-правового забезпечення, враховуючи швидкі зміни в інформаційно-комунікаційних технологіях та появу нових викликів для безпеки інформації.

Розділ вказує на важливість розробки та впровадження комплексних стратегій інформаційної безпеки, які б враховували специфіку сучасного інформаційного середовища в Україні.

РОЗДІЛ 2

РОЛЬ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ В ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Функції та повноваження органів публічної влади у сфері інформаційної безпеки

Інформаційна безпека відіграє важливу роль у захисті інтересів будь-якої держави світу. Розвинене й захищене інформаційне середовище є необхідною умовою розвитку суспільства й держави. У сучасному світі спостерігається значний ріст процесів управління, спричинений інтенсивним впровадженням новітніх інформаційних технологій. Це спричинює збільшення небезпеки несанкціонованого втручання у роботу інформаційних систем, а наслідки такого втручання стають дуже серйозними.

Країни, які не можуть забезпечити своїм громадянам вільний доступ до різноманітних джерел інформації, а також контроль над непоширенням конфіденційної інформації, зустрічаються з викликами, пов’язаними зі збереженням цілісності суспільства й захистом від негативного впливу інформації. Вирішення цього комплексного питання дозволить не лише захистити інтереси суспільства та держави, але й сприятиме реалізації прав громадян на отримання всебічної якісної інформації. Проблема забезпечення ефективної безпеки інформації у державі передбачає вирішення ряду великих завдань: розробку теоретичних основ, створення відповідальних систем органів, захист інформації, її автоматизація, нормативно-правове регулювання забезпечення безпеки інформації, розробка та виробництво засобів захисту інформації, а також підготовка кваліфікованих фахівців.

Як зауважують Є. Архипова та В. Черниченко [42], інформаційна безпека є одним з основних понять як у науковому дискурсі, так і в державному

управлінні. Саме тому забезпечення належної інформаційної безпеки органів державної влади посідає чільне місце у системі інформаційної безпеки особи, суспільства і держави, а тому й у забезпеченні національної безпеки загалом. На їхню думку, перед Україною стоїть важливе завдання – зайняття міцних позицій в інформаційній сфері. Відповідно, вони також окреслили види інформаційних загроз у державі, з огляду на діяльність органів державної влади:

- небезпеки, що є результатом спланованих та усвідомлених дій державної влади з метою створення авторитарного та іншого режиму;
- загрози, що можуть виникати через діяльність еліти в інтересах лише вузького кола осіб;
- небезпеки, що є наслідком надмірної закритості органів влади від громадськості;
- небезпеки, що є наслідком взаємодії державного апарату з представниками кримінальних кіл.

У цьому аспекті Є. Архипова та В. Черниченко доцільно зазначають, що головним завданням усіх заходів, спрямованих на формування та підтримання на визначеному рівні інформаційної безпеки, є мінімізація загроз через такі фактори, як недостовірність, неповнота та несвоєчасність інформації, її отримання та поширення незаконним шляхом. Вони зауважують, що «комплекс питань інформаційної безпеки держави складається, зокрема, зі сфер діяльності, таких як захист і обмеження обігу інформації, захист інформаційної інфраструктури держави, безпека розвитку інформаційної сфери, захист національного інформаційного ринку, попередження інформаційного тероризму та інформаційної війни».

На думку П. Яковлєва [43], який проаналізував функції державного регулювання у сфері забезпечення інформаційної безпеки в Україні, державне регулювання у сфері інформаційної безпеки складається із таких груп функцій:

- функції організаційного забезпечення;
- функції правового забезпечення;

- функції інформаційного забезпечення;
- функції матеріально-технічного та фінансового забезпечення;
- функції державного контролю;
- функції оперативного реагування на загрози;
- функції оперативного реагування на правопорушення у сфері інформаційної безпеки.

Також він наголошує, що однією із найбільш важливих функцій державного регулювання у сфері забезпечення інформаційної безпеки варто вважати функцію створення умов для формування безпечного інформаційного простору в Україні. Значення цієї функції є вирішальним, оскільки в умовах протидії інформаційній агресії з боку рф ззовні та її прихильників усередині держави, необхідно запропонувати адекватне заміщення інформації на таку, що давала б можливість громадянам України адекватно оцінювати ситуацію в країні та не піддаватися на інформаційні провокації, позбавитися негативного впливу ворожої пропаганди, не допустити використання інформаційного простору держави у деструктивних цілях або для дій, спрямованих на дискредитацію України на міжнародному рівні.

Органи публічної влади в Україні у сфері інформаційної безпеки виконують різноманітні функції та мають різні рівні відповідальності, спрямовані на забезпечення захисту інформаційних ресурсів та запобігання загрозам у цій сфері. Як зауважують Г. Почепцов та С. Чукут, в Україні працює ряд центральних органів державної виконавчої влади, які покликані здійснювати державну інформаційну політику. У забезпеченні права особи на інформаційну безпеку велику роль відіграють повноваження Президента та Ради національної безпеки і оборони України. До повноважень Президента України належать затвердження стратегічних документів щодо сфери забезпечення права особи на інформаційну безпеку, видання указів та розпоряджень у цій сфері. Водночас Президент очолює Раду національної безпеки і оборони України, яка, відповідно до Конституції України та у встановленому Стратегією інформаційної безпеки,

порядку здійснює «координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері, зокрема, з використанням спроможностей Центру протидії дезінформації».

Відповідно до Закону України «Про комітети Верховної Ради України» [44] та Постанови Верховної Ради України «Про перелік, кількісний склад і предмети відання комітетів Верховної Ради України дев'ятого скликання» [45], у Верховній Раді України утворено та діють два комітети, безпосередньо у своїй діяльності пов’язані із забезпеченням інформаційної безпеки України. Це Комітет із питань гуманітарної та інформаційної політики й Комітет з питань свободи слова. До предметів відання Комітету Верховної Ради України з питань гуманітарної та інформаційної політики [46], серед іншого, належить державна політика у сфері інформації та інформаційної безпеки, крім питань, що належать до сфери національної безпеки та оборони. У контексті забезпечення інформаційної безпеки варто зауважити, що комітети, котрі проводять слухання або засідання, мають право ухвалити рішення про проведення їх у закритому режимі, якщо інформація, яка буде використана при проведенні слухань або засідань, містить державну чи іншу охоронювану законом таємницю. Зі свого боку, Комітет зі свободи слова є відповідальним за забезпечення свободи слова, прав громадян на інформацію, за захист прав і свобод працівників засобів масової інформації, а також за гарантії діяльності засобів масової інформації, захист прав журналістів і працівників засобів масової інформації [47].

Як зауважують Г. Почепцов та С. Чукут, у своїй діяльності для підготовки законопроектів Комітет залучає провідних фахівців у сфері інформаційного законодавства, регулярно ініціює та організовує парламентські слухання, присвячені проблемам інформаційних відносин та свободі слова в Україні, реагує на звернення громадян щодо порушення їхніх прав на інформацію та свободу слова.

Відповідно до Закону України «Про Кабінет Міністрів України» [48], повноваження Кабінету Міністрів України у сфері інформаційної безпеки включають розробку програм, виділення фінансових ресурсів, координацію

діяльності органів виконавчої влади та контроль за їх виконанням. Кабінет Міністрів України також забезпечує формування та реалізацію інформаційної політики держави, забезпечує інформаційний суверенітет, фінансування програм, пов'язаних з інформаційною безпекою, спрямовує і координує роботу міністерств, інших органів виконавчої влади у цій сфері. Уряд розробляє та затверджує план заходів з реалізації Стратегії інформаційної безпеки, на основі якого відповідні органи виконавчої влади реалізують заходи щодо забезпечення інформаційної безпеки.

Державний комітет телебачення і радіомовлення України, як центральний орган виконавчої влади зі спеціальним статусом, бере безпосередню участь у формуванні та забезпеченні реалізації державної політики в інформаційній сфері, а також відповідає за сприяння конституційного права на свободу слова, забезпечення розвитку інформаційної сфери, розширення національного інформаційного простору. Відповідно до Положення «Про Державний комітет телебачення та радіомовлення України» [49], орган також забезпечує у межах своїх повноважень реалізацію державної політики стосовно державної таємниці, захисту інформації з обмеженим доступом, а також технічного захисту інформації.

Водночас, відповідно до Закону України «Про медіа» [50], Національна рада з питань телебачення та радіомовлення є органом державного регулювання діяльності у сфері медіа й органом нагляду (контролю) у цій сфері. Зокрема, Національна рада з питань телебачення та радіомовлення, окрім своїх основних завдань щодо захисту прав громадян на свободу думки й слова, на вільне виявлення поглядів і переконань і забезпечення виконання телерадіоорганізаціями вимог чинного законодавства України у сфері телебачення і радіомовлення, реклами, авторського права і суміжних прав та контроль за його додержанням, виконує функцію забезпечення інформаційної безпеки зазначеної діяльності медіа.

Як один з основних суб'єктів кібербезпеки України, Державна служба спеціального зв'язку та захисту інформації відповідальна за кіберзахист

державних інформаційних ресурсів та об'єктів критичної інфраструктури, а також координування діяльності різних суб'єктів, які мають забезпечувати кіберзахист країни. Це, зокрема, стосується безпеки всіх інформаційних систем і контролю захисту інформації в установах та організаціях. Водночас, відповідно до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», «реалізація державної політики щодо захисту критичної технологічної інформації, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснення державного контролю у цих сферах є одним з основних завдань, включно з визначенням вимог до цього захисту», це стосується й упровадження комплексних систем захисту інформації на об'єктах інформаційної діяльності та в інформаційно-комунікаційних системах.

Говорячи про забезпечення захисту інформації, Служба безпеки України, як державний орган спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку України, відповідає за національну безпеку в інформаційній сфері, боротьбу з кіберзлочинністю, а також здійснення контррозвідки. Зокрема, згідно із Законом України «Про Службу безпеку України» [51], орган здійснює заходи контррозвідувального забезпечення дипломатичних представництв, консульських та інших державних установ, а також заходи, пов'язані з охороною державних інтересів у сфері зовнішньополітичної та зовнішньоекономічної діяльності, безпекою громадян України за кордоном. Також Служба безпеки України здійснює заходи, направлені на охорону державної таємниці та контроль за додержанням порядку обліку, зберігання та використання документів, що містять службову інформацію, зібрану під час роботи.

Міністерство цифрової трансформації, як створений у 2019 році центральний орган виконавчої влади, відповідає за формування та реалізацію державної політики у сфері національних електронних інформаційних ресурсів, зокрема, і забезпечує розвиток цифрового суспільства та безпеку цифрового простору. Відповідно до Положення Кабінету Міністрів України «Про Міністерство цифрової трансформації» [52], Міністерство також здійснює

заходи щодо створення та забезпечення функціонування національного реєстру електронних інформаційних ресурсів. До основних завдань також відноситься й розробка пропозицій щодо визначення цілей і завдань державної інформаційної політики.

Окрім того, відповідно до Закону України «Про Національну поліцію» [53], Національна поліція України веде боротьбу з кіберзлочинністю, розслідування кібератак, зокрема, через окремий свій структурний підрозділ, який називається Департамент кіберполіції. Національна поліція України забезпечує захист інформації громадян, співпрацюючи з іншими правоохоронними та владними структурами. Задля комплексного захисту інформації Національна поліція України здійснює розвиток та впровадження систем кіберзахисту для захисту інформаційних ресурсів поліції від кібератак та інших кіберзагроз, із використанням сучасних технологій та програмного забезпечення для захисту інформаційних баз даних і службових систем.

Як зауважує Г. Шорохова [54], у сучасних умовах для оперативного та ефективного забезпечення діяльності поліції України щодо превентивної та профілактичної діяльності, спрямованої на запобігання скоєнню правопорушень; виявленню причин та умов, що сприяють учиненню кримінальних та адміністративних правопорушень, та вжиттю заходів щодо їх усунення; протидії злочинності; розкриттю і розслідуванню злочинів є комплексне застосування оперативно-технічних засобів, інформаційно-пошукових систем, інформаційно-телекомунікаційних засобів та технологій, що потребує запровадження надійної системи інформаційної безпеки.

Водночас, на думку О. Красікова [55], забезпечення інформаційної безпеки правоохоронних органів України здійснюють за двома формами:

- організаційною (організація роботи правоохоронних органів, пов’язаної з обігом, збиранням, обробкою, зберіганням та використанням інформації, взаємодія працівників правоохоронних органів щодо забезпечення інформаційної безпеки);

- правовою (видання наказів та розпоряджень, розроблення положень, інструкцій, складання планів тощо).

Тож, для протидії російській інформаційній війні Україні необхідно й надалі провадити певний ряд заходів для забезпечення інформаційної безпеки та відстоювання своїх інтересів на міжнародній арені. Насамперед це стосується ведення так званої інформаційної контрпропаганди, яка може передбачати запуск інформаційних кампаній, зокрема, саме державними органами України, для протидії російській пропаганді як усередині України, так і на зовнішню аудиторію. Цього можливо досягнути саме завдяки поширенню правдивої інформації з постійним представленням доказів для спростування міфів, створених російськими засобами масової інформації. До цього процесу також необхідно долучати, окрім вітчизняних, і міжнародних експертів для кращого результату.

Подальший захист інформаційної інфраструктури, зміцнення кіберзахисту для запобігання кібератак та захисту важливих інформаційних систем – основа, яка має й надалі бути забезпечена відповідальними органами, із подальшим відповідним розвитком. Зокрема, і через встановлення міжнародних зв’язків для обміну інформацією та підтримки у сфері інформаційної безпеки. Насамкінець кожен орган у системі державної влади зобов’язаний мати власну систему швидкого реагування на випадки дезінформації та поширення фейків: через розробку системи моніторингу для виявлення потенційно дезінформаційних матеріалів і фейків у реальному часі та використання сучасних технологій та аналітичних інструментів для аналізу інформації в Інтернеті, соціальних мережах, засобах масової інформації та інших джерелах. Розробка стандартів та процедур реагування на дезінформацію також має передбачати визначення етапів і термінів реагування на вже виявлені випадки.

2.2. Досвід інших країн у вирішенні проблем інформаційної безпеки та можливість його впровадження в українській практиці

Як зауважує Кушнір В.О. у статті «Аналіз досвіду Сполученого Королівства Великої Британії та Північної Ірландії щодо створення ефективного механізму стратегічних комунікацій як найважливішого елемента системи інформаційної безпеки держави» [56], досвід Великої Британії використовується не лише в рамках реформування вітчизняного оборонного відомства, а й під час реформи системи державних комунікацій всієї країни, яка є необхідною передумовою для успішного проведення реформ та побудови нового типу відносин держави та громадян. Саме тому вивчення унікального досвіду щодо побудови та розвитку стратегічних комунікацій у країнах – членах Північноатлантичного альянсу важливе для України.

У Великій Британії вважають, що стратегічні комунікації мають сприяти просуванню національних інтересів за допомогою використання різних видів оборони для впливу на поведінку цільових аудиторій. Стратегічні комунікації мають важливе значення для розроблення та впровадження національної стратегії, що означає загальний набір ідей, уподобань і методів, які пояснюють різновиди діяльності (дипломатична, економічна і військова) та сприяють досягненню визначеної мети.

У «Практичному посібнику для працівників комунікаційних структур в органах влади», підготовленому в рамках проекту «Будуємо мости заради реформ і довіри», що виконав Інститут масової інформації України за підтримки Уряду Великої Британії [57], наголошується, що у нинішньому середовищі лише функції інформування суспільства недостатньо. Для ефективного діалогу та двостороннього спілкування влади із громадянами посередництвом різних каналів та інструментів необхідне щоденне комунікування, адже інформація – це те, що виходить на широкий загал, а комунікація – те, що доходить до цільових груп.

І саме органи влади мають бути дуже зацікавленими у тому, щоби комунікувати з населенням для формування розуміння у громадян своїх дій і, як наслідок, підтримки таких дій. У 2013 році у Сполученому Королівстві було розпочато реформу урядових комунікацій [58]. Тут варто зауважити, що урядові комунікації в аспекті забезпечення інформаційної безпеки необхідно захищати, адже, станом на сьогодні, вони не є достатньо захищеними, з огляду як на внутрішні процеси роботи з інформацією, так і зовнішні загрози у вигляді кіберзагроз. Саме тому у Великій Британії для аналізу було визначено ряд основних питань, аналіз яких показав, що наявний дуже слабкий зв'язок між стратегічними цілями та комунікативною стратегією, існує слабка координація комунікацій між різними урядовими структурами, а також було знайдено докази неефективної роботи з інформацією.

Для досягнення мети з покращення було запущено політику єдиного голосу, тобто 24 міністерських департаменти, 22 позаміністерських відділи, 349 агенцій, 150 комунікаційних кампаній, п'ять основних напрямів – і на все це було запроваджено один план. Політичні заяви відокремлювалися від урядових комунікацій, зокрема, політичними комунікаціями почали займатися лише політичні радники та партії. Проактивні комунікації домінували, а на критику в Уряді майже не реагували. В усіх нових пунктах плану відбувалися тренінги з працівниками щодо того, як потрібно працювати з інформацією та дезінформацією у державних органах. Зокрема, політика єдиного голосу передбачала ряд правил. Пріоритетні напрями комунікації формуються на основі програми Уряду, єдиний план створює, узгоджує та координує комунікаційний офіс, реалізовують комунікаційний план і кампанії профільні департаменти, оцінку ефективності проводить Рада з оцінювання, до складу якої входять представники влади, медіа-ринку та громадськості, а в кризу комунікації підпорядковуються COBRA, який є комітетом із надзвичайного реагування. У складі цього комітету постійно працює команда з питань державної оцінки ризиків, яка щорічно публікує прогноз ризиків на наступні п'ять років.

Члени цієї команди створюють плани дій на всі можливі кризові ситуації, включно з тими, що пов'язані з інформаційною безпекою. Кризова команда працює цілодобово, формується з волонтерів різних урядових структур, підпорядковується єдиному центру управління. Аналітики кризової команди щоденно готують по дві сторінки, що називаються «відбиток ситуації» з основними цитатами, фактажем, посиланнями та статистикою. Модель парламентської комунікації Сполученого Королівства Великої Британії та Північної Ірландії відрізняється від інших законодавчою та історичною особливістю внаслідок поділу Парламенту на дві палати, що додатково впливає на те, як саме відбуваються комунікації у соціальних мережах. Так, у Twitter та на YouTube, окрім єдиної сторінки Парламенту, є ще й окремі сторінки його палат: основна сторінка публікує контент загального інформативного, культурного, дипломатичного спрямування, у той час як спеціалізовані сторінки ведуть більш докладне інформування про роботу палат, конкретні ухвалені рішення чи проведені засідання.

Варто звернути увагу також і на те, що всі сторінки Парламенту Сполученого Королівства у соцмережах верифіковані, що впливає на рівень довіри користувачів і захист інформації, розміщеної на цій сторінці. Комунікації є централізованими, а при Палаті представників працює окремий структурний підрозділ, що веде всю комунікацію та опікується контактами з пресою та медіа. Не можна оминути факту наявності єдиної комунікаційної стратегії та побудови взаємодії зі стейкхолдерами на основі брендбуку, що був розроблений для комунікацій Парламенту креативною агенцією. При парламенті Сполученого Королівства працює група фахівців – Служба зв'язків зі ЗМІ офісу з комунікацій Палати представників Парламенту. Цей підрозділ відповідає майже за цілодобову комунікацію Парламенту та контакти із пресою та ЗМІ як у будні, так і у вихідні дні.

Стратегічні парламентські комунікації спрямовані на перехід від локальних до глобальних через:

- Регіональну комунікаційну стратегію;

- Міжпарламентську комунікаційну мережу (об’єднання фахівців комунікаційників);
- Створення мережі фахівців із парламентських комунікацій (обмін досвідом та знаннями);
- Парламентські комунікації як об’єкт академічного дослідження.
- Водночас взаємодія із широкою громадськістю відбувається через:
- Роз’яснення функцій Парламенту;
- Підготовку та трансляцію дебатів як механізму сприяння парламенту у виконанні його функцій;
- Допомогу депутатам у взаємодії із громадськістю у ході організації та проведення дебатів;
- Донесення до громадськості важливих питань стосовно рішень та роботи парламенту.

У питанні російської пропаганди, Велика Британія роками перебуває під її постійним тиском: на Уряд і Парламент також покладаються соціальні медіакампанії, які мають розвінчувати фейки та пропаганду. Також варто відзначити наявність виробленого гайдлайну з протидії дезінформації через стратегічні комунікації під назвою RESIST:

- Recognise mis- and disinformation (Розпізнавання дезінформації).
- Early warning (Раннє попередження).
- Situational insight (Ситуаційний аналіз).
- Impact analysis (Аналіз впливу).
- Strategic communication (Стратегічна комунікація).
- Tracking effectiveness (Відслідковування результативності).

Окрім того, Офісом комунікацій у Парламенті Сполученого Королівства називають медійну команду, яка займається, як зазначається на офіційному вебсайті Палати громад, вільним, справедливим і безперешкодним висвітленням політичних і парламентських процесів. Також зауважується, що Палата громад

підтримує роботу всіх засобів масової інформації, а також надає доступ, приміщення та інформацію до парламентської прес-галереї.

Офіс комунікацій відповідає на запити засобів масової інформації, пов'язані з роботою та процедурними питаннями Палати, а також із корпоративними питаннями, що стосуються Палати громад. Окремо команда займається запитами на проведення комерційних зйомок і наглядає за бібліотекою фотографій і відеоматеріалів Палати громад. Відповідно до Першого звіту 2023-2024 «Комунікація: Наскільки ефективно комунікує Палата громад?» [59], до команди Офісу комунікацій Палати громад входять семеро людей, які активно співпрацюють із прес-секретарем Спікера, Прес-службою Палати лордів, медіа-командою спеціального Комітету та Парламентським комісаром із дотримання стандартів. Одним з основних своїх завдань, окрім тісної співпраці з усіма командами комунікаційників у всіх службах Палати громад, визначають керування та координацію діяльності з взаємодії з різними стейкхолдерами на національному та регіональному рівнях у всій Великій Британії.

У своїх комунікаційних правилах Офіс комунікацій визначає ряд аспектів, що ускладнюють їхню роботу у забезпеченні інформаційної діяльності та безпеки, зокрема. Це – витоки інформації, контраверсійні запити та політичний баланс через ширший контент. Для боротьби з основними ускладнювальними факторами Офіс комунікацій Палати громад готує щоденні зведення новин і вечірній брифінг за запитом на рівні топ-менеджменту, працюють у межах міжпарламентської комунікаційної мережі та парламентської комунікаційної мережі Сполученого Королівства Великої Британії, постійно покращують зовнішні зв'язки, а також виставляють певні вимоги до співпраці зі ЗМІ. Окрім того, обидві палати Парламенту Сполученого Королівства мають значний рівень кіберзахисту, співпрацюючи з різними іншими структурами, зокрема, урядовими й приватними. У питаннях моніторингу та проектування можливих інформаційних загроз також використовуються програми на основі роботи

штучного інтелекту, водночас здебільшого для аналізу великого обсягу даних для виявлення та прогнозування загроз і ризиків.

Для України важливо розвивати аналогічні структури для координації та реагування на загрози інформаційній безпеці та, зокрема, кіберзагрози, які є одним з основним складників забезпечення інформаційної безпеки, співпрацюючи з урядовими та приватними секторами. Впровадження сучасних інструментів аналітики та штучного інтелекту для ефективного моніторингу та виявлення загроз у сфері інформаційної безпеки є запорукою так званої гри на випередження.

Основний висновок із досвіду Великої Британії полягає у необхідності комплексного та гнучкого підходу до інформаційної безпеки, який враховує сучасні кіберзагрози, які є швидкозмінними. Україна може взяти за увагу ці практики для вдосконалення власної системи інформаційної безпеки, особливо в умовах війни та гібридних загроз. Окрім того, цікавим і доречним для України досвідом є те, як працює комітет із надзвичайного реагування COBRA (Cabinet Office Briefing Rooms – кімнати для брифінгу Кабінету Міністрів), який використовується для координування дій державних органів у відповідь на національні чи регіональні кризи або під час інших світових подій із серйозними наслідками для Великої Британії. Саме цим Комітетом розробляються плани реагування, включно з інформаційним висвітленням реакцій керівництва країни.

Варто зазначити, що після повномасштабного вторгнення Російської Федерації у складі Апарату Верховної Ради України було створено відділ моніторингу, який якраз і має функції, що передбачають аналіз поточної ситуації та планування, з огляду на різні чинники: політичні, економічні, соціальні й так далі. Впровадження такої команди в усіх державних структурах України виведе на значно вищий рівень як роботу самих структур, так і рівень щоденної та стратегічної комунікацій.

Також для аналізу було обрано систему роботи з інформацією та планування стратегічних комунікацій Організації Північноатлантичного договору.

Як наголошує у своїй статті «Стратегічна комунікація в НАТО: потреба в єдиному підході до політики безпеки» К. Вельяновська [60], із моменту свого заснування Організація Північноатлантичного договору зіштовхнулася з рядом перешкод і вона продовжує зазнавати модифікацій. Стратегічна комунікація Альянсу НАТО є початковою точкою для створення позитивного іміджу організації, сумісного з її внутрішньою організаційною структурою, місією та баченням. Щодо щоденних подій і зміни у концепції політичної безпеки в усьому світі, це важливо для того, щоб НАТО було представлено громадськості як організація високої цілісності, а також як організація з уніфікованою та синхронізованою політикою та робочими завданнями. Створення ефективної та ефективної комунікаційної стратегії вирішальне значення для НАТО. Особливо важливо для Альянсу створити єдиний підхід у комунікації між державами-членами та країнами-партнерами у межах Організації та серед громадськості.

Україна та її відносини з НАТО є лише одним із прикладів підтримки та практичної співпраці з боку НАТО, як через різноманітні програми, так і в межах політичного діалогу. НАТО підтримує різноманітні ініціативи, зокрема у сфері безпеки і процесу реформ. Ці форми підтримки є життєво важливими для демократичного розвитку кожної країни з метою посилення обороноздатності. На що спрямований Альянс, і найкраще може бути проілюстрований поточними інтервенціями на території України, це повна підтримка суверенітету та територіальної цілісності. Водночас варто зауважити, що добре продуманий підхід НАТО до публічної комунікації своїх держав-членів і до зовнішньої комунікації також запобігатиме ряду маніпулятивної та негативної пропаганди про справжнє значення НАТО, особливо у плані спекуляцій щодо намірів організації на європейському континенті, у такий спосіб забезпечуючи інформаційну безпеку НАТО та його держав-членів. Зокрема, що нині й намагається здійснити Російська Федерація, виступаючи проти євроатлантичного шляху України та наполягаючи, що НАТО все більше «розширює зони впливу для тиску на Росію».

Задля стратегічного процесу своїх комунікацій НАТО на постійній основі розвиває довгострокові плани та належний підхід до уваги та зацікавленості держав-членів та тих країн, які не є державами-членами НАТО. Досягнення високого рівня комунікації в Альянсі визначено як важливу засаду подальшого розвитку стійких та ефективних комунікацій як усередині Організації, так і поза її межами. Національні стандарти інформаційної безпеки, визначені НАТО, сприяють взаємодії між органами влади на всіх рівнях, регулюючи обмін інформацією та встановлюючи загальні принципи захисту. Важливим складником цього процесу є систематична комунікація та обмін досвідом між різними рівнями влади, щоб спільно реагувати на виклики й загрози інформаційної безпеки.

Стандарти НАТО також допомагають у створенні єдиної стратегії та виробленні спільного підходу до захисту інформаційної інфраструктури. Взаємодія між різними рівнями влади враховує ці стандарти та сприяє вдосконаленню спільних заходів з підвищення інформаційної безпеки. Окрім того, варто зауважити, що у великій системі НАТО є окремий підрозділ, який відповідає за комунікації та інформування – Агенція зв'язку та інформації. Як зазначається на офіційному вебсайті саме цієї Агенції, команда з трьох тисяч людей допомагає НАТО та її країнам-членам спілкуватися та працювати разом для здійснення основної місії – збереження миру та безпеки для майже одного мільярда громадян. Агенція перебуває на передовій боротьби з кіберзагрозами, захищаючи мережі НАТО 24 години на добу та сім днів на тиждень, аби запобігти всім можливим інформаційним атакам. Зокрема, одним із завдань Агенції зв'язку та інформації є надання послуг, критично важливих для здатності НАТО виконувати свої основні завдання. Фахівці проводять консультації щодо врегулювання криз, працюючи у партнерстві й із некомерційними організаціями також. Серед інших не менш важливих завдань – розробка зовнішніх кампаній терміном на рік і більше, з огляду на потреби, пошук нових способів комунікації із зовнішніми зацікавленими сторонами та внутрішньою аудиторією, включно з країнами, які розглядають можливість подання заявки членство в Організацію

Північноатлантичного договору, а також взаємодія з іншими органами НАТО, зацікавленими сторонами, засобами масової інформації та журналістами.

Станом на сьогодні, перед НАТО все так само стоїть завдання розробляти світові стандарти для протидії будь-яким загрозам у сфері інформаційних технологій, особливо у контексті військової сфери, з урахуванням різноманітних можливих застосувань цих технологій. Так, як зауважують Бігдан М. та Войціховський А. [61], нова Стратегічна концепція оборони та безпеки держав-членів НАТО, що була схвалена главами держав та урядів під час Лісабонського саміту держав-членів НАТО у 2010 році, фактично прирівняла загрози в інформаційному просторі до воєнних загроз, що передбачає можливість застосування у відповідь національні збройні сили. Остаточне визнання Альянсом інформаційного простору як операційної «території» для ведення бойових дій відбулося за результатом саміту держав-членів НАТО, що відбувся у 2016 році у Варшаві Польща. Із метою протидії загрозам в інформаційному просторі у 2011 році у НАТО виникла ідея щодо формування Групи швидкого реагування.

Будь-яка країна-член НАТО, котра була атакована в інформаційному просторі, має право та можливість звернутися по допомогу до Альянсу. Таке звернення розглядається Комісією з управління кіберзахистом. Водночас запити не від держав-членів Організації затверджує Північноатлантична рада Організації. Зі свого боку, НАТО має ряд конкретних вимог до держав-членів щодо інформаційної безпеки та відповідної підтримки користувачів, зокрема у сфері навчання. В основі Північноатлантичного альянсу є ряд спеціалізованих структур: Кооперативний кіберцентр передового досвіду, Школа комунікаційних та інформаційних систем і Центр стратегічних комунікацій. Зазначені структури відповідають за співпрацю та обмін інформацією шляхом навчання та наукових досліджень, здійснюють підготовку щодо роботи комунікаційних та інформаційних систем НАТО, а також забезпечують покращення стратегічних комунікацій і можливостей цієї комунікації, проводять

дослідження щодо пошуку практичних рішень наявних і потенційних проблем, організовують і проводять інформаційні операції Альянсу.

Однією з основних цілей НАТО у плані співробітництва між державами-членами, партнерами та іншими країнами у сфері забезпечення інформаційної безпеки, особливо в умовах порушення Російською Федерацією міжнародного правопорядку через агресивну повномасштабну війну проти України, є:

- забезпечення безпечного функціонування об'єктів критичних інформаційно-комунікаційних інфраструктур;
- розробка ефективних заходів для протидії загрозам в інформаційному просторі;
- надання підтримки державам у відновленні нормального функціонування відповідної інфраструктури, яка постраждала внаслідок зовнішніх атак в інформаційному просторі;
- створення системи оперативного реагування на будь-які загрози в інформаційній сфері держав.

Отже, стандарти НАТО у галузі інформаційної безпеки можуть бути Україні у нагоді як джерело для вдосконалення власної регламентації цієї сфери, зокрема, конкретних напрацювань у вигляді стратегій захисту інформації. Стандарти НАТО можуть допомогти Україні визначити загальні принципи та стратегії інформаційної безпеки, зокрема, розробку політики та стратегій захисту інформації на різних рівнях влади, що є особливо важливим і корисним в умовах повномасштабного вторгнення Російської Федерації в Україну, а також, з огляду на стратегічну мету України вступити в Організацію Північноатлантичного договору як повноцінний і повноправний член. Водночас стандарти НАТО можуть служити як вихідний пункт для визначення технічних і технологічних вимог щодо захисту інформації. Це може забезпечуватися завдяки впровадженню передових технологій і практик щодо кібербезпеки. Оскільки кібербезпека є основною частиною інформаційної безпеки, стандарти НАТО у цій сфері можуть допомогти Україні розробляти та впроваджувати ефективні

заходи щодо захисту від кіберзагроз. У цьому аспекті варто зауважити, що в Україні затвердженими є як Стратегія національної безпеки України, так і Стратегія інформаційної безпеки, яка є більш детальною саме у питаннях забезпечення інформаційної безпеки України. Зокрема, у Стратегії національної безпеки визначено важливість розвиток стратегічних відносин із ключовими іноземними партнерами, насамперед з Європейським Союзом і НАТО та їх державами-членами. Водночас у Стратегії інформаційної безпеки також вказано більш докладно про важливість боротьби з дезінформаційними стереотипами, запущеними Росією, щодо ЄС і НАТО з метою послаблення консолідації суспільства щодо зовнішньополітичного курсу України, гальмування проведення реформ, що негативно впливає на загальну суспільно-політичну ситуацію в державі.

Окрім того, Україна може використовувати стандарти НАТО для розвитку програм тренувань і навчання для персоналу, щоби підвищити кваліфікацію та спроможність у справах інформаційної безпеки. Зокрема, через міжнародну співпрацю Україна має змогу засвоювати стандарти НАТО, що сприятиме зміцненню міжнародної співпраці у галузі інформаційної безпеки, а також взаємодію з іншими країнами-членами НАТО та партнерами для обміну досвідом і вдосконалення своїх заходів з захисту інформації. Стандарти НАТО щодо комунікацій та інформаційної війни також можуть стати корисними для розробки стратегій впливу та взаємодії з громадськістю у контексті інформаційної безпеки. Важливо акцентувати, що адаптація стандартів НАТО вимагає урахування конкретних умов та викликів, із якими зіштовхується Україна, зокрема, умов гібридної війни з Російською Федерацією. Застосування стандартів повинно бути здійсненою з урахуванням національного контексту та потреб.

Отже, взаємодія між різними рівнями органів публічної влади у контексті забезпечення інформаційної безпеки на дотримання стандартів НАТО є надзвичайно важливою у сучасних умовах, коли інформаційні загрози стають усе більш складними та небезпечними, зокрема, в умовах повномасштабного

вторгнення Російської Федерації в Україну. Стандарти інформаційної безпеки НАТО визначають не лише технічні аспекти захисту, а й стратегічні підходи до вирішення сучасних викликів. Укладення відповідних стандартів та їх дотримання на всіх рівнях органів влади є критичним для створення спільного, координованого підходу до інформаційної безпеки. Важливо зазначити, що взаємодія між різними рівнями влади передбачає не лише технічну справність, а й обмін інформацією, координацію стратегій та спільні заходи з навчання та підготовки персоналу. Такий підхід дозволяє ефективно реагувати на загрози й сприяє підвищенню рівня інформаційної безпеки загалом.

Взаємодія органів влади на всіх рівнях за стандартами НАТО стає стратегічним фактором у гармонізації підходів та узгодженій роботі системи захисту інформації. Це віддзеркалює готовність країни протидіяти сучасним викликам у сфері інформаційної безпеки й сприяє збереженню національного суверенітету та стабільності в інформаційному просторі.

Висновки до Розділу 2

Проведено аналіз функцій та повноважень органів публічної влади, які відповідають за забезпечення інформаційної безпеки в Україні. Ефективна система інформаційної безпеки передбачає чітке розподілення функцій та повноважень між різними рівнями влади.

Важливим аспектом дослідження була взаємодія між цими рівнями органів публічної влади для забезпечення єдиної та координованої стратегії інформаційної безпеки.

Проаналізовано стандарти інформаційної безпеки, затверджені НАТО. Було встановлено, що ці стандарти можуть слугувати основою для розвитку та вдосконалення системи інформаційної безпеки в Україні. Важливо враховувати відповідність цих стандартів специфіці українського контексту та потреб.

Аналіз досвіду інших країн, зокрема, Парламенту Сполученого Королівства Великої Британії та Північної Ірландії, акцентував важливість упровадження сучасних підходів та технологій у сфері інформаційної безпеки. Реалізація найкращих практик інших країн може сприяти підвищенню ефективності заходів із забезпечення інформаційної безпеки в Україні.

РОЗДІЛ 3

РЕАЛІЗАЦІЯ ЗАХОДІВ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРЕС-СЛУЖБОЮ АПАРАТУ ВЕРХОВНОЇ РАДИ УКРАЇНИ В УМОВАХ ПОВНОМАСШТАБНОГО ВТОРГНЕННЯ РФ

3.1. Основні функції та завдання Прес-служби Апарату Верховної Ради України в умовах військово-інформаційної агресії Російської Федерації

Комунікації Парламенту України є невід'ємним складником у розбудові демократичної держави на шляху до встановлення миру та стійкого проєвропейського розвитку України та українського суспільства. Розбудова демократичної держави нерозривно пов'язана із горизонтальною та вертикальною комунікацією для супроводу демократичних процесів у державі, комунікації із внутрішніми та зовнішніми цільовими аудиторіями, підтримки та підвищення рівня довіри до Українського Парламенту як надійної державної інституції всередині країни та у міжнародному просторі. Вступ України до Європейського Союзу окреслюватиме процеси вдосконалення політик державних інституцій та, зокрема, у розрізі комунікацій, для збільшення спроможності таких інституцій і відповідності інтеграційному курсу.

У своїй роботі Верховна Рада України має ряд затверджених проектом Комунікаційної стратегії на 2024-2027 роки (попередня Комунікація втратила чинність, нині на фінальному етапі перебуває новий проект) стратегічних принципів і цінностей комунікації Верховної Ради України. Це, зокрема, просвітницька роль комунікацій Українського Парламенту, формування довіри громадян через ресурси Верховної Ради України як через основне джерело достовірної інформації про законотворчий і законодавчий процес в Україні, згуртованість суспільства через інформаційну екосистему платформ Верховної

Ради України, платформа парламентської дипломатії для формування міжнародної підтримки для держави, Парламент як майданчик просування державницької позиції, відстоювання українських національних інтересів, Парламент як відкритий публічний простір в умовах мирного часу та максимальне забезпечення висвітлення діяльності, відповідно до правил і законів, в умовах воєнного стану.

Із початком повномасштабного вторгнення Російської Федерації в Україну 24 лютого 2022 року Апарат Верховної Ради України, зокрема, Прес-служба, як окремий його підрозділ, відповідальний за забезпечення інформаційної діяльності, зміг перейти на військові рейки роботи, забезпечивши безперебійний та постійний законодавчий процес задля життя держави та майбутньої перемоги. Загалом відтоді парламентська комунікація зазнала суттєвих змін через необхідність дотримання заходів безпеки та пов'язаних із цим обмежень. Водночас для забезпечення роботи Верховної Ради України та її Апарату у воєнних умовах було прийнято ряд нормативно-правових актів та розпорядчих документів.

Так, Розпорядженням Голови Верховної Ради України «Про деякі особливості забезпечення діяльності Верховної Ради України в умовах дії воєнного стану в Україні» було врегульовано такі питання, як:

- допуск до адміністративних будинків, споруд і службових приміщень Верховної Ради України;
- охорона та захист народних депутатів України, працівників Апарату Верховної Ради України,
- порядок та місце проведення засідань комітетів Верховної Ради України, тимчасових спеціальних комісій, тимчасових слідчих комісій Верховної Ради України, депутатських фракцій (депутатських груп) у Верховній Раді України;
- порядок опрацювання звернень громадян;
- порядок та місце проведення брифінгів та прес-конференцій тощо.

Іншим розпорядженням Керівника Апарату Верховної Ради України працівникам Апарату, які не мали можливості дістатися до своїх робочих місць, було надано право виконувати завдання за межами адмінбудівель Парламенту, тобто працювати дистанційно. У такий спосіб було значно підвищено, як рівень інформаційної безпеки через можливість працювати, хоч і дистанційно, але на захищених внутрішніх платформах, так й ефективність роботи. Зважаючи на виникнення реальної загрози захоплення службових документів, працівниками режимно-секретного органу був вжитий комплекс заходів із недопущення розголошення відомостей, які б могли створити загрозу життю і здоров'ю керівництва Парламенту, народних депутатів України чи працівників Апарату, яким надано допуск та доступ до державної таємниці, а також розголошення цієї інформації, зокрема, потрапляння до рук ворога.

Із 25 лютого 2022 року, враховуючи розвиток бойових дій на території України, активні бойові дії російських збройних сил та їхніх диверсійно-розвідувальних груп на околицях Києва та безпосередньо в місті, збільшення загрози захоплення державної влади в Україні та, зокрема, Верховної Ради України, роботи з недопущення втрат секретних документів, що могли вплинути на обороноздатність країни, бойові спроможності Збройних Сил України та правоохоронних органів, продовжувалися у посиленому режимі.

Відтак, посилення заходів охорони документів із обмеженим доступом є важливим складником національної безпеки в органах, де працюють із конфіденційними або секретними документами. Саме тому для забезпечення високого рівня безпеки конфіденційних документів і запобігання несанкціонованому доступу до них, збереження їхньої конфіденційності та цілісності, було вжито ряд заходів, зокрема:

- посилений режим роботи з недопущення втрат секретних документів;
- повний захист матеріальних носіїв секретної інформації;

- відбір документів із обмеженим доступом із подальшим їх переміщенням та евакуацією у безпечні місця;
- знищення матеріальних носіїв інформації із обмеженим доступом, що не мають історичної та наукової цінності;
- перевірка всіх режимних приміщень на предмет наявності у них залишків матеріальних носіїв інформації.

Варто зауважити, що із 17 години дев'ять хвилин 23 лютого по 12 годину дня 24 лютого відбулася найпотужніша за всі часи незалежності України кібератака Російської Федерації на веб-ресурси Верховної Ради України. Злочинна спроба агресора заблокувати діяльність Парламенту України провалилася — Апарат відбив ворожі атаки. Відтоді Росія ще не раз намагатиметься зірвати процес роботи Верховної Ради України та її Апарату. 28 лютого 2022 року Апарат Верховної Ради звернувся до Європарламенту із проханням про надання технічної та експертної підтримки у захисті парламентських інформаційних ресурсів і забезпечення безперебійної роботи Парламенту. За лічені дні було отримано позитивну відповідь про готовність такої підтримки.

Окремим здобутком, який допоміг організувати роботу Апарату Верховної Ради України в умовах воєнного стану, стало застосування Єдиної автоматизованої системи документообігу, яку було впроваджено ще на початку пандемії COVID-19, — справжньої цифрової платформи для створення й опрацювання всіх видів документів – проектів законів, висновків і звітів комітетів, порівняльних таблиць до проектів законів. Завдяки цьому Парламент України швидко організував роботу в умовах воєнного стану. Народні депутати України та працівники структурних підрозділів Апарату перейшли на віддалений захищений режим роботи з документами і проектами законів.

Забезпечення безперебійної роботи Верховної Ради України, а також дотримання всіх безпекових заходів стало можливим завдяки значній допомозі Європейського Парламенту. Перший пакет такої матеріально-технічної

допомоги передбачав заходи щодо технічної підтримки захисту парламентських інформаційних ресурсів, другий — удосконалення їхнього захисту. Також було здійснено резервне копіювання у хмарному сховищі на території Євросоюзу, а ще створено гібридну хмару, що передбачає розширення та поєднання наземної інфраструктури за рахунок хмарних ресурсів. Резервне копіювання та створення гібридної хмари забезпечили надійний доступ до документів і проектів законів, а також їх безперебійну міграцію між різними ресурсами. Ці заходи сприяють забезпеченню безпеки та ефективності роботи Верховної Ради України в умовах сучасних викликів.

Нині, завдяки співпраці з міжнародними партнерами, передусім експертами Європарламенту, постійно оновлюється план безперервної роботи ІТ-інфраструктури та її відновлення у критичних ситуаціях. Безперебійна й захищена робота ІТ-сектору Апарату Верховної Ради України забезпечила виконання головної функції Парламенту: вчасно приймати якісні та необхідні закони в умовах війни. Народні депутати України, комітети Верховної Ради України отримали можливість основну роботу з підготовки законопроектів здійснювати дистанційно. Тому вже у сесійній залі парламентарії лише голосували за законодавчі акти. Забезпечення резервних каналів зв’язку — це важливий і необхідний елемент реалізації безпеки у роботі Верховної Ради України та її Апарату в умовах воєнного стану. Належне планування та імплементація резервних засобів допомагають зменшити ризики й зберегти продуктивність та комунікацію навіть в умовах відсутності основного зв'язку.

Зокрема, проведено ряд заходів:

- Резервування основних каналів стаціонарного та мобільного зв’язку.
- Забезпечення альтернативного доступу до мережі Інтернет, завдяки чому забезпечено альтернативний доступ до мережі Інтернет із використанням технології бездротового доступу WiFi в укриттях адміністративних будинків Парламенту та в пункті незламності, який підтримується Апаратом ВРУ — із використанням терміналів супутникового зв’язку.

У такий спосіб було практично забезпечено автономну діяльність Парламенту. Задля реалізації основ інформаційної безпеки у роботі Верховної Ради України та її Апарату було також запроваджено ряд заходів:

- інформаційні обмеження при проведенні пленарних засідань, що передбачають відсутність анонсування та прямої телевізійної трансляції;
- обмеження допуску журналістів, а також часові обмеження щодо публікацій на офіційних сторінках Верховної Ради України у соціальних мережах, на офіційному веб-сайті та у засобах масової інформації.

Із вересня 2022 року розпочав роботу тимчасовий пресцентр, що розташований поза межами постів охорони, встановлених для безпеки та оборони території, що прилягає до центрального адміністративного будинку Верховної Ради України, до завершення дії воєнного стану в Україні. Тимчасовий прес-центр підготовлений для проведення брифінгів, прес-конференцій, записів інтерв'ю та інших заходів народних депутатів України за участю представників медіа.

Окрім того, у перший день повномасштабного вторгнення було створено «комунікаційний штаб», який об'єднав комунікаційні підрозділи Апарату Верховної Ради України (Прес-службу та Інформаційне управління), парламентський телеканал «РАДА», парламентську газету «Голос України», прес-секретарів та помічників керівництва Парламенту, а також представників програми «РАДА: Наступне покоління» ГО «Інтерньюз-Україна». Це було зроблено з метою уніфікації інформаційного висвітлення роботи Парламенту в умовах воєнного стану. У межах роботи Штабу до сьогодні здійснюється координація всіх комунікаційних процесів та розвиток і контентна підтримка офіційних інформаційних ресурсів платформ Верховної Ради України, планування інформаційного висвітлення на коротко- та довгострокові терміни. Робота комунікаційних підрозділів тривала й триває безперервно та щодобово — 24/7.

Варто зазначити, що у жовтні 2022 року відбулося реформування структурних підрозділів Апарату Верховної Ради України, внаслідок чого комунікаційний складник і висвітлення діяльності Парламенту України зосереджені в одному підрозділі – Прес-службі Апарату Верховної Ради України, що передбачено рекомендаціями Місії Європейського Парламенту з оцінки потреб щодо внутрішньої реформи та підвищення інституційної спроможності Верховної Ради України. Нині Прес-служба Апарату Верховної Ради України має два основних напрями роботи: висвітлення діяльності Парламенту України та організаційно-комунікаційна діяльність, яка включає роботу з іноземними гостями та комунікацію з українськими та закордонними засобами масової інформації. Окремою частиною роботи є налагодження зв'язків та співпраці з прес-службами інших країн, зокрема, Європейського Союзу та Сполучених Штатів Америки. Це здійснюється через ознайомчі візити та підтримку комунікаційних зв'язків і надалі.

Зокрема, Прес-служба Апарату Верховної Ради України:

- веде офіційний вебсайт та офіційні сторінки Верховної Ради України у соцмережах, які після початку повномасштабного вторгнення рф стали джерелом оперативних та достовірних новин як для української, так і для міжнародної аудиторії;
- здійснює інформаційний супровід діяльності комітетів Парламенту, керівництва Парламенту й Апарату Верховної Ради України, включно з висвітленням їхніх закордонних візитів та заходів, а також зустрічей та заходів у Парламенті та Україні;
- здійснює інформаційний супровід іноземних делегацій, які відвідують із візитами Парламент, зокрема, супроводжує делегації з пулом журналістів до постраждалих від російського вторгнення міст, містечок та селищ;

- здійснює комунікаційну співпрацю з Європейським Парламентом, зокрема, у квітні 2022 року створено сторінку Верховної Ради України у структурі офіційного веб-сайту Європейського Парламенту;
- завершила комплексну роботу над Комунікаційною стратегією Верховної Ради України на 2023-2027 роки, у межах якої розробила стратегію розвитку соціальних мереж Парламенту, яка у подальшому буде розроблятися на кожні наступні два роки;
- забезпечує інформаційну безпеку певних напрямів висвітлення діяльності Парламенту.

Із 24 лютого 2022 року понад 80 офіційних делегацій здійснили свої робочі та офіційні візити в Український Парламент. Питання фізичної безпеки цих делегацій — питання відповідальності України, що стало серйозним викликом для Парламенту України та Апарату Верховної Ради України. Станом на сьогодні, усі офіційні делегації забезпечуються супроводом спеціальними підрозділами безпеки та окремим транспортом упродовж усього їхнього перебування в країні – від кордону й до кордону. Делегації, що залишаються в країні більш ніж на один день, розміщуються у готелях, що обов'язково мають надійні підземні укриття, де можна безпечно перебувати під час ракетної атаки.

Водночас Верховна Рада України та її Апарат також просять іноземних гостей дотримуватися певної процедури інформаційного висвітлення їх перебування в Україні, щоби зменшити ризики відслідковування їх місцезнаходження агресором. Аби забезпечити захист іноземних гостей в умовах повномасштабної війни Росії проти України, було ухвалено та запроваджено ряд правил:

- супровід спеціальними підрозділами безпеки;
- переміщення спеціальним транспортом;
- розміщення у готелях, що мають надійні підземні укриття;
- спеціальна процедура інформаційного висвітлення візитів.

Однією з найперших іноземних делегацій, що приїхали до Києва у перші місяці війни, була делегація Європейського Парламенту, очолювана його Президенткою Робертою Мецолою. Це сталося на початку квітня 2022 року, коли російські війська лише почали відступ від столиці. Безпрецедентна міжнародна підтримка засвідчена також візитами в перші місяці від початку вторгнення Голови Саейму Латвійської Республіки І. Мурнієце, Спікера Сейму Литовської Республіки В. Чмілітє-Нільсен, Спікера Рійгікогу Естонської Республіки Ю. Ратаса, Голови Сенату Парламенту Чеської Республіки М. Вистрчіла та Маршалка Сенату Республіки Польща Т. Гродзького та багатьма іншими лідерами парламентів та країн.

Такі поїздки сприяли донесенню достовірної та об'єктивної інформації до міжнародних партнерів та переконання їх у необхідності надання Україні допомоги, зокрема, військової, ухвалення відповідних заяв щодо держави-терориста для її відповідальності та отримання справедливого покарання за жорстоку війну.

Варто наголосити, що саме забезпечення інформаційної безпеки у висвітленні діяльності Верховної Ради України з початком повномасштабного вторгнення стало на одне з перших місць у черговості важливості роботи. Якщо раніше це питання стосувалося здебільшого кібербезпекових факторів, то у нинішніх умовах кризова комунікація вийшла на знатно інший рівень – від правил ведення офіційних сторінок у соціальних мережах і конкретних часових рамок висвітлення заходів до напрацювання схеми інформаційної боротьби з російськими наративами, реагування на них і абсолютного іншого формату роботи. Насамперед режим роботи «9 ранку – 18 вечора» змінився на роботу 24/7. У перші місяці повномасштабної війни, а саме із лютого по квітень, Комунікаційний штаб працював цілодобово, маючи ранкові, денні та нічні зміни щодня. Із тим, як минули вже майже два роки повномасштабного вторгнення Росії, сам графік роботи декілька разів змінювався – з огляду на потреби цільової аудиторії, а також аналіз кожної офіційної сторінки Верховної Ради України у

соціальних мережах було вже встановлено окремий постійний графік. А втім, робота щоденна, включно з вихідними, так і залишилася чинною.

Умови правового режиму воєнного стану, зокрема, визначають і певні інформаційні обмеження при проведенні пленарних засідань у будівлі Українського Парламенту. У воєнний час було визначено, що Парламент України працює режимі одного тривалого пленарного засідання під час кожної сесії та інформаційного «режиму тиші». На відміну від мирного часу, засідання не анонсуються, не ведеться пряма телевізійна трансляція пленарних засідань. Під час засідання та півгодини після його закінчення запроваджено режим інформаційної тиші – тобто заборона на будь-які публікації у засобах масової інформації або повідомлення на офіційних сторінках Верховної Ради України у соціальних мережах щодо перебігу засідання. Це дозволяє знизити ризики визначення будівлі Верховної Ради України потенційною ціллю для обстрілів під час перебування у ній великої кількості народних депутатів України та часто й іноземних гостей. Повний відеозапис засідань Парламенту України, брифінгів та коментарів народних депутатів України демонструються в ефірі, зокрема, у «Єдиному телемарафоні» у час, коли засідання Верховної Ради України не проводяться. До повномасштабної війни на третьому поверсі будинку Верховної Ради України було створено Пресцентр, облаштований та обладнаний для роботи ЗМІ та проведення брифінгів. У відповідь на обмеження через пандемію COVID-19 та безпекові фактори унаслідок війни більшість комунікацій перейшла в онлайн, включно з процесом акредитації журналістів, проведення онлайн-трансляцій тощо.

3.2. Організація системи моніторингу та аналізу інформаційної активності взаємодії Верховної Ради України із засобами масової інформації України та світу

Інформаційна активність є основним складником роботи будь-якого парламенту у сучасному світі. Забезпечення ефективної взаємодії із засобами масової інформації вимагає належної системи моніторингу та аналізу, зокрема, чіткого визначення мети та завдань системи моніторингу, що може включати виявлення головних тем, взяття на контроль публікацій, сприяння взаєморозумінню із громадськістю тощо. Водночас обираючи інструменти, важливо враховувати різноманіття засобів масової інформації. Використання моніторингових програм, соціальних мереж та аналітичних інструментів дозволить отримати повний обсяг інформації. Визначення головних показників продуктивності допоможе оцінювати результативність системи моніторингу. Це може бути кількість опублікованих матеріалів, рівень взаємодії із громадськістю, ефективність розповсюдження інформації тощо. Використання аналітичних методів дозволить розкрити глибину інформації. Аналіз настроїв громадськості, виявлення трендів і формування рекомендацій щодо взаємодії може бути реалізовано за допомогою сучасних аналітичних інструментів.

Створення системи звітності та забезпечення зворотного зв’язку є обов’язковим елементом у цьому процесі. Це дозволить регулярно оцінювати результати моніторингу та адаптувати стратегії, відповідно до виявлених вимог. Як варіант, співпраця з експертами з інформаційної безпеки та засобами масової інформації дозволить удосконалити систему моніторингу та надати інсайти щодо сучасних тенденцій та загроз. У цьому процесі важливо дотримуватися принципів конфіденційності при обробці інформації, адже захист особистих даних та надійність системи є пріоритетом.

Динамічність інформаційного простору вимагає постійного вдосконалення системи моніторингу. Реагування на нові технології та тренди є основою успіху

будь-якої організації, зокрема, і державних органів у їхній комунікації та аналізу результатів. Створення ефективної системи моніторингу та аналізу інформаційної активності є критичним завданням для сучасних парламентських органів. Ухвалення чітко визначених ключових показників ефективності має важливе значення для вимірювання успіху діяльності у досягненні поставлених цілей, а також для підвищення прозорості та підзвітності комунікаційних активностей Парламенту. Основні показники ефективності можуть бути кількісними або якісними. Кількісні показники визначають вимірювану інформацію й піддаються математичній перевірці, тоді як якісні показники відображають причини, особисті погляди, ставлення тощо. У гарній системі моніторингу обидва типи індикаторів доповнюють одне одного.

Саме таку систему моніторингу впроваджено у Відділі моніторингу та аналізу Інформаційного управління Апарату Верховної Ради України. Цим відділом для інформування керівництва Парламенту України та народних депутатів України готуються щоденні аналітичні огляди: головні події дня, інформаційні повідомлення, випущені у засобах масової інформації, що стосуються діяльності Верховної Ради України, а також анонсуються події та заходи. За результатами такого моніторингу та аналізу, відбувається оцінка ефективності Комунікаційної стратегії та її коригування. Після проведення моніторингу та збору даних, проводиться аналіз показників та метрик для визначення досягнення стратегічних цілей. Це дозволяє зрозуміти, наскільки ефективною була комунікація та які її складники потребують корекції.

Після аналізу можуть виявитися проблеми, які необхідно вирішити для покращення ефективності стратегії комунікації. Використання результатів моніторингу та аналізу забезпечує гнучкість реалізації Комунікаційної стратегії Верховної Ради України, а також прогнозування тенденцій та ризиків в інформаційному полі, які необхідно враховувати у формуванні інформаційної політики.

Окрім того, Відділ моніторингу та аналізу, відповідно до покладених на нього завдань, забезпечує:

- пошук та систематизацію оприлюдненої про Парламент України інформації;
- аналітичний моніторинг висвітлення діяльності Верховної Ради України та її керівництва у медіа та у соціальних мережах;
- підготовку аналітичних звітів та рекомендацій на основі моніторингових досліджень інформаційного поля Верховної Ради України;
- оперативне інформування про резонансні події в державі й за кордоном;
- оперативний моніторинг інформаційного поля за визначеними темами для протидії можливим загрозам;
- підготовку угод зі спеціалізованими моніторинговими організаціями.

Водночас у межах своїх повноважень Відділ моніторингу та аналізу слідкує за публікаціями в українських і закордонних засобах масової інформації, зокрема, новинами, коментарями та аналізом політичних гасел, а також проводить моніторинг соціальних мереж для виявлення публічного відгуку та настроїв. У такий спосіб Відділ вивчає реакції громадськості на законопроекти та парламентські рішення, аналізуючи настрої та думки громадськості щодо роботи Верховної Ради України. Не менш важливим аспектом роботи Відділу є розробка стратегій реагування на інформаційні кризи та негативні події, а також співпраця з Прес-службою Апарату Верховної Ради України для виведення позитивної інформації.

Отже, запроваджена у 2022 році практика щотижневого моніторингу та фіксації основних показників діяльності Верховної Ради України засвідчила свою ефективність та має продовжувати використовуватись у подальшій роботі. Адже це допомагає своєчасно відстежувати позитивні й негативні тренди та враховувати їх у плануванні подальшої комунікації.

3.3. Навчання та підготовка персоналу Прес-служби Апарату Верховної Ради України щодо протидії дезінформаційним кампаніям

Насамперед варто наголосити, що забезпечення ефективного функціонування Прес-служби Верховної Ради України у сучасних умовах вимагає вдосконалення навичок та знань персоналу з протидії дезінформації. Запровадження систематичного навчання та підготовки є основним аспектом у забезпеченні стійкості до інформаційних загроз та дестабілізації, зокрема, в умовах повномасштабного вторгнення Росії. Команда Прес-служби повинна мати глибоке розуміння можливих джерел дезінформації та методів, які використовуються для створення фейків. Навчання на постійній основі включає аналіз інформаційних впливів, виявлення маніпуляцій та розпізнавання характерних ознак дезінформації. У сучасному цифровому середовищі важливо оволодіти технічними навичками виявлення та аналізу дезінформаційних матеріалів. Курси з кібербезпеки, аналітики соціальних мереж та використання аналітичних інструментів допоможуть підвищити ефективність виявлення та розкриття дезінформаційних кампаній.

Навчання має охоплювати розробку ефективних комунікаційних стратегій для запобігання поширенню дезінформації та відповіді на інформаційні атаки. Персонал має вміло використовувати соціальні мережі, офіційні засоби масової інформації та інші канали для швидкого та точного розповсюдження правдивої інформації. Проведення симуляцій дезінформаційних кампаній та тренування на випадок кризових ситуацій допоможе отримати практичні навички виявлення та реагування на загрози. Регулярні тренінги підвищать готовність до ведення інформаційної боротьби. Залучення експертів у галузі інформаційної безпеки для проведення лекцій та майстер-класів сприятиме обміну досвідом та впровадженню нових методів виявлення дезінформації.

Навчання має включати аспекти психології впливу та реакції на дезінформацію. Персонал повинен бути готовим до роботи у стресових ситуаціях та зберігання професійного спокою у найскладніших обставинах, що особливо стало актуальним із 24 лютого 2022 року, коли спочатку половина команди евакуювалися з Києва, а повернувшись на початку квітня, одразу після звільнення від російських загарбників, фізично до офіса, завжди мати постійну загрозу життю через ракетні обстріли. Окрім того, навчання повинно орієнтуватися на аналіз інформаційного простору як України, так і Верховної Ради України, та вивчення особливостей його функціонування. Розуміння трендів та патернів споживання інформації допоможе виявляти потенційні точки дезінформації.

Зокрема, в уже проведеному ряді навчань визначено, що внутрішня дезінформація – це фейки та неправдива інформація, що поширюється громадянами України, медіа, лідерами думок тощо, свідомо або несвідомо, усвідомлюючи вплив поширення неправдивої інформації на внутрішньополітичну ситуацію або цілком ігноруючи його. До джерел дезінформації відносяться:

- Анонімні Telegram/Viber-канали. Їхня небезпека полягає у тому, що особа або група осіб, що ведуть той чи інший канал, невідома. Достатньо часто адміністратори таких каналів роблять вибір на користь «хайпу» і нехтують фактчекінгом, що призводить до поширення серед підписників неправдивої інформації, а також в самому українському медіаполі, коли, женучись за охопленням та статистикою, інші Telegram-канали та ЗМІ використовують такі новини як джерело.
- Блогери та лідери думок. Унаслідок відсутності культури фактчекінгу та впливу емоційного складника від побачених чи почутих новин із того чи іншого питання, досить часто українські блогери та лідери думок із великим охопленням підписників у соціальних мережах поширюють фейки та недостовірну інформацію.

- Ботоферми. Використання ботоферм для просування фейків отримує успіх у суспільстві з тих питань, щодо яких недостатньо інформування та комунікації з боку Парламенту.

Протидія дезінформації включає, але не обмежується такими заходами:

- заяви парламентарів (в усній або текстовій формі) мають попередньо проходити перевірку на достовірність;
- система інформування у соціальних мережах налаштована для боротьби із поширенням фейків;
- комунікація на випередження з метою забезпечення більшої поінформованості населення;
- механізм розвінчання найпоширеніших міфів та фейків, основних меседжів, що викривлено висвітлюються, шляхом регулярної та постійної комунікації та забезпечення зворотного зв'язку.

Варто зауважити, що фейки та дезінформація є поняттями, які у контексті забезпечення інформаційної безпеки вможуть співвідноситися, але все ж мають певні відмінності. Якщо фейки – це вигадані інформаційні матеріали, створені з метою обману або створення невірного враження, то під дезінформацією треба розуміти передачу невірної чи прихованої інформації з метою введення в оману, впливу на громадську думку чи досягнення певних цілей. Окрім того, дезінформація – це не лише про розповсюдження саме фейків, це може бути цілеспрямоване розповсюдження старих новин, спотворення їхнього контексту або зазначених статистичних даних, а також використання вибіркових фактів. Водночас під міфами варто розуміти вже усталені розуміння певних речей, які можуть включати елементи правдивої історії, але їхні деталі можуть бути прикрашеними або переробленими. Варто наголосити, що міфи можуть бути корисними для пояснення певних аспектів світу, але вони не завжди відповідають фактам і можуть бути використані для формування певного світогляду та нав'язування думки. Тобто і фейки, і міфи, і дезінформація можуть бути елементами пропаганди Російської Федерації, саме тому важливо вміти

розрізняти як різницю між ними, так і розрізняти їх між собою в інформаційному просторі, постійно вивіряючи кожен факт для споживання та сприйняття.

Водночас попередження таких дезінформаційних загроз передбачає організацію фактчекінгових кампаній для працівників-комунікаційників у межах Парламенту, а також засобів масової інформації у формі курсів або інтенсивів під егідою парламенту, сприяння розвитку медіаграмотності та інформаційної гігієни у населення, налагодження системи медіамоніторингу для своєчасного застосування інструменту кризових комунікацій. Джерелами зовнішньої дезінформації визначено пропагандистські російські телеканали та телепрограми, Telegram- та Viber-канали, окремі «лідери думок» та блогери, воєнкори, проросійські медіа та філії російських каналів і медіа за кордоном, YouTube-канали російських та проросійських блогерів, TikTok (як державна замовна пропаганда, так і поширення її окремими громадянами), ботоферми.

Серед факторів протидії Прес-службою Апарату Верховної Ради України визначено розробку та ухвалення стратегії протидії дезінформації в парламентських комунікаціях у відповідності до Стратегії інформаційної безпеки, створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам, зокрема, створення системи протидії дезінформації та інформаційним операціям, спрямованої на запобігання, максимально швидке виявлення та реагування держави і суспільства на інформаційні загрози. Також у межах проведеного навчання започатковано заходи щодо запобігання та протидії поширенню дезінформації та деструктивної пропаганди стосовно європейської та євроатлантичної інтеграції України, посилення відповідальності за поширення недостовірної інформації (дезінформації), запровадження дієвих механізмів виявлення, фіксації, обмеження доступу та/або видалення з українського сегмента мережі Інтернет інформації, розміщення якої обмежено або заборонено законом.

Важливу роль у цьому має ефективна взаємодія державних органів, органів місцевого самоврядування та інститутів громадянського суспільства у формуванні та реалізації державної політики в інформаційній сфері. Ефективне

навчання та підготовка персоналу Прес-служби Верховної Ради України щодо виявлення та протидії дезінформаційним кампаніям має стати постійним процесом. Регулярне оновлення курсів, адаптація до нових викликів і забезпечення відкритого обміну досвідом є ключовими складовими успіху у цій стратегічно важливій галузі.

Отже, підготовка персоналу Прес-служби Верховної Ради України щодо виявлення та протидії дезінформаційним кампаніям, спрямованим на дестабілізацію роботи, вимагає комплексного та системного підходу. Оптимальна стратегія передбачає об'єднання теоретичних знань та практичних навичок у сфері інформаційної безпеки та медіа-аналізу. Співробітники повинні мати глибоке розуміння сучасних інформаційних викликів та загроз, пов'язаних із дезінформацією, зокрема, постійно засвоювати концепції інформаційної безпеки, основ та стратегій протидії дезінформації, здобувати навички моніторингу соціальних мереж, аналізу засобів масової інформації та реакції громадськості, володіти інструментами медіа-аналізу та вміти виявляти фейки.

Розробка й удосконалення стратегій виявлення та реагування на дезінформаційні кампанії, а також встановлення ефективної системи попередження та відповіді на інформаційні кризи – основа ефективної роботи Відділу моніторингу та аналізу Апарату Верховної Ради України. Загальна мета роботи такого підрозділу у межах створення високопрофесійної, гнучкої та відкритої до інновацій команди, яка ефективно бореться з викликами інформаційної безпеки, забезпечить стабільну та об'єктивну роботу Прес-служби Верховної Ради України в умовах сучасного інформаційного простору. Гармонійне функціонування системи інформаційної безпеки відділу Прес-служби Верховної Ради України передбачає комплексні заходи та високий ступінь готовності до реагування на сучасні виклики та загрози інформаційного середовища. Зокрема, це стосується захисту інформаційних ресурсів, інформаційної гігієни, моніторингу та аналізу засобів масової інформації, активної взаємодії, стійкої системи комунікацій, ефективної реакції на кризи, гнучкості та пристосовуваності.

Висновки до Розділу 3

Прес-служба Апарату Верховної Ради України грає важливу роль у забезпеченні інформаційної безпеки в умовах агресії Росії, виконуючи завдання з ретельного моніторингу інформаційного простору та вчасної реакції на загрози, окрім свого основного завдання з висвітлення діяльності та взаємодії з медіа.

Визначено необхідність удосконалення наявної системи моніторингу та аналізу для вчасного виявлення та реагування на інформаційні загрози. Запропоновані конкретні кроки щодо оптимізації процесів та вдосконалення інструментів аналізу.

Проаналізовано вже наявні варіанти навчання та підготовки персоналу Прес-служби. Запропоновано нові рекомендації для покращення програм навчання з урахуванням останніх трендів у сфері дезінформації.

У Розділі 3 вказано на важливість дієвого функціонування Прес-служби Верховної Ради України у контексті забезпечення інформаційної безпеки.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

Перед виконанням кваліфікаційної роботи на тему «Діяльність органів публічної влади у системі інформаційної безпеки України» було визначено ряд завдань, які, за результатами, було досягнуто.

Метою дослідження було визначення напрямів діяльності органів публічної влади у системі забезпечення інформаційної безпеки України, з огляду на теоретичну основу, роль цих органів у забезпеченні інформаційної безпеки та реалізації цих процесів у роботі Прес-служби Верховної Ради України в умовах військової агресії Російської Федерації проти України, надання рекомендацій через проведений аналіз.

Вказаної мети шляхом було досягнуто шляхом виконання ряду завдань, серед яких:

- досліджено теоретичні аспекти терміну «інформаційна безпека»;
- проаналізовано актуальні загрози, виклики та визначено пріоритети у сфері інформаційної безпеки в Україні;
- проаналізовано правову базу, що регулює інформаційну безпеку в Україні;
- розглянуто функції та повноваження органів публічної влади, визначено їхню роль і відповідальність у забезпеченні інформаційної безпеки;
- проаналізовано досвід інших країн та організацій із розвинутою системою інформаційної безпеки;
- проаналізовано функції та завдання Прес-служби Верховної Ради України у сфері забезпечення інформаційної безпеки в умовах агресії Росії;
- розглянуто аспекти створення та оптимізації системи моніторингу та аналізу інформаційної активності у контексті взаємодії Верховної Ради України із засобами масової інформації;
- проаналізовано запроваджені варіанти навчання та підготовки персоналу Прес-служби Верховної Ради України щодо виявлення та протидії

дезінформаційним кампаніям, а також надано нові рекомендації із цього питання.

Отримані у ході дослідження результати підтверджують досягнення поставленої мети й вирішення завдань, дають підстави сформулювати певні практичні рекомендації, спрямовані на зміцнення аспектів забезпечення інформаційної безпеки України та покращення ефективності діяльності відповідних публічних органів влади в Україні. Зокрема, Прес-служби Апарату Верховної Ради України, аналіз якої також був здійснений. Насамперед рекомендується продовження вдосконалення законодавства щодо сфери забезпечення інформаційної безпеки, зокрема, з огляду на сучасні виклики та міжнародний досвід через співпрацю з партнерами України – Європейським Союзом, Організацією Північноатлантичного договору, іншими парламентами європейських країн. Для того, аби цей досвід переймався повноцінно, необхідно зміцнити координацію між необхідними органами публічної влади в Україні для ефективного вирішення питань інформаційної безпеки. Це може забезпечуватися через створення координаційних груп між установами.

На прикладі роботи Прес-служби Апарату Верховної Ради України було проаналізовано чинний стан протидії фейкам, дезінформації та пропаганді, зокрема, Російської Федерації. Ця робота має посилено продовжуватися з подальшим удосконаленням як під час самої війни, так і після перемоги України. Для цього органи публічної влади в Україні мають бути забезпечені відповідними необхідними ресурсами на підтримку виконання поставлених завдань в умовах інформаційної агресії, зокрема, має бути забезпечений захист від кібератак із боку ворога. Також важливо постійно оновлювати програми навчання та підготовки тренінгів для працівників усіх органів та відділів усередині їхньої структури, з огляду на появу сучасніших методів боротьби з дезінформацією.

Щоби забезпечити досягнення визначених рекомендацій, необхідно залучати експертів для проведення аналізу поточного стану, а також розробки стратегічних комунікацій як кожного органу окремо, так і всієї можливої

системи разом. Адже розробка єдиного стратегічного плану дій чітко б визначала межі відповідальності, завдання та правила такої взаємодії, що мало б підтверджуватися відповідним законодавчим актом або ж змінами до профільних чинних.

Упровадження сучасних інформаційних технологій та аналітичних інструментів для ефективного моніторингу інформаційної активності, а також співпраця з науковими установами та ІТ-компаніями для розробки інноваційних рішень сприяла б якісній роботі відділів моніторингу та аналізу у державних органах України. Насамкінець варто наголосити, що повноцінний вступ України до Європейського Союзу та НАТО й перехід від країни-кандидати на вступ і статусу партнера з розширеними можливостями значно покращить рівень забезпечення інформаційної безпеки України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ліпкан В., Максименко Ю., Желіховський В. Інформаційна безпека України в умовах євроінтеграції : Навч. посіб. Київ : КИЇВ. НАЦ. УН-Т ВНУТР. СПРАВ, 2006. 280 с. URL: https://moodle.znu.edu.ua/pluginfile.php/470939/mod_resource/content/1/%D0%86%D0%9D%D0%A4%D0%9E%D0%A0%D0%9C%D0%90%D0%A6%D0%86%D0%99%D0%9D%D0%90%20%D0%91%D0%95%D0%97%D0%9F%D0%95%D0%9A%D0%90%20%D0%A3%D0%9A%D0%A0%D0%90%D0%87%D0%9D%D0%98%20%D0%92%20%D0%A3%D0%9C%D0%9E%D0%92%D0%90%D0%A5%20%D0%84%D0%92%D0%A0%D0%9E%D0%86%D0%9D%D0%A2%D0%95%D0%93%D0%A0%D0%90%D0%A6%D0%86%D0%87.pdf (дата звернення: 01.12.2023).

2. Цілі сталого розвитку. *Дія.Бізнес - Головна сторінка*. URL: https://business.diia.gov.ua/handbook/sustainable-development-goals/cili-stalogo-rozvitku (дата звернення: 01.12.2023).

3. Юдін О., Богуш В. Інформаційна безпека держави : Підручник. Київ : МК-Пресс, 2005. 432 с. URL: http://icit.nau.edu.ua/index.php?option=com_content&view=article&id=106 (дата звернення: 01.12.2023).

4. Архипова Є. Синергетичний вектор дослідження безпеки в сучасному суспільстві. *Філософські науки*. 2014. Т. 1 (40). URL: http://journal-phipsyped.kpi.ua/issue/view/1849 (дата звернення: 01.12.2023).

5. Інформаційна та кібербезпека: соціотехнічний аспект : Підручник / В. Бурячок та ін. Київ : МОН УКРАЇНИ Держ. ун-т телекомунікацій, 2015. 288 с. URL: https://duikt.edu.ua/uploads/p_303_79299367.pdf?file=p_303_79299367.pdf (дата звернення: 01.12.2023).

6. Почепцов Г., Чукут С. Інформаційна політика : навч. посіб. 2-ге вид. Київ : Знання, 2008. 663 с. URL: https://westudents.com.ua/knigi/365-nformatsyna-poltika-pocheptsov-gg.html (дата звернення: 01.12.2023).

7. Чукут С., Яценко В. Комунікаційні стратегії в публічному управлінні та адмініструванні: зарубіжний та український досвід. *Інвестиції: практика та досвід*. 2021. № 12. С. 8. URL: http://www.investplan.com.ua/pdf/12_2021/14.pdf (дата звернення: 01.12.2023).

8. Ткачова Н., Іваницька О., Похожалова А. Стратегія розвитку комунікацій держави та суспільства під час дії правового режиму воєнного стану. *Дніпровський науковий часопис публічного управління, психології, права*. 2022. № 5. С. 5. URL: https://scholar.google.com.ua/citations?hl=ru&user=V0tbigwAAAAJ&view_op=list_works&sortby=pubdate (дата звернення: 01.12.2023).

9. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII : станом на 27 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 01.12.2023).

10. Конституція України : від 28.06.1996 р. № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 01.12.2023).

11. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI : станом на 8 жовт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 01.12.2023).

12. Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 01.12.2023).

13. Захист персональних даних: правове регулювання та практичні аспекти : Науково-практ. посіб. Страсбург : Рада Європи, 2015. 220 с. URL: https://rm.coe.int/168059920c (дата звернення: 01.12.2023).

14. Міжнародний пакт про громадянські і політичні права : Пакт Орг. Об'єдн. Націй від 16.12.1966 р. : станом на 19 жовт. 1973 р. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (дата звернення: 01.12.2023).

15. Конвенція про права дитини : Конвенція Орг. Об'єдн. Націй від 20.11.1989 р. : станом на 16 листоп. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/995_021#Text (дата звернення: 01.12.2023).

16. Директива 95/46/ЄС Європейського Парламенту і Ради "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних" : Директива Європ. Союзу від 24.10.1995 р. № 95/46/ЄС : станом на 25 трав. 2018 р. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text (дата звернення: 01.12.2023).

17. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 01.12.2023).

18. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 01.12.2023).

19. Клочко О., Семенець-Орлова І. Національна безпека: український вимір. *Наукові праці Міжрегіональної академії управління персоналом. Політичні науки та публічне управління*. № 2. С. 10. URL: http://journals.maup.com.ua/index.php/political/article/view/2138/2636 (дата звернення: 01.12.2023).

20. Про Стратегію інформаційної безпеки : Рішення Ради нац. безпеки і оборони України від 15.10.2021 р. : станом на 30 груд. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/n0080525-21#Text (дата звернення: 01.12.2023).

21. Кобко Є. Інформаційна безпека в системі національної безпеки: сучасність і перспективи. • *National law journal: teory and practice*. 2019. С. 5. URL: http://www.jurnaluljuridic.in.ua/archive/2019/2/part_2/11.pdf (дата звернення: 01.12.2023).

22. Степко О. Аналіз головних складових інформаційної безпеки держави. *Інститут міжнародних відносин Національного авіаційного університету*. 2013. Т. 1, № 3. С. 10. URL:

https://jrnl.nau.edu.ua/index.php/IMV/article/view/3214/3172 (дата звернення: 01.12.2023).

23. Юдін О., Богуш В. Інформаційна безпека держави : навч. посіб. Харків : Консум. 576 с. URL: https://studfile.net/preview/5376129/ (дата звернення: 01.12.2023).

24. Аніщук В. Інформаційна безпека як об’єкт посягання злочинів проти основ національної безпеки України. Науковий вісник Ужгородського національного університету. 2023. URL: http://visnykpravo.uzhnu.edu.ua/article/view/284126/278265 (дата звернення: 30.11.2023).

25. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки" : Указ Президента України від 28.12.2021 р. № 685. URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 01.12.2023).

26. Ukrinform. Абсолютна більшість журналістів вважають, що в українських ЗМІ є цензура. Укрінформ - актуальні новини України та світу. URL: https://www.ukrinform.ua/amp/rubric-society/3704250-absolutna-bilsist-zurnalistiv-vvazaut-so-v-ukrainskih-zmi-e-cenzura.html (дата звернення: 30.11.2023).

27. Цензура під час війни: в Міноборони розповіли, як вдалося уникнути жорстких заходів. Новини України - останні новини України сьогодні - УНІАН. URL: https://www.unian.ua/politics/cenzura-v-ukrajini-pid-chas-viyni-stalo-vidomo-chomu-jiji-ne-zaprovadili-novini-ukrajina-amp-12317118.html (дата звернення: 01.12.2023).

28. Інформаційна безпека в україні: сучасний стан. International scientific journal «Grail of Science». 2023. URL: https://doi.org/file:///C:/Users/ladmin/Downloads/34.pdf (дата звернення: 01.12.2023)

29. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року "Щодо реалізації єдиної інформаційної політики в умовах

воєнного стану" : Указ Президента України від 19.03.2022 р. URL: https://www.president.gov.ua/documents/1522022-41761 (дата звернення: 30.11.2023).

30. Плєхова Г., Костікова М. Актуальні проблеми інформаційної безпеки. Матеріали Всеукраїнської науково-практичної Internet-конференції «Моделювання та інформаційні технології в науці, техніці, кібербезпеці та освіті». URL: https://rcf.khadi.kharkov.ua/fileadmin/F-HIGHWAY/Інформатики_і_прикладної_математики/Матеріали_Всеукр.конф._2022_-1-ред.pdf#page=68 (дата звернення: 30.11.2023).

31. Ілюшик О., Дідик Н. Діяльність державних органів щодо забезпечення права особи на інформаційну безпеку. Львівський державний університет внутрішніх справ. 2021. URL: http://www.lsej.org.ua/12_2021/62.pdf.

32. Кормич Б. Інформаційна безпека: організаційно-правові основи : навч. посіб. Київ : Кондор, 2004. 384 с. URL: https://lib.univer.km.ua/sites/default/files/Право/Кормич%20Б%20А%20Інформаційна%20безпека%20організаційно%20правові%20основи.pdf (дата звернення: 01.12.2023).

33. Ткаченко В., Паливода В. Загрози інформаційній безпеці україни як проблематика національної безпеки. Сумський національний аграрний університет. 2022. URL: http://lsej.org.ua/10_2022/123.pdf.

34. Chernysh V. Smart power vs hybrid threats. *Georgia Today on the Web*. URL: http://gtarchive.georgiatoday.ge/news/8381/Smart-Power-vs-Hybrid-Threats (date of access: 01.12.2023).

35. Черниш В., Махедеван П. Інформаційний вимір гібридної війни. *Вісник НТУУ "КПІ"*. 2017. № 1,2. С. 13. URL: https://ela.kpi.ua/bitstream/123456789/25045/1/VPSP2017-1-2_9-21.pdf (дата звернення: 01.12.2023).

36. Interfax-Ukraine. П’ять загроз інформаційній безпеці України після війни. Інтерфакс-Україна. URL: https://interfax.com.ua/news/blog/897645.html (дата звернення: 01.12.2023).

37. Про засудження та заборону пропаганди російської імперської політики в Україні і деколонізацію топонімії : Закон України від 21.03.2023 р. № 3005-IX : станом на 26 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/3005-20#Text (дата звернення: 02.12.2023).

38. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 17 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 04.12.2023).

39. Про Стратегію кібербезпеки України : Рішення Ради нац. безпеки і оборони України від 27.01.2016 р. : станом на 18 берез. 2016 р. URL: https://zakon.rada.gov.ua/laws/show/n0003525-16#Text (дата звернення: 03.12.2023).

40. Про оборону України : Закон України від 06.12.1991 р. № 1932-XII : станом на 15 квіт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (дата звернення: 05.12.2023).

41. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 р. № 3475-IV : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 01.12.2023).

42. Архипова Є., Черниченко В. Забезпечення інформаційної безпеки в органах державної влади як нагальна потреба сьогодення. *Державне управління у сфері державної безпеки та охорони громадського порядку*. 2018. № 4. С. 4. URL: https://ela.kpi.ua/bitstream/123456789/30267/3/2018_IB-v-orhanah-derzh-vlady.pdf (дата звернення: 03.12.2023).

43. Яковлєв П. О. Функції державного регулювання у сфері житлово-комунальних послуг / П. О. Яковлєв // Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція. - 2015. - Вип. 13(1)

44. Про комітети Верховної Ради України : Закон України від 04.04.1995 р. № 19. URL: https://zakon.rada.gov.ua/laws/show/116/95-%E2%F0#Text (дата звернення: 01.12.2023).

45. Про перелік, кількісний склад і предмети відання комітетів Верховної Ради України дев'ятого скликання : Постанова Верхов. Ради України від 18.12.2020 р. № 19-IX : станом на 23 лют. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/19-IX#Text (дата звернення: 03.12.2023).

46. Офіційний вебсайт. *Комітет з питань гуманітарної та інформаційної політики*. URL: https://kompkd.rada.gov.ua/uploads/documents/32652.pdf (дата звернення: 03.12.2023).

47. Офіційний вебсайт. *Комітет Верховної Ради України з питань свободи слова*. URL: https://komsvobslova.rada.gov.ua/news/pro_Comitet/zagalna/72635.html (дата звернення: 03.12.2023).

48. Про Кабінет Міністрів України : Закон України від 27.02.2014 р. № 794-VII : станом на 3 серп. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/794-18#Text (дата звернення: 03.12.2023).

49. Про Державний комітет телебачення та радіомовлення України : Постанова Каб. Міністрів України від 29.03.2017 р. № 341 : станом на 7 лют. 2023 р. URL: https://comin.gov.ua/pro-nas/polozhennya-pro-derzhkomteleradio/polozhennia-pro-derzhavnyi-komitet-telebachennia-i-radiomovlennia-ukrainy (дата звернення: 03.12.2023).

50. Про медіа : Закон України від 13.12.2022 р. № 2849-IX : станом на 2 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text (дата звернення: 03.12.2023).

51. Про Службу безпеки України : Закон України від 25.03.1992 р. № 2229-XII : станом на 2 серп. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text (дата звернення: 01.12.2023).

52. Питання Міністерства цифрової трансформації : Постанова Каб. Міністрів України від 18.09.2019 р. № 856 : станом на 15 листоп. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/856-2019-п#Text (дата звернення: 01.12.2023).

53. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII : станом на 5 жовт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 03.12.2023).

54. Шорохова Г. Деякі питання інформаційної безпеки діяльності територіальних органів поліції україни. *Актуальні проблеми державного будівництва та місцевого самоврядування, адміністративне та фінансове право, адміністративний процес, інформаційне право*. URL: https://univd.edu.ua/science-issue/issue/4059 (дата звернення: 03.12.2023).

55. Красіков Д. О. Правове забезпечення інформаційної безпеки в діяльності органів внутрішніх справ України: автореф. дис. ... канд. юрид. наук: 12.00.07 / Д. О. Красіков. – К., 2012).

56. Кушнір В. Аналіз досвіду Сполученого Королівства Великої Британії та Північної Ірландії щодо створення ефективного механізму стратегічних комунікацій як найважливішого елемента системи інформаційної безпеки держави. Національний університет оборони України імені Івана Черняховського. 2020. URL: http://pag-journal.iei.od.ua/archives/2020/19-2020/10.pdf.

57. Казанжи З. Практичний посібник для працівників комунікаційних структур в органах влади : навч. посіб. Київ, 2016. 112 с. URL: https://imi.org.ua/wp-content/uploads/2017/06/posibnyk.pdf.

58. Реформа урядових комунікацій у Великобританії. Share & Discover Presentations | SlideShare. URL: https://www.slideshare.net/CommReformGroup/ss-56653943 (дата звернення: 30.11.2023).

59. House of Commons Administration Committee. Communicating the commons: how effectively does the house of commons administration communicate about parliament?. URL: https://committees.parliament.uk/publications/42252/documents/210055/default/ (date of access: 30.11.2023).

60. Veljanovska Blahzevska K. Strategic communication in NATO: need for a unified approach to security policy. *Faculty of security studies and vice-rector for*

science at MIT university. P. 25. URL: https://securityanddefence.pl/pdf-103290-36224?filename=Strategic%20communication.pdf (date of access: 03.12.2023).

61. Бігдан М., Войціховський А. Діяльність НАТО із забезпечення інформаційної безпеки. *Протидія кіберзлочинності та торгівлі людьми*. 2023. С. 3. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/c434bd11-5eb3-4073-a241-ce9b14c4be63/content (дата звернення: 02.12.2023).