НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕХНІЧНІ АСПЕКТИ ТА МЕТОДИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ВПЛИВАМ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Кушко Андрій Миколайович

Керівник: к.т.н., доцент
Кухаренко Сергій Вікторович

Рецензент: к.т.н., доцент
Бойко Віктор Дмитрович

Одеса – 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Кушку Андрію Миколайовичу

1. Тема роботи: «Технічні аспекти та методи протидії інформаційним впливам»
Керівник роботи: к.т.н, доцент Кухаренко Сергій Вікторович
затверджені наказом НУ ОЮА від «02» квітня 2024 року № 809-06
2. Строк подання здобувачем роботи «20» травня 2024 рік
3. Дата видачі завдання«15» вересня 2023 рік

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему “Технічні аспекти та методи протидії інформаційним впливам” на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека. Робота виконана на 52 сторінках загального тексту та 44 сторінках основного тексту. Список використаних джерел містить 22 найменування за переліком посилань.

Метою роботи є дослідження та оцінка механізмів інформаційних впливів, аналіз потенційних загроз і вразливостей, а також розробка ефективних стратегій протидії маніпулюванню думкою в інформаційному суспільстві.

Під час дослідження було здійснено аналіз загроз інформаційного простору країни, досліджено методи протидії інформаційним впливам та потенційним загрозам, а також оцінено ефективність існуючих стратегій забезпечення безпеки інформаційного середовища.

У ході роботи було представлено метод, що передбачає комплексний підхід до підвищення медіаграмотності громадян, вдосконалення законодавчого регулювання та впровадження новітніх технологій для моніторингу та нейтралізації дезінформації.

Можливі напрями подальших досліджень включають розробку нових технологій для виявлення та протидії фейковій інформації, вдосконалення стратегій інформаційної безпеки з урахуванням постійного розвитку штучного інтелекту, а також поглиблене вивчення впливу інформаційно-психологічних операцій на різні сегменти суспільства.

ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНИЙ ВПЛИВ, ДЕЗІНФОРМАЦІЯ, ІНФОРМАЦІЙНІ АТАКИ.

ABSTRACT

The qualification work on the topic "Technical aspects and methods of countering information influences" for the first (bachelor`s) level of higher education in the specialty 125 Cybersecurity, educational program: Cybersecurity. The work is executed on 52 pages of the general text and 44 pages of the main text. The list of references includes 22 titles according to the list of references.

The purpose of the work is to study and evaluate the mechanisms of information influence, analyze potential threats and vulnerabilities, and develop effective strategies to counteract opinion manipulation in the information society.

The study analyzed the threats to the country's information space, investigated methods of counteracting information influences and potential threats, and assessed the effectiveness of existing strategies to ensure the security of the information environment.

In the course of the study, a method was presented that provides for a comprehensive approach to increasing media literacy of citizens, improving legislative regulation and introducing the latest technologies to monitor and neutralize disinformation.

Possible areas for further research include the development of new technologies to detect and counteract fake information, improving information security strategies in view of the constant development of artificial intelligence, and an in-depth study of the impact of information and psychological operations on various segments of society.

INFORMATION SECURITY, INFORMATION INFLUENCE, DISINFORMATION, INFORMATION ATTACKS.

ЗМІСТ

ВСТУП

В сучасному цифровому світі важко переоцінити важливість інформації. Актуальним питанням постає взаємозв’язок між інформаційними потоками та забезпеченням безпеки в контексті зростання кількості кіберзагроз та розповсюдження дезінформації.

В час, коли наша країна перебуває в стані війни, захист інформаційного простору є основним аспектом національної інформаційної безпеки. Здатність маніпулювати думкою суспільства та впливати на стан країни ззовні є дієвим інструментом для ворогів. З розвитком штучного інтелекту, поширення дезінформації зростає щодня, а різновид фейкової інформації набуває нових форм та модифікацій, підлаштовуючись під потреби суспільства. Отже, формування підходів протидії інформаційним впливам є надзвичайно важливим при веденні інформаційного протиборства.

Інформаційно-психологичні операції, кібернетичні атаки, мережеві війни є вагомими компонентами сучасних інформаційних конфліктів, в той же час їх застосування зумовлює більш ретельну взаємодію в питанні підвищення медіаграмотності громадян. Тому в рамках законодавства закріплені визначені загрози інформаційні безпеці та запропоновані завдання з підвищення захищеності інформаційного простору. Законодавче регулювання є вирішальним фактором в формуванні протидії інформаційним впливам. Крім того, важливою складовою є впровадження сучасних технологічних рішень у сфері кібербезпеки, що дозволять більш ефективно виявляти та нейтралізувати загрози.

Метою кваліфікаційної роботи є дослідження та оцінка механізмів інформаційних впливів, а також розробка ефективних стратегій протидії маніпулюванню думкою в інформаційному суспільстві.

Об’єкт дослідження – загрози інформаційного простору країни.

Предмет дослідження – методи протидії інформаційним впливам та потенційним загрозам інформаційного простору.

Практична цінність роботи полягає в тому, що було здійснено аналіз стратегій забезпечення безпеки інформаційного середовища, беручи до уваги усі актуальні засоби ведення інформаційної війни. Існуючи заходи значно вдосконалять знання громадян щодо потенційних видів інформаційних загроз суспільству та державі в цілому.

Під час виконання кваліфікаційної роботи дослідження проведеного у першому розділі були опубліковані у вигляді тез на Всеукраїнській науково-практичній конференції здобувачів вищої освіти «Суспільство та держава в умовах воєнного стану: виклики та перспективи», 27 квітня 2024 року.

1 ТЕОРЕТИЧНІ АСПЕКТИ ІНФОРМАЦІЙНИХ ВПЛИВІВ

1.1 Основні визначення та засоби інформаційних впливів

Інформаційні впливи визначаються як спроби змінити або сформувати думки, переконання чи поведінку інших людей через передачу інформації або маніпулювання нею. Ці впливи можуть бути як позитивними, спрямованими на підвищення обізнаності або розуміння певних питань, так і негативними, спрямованими на маніпуляцію або обман.

Серед науковців немає загальної згоди щодо науково-теоретичного розуміння та опису інформаційного впливу, а також його основних форм і методів реалізації. Інформаційний вплив розглядався дослідниками в різних контекстах, таких як маніпуляція, соціологічний вплив тощо. Важливо зазначити, що деякі дослідники не надавали належної уваги феномену інформаційного впливу, розглядаючи його як частину загального контексту, а не окреме явище. М.І. Семечкін визначає інформаційний вплив як використання інформації, фактів і знань для здійснення впливу. Такий вчений як М. Кордуелл визначає інформаційний вплив як форму соціального впливу, що виникає у випадку, коли індивід не може прийняти рішення самостійно і звертається до зовнішньої думки.

Також варто відзначити, що завдяки розвитку інформаційних технологій та загальному науково-технічному прогресу ми спостерігаємо появу нових інноваційних підходів, які використовуються в сучасних інформаційних протистояннях у політичній сфері. Процес використання інформаційно-комунікативних методів впливу постійно еволюціонує. З кожним періодом концепція інформаційного впливу зазнає теоретичних, методологічних та структурних модифікацій. Віртуалізація інформаційного простору призвела до «об’єднання в мережі» споживачів інформації, що спричинило частковий зсув впливу таких ЗМІ, як газети, радіо, телебачення, у віртуальний простір [1].

Необхідно розглядати методи інформаційного впливу в контексті соціальних комунікацій, з особливим урахуванням потенційно небезпечних ефектів для аудиторії. Відповідно до думки такого вченого, як О. Зіменка, інформаційний

вплив є «способом впливу на свідомість особистості через застосування ЗМІ з метою зміни сформованих оцінок, думок, переконань і цінностей для подальшої модифікації її поведінкових реакцій на події, що відбуваються». Згідно з підходом який виділяють інші вчені, а саме В. Хорошка та Ю. Хохлачової в контексті медіа інформаційний вплив розглядається як «поширення певних ідей, поглядів або ідеології через засоби масової інформації та різні комунікаційні канали». З огляду на вищезазначені аспекти інформаційної безпеки держави, інформаційний вплив можна визначити як «організоване та цілеспрямоване використання спеціальних інформаційних засобів і технологій для внесення деструктивних змін у свідомість особистості, соціальних груп або населення (зокрема, корекція поведінки), в інформаційно-технічну інфраструктуру об'єкта впливу, а також в її фізичний стан».

Низка вчених визначають інформаційний вплив або пропаганду як усвідомлені та систематичні спроби формування сприйняття, маніпулювання свідомістю та впливу на поведінку суспільства у певному напрямку. Не дивлячись на те що, інформаційний вплив, хоч й почався з самого початку історії суспільства, він був першим об'єктом досліджень американської школи вивчення ЗМІ. Ця школа в свою чергу активно досліджувала інформаційний вплив, зокрема на прикладі Першої світової війни. На основі даного дослідження було визначено три основні види інформаційного впливу:

1. «Білий» вплив: це ситуація, коли журналіст відверто виступає як джерело інформації і дозволяє пов'язати свої матеріали з реальними джерелами. Прикладом такого типу впливу є офіційні заяви президента, уряду або інших офіційних інформаційних агентств.

2. «Сірий» вплив: у цьому випадку журналіст використовує спеціально створені джерела або забезпечує публікацію матеріалів у незалежних засобах масової інформації, проте без прямого зв'язку з офіційними джерелами. Прикладом цього може бути інформація, яка розповсюджується через альтернативні ЗМІ або неурядові організації.

3. «Чорний» вплив: у цьому випадку журналіст представляє матеріали від імені третіх осіб, наприклад, підпільної організації.

Спосіб передачі інформації також відіграє певну роль у її впливі, при цьому використовуються різні канали, такі як традиційні ЗМІ, соціальні мережі, електронна пошта та спеціалізовані вебресурси. Кожен канал має свої унікальні характеристики та можливості впливу на аудиторію.

Отже, підсумовуючи усе вищезазначене, можемо зробити висновок, що серед різновидів інформаційного впливу можна відзначити такі явища, як інформаційні атаки на мобільний зв'язок, діяльність в мережі Інтернет з метою підміни або поширення специфічних повідомлень, блокування або приглушення сигналу для заміни контенту, усна комунікація для формування або зміни поглядів, дій та поведінки цільової аудиторії. Зміна підходів до інформаційного впливу залежить від умов розповсюдження інформації в різних просторах, таких як інформаційний, віртуальний та фізичний. Це передбачає оперативну зміну або «перемикання» з одного каналу комунікації на інший. Серед визначених тенденцій можна відзначити агресивний характер повідомлень, використання різних каналів комунікації, поширення дезінформації та деструктивних думок [2].

1.2 Аналіз розвитку інформаційних конфліктів

Задля того, щоб краще розуміти структуру інформаційних впливів та їх значення в сучасному світі, необхідно розглядати також історичний аспект. Модифікація інформаційних впливів та конфліктів відбувається ще з давних часів по сьогодення. Думка суспільства ніколи не була сталою, а її формування завжди відбувалося через різні обставини.

Розвиток інформаційних конфліктів відбувався паралельно з політичними змінами у суспільстві, а їх взаємодія формувала нові контексти та динаміку цих конфліктів.

У попередні історичні епохи інформаційні конфлікти часто були спрямовані на утримання влади та придушення опозиції, особливо в періоди монархій та абсолютного правління. Інформаційні ресурси суворо контролювалися централізованими інституціями. У ранніх східних державах інформаційні

протистояння мали різноманітний характер і супроводжували військові операції, політичні, економічні та релігійні процеси. У той самий період історії відбувалися перші спроби використання інформаційно-комунікаційних технологій, що були необхідні для повного та всебічного функціонування державної політики, економіки, військової сфери та торгівлі.

Зокрема, у Помпеях були знайдені написи, які можна інтерпретувати як такі, що дискредитують, компрометують або позитивно відгукуються про певних осіб, які були обрані на посади в міських магістратах. Міжнародні події, такі як військові конфлікти, дипломатичні стосунки та міжнародна торгівля, супроводжувалися застосуванням демаршів та дезінформації через шантаж ворожих лідерів.

У той же час було видано книгу «Мистецтво війни, де було визначено декі елементи інформаційної війни задля забезпечення переваг в битвах військового та міжнародного значення.

В епоху Середньовіччя та Відродження церква відігравала домінуючу роль у суспільстві, контролюючи різні аспекти, в тому числі й інформаційно-комунікаційні технології. Медіа-технології цієї епохи базувалися на традиційних інструментах, таких як мова, мистецтво, писемність, реклама та література. Однак з’явилися і нові інструменти, такі як пропаганда і психологічна війна. У боротьбі проти Реформації Католицька Церква створила Конгрегацію поширення віри. Це був перший відомий центр інформаційно-психологічних спецоперацій. Слід відзначити, що Лідери Київської Русі перейняли методи інформаційної війни у візантійців, поєднали їх з досвідом варягів та створили власну систему.

Отже, в цей період часу базовий інформаційний процес включав дослідження світу, наукове пізнання та трансформацію зовнішнього середовища, фіксацію через науку, мистецтво, архітектуру, рекламу та писемність, і передачу за допомогою мови, мистецтва, реклами та писемності.

Конфлікти XIX століття супроводжувалися інформаційною війною з використанням преси, яка стала глобальною медіа-технологією. Зокрема, термін «преса» походить від першої масової газети під назвою «La Presse» у 1831 році. Преса стала інструментом масового впливу на свідомість суспільства, дозволяючи

маніпулювати, дезінформувати, залякувати, стимулювати і закликати. Наприкінці 1800-х років з’являється ще один глобальний засіб масової інформації, такий як радіо.

У XVII-XIX століття базовий інформаційний процес включав дослідження суспільних процесів, наукове пізнання та трансформацію навколишнього середовища, фіксацію через науку, мистецтво, архітектуру, рекламу, писемність та ранні медіа, і передачу за допомогою мовлення, мистецтва, реклами, писемності та ранніх медіа. Основними носіями інформації для людей в цих століттях були книжки, офіційна документація, листи, зокрема на папері, а також твори мистецтва, що використовували різноманітні матеріали, такі як папір, тканина та інші, характерні для минулих епох. Освітні установи, дослідницькі центри, адміністративні структури та засоби масової інформації стали центрами створення та поширення інформації.

Під час двох світових війн використання засобів масової інформації для пропаганди та маніпулювання громадською думкою набувало все більшого значення. У середині XX століття значний внесок в розвиток теорії та методології ведення інформаційних війн зробив канадський соціолог Г.М.Мак-Люен. У середині XX століття значний внесок в розвиток теорії та методології ведення інформаційних війн зробив канадський соціолог Г.М.Мак-Люен. Він класифікував історію розвитку людства за типами медіа, які воно використовувало на різних етапах, враховуючи епоху дописемного періоду, писемну культуру та сучасний період, що характеризується як «електронне суспільство». Маклюен також запровадив класифікацію медіа на основі їхніх функцій та можливостей, розділивши їх на «гарячі» (інформаційні) та «холодні» (емоційні). Загалом, робота Маклюена відіграла вирішальну роль у розумінні та формуванні сфери інформаційної війни.

Конкуренція між Сполученими Штатами та Радянським Союзом призвела до боротьби за ідеологічну перевагу за допомогою пропаганди та інформаційних кампаній. Фінальне протистояння «Холодної війни» стало найбільш успішною інформаційною кампанією для США, що спричинило прискорення процесів, що

призвели до розвалу СРСР. Головною фігурою цього протистояння став 40-й президент США Рональд Рейган, який оголосив хрестовий похід проти «Імперії Зла» ще в 1979 році та розпочав безкомпромісну економічну та інформаційно-психологічну війну з СРСР та його союзниками.

Під час цих конфліктів сформувалася сучасна американська доктрина інформаційно-психологічної війни, з'явилися спеціалізовані стратегії, методи та військові підрозділи, такі як PSYOPS або з 2010 р. – центри MISO. Термін «інформаційна війна» був офіційно використаний в 1992 році, а розширене тлумачення терміну було надано в 1993 році.

Польовий статут армії США FM-106 «Інформаційні операції» та Доктрина об'єднаних інформаційних операцій стали ключовими документами в регулюванні інформаційної війни. Використання традиційних і нових медіа, таких як кіно, телебачення, та Інтернет, підвищило ефективність інформаційно-комунікаційної діяльності в рамках військових конфліктів.

Наприкінці XX століття та на початку XXI століття світ переходить у цифрову еру, де значна частина життя стає віртуальною. Водночас інформаційна війна переноситься в Інтернет. Особливо важливим стає формат кібервійни, який стає важливою складовою сучасних конфліктів і забезпечує переваги в реальних протистояннях. Незважаючи на появу нових технологій ведення інформаційних війн, головне завдання залишається незмінним: отримання переваг у забезпеченні військових, економічних та політичних конфліктів.

Розвиток інформаційно-комунікаційних технологій у XX-XXI столітті призвів до появи онлайн та офлайн мережевих структур, з особливим акцентом на онлайн структурах, таких як соціальні мережі у форматі WEB 2.0. Інтернет відіграв ключову роль у цьому розвитку, а саме поняття «соціальна мережа» набуло нового значення і відкрило перед людством великі перспективи. Перша віртуальна соціальна мережа Classmates.com була створена в 1995 році Ренді Конрадсом, щоб допомогти зареєстрованим користувачам встановлювати і підтримувати зв'язки з друзями і знайомими. Згодом з'явилися інші мережі, такі як Friendster, LinkedIn, MySpace, Tribe і Hi5.

У 2004 році були створені такі соціальні мережі, як Orkut, Bebo і Yahoo 360, і в тому ж році Марк Цукерберг розробив Facebook, який зараз є беззаперечним світовим лідером у сфері соціальних мереж.

Підсумовуючи інформаційно-комунікаційні досягнення XX-XXI століть було виявлено певні особливості розвитку інформаційних війн. Протягом усього цього періоду інформація створювалася шляхом вивчення суспільних процесів, наукових знань та умов навколишнього середовища. Вона фіксувалася за допомогою різних засобів, таких як наука, мистецтво, архітектура, реклама та писемність. У сучасному світі основними носіями інформації для людей є цифрові пристрої, друковані книги, офіційні документи та особисті листи на папері. Твори мистецтва, як віртуальні, так і фізичні, також відіграють певну роль у передачі інформації. В інформаційних війнах цього періоду переважають цифрові віртуальні конфлікти та реальні інформаційно-психологічні операції. Ці війни часто пов’язані з військовими конфліктами, політичними та економічними процесами. Виробництво контенту стало найважливішою функцією суспільства, забезпечуючи матеріалом економічні процеси, мистецтво, військову справу, державне управління, науку, релігію тощо. Дослідницькі центри, військові структури, навчальні заклади, адміністративні органи та самі медіа перетворилися на фабрики контенту.

У світі швидкісного споживання інформації, політичні конфлікти відбуваються на широкому спектрі платформ, включаючи соціальні медіа, блоги, форуми тощо. Політичні сили змагаються за контроль над наративами та переслідують власні цілі через інформаційний простір.

У кожному історичному періоді політичні зміни у суспільстві формували нові контексти для інформаційних конфліктів, відображаючи суттєві зміни у способах сприйняття, розповсюдження та маніпулювання інформацією.

1.3 Роль інформаційної війни в сучасному світі

Інформаційна війна стала однією з найважливіших складових в сучасному світі, відображаючи зміни в сферах політики, економіки, та соціальних відносинах. Вона визначається як збір, обробка, поширення та контроль над інформацією для досягнення певних цілей.

Переосмислення суспільних явищ та їх регулювання стає необхідністю в контексті трансформації суспільної реальності, екологічних проблем, тероризму, нового «великого переселення народів» та інших аспектів, які виникають у зв’язку з глобалізацією. Система міжнародного захисту, яка становить основу права, правової системи та системи законодавства, також піддається перетворенням.

Невизначеність місця особистості та проблеми захисту прав людини є наслідком глобальних викликів, що постійно зростають та змінюють правову та політичну реальність.

Інформаційна війна, яка є сучасним глобалізаційним явищем, створює особливий виклик для сучасних систем цінностей. Проблеми забезпечення інформаційної безпеки є надзвичайно важливими для кожної країни світу, тому науковий аналіз даної тематики сприятиме кращому розумінню загроз та викликів глобалізованого суспільства [3].

Однією з ключових ролей інформаційної війни є вплив на громадську думку та перекручення реальності. Інформаційні кампанії можуть використовувати маніпуляцію фактами та викривленнями для формування певних поглядів та уявлень серед населення. Це може включати дезінформацію, фейкові новини, або навіть цілеспрямовані кібератаки на системи зв’язку та інформаційні платформи.

Неправдива інформація є основою такої війни. Військова агресія, яка передбачає неоголошений збройний конфлікт і призводить до захоплення територій і значних людських втрат, часто здійснюється під прикриттям благородних цілей, таких як патріотизм, захист корінних народів, прав і свобод людини, боротьба з тероризмом [3].

Інформаційна-пропагандистська війна може розглядатися у таких форматах як: інформаційна війна, психологічна війна та кібернетична війна. Поняття «інформаційна війна» описує широкомасштабну боротьбу в інформаційному просторі, використовуючи різноманітні методи, прийоми, способи, канали і засоби для впливу на свідомість і психіку людей, з метою зміни їх світогляду та досягнення певних цілей». Основна мета такої війни полягає в забезпеченні достатнього рівня національної безпеки в сферах життя суспільства з одночасним зниженням рівня захищеності національної безпеки сторони опонента» [4].

У сучасній науковій літературі зазначають, що інформаційна війна – термін, який можна розглядати з різних аспектів. По-перше, це вплив на цивільне населення і / або військовослужбовців іншої країни через поширення певної інформації. По-друге, експерти виділяють ознаки, що вказують на прояви такої боротьби. До них відносять:·контроль над медіа; пряме управління засобами інформації та зв'язку впливовими особами; втручання державних органів у діяльність ЗМІ, включаючи обмеження свободи слова; домінування кількох засобів масової інформації й інформаційних агентств на світовому ринку новин; нерівність у доступі до меді між різними групами суспільства; опублікування різних матеріалів, що дискредитують певну політичну партію, рух або подію [3].

Крім того, інформаційна війна використовується для дестабілізації та психологічного тиску на противників. Це може включати розповсюдження загроз, шантаж, чи маніпуляцію громадською думкою, щоб створити атмосферу нестабільності та нервового напруження.

Термін «інформаційна війна» зараз знайомий усім нам, оскільки ми всі тісно пов'язані з нею, як ніколи раніше. Американський фахівець Маклюен аналізує значення інформації в сучасному світі та висловлює свою думку, що війна за допомогою інформації – це істинно тотальна війна. Інформаційна війна на сьогоднішній день стала одним з найнебезпечніших видів зброї. Основою існування багатьох тоталітарних режимів стало використання компроматів, поширення негативних інформаційних матеріалів, розповсюдження фейкової інформації. З прогресом новітніх технологій, вплив інформації на еволюцію

людства збільшився в тисячі разів. Інформація здатна впливати на колективну свідомість населення, це в свою чергу дозволяє маніпулювати громадською думкою та досягати різного виду цілей, наприклад, знищення ворога, усунення конкурентів або розпалювання конфліктів.

Поширення владою або відповідальною за цей процес особою великого обсягу інформацію, дозволяє формувати громадську думку, викликати послідовні логічні роздуми, цілісну систему поглядів з окремих питань на користь організатора інформаційної кампанії. В результаті виникає усвідомлення окремих фактів чи подій у необхідному для маніпулятора вигляді, формування бажаного світогляду або життєвої позиції щодо питань раніше суперечливих. За відсутності протиріч і стійкої системи переконань, метою інформаційної війни є створення сумнівів, посіяння протиріч та підозр в існуючі переконання. Людина впродовж свого життя шукає відповіді на питання, що її хвилюють, суперечливі теми, що є невід'ємною частиною безперервних процесів пізнання.

Французський соціолог Жак Еллюль ввів поняття вертикальної та горизонтальної пропаганди (Ellul J. Propaganda. The formation of men's attitudes. – New York, 1965). Вертикальна пропаганда являє собою інформаційний потік зверху до низу з пасивним прийняттям аудиторії. Горизонтальна пропаганда, в свою чергу, розгортається всередині групи, не маючи при цьому лідера. Цьому виду пропаганди характерна рівність учасників. Водночас Ж. Еллюль розрізняє поняття політичної та соціологічної пропаганди. Політична пропаганда налічує техніки впливу держави, партії, адміністрації, а соціологічна функціонує задля об'єднання групи, просуваючи певний спосіб життя і поведінку, як суспільну норму. Соціологічну пропаганду важче розпізнати, оскільки вона просувається через економічні, політичні та соціологічні чинники. З іншого боку, політична пропаганда поширює ідеологію через засоби масової інформації. Різниця між вертикальною та горизонтальною пропагандою ґрунтується на напрямку комунікації та структурі, тоді як політична від соціологічною відрізняється видами ЗМІ, де вони застосовуються.

Прикладом може виступати міждержавний конфлікт між Україною та Росією, в якому для отримання стратегічних та політичних переваг використовуються низка тактик, у тому числі політична та соціологічна пропаганда. Здійснюють її урядові та неурядові організації в інформаційному просторі України, Росії, інших країн та міжнародних організацій. Мета цих заходів – деморалізувати або ввести в оману супротивника та протидіяти діям іншої сторони у протистоянні між Україною та Росією [5].

Крім того, інформаційна війна стає все більш важливою в контексті кібербезпеки та кібератак. Зокрема, інформаційна війна набуває особливої важливості в контексті міжнародних конфліктів та гібридної війни, де вона використовується як інструмент для досягнення політичних, військових та економічних цілей.

Нижче наведені основні закономірності інформаційної війни: наявність залежності ефективності ведення війни від якості і кількості засобів впливу; взаємозв’язок поставлених цілей інформаційної війни та наявності ресурсів та засобів їх застосування; необхідність узгодженості інформаційних дій у часі і просторі задля вирішення завдань інформаційної війни; нерівномірність впливового факторів різних сил і засобів на інформаційній сферу ворога. Фундаментальні основи інформаційної війни можна підсумувати наступним чином: узгодженість її цілей із політичними завданнями війни; концентрація та підготовка сил у вирішальних моментах; динамічність та ініціативність під час ведення інформаційної війни; скоординоване спільне застосування всіх видів сил і засобів ведення інформаційної війни; використання раптових інформаційних ударів; готовність до захисту власної інформації і нищівного впливу на інформаційний простір противника; готовність до безперервної інформаційної війни; гнучкість у маневруванні сил і засобів ведення інформаційної війни; приділення уваги духовним аспектам задля виконання поставлених завдань; забезпечення боєздатності та невідкладне відновлення сил і засобів ведення інформаційної війни; стійке управління силами і засобами ведення інформаційної

війни; рішучість у виконанні поставлених завдань; реалізація ухвалених рішень та визначених завдань [4].

Інтегративні технології впливу на індивідуальну, групову та масову свідомість відіграють важливу роль у формуванні принципів ведення інформаційної війни: Виокремлюють наступні методики: втручання інформаційний простір інших суб'єктів; застосування рефлексивного керування; технологія руйнування ідентичності; здійснення національної консолідації, в тому числі об'єднання проти ворога та заради експансії; проведення інформаційно-пропагандистської війни; ведення інформаційної та мережної війни; технології спеціальних інформаційних операцій; використання технології дезінформації. Також у сучасну епоху особливої актуальності набули пропагандистські технології. [6, с. 46-66] Вони сприяють: руйнуванню інформаційних монополій; переділу інформаційного впливового значення між гравцями; формуванню керованих масових груп; впливу на усвідомлення; маніпулюванню героїзацією; управлінню сприйняттям ворогів; контролю над джерелами інформації; керуванню парадоксальністю повідомлень; управлінню комунікаційними каналами; керуванню фреймами; контролю над рівнем розважальності; формуванню сакральності; використанню технологій в пропагандистських цілях; керуванню історичними наративами; управлінню великими обсягами інформації. Технології, що впливають на індивідуальну, групову та масову свідомість застосовуються через: ЗМІ та спеціальні засоби інформаційно-пропагандистської спрямованості, а також глобальні комп'ютерні мережі та програмні засоби поширення в них заангажованих матеріалів; засоби, які несанкціоновано модифікують інформаційне середовище, для впливу на процес прийняття рішення; засобів створення віртуальної реальності та поширення чуток; методи здійснення підпорогового психосемантичного впливу; інструменти генерування акустичних та електромагнітних полів [4].

Отже, роль інформаційної війни в сучасному світі не може бути недооціненою. Вона впливає на політичні процеси, економічні ринки та соціальні відносини, визначаючи стратегії та результати сучасних конфліктів. І навіть

більше, вона створює потенційну загрозу для кібербезпеки та міжнародного порядку, вимагаючи постійного уваги та заходів з протидії.

1.4 Законодавче регулювання інформаційної безпеки

Інформаційна безпека в сучасному світі стала однією з найбільш актуальних і складних проблем. З поглибленням цифровізації суспільства і зростанням кількості цифрових загроз по всьому світу, значення законодавчого регулювання в сфері інформаційної безпеки стає надзвичайно важливим.

Поняття інформаційної безпеки громадянина закріплене у ряді нормативних актів і є складовою конституційної норми. Однак воно не має достатнього рівня деталізації та законодавчого врегулювання. Тому особливо важливими стають питання регулювання інформаційної сфери та створення відповідних умов для розвитку вітчизняного інформаційного виробництва.

Експертиза українського законодавства у сфері інформаційної безпеки, яка була проведена представниками ОБСЄ протягом останніх років, підтверджує, що в цілому законодавча та нормативно-правова база функціонування інформаційної сфери відповідає стандартам Європейського Союзу. Однак існує серйозна проблема недотримання цих норм усіма суб’єктами інформаційних відносин, зокрема, державними органами на всіх рівнях. Низький рівень правової культури серед громадян України вимагає розгляду ситуації з іншого ракурсу порівняно з країнами Європейського Союзу.

На сьогоднішній день існує велика кількість правових актів, які регулюють різні питання, такі як інформаційна війна, управління інформаційною безпекою, загрози інформаційній безпеці держави, захист прав і свобод людини в інформаційній сфері, види захисту інформаційної безпеки держави, а також джерела загроз інформаційній безпеці. До цих нормативно-правових актів належать закони, акти Президента України, Верховної Ради України, Кабінету Міністрів України, центральних органів виконавчої влади. Вони також спрямовані на досягнення цілей та завдань, що визначені Стратегією інформаційної безпеки.

Нормативно-правові акти, які є основою регулювання інформаційної безпеки в Україні, можна класифікувати залежно від обсягу приписів, що містяться в актах, та ступеня регулювання відносин. Виокремлюють акти, які безпосередньо регулюють забезпечення інформаційної безпеки в Україні та акти, що не містять прямих нормативних положень щодо забезпечення інформаційної безпеки, але прямо або опосередковано регулюють інформаційні відносини. Залежно від юридичної сили розглядаються такі акти: Конституція України, Закони України (зокрема, «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про національну безпеку України», «Про захист персональних даних» тощо) та підзаконні акти (нормативні акти Президента України, Кабінету Міністрів України, Державної служби спеціального зв'язку та захисту інформації України тощо).

Конституція України від 28 червня 1996 року, № 254к/96-ВР є основним правовим документом для забезпечення інформаційної безпеки в країни. Вона встановлює конституційні принципи права на інформацію, конкретні джерела інформації, до яких держава гарантує доступ, а також ряд інших важливих положень, які визначають розвиток законодавства у галузі забезпечення інформаційної безпеки.

Також слід зазначити, що Закон України «Про інформацію» від 02.10.1992 р. № 2657-XII регулює різні аспекти інформаційних відносин, включаючи створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації [7]. Він охоплює основні принципи, визначає суб'єкти та об'єкти інформаційних відносин, гарантує право на інформацію та його забезпечення. Закон класифікує інформацію та встановлює відповідальність за порушення законодавства про інформацію.

Серед підзаконних актів важливе місце посідає Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.2021 р. № 685/2021. Вона визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, а також стратегічні цілі та завдання, спрямовані на протидію цим загрозам, захист прав на інформацію та персональних даних осіб [8].

Україна має історично утверджений принцип договірної системи, який відрізняється від західноєвропейського підходу до права. Більшість відносин у суспільстві регулювалися звичаями та неформальними домовленостями.

Однією з найважливіших проблем правової політики держави є недостатня ретельність і точність дотримання законодавства, зокрема в інформаційній сфері. Певні сили намагаються створити нові сфери невразливості та переваг, що діють за межами законодавства. Забезпечення єдності та невідворотності застосування закону є одним з ключових завдань держави.

Іншою важливою проблемою є несистемність вітчизняної правової політики в інформаційній сфері. В умовах сучасних реалій більшість законодавчих актів приймаються з метою вирішення тактичних завдань або задоволення кланових інтересів, іноді без врахування стратегічних орієнтирів і реальних умов України.

Багато питань функціонування інформаційної сфери досі не вирішені на законодавчому рівні. Це стосується як інфраструктури, так і діяльності ЗМІ, інформаційно-аналітичних установ та інших аспектів. При аналізі законодавчого забезпечення важливої складової інформаційної політики держави, як інформаційної прозорості та відкритості управління органами державної влади, виявляється, що в Україні є певна законодавча база.

Головним недоліком чинного законодавства є його пасивний характер, коли лише декларується необхідність забезпечення відкритості органів державної влади в відповідь на звернення громадян чи ЗМІ. Громадянин, який бажає отримати певну інформацію, повинен підготувати та подати запит до відповідної установи, а потім очікувати на відповідь протягом місяця. Це призводить до того, що державні органи фактично відсутні в інформаційному просторі. Часом стається так, що про державну політику повідомляють не самі державні органи, а треті сторони, часто опоненти. У таких умовах законодавство демократичних країн передбачає активну інформаційну діяльність, обов’язкову звітність влади перед громадянами незалежно від наявності звернень чи запитів щодо надання інформації, а також обов’язкове, а іноді навіть надмірно активне, інформування громадян про поточну діяльність органів державної влади.

Ще одним яскравим прикладом виступає проблема приватності та захисту даних, з розвитком Інтернету і цифрових технологій зросла і потреба у захисті приватності та особистих даних громадян. Проте, існуюче законодавство часто не встигає відповідати на нові виклики які тісно пов’язані зі збереженням та обробкою персональної інформації. Ще однією проблемою виступає недостатня відповідальність за порушення безпеки. У багатьох випадках порушення інформаційної безпеки лишаються без належного реагування та відповідальності. Недостатнє законодавче забезпечення щодо відшкодування збитків або покарання винних сторін може стимулювати нові атаки та порушення.

Невиключені випадки обмеження прав людини в галузі інформації, задля забезпечення конфіденційності та безпеки особистої інформації, що допомагає створювати більш ефективну та прозору систему захисту інформаційних прав людини. Випадки та причини обмеження реалізації інформаційних прав людини включають в себе міжнародні та національні норми, та стосуються захисту прав і свобод людини, необхідні для захисту безпеки держави, а саме:

1) охорона, захист громадського порядку, громадської безпеки, національної безпеки, територіальної цілісності;

2) необхідні для захисту здоров’я населення та моральних засад;

3) необхідні для забезпечення та захисту: прав і свобод людини, конфіденційності особистого життя, репутації людини, інтересів малолітніх;

4) для запобігання заворушенням або злочинам, забезпечення інтересів правосуддя, підтримання авторитету і неупередженості правосуддя, запобігання розголошенню інформації, одержаної конфіденційно;

5) права держави та її компетентних органів вводити певні процедури щодо ліцензування мас-медіа.

Підсумовуючи усе вищезазначене, можемо зробити такі висновки, що законодавче регулювання в сфері інформаційної безпеки є надзвичайно важливим для забезпечення захисту від цифрових загроз у сучасному світі. Проте існують численні проблеми, які потребують уваги та вирішення на рівні законодавства для забезпечення ефективного захисту інформації та особистих даних. Розвиток

глобального співробітництва та уніфікація законодавства можуть допомогти у вирішенні цих проблем і забезпечити стійкий розвиток цифрового суспільства.

Правове регулювання інформаційної безпеки в Україні – це складна система нормативно-правових актів різної юридичної сили, що регулює відносини у сфері протидії загрозам в інформаційній сфері. Вона також включає активну участь державних та місцевих органів управління, спрямовану на постійний розвиток і вдосконалення інформаційної безпеки [9].

2 ОСОБЛИВОСТІ ІНФОРМАЦІЙНИХ ВПЛИВІВ

2.1 Інформаційно-психологічні операції

Сучасні інформаційні впливи на суспільство відзначаються переліком особливих характеристик, це спостерігається у проведенні акцій, що використовують дезінформацію, розголошення компромату, приховування та спотворення фактів. Ці аспекти вже протягом тривалого часу стали об’єктом досліджень багатьох науковців. Їх дослідження сфокусовані на широкому спектрі проблем, зокрема на нормативно-правовому регулюванні інформаційної безпеки в Україні, загрозах інформаційної безпеці в нашій країні та в світі, а також на технічних, психологічних, лінгвістичних засобах та методах маніпулювання, а також на шляхах захисту від негативного впливу на свідомість масової аудиторії.

Аналізуючи визначення вчених можемо зробити такий висновок, що інформаційно-психологічна операція – це стратегічно спланована і реалізована діяльність, на життєві установки та поведінку людей для досягнення заздалегідь визначених цілей, часто пов’язаних з ухваленням управлінських рішень. У широкому розумінні поняття «психологічна війна» описується як «цілеспрямоване та систематичне використання політичними противниками пропаганди та інших інструментів (включаючи дипломатичні, військові, економічні, політичні та інші), щоб впливати на думки, настрої, почуття і, в кінцевому підсумку, на поведінку супротивника, з метою змусити його діяти в напрямках, що вигідні для виконавців цієї війни».

У польовому статуті ЗС США FM-33-1 «Психологічні операції» визначено, що головна мета спеціальних психологічних операцій полягає в тому, щоб змінити поведінку союзників і противників США в сприятливому для країни напрямі. Основним завданням інформаційних операцій за визначенням деяких науковців, є здійснення управлінського впливу на масову свідомість з метою досягнення конкретних цілей, таких як внесення в суспільну свідомість та свідомість окремих осіб певних ідей та поглядів, дезорієнтація та дезінформація людей, ослаблення усталених переконань та основ суспільства, а також залякування мас. Цілями

психологічної війни можуть бути: запобігання можливому військовому конфлікту, ослаблення морального духу військових і цивільного населення противника, спонукання їх відмовитися від участі в бойових діях, а також створення передумов для досягнення воєнно-політичних цілей з мінімальними людськими та матеріальними втратами. Сучасні технології психологічних війн та інформаційно-психологічної агресії ґрунтуються на стратегії непрямих дій, що передбачає маніпулювання цінностями та переконаннями супротивника з метою зниження його морально-психологічного потенціалу та готовності до оборонної війни. Отже, у політиці та війні стратегічний напад спрямований на послаблення опору опонента або ворога заздалегідь, шляхом зміни його цінностей, мети та уявлень про політичну або військову діяльність, та розмивання понять про образ війни, перемоги, Батьківщини та ворога [4].

Останнім часом інтернет та соціальні мережі перетворилися в широко застосовані інструменти маніпулювання думкою. Сучасні технології дозволяють не лише поширювати дезінформацію, але й спрямовувати інформаційно-психологічний вплив на конкретні аудиторії. Треба зазначити, що потенціал використання штучного інтелекту в інформаційно-психологічних операціях є величезним.

Штучний інтелект є технічною системою, яка володіє ознаками інтелекту, включаючи розпізнавання та розуміння, прийняття рішень та навчання. Експерти НАТО визначають штучний інтелект як систему, що здатна виконувати обґрунтовані дії, адаптуватися до фізичного або цифрового середовища з метою досягнення певних цілей.

Технології штучного інтелекту відкривають широкі можливості для здійснення інформаційно-психологічних операцій. Вони можуть використовуватися для створення діпфейків та «фейкових людей», створення точних психологічних портретів людей у соціальних мережах, просування інформаційного контенту за допомогою чат-ботів, аналіз тональності інформаційного трафіку в мережі, прогнозування наслідків інформаційно-психологічних операцій та багато іншого.

Використання технологій штучного інтелекту, разом з Big Data та іншими методами і прийомами інформаційно-психологічних операцій, може привести до нового рівня генерування псевдореальності, яка значно змінить рівень та наслідки таких операцій [10].

Українські науковці підкреслили, що «протистояння інформаційно-психологічним операціям є надзвичайно складним завданням, оскільки практично неможливо відстежити етапи їхнього планування та підготовки. Під час активної фази таких операцій, держава, яка стала об’єктом інформаційно-психологічної агресії, лише починає аналізувати ситуацію та намагається передбачити її подальший розвиток, витрачаючи значний час на підготовку персоналу та реалізацію контрзаходів». Основною метою таких інформаційно-психологічних впливів на міжнародній арені є заміна ціннісної матриці об’єкта впливу, в той час як завданням інформаційно-психологічної війни є руйнування соціуму шляхом проникнення в його систему світосприйняття та нав’язування картини світу, що в подальшому сприяє бажаному типу суспільної поведінки цього об’єкта. Більшість дослідників підкреслюють, що ці впливи спрямовані на свідомість з метою зміни чи корекції поведінки окремої особи чи суспільства. Інформаційно-психологічний вплив охоплює будь-яку активність в межах інформаційно-комунікативного простору, спрямовану на цілеспрямоване поширення спеціально відібраної інформації у формі значень, знаків, образів або сигналів, що викликають психоемоційну реакцію та призводять до зміни світогляду в потрібному напрямку. Об'єктом такого впливу у міжнародних відносинах можуть бути різні особи та групи, такі як глави держав, чиновники, дипломатичні установи, громадські діячі, громадяни, а також різні організації та суспільні групи. Суб’єктами цих впливів можуть бути як внутрішні, так і зовнішні учасники, зокрема держави та їхні структури. Дипломатичні суб’єкти виступають важливим чинником у реалізації міжнародних відносин та зовнішньої політики, і вони можуть бути як об’єктом, так і суб’єктом інформаційно-психологічних впливів. Від їхньої діяльності залежить співпраця міжнародна у різних сферах, стабільність у регіонах та інші аспекти міжнародної взаємодії.

Негативні інформаційно-психологічні впливи у дипломатичній діяльності включають такі аспекти:

1. Впливи на посадових осіб дипломатичної сфери, які виявляються у їхніх уявленнях та емоційно-вольовій сфері, а також у груповій свідомості. Ці впливи можуть бути використані з метою явного або прихованого спонукання до дій, спрямованих на шкоду інтересам країни, суспільства, нації.

2. Впливи на інформацію та інформаційні потоки, що призводять до витоку, спотворення, знищення або перетворення інформаційних потоків, що має негативні наслідки.

3. Інформаційно-психологічні впливи, що негативно впливають на здоров'я та психіку посадових осіб, а також на окремих осіб, групи або інші соціальні утворення, що беруть участь у дипломатичній діяльності [11].

Існують певні можливі наслідки цих негативних інформаційно-психологічних впливів у дипломатичній сфері які безпосередньо включають в себе:

– підвищення рівня заангажованості посадових осіб;

– маніпулювання прийняттям рішень посадовими особами;

– несанкціоноване управління інформаційними потоками;

– дискредитація органів державної влади та управління;

– витік службової інформації в ЗМІ та інше.

До механізмів негативного інформаційно-психологічного впливу відносять різноманітні аспекти соціальної перцепції, сприйняття, пам'яті, уваги та інші. Ці механізми можуть бути використані для реалізації деструктивного впливу, залишаючись непомітними та маніпулюючи почуттями та настроями цільової аудиторії. Серед них можна виділити такі як ідентифікація, емоційне зараження, навіювання, емпатія, наслідування, переконання. Ці механізми можуть діяти як свідомо, так і підсвідомо, і їхнє застосування може бути набагато ефективнішим у порівнянні з прямими методами впливу.

Деструктивний інформаційно-психологічний вплив реалізується таким чином, що він може залишатися непомітним, контролювати волю та емоції об'єкта

впливу, примушувати до інерції, програмувати думки та поведінку, приховувати дійсну інформацію та спонукати об’єкт впливу діяти згідно до своїх слабких сторін.

Для досягнення більшої ефективності інформаційно-психологічного впливу можуть застосовуватися такі прийоми, як подання фальшивої інформації в потрібний момент, навмисне втаємничення правдивої інформації, а також перенасичення інформацією, що ускладнює зрозуміння дійсної ситуації. Ці методи дозволяють програмувати дії та поведінку з метою маніпулювання, дезінформації та змушення до прийняття певних рішень.

Негативні інформаційно-психологічні впливи, зокрема в міжнародних відносинах, спрямовані на порушення цілісності, доступності та конфіденційності інформації. Це може включати погіршення доступу до інформації, перехоплення та зміну її змісту з метою впливу на сприйняття та рішення. Науковці зазначають, що безконтрольне використання інформаційно-психологічних методів може становити соціальну небезпеку, оскільки їхня мета полягає у маніпулюванні свідомістю та програмуванні дій та поведінки осіб та суспільства.

В міжнародній сфері, особливо в дипломатичній діяльності, велике значення має виявлення та нейтралізація деструктивних інформаційно-психологічних впливів. Це обумовлено тим, що при ухваленні зовнішньополітичних рішень необхідно враховувати їхні можливі наслідки для всіх зацікавлених сторін, враховуючи суб’єктів дипломатичної діяльності, а також людей, суспільство та державу.

Вчені акцентують увагу на важливості забезпечення інформаційної безпеки суб’єктів дипломатичної діяльності, виявляти негативні інформаційно-психологічні впливи, а також на ліквідації загроз.

Чим більш досконало забезпечена інформаційно-комунікаційна безпека держави, тим складніше вести гібридні війни, такі як інформаційні, психологічні, консцієнтальні, мережеві, кібернетичні тощо. Поняття, такі як інформаційна та консцієнтальна війна, мають певний зв’язок між собою, оскільки вони використовують інформаційно-психологічні впливи як знаряддя зброї з метою впливу на свідомість та поведінку людей та суспільства. Інформаційна війна

полягає в протистоянні між різними суб'єктами, такими як держави, неурядові, економічні чи інші структури, і має на меті досягнення воєнних, соціально-політичних чи економічних переваг над супротивником.

Консцієнтальна війна – це боротьба, спрямована на вплив на свідомість. Ця форма війни має свої особливості, включаючи такі характеристики, як: тривала латентність; різноманітність, гнучкість та непередбачуваність методів впливу; використання насильницьких методів для спотворення інформаційно-комунікативного простору; розмиття розмежування між «другом» і «ворогом»; руйнування духовних цінностей, уявлень про добро і зло, а також здатності людини до вільної самоідентифікації, руйнування ідентичності та самоідентифікації людини.

На жаль, деякі держави продовжують розвивати та вдосконалювати технологічний та інтелектуальний потенціал для масового впливу на суспільство. Постійний, агресивний інформаційно-психологічний вплив викликає також порушення соціально-економічних процесів і зв'язків та приводить до загибелі держави, а народ стає роз'єднаний, деморалізований і нездатний чинити опір. Це досягається не обов'язково шляхом військового вторгнення або економічного протистояння, а шляхом використання технологій інформаційно-психологічного впливу для керування і примушування об'єктів діяти в потрібному напрямку [11].

2.2 Кібернетичні атаки

На законодавчому рівні визначення поняття кібератаки зазначено в ст.1 п.4 Закону України від 05.10.17 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України», «кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються,

зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту» [12]. Водночас, визначення поняттю кібернетична війна відсутнє, але деякі науковці розглянули це питання. Зокрема, В. В. Зеленін надає таке визначення, що кібервійна – це форма війни, що ведеться у сфері програмного забезпечення інформаційних каналів. Така війна передбачає використання програмних кодів для спричинення збитку, захоплення контролю, створення технічних збоїв, припинення функціонування фізичних об'єктів, насамперед інформаційного зв'язку. Серед завдань кібернетичної війни можуть бути:

– спричинення розладу в суспільстві та економіці;

– знищення і перехоплення даних;

– блокування супротивнику доступу до інформаційних ресурсів [4].

Провідний фахівець О. О. Мережко, говорячи про кібернетичну війну зазначає, що це використання мережі Інтернет та пов'язаних з нею технологічних та інформаційних заходів однією країною задля спричинення збитків економічній, політичній, військовій, технологічній та інформаційній безпеці та суверенітету іншої країни.

Форми існування кібернетичної війни поділяють на такі: вандалізм, пропаганда, збір інформації, відмова сервісу, втручання в роботу обладнання, атаки на об'єкти критичної інфраструктури, державні органи та медіа. Якщо ми говоримо про безпосередньо кібератаки, то це можуть бути: злом вебсторінок приватних осіб або організацій з метою отримання конфіденційної інформацій; атаки з аномальної кількості комп'ютерів або DDoS-атаки для припинення роботи комп'ютерних систем або сайтів; атаки на комп'ютери, що здійснюють адміністративно-контрольні завдання в державних, громадських, військових та комерційних організаціях; атаки на комп'ютерні системи, що забезпечують безперебійний

контроль функціонування міста, а саме водопостачання, електропостачання, пожежної безпеки, транспортного сполучення, телефонних ліній тощо [13].

Ретельно спланована атака хакерами, може призвести до значних наслідків, таких як порушення роботи телефонної мережі або банківських систем. Вразливі також системи енергопостачання та системи контролю повітряного руху. Найнебезпечнішими діями хакерів є впровадження ними комп'ютерних вірусів у програмне забезпечення, що керує критично-важливими системами [14].

Підчас повномасштабної вторгнення в нашу країну, набула важливого значення тема захисту національного кіберпростору. IT-спеціалісти з різних куточків світу долучились до підтримки українського кібернетичного протиборства. Саме за допомогою DDoS-атак, було призупинено роботу різних важливих інфраструктур ворога, заблоковано функціональність деяких урядових сайтів та сайтів промислової сфери.

Цей вид кібератаки передбачає залучення декількох комп'ютерів, що заражені бот мережами, або координацію дій декількох користувачів. Завдяки масовому супротиву, було дезорієнтовано противника та виведено з ладу його логістичні центри та мережі. Отже, можемо сказати, що розподілені атаки відмови в обслуговуванні, результатом яких є блокування сайту через перенавантаження трафіку, виступають одним із найефективнішим видом кібератаки [15].

Також хакери можуть використовувати фішингові електронні листи із зараженим вкладенням, щоб інфікувати комп'ютери. В такі повідомлення можуть бути впроваджені таке шкідливі програми як стилери, програми-вимагачі, трояни, кейлогери, що вміють фіксувати дії користувачів. У результаті зараження комп'ютера, відбувається дублювання та винищення файлів, встановлення зв'язку з зараженими серверами, завантаження та запуск інших зловмисних програм. Водночас, зловмисники можуть вимагати підтвердження збоку користувача персональних даних задля перехоплення доступу. Загалом, кібернетичні атаки збоку супротивника несуть окрім руйнівного ефекту, також і непереоцінений досвід боротьби з різними видами атак, що безперечно позитивно впливає на

подальший розвиток та оптимізацію вітчизняної системи інформаційної безпеки, оперативно реагуючи на відповідні загрози.

Підсумовуючи усе вищезазначене, можемо зробити такий висновок, що будь-яка кібернетична війна починається з кібератаки. Безпосередньо кібернетична атака відбувається в кіберпросторі, віртуальному просторі, в якому можна здійснювати комунікації в мережі Інтернет. Можемо дійти до висновку, що регулювання кіберпростору має значний вплив в контролі над інформацією та мережею Інтернет [13].

2.3 Мережеві інформаційні війни

Аналізуючи праці багатьох науковців, можемо зробити такий висновок, що сучасні конфлікти мають мережевий характер. Поняття "мережева війна" представляє собою інформаційне-комунікаційне протистояння у форматі офлайн та онлайн мережевих структур. Під поняттям «офлайн мережеві структури» виокремлюють організації або тимчасові об’єднання індивідуумів на основі однакової активності або спільних інтересів.

За характеристикою сучасного інтернет-середовища, вебтехнології поділяють на такі формати, як WEB 1.0, WEB 2.0 та WEB 3.0. Формат WEB 1.0 складається з вебресурсів, де творець ділиться контентом з іншими користувачами, а вони мають змогу лише споживати його. Щодо WEB 2.0, то це формат інтернет-майданчиків, де кожен може одночасно бути і редактором, і читачем. WEB 3.0 – формат, у якому користувачі проходять етап аватарізації. Інтернет-ресурси формату WEB 2.0-3.0 становлять онлайн мережеву структуру, включаючи в себе такі соціальні мережі, як Facebook, Instagram, Telegram, TikTok тощо. Соціальні медіа є одними з найефективніших інструментів для ведення інформаційної війни. Головними перевагами використання соціальних мереж є швидкодія у комунікації з користувачами; взаємодія, заснована на персональних інтересах споживачів контенту та невелика затратність у порівнянні з телебаченням або радіо. Звідси й

пояснення акцентованого вектору використання соціальних мереж під час інформаційних війн.

У таких війнах перемога зазвичай досягається не за допомогою військової сили, а через вплив мережевих організацій. У мережевій війні країна стикається з діями противника у вигляді різноманітних акцій, таких як провокації, дезінформація, дипломатичні маніпуляції, політичні рухи.

Мережева війна представляє собою багатогранний конфлікт, що розвивається у всіх сферах – від економіки та політики до соціальних та військових аспектів [16].

Перш аніж перейти до визначення мети мережевої війни потрібно розглянути стратегію планування інформаційних протистоянь, риси певних комунікаційних процесів. Розрізняють такі напрями завдань стратегії, як консолідація, заспокоєння, залякування, невдоволення та протести. Під консолідацією розуміють потребу в співпраці осіб цільових груп для досягнення конкретних результатів. Наприклад, під час військової агресії виникає необхідність мобілізувати суспільство, або для подолання певного соціального чи економічного питання також потрібна впевнена самоорганізація спільноти. Як правило, лідерами громадської думки стають відомі медіа-персонажі або блогери. Задля зменшення громадського тиску, невдоволення населення постає вимога заспокоєння. При наявності ознак підбурення представників окремих цільових груп, в тому числі країною-супротивником, виникає термінова необхідність поширювання заспокійливого контенту, що швидко розповсюджується та сприяє формуванню національного духу та незламності. Виокремлюють такий підхід як залякування, що застосовується задля вчасної зупинки певних процесів соціально-економічної або політичної трансформації. В той же час поставлене мета невдоволення викликає настрої опору, дезорієнтує різні категорії населення та створює підґрунтя для протестів. Схожість завдання консолідації та протестів маємо в єднанні і розголошенні певних думок, але з різною ціллю. Останнє, в свою чергу, може призвести до певного хаосу або революції всередині країни.

Розглянемо, які існують завдання, зокрема, в рамках SMM-комунікацій. Слід зазначити, що суб'єктами є учасники інтернет-комунікацій, а контент, в свою чергу, виступає основним об'єктом інтернет-відносин. Саме тому, коли ми говоримо про завдання інтернет-комунікацій, то згадуємо про контент. По-перше, це створення контенту, а саме певних ілюстрацій, фото, відео, аудіо та текстових повідомлень. По-друге, поширення цього контенту за допомогою соціальних онлайн мереж. По-третє, систематизація контенту, тобто пошук таргетованої інформації, аналіз подій в режимі реального часу. Водночас, необхідно розрахувати приблизну цільову аудиторію для більш якісного виконання завдань. Беруть до уваги такі показники: стать, вік, соціальне положення, соціальні об'єднання.

Після визначення завдань, підтверджують тактику планування інформаційних процесів. На цьому етапі, визначають канали комунікацій та різновид активності. Обирається певна соціальна мережа та починають проявлятися ознаки певної функціональної діяльності з метою впливу на цільові групи. Виокремлюють активність на чужих та власних майданчиках.

Засоби, що застосовуються залежить від платформ, але загалом, це створення каналів, залучення інфлюенсерів, інтеграція з групами, що мають більшу аудиторію, розробка трендового контенту, персональний брендинг та вірусний маркетинг. Аби перевірити результати проводять моніторинг діяльності або SMM-аудит.

У сутності, мережева війна – це специфічний вид ведення війни, що використовує доктрину, стратегії та технології, адаптовані до сучасних умов інформаційного суспільства. Вона здійснюється переважно глобальними інституціолізованими структурами, які включають мас-медіа, транснаціональні корпорації, релігійні організації, політичні еліти та спецслужби. Ці структури інтегруються в одну гнучку та різноманітну мережу.

Отже, мета мережевої війни полягає у досягненні інформаційного впливу, формуванні масової свідомості, моделюванні поведінки ворога, а також союзних і нейтральних сторін за допомогою мережевих структур Результатами цих дій є зміни у правлінні, «кольорові революції», контроль над інформаційним простором,

розташування військових баз і контингентів, вплив на свідомість мас, втручання в прийняття стратегічних рішень політичних еліт, вплив на результати виборів і інші електоральні процеси. Існує думка, що мережева війна будується на принципах рекламної кампанії.

3 МЕТОДИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ВПЛИВАМ

3.1 Безпека інформаційного простору та протидія загрозам

З розвитком технологій інформаційних впливів та методів поширення в інформаційному середовищі актуальним постає питання визначення загрози для вітчизняного інформаційного простору. Зокрема, для ефективного реагування на ці виклики була розроблена Стратегія інформаційної безпеки.

Згідно із вищезазначеним документом, інформаційна загроза – потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні. Загрози поділяють на глобальні та національні.

Перш за все, стратегія акцентує увагу на інформаційних операціях збоку Російської Федерації, що направлені на дестабілізацію інформаційного простору України і не тільки. Найефективнішим методом відсічення таких операцій є обмежувальні заходи (санкції) та дієвий механізм моніторингу і відповідальності за втручання в інформаційне середовище. Піддається сумнівам спроможність критичного мислення суспільства через недостатній рівень медіаграмотності за умов стрімкого поширення впливу соціальних мереж.

Національні виклики, загалом, відзначають інформаційний вплив держави-агресора на населення України. Безперечно, інформаційна напруга присутня й на тимчасово окупованих територіях України. Це є суттєвою проблемою для функціонування розвиненої національної інформаційної інфраструктури. Крім того, відсутній злагоджений механізм взаємодії між органами державної влади, що залучені до протидії загрозам в інформаційній сфері. Спроби впливу на свідомість громадян України у питанні європейської та євроатлантичної інтеграції країни також мають відбиток на суспільно-політичний стан в країні.

З цієї причини, були впроваджені стратегічні цілі та напрями забезпечення інформаційної безпеки. Стратегія, що розрахована до 2025 року, має забезпечити захищений інформаційний простір, ефективне функціонування системи стратегічних комунікацій; здійснення ефективної протидії поширенню незаконного контенту; забезпечення сталого процесу інформаційної реінтеграції громадян України, які проживають на тимчасово окупованих територіях України, та поширення українського телерадіомовлення на територіях України, прилеглих до тимчасово окупованих територій; суттєве підвищення рівня медіакультури та медіаграмотності населення; дотримання конституційних прав особи на вільне вираження своїх поглядів і переконань, захист приватного життя; забезпечення захисту прав журналістів; формування української громадянської ідентичності [8].

Проаналізувавши різновиди інформаційних впливів та їх наслідки можна з впевненістю стверджувати, що на кожний вплив є свій метод протидії. Попередній прийом захисту від інформаційної атаки – дія на випередження. Оперативно реагуючи на потенційні загрози, утворюється бар'єр в сприйнятті людиною неправдивої інформації. Цільова група, на яку був розрахований інформаційний вплив вже буде категорично ставитися до поданої інформації.

У випадку неочікуваної атаки з боку супротивника, виникає потреба в оперативному реагуванні вже на здійснений напад. Така ситуація вимагає інформації, що спростує та роз'яснить існуюче питання. Існує практика залучення ЗМІ або блогерів до спростовування інформаційного вкиду за допомогою контенту.

Також розглядають такі засоби придушення інформаційних атак як:

– обмеження доступу до певних ресурсів, вебсайтів або соціальних мереж;

– нейтралізація інформаційної бомби за допомогою штучного виникнення іншої, зазвичай більш сенсаційної та гучної;

– акцентування уваги на тому повідомленні, що має більш сприятливий вплив на суспільну думку;

– породження сумнівів щодо ресурсу поширення інформації або розповсюдження компромату;

– пряме спростування інформаційного повідомлення;

– ігнорування новини, мовчазна реакція;

– мінімізація негативу шляхом просування нейтральної або позитивної інформації про об’єкт;

– стимулювання імунітету в суспільства до негативу про об’єкт [17].

Як вже було зазначено в стратегії, основним аспектом зменшення впливу на думку людей є розвиток критичного мислення кожного з нас. Саме якісний аналіз та оцінка інформаційного потоку дозволить кожному з нас не піддаватися паніці та розрізняти факти від маніпуляцій думкою. Впровадження напряму підвищення медіаграмотності є аргументованим рішенням, оскільки лише ретельний вибір джерел інформації може сприяти розвитку критичного мислення суспільства [18].

3.2 Міжнародний досвід інформаційного протиборства

Інформаційне протиборство, як важливий аспект міжнародних відносин, стає все більш актуальним у сучасному світі, насиченому технологіями та засобами масової комунікації. Ця проблема знаходить відображення як у різноманітних політичних конфліктах, так і в економічній та культурній сферах. Зважаючи на це, міжнародний досвід у цьому питанні стає об’єктом дослідження та аналізу для розуміння принципів, методів та наслідків інформаційного протиборства.

Міжнародний досвід у сфері інформаційного протиборства демонструє різноманітні підходи та методи, використовувані для досягнення своїх цілей.

Суспільно-політичні та безпекові зміни, що стали помітними в Україні та світі протягом останніх років, підштовхнули до більшої інтеграції українського інформаційного простору у глобальному контексті. Відповідно до агресивних дій країни-агресора, яка проводить гібридну війну проти України, зросла потреба у відповідних заходах з протидії. Зокрема, необхідною стала побудова ефективної системи контролю за поширенням фейкової інформації, особливо тієї, що завдає шкоди національним інтересам. Це стало пріоритетом для багатьох демократичних країн, зокрема для країн Європейського Союзу, які вже відчули негативний вплив зовнішньої інформації.

Наприклад, в Німеччині за сприянням Гайко Йозефа Мааса, міністра юстиції та захисту прав споживачів, було створено робочу групу для розробки законопроекту з метою протидії поширенню фейкової інформації у соціальних мережах. Цей процес передував невдалим спробам домовитися з керівництвом компаній, таких як Facebook, Google і Twitter, щодо видалення шкідливого контенту. Проте результати були не задовільними, оскільки компанії не досягли мети у видаленні незаконного контенту у встановлені терміни.

У зв'язку з цим уряд Німеччини активізував розробку законопроекту, який регламентує поширення інформації в Інтернеті. Він визначає соціальні мережі як провайдерів телекомунікаційних послуг, які у комерційних цілях використовують інтернет-платформи для обміну контентом між користувачами.

Також в ньому визначено, що оператори соціальних мереж, які мають більше двох мільйонів зареєстрованих користувачів (переважно Twitter, Facebook та YouTube), повинні негайно (протягом 24 годин) реагувати на скарги шляхом видалення контенту, який однозначно містить протиправну інформацію (порушення відповідних розділів Кримінального кодексу Німеччини). Ця протиправна інформація може включати поширення пропагандистських матеріалів антиконституційного характеру, заклики до насильницьких злочинів, а також розпалювання ненависті та поширення зображень насильства. Навіть якщо особа, яка подає скаргу, не має особистого облікового запису, оператори все одно зобов'язані реагувати. У випадках, коли перший аналіз інформації не дозволяє однозначно визначити протиправність або потрібні додаткові дослідження для встановлення об'єктивної істини, термін реагування може бути збільшений до сьомі днів. Оператори соціальних мереж зобов'язані забезпечити зрозумілий та доступний для користувачів спосіб повідомлення про наявність негативного контенту. Вони також повинні надати користувачам можливість подавати скарги на негативний контент шляхом позначення постів або через форму зворотного зв'язку. У випадку, якщо механізм реагування на скарги користувачів щодо негативного контенту не буде ефективним, штрафи можуть становити до п'яти мільйонів євро для особи, відповідальної за організацію процедури розгляду скарг,

та до 50 мільйонів євро для компанії. Також можуть бути накладені штрафи, якщо мережа не виконає належним чином свої зобов'язання щодо звітності.

У Франції нижня палата французького парламенту, прийняла законопроект щодо «боротьби з маніпулюванням інформацією». У цьому законопроекті йдеться про регулювання «фейків», дезінформації, маніпуляцій, відвертої брехні та агресивної пропаганди, що розповсюджуються через ЗМІ або соціальні мережі.

Серед ключових та, можливо, контроверсійних положень (які гостро критикуються в медійному середовищі Франції), є розширення повноважень національного регулятора, Вищої аудіовізуальної ради, яка отримала право припиняти трансляцію телеканалів, що контролюються іноземною державою. Також у законі звертається увага на втручання іноземних держав та їх засобів масової інформації у виборчий процес.

Партіям та окремим кандидатам стає значно простіше подавати судові позови з вимогою припинення поширення фальсифікованої інформації. Суди зобов'язані розглядати такі справи протягом 48 годин.

Закон також містить спеціальні положення для соціальних мереж, зокрема Facebook та Twitter. Їм доручено надавати інформацію про замовний контент.

У Великобританії та Італії досить активно ведеться дискусія щодо нормативного регулювання поширення фейкової інформації. Між керівництвом Великої Британії та Республіки Польща було укладено домовленості про створення спільного підрозділу з протидії поширенню дезінформації, особливо з боку РФ.

Щодо колегіальних органів ЄС, було створено експертну групу, яка працює над критеріями фейкових новин та інструментами для боротьби з цим явищем. В Брюсселі було обговорено план ЄС щодо протидії дезінформації, який передбачає збільшення фінансування на ці цілі, збільшення кількості персоналу для протидії дезінформації та створення робочої групи зі стратегічних комунікацій. Також планується створення системи швидкого попередження, яка виявлятиме фейки та надаватиме правдиву інформацію.

Рада Європи працює над відповідними рекомендаціями. Комітет експертів розробив два проекти, які обговорюються медіаорганізаціями та експертами країн-

членів ЄС і стосуються підтримки сприятливого середовища для якісної роботи журналістів та підвищення медіа- та інформаційної грамотності в цифровому просторі.

У січні 2019 року Єврокомісія опублікувала перший звіт про протидію пропаганді, де згадується про успіхи у боротьбі з політичною дезінформацією інтернет-платформами, такими як Facebook, Google та Twitter.

З метою підвищення рівня обізнаності співробітників правоохоронних органів країн ЄС з новітніми технологіями боротьби з кіберзлочинністю діють відповідні курси на базі Європейського поліцейського коледжу у графстві Гемпшир, а також функціонує Об'єднаний центр передових технологій з кібер-оборони НАТО в місті Таллінні [19].

Варто також звернути увагу на те, що інформаційне протиборство може мати серйозні соціальні та психологічні наслідки. Зокрема, дезінформація та маніпуляція інформацією можуть призводити до поглиблення поділу в суспільстві, підривання довіри до державних та міжнародних інституцій, а також загрожувати демократичним цінностям та процесам.

У зв'язку з цим, ефективне протистояння інформаційному протиборству вимагає комплексного підходу та спільних зусиль з боку держав, міжнародних організацій, громадськості та приватного сектору. Це може включати розвиток механізмів виявлення та протидії дезінформації, підвищення кібербезпеки, підтримку незалежних ЗМІ та медіаосвіти, а також сприяння розвитку критичного мислення серед громадян.

3.3 Методика виявлення дезінформації

На сьогоднішній день існує безліч способів дізнатися будь-яку інформацію в світі. З розвитком мережі Інтернет, в людей з'явилася можливість слідкувати за новинами, отримувати інформацію та поширювати її, освоювати новий матеріал миттєво. З одного боку, це є беззаперечний плюс для розвитку суспільства. Але, в той же час, неконтрольований потік інформації формує думки та настрої

суспільства. Через це виникає необхідність у фільтруванні інформації яку ми споживаємо.

Було проведено величезну кількість досліджень, що підтвердили зростання залежності людей від соціальних мереж, Зокрема, в 2023 році громадянська мережа «Опора» визначила, що найпопулярнішим джерелом інформації для українців виступають соціальні мережі. Майже вісімдесят відсотків опитуваних споживають інформацію через соціальні мережі [20]. Звісно, обмаль повідомлень, що поширюються в мережевому просторі є неперевіреними та фейковими. Однією з причин виступає легка можливість будь-кому розповсюдити провокативну інформацію без ретельного аналізу її джерела. Тому виникає нагальна потреба в актуалізації питання виявлення дезінформації в нашому інфопросторі.

По-перше, слід зазначити, що відповідно до концепції ЮНЕСКО, поняття дезінформації потрібно розглядати в сукупності ще з такими термінами як недостовірна інформація та шкідлива інформація. Суть дезінформації поділяють на:

– хибна(не відповідаючи дійсності);

– маніпулятивна(маюча на меті вплив на психіку людей);

– сфабрикована(вигадана навмисно);

– безпідставна(з прихованим або відсутнім джерелом).

Недостовірна інформація – така інформація, що має хибний та дезорієнтуючий зміст. Шкідлива інформація, в свою чергу, відзначається завданням причинити шкоду населенню. Може включати в себе витоки даних та формування ненависті.

Дезінформація об’єднує в себе ці поняття. Зазвичай, мета її створення – отримання певних економічних, політичних та інших переваг. Процесом розповсюдження дезінформації називають дезінформуванням.

Задля розуміння щодо побудови методів виявлення дезінформації, також необхідно розрізняти існуючі форми та методи поширення. Форми дезінформації поділяються на: текстовий, відео та аудіо контент. Методи поширення –

координована неавтентична поведінка (боти), таргетинг, діпфейки та фейкові новини.

Розглянемо види дезінформації більш детально. Текстовий формат є найпростішим для створення. Його можна побачити у багатьох соціальних мережах. Відеоконтент у 2024 році, зважаючи увагу на швидкий розвиток соціальних мереж, що базуються на відеопостингу, є навіть більш дієвим, аніж текстовий. Аудіоконтент розповсюджується на радіо або у подкастах.

Координована неавтентична поведінка характеризується аномальною кількістю фейкових акаунтів, що розповсюджують певні інформаційні повідомлення. Зазвичай це можуть бути інформаційні бомби або сенсаційні гучні заголовки. Як результат, читачі цих новостворених акаунтів, стають жертвами інформаційного впливу.

Мета таргетованих повідомлень – поширити дезінформацію серед тих людей, чия думка буде найбільш вразлива. Аналізуються дані про вподобання особи або її політичні погляди шляхом моніторингу підписок, лайків, коментарів, мережевого трафіку тощо.

Діпфейки є новим видом дезінформації. З розвитком штучного інтелекту, в Інтернеті було розповсюджено величезну кількість фейкових аудіо та відеоконтенту. Такий контент називають діпфейками, що можуть ввести в оману звичайного користувача [21].

Фейкові новини розповсюджуються з метою дисбалансу політичних поглядів суспільства. Серед фейкових новин розрізняють впливові, сатиричні та клікбейт. Задля нейтралізації фейкових новин можуть бути застосовані такі засоби як виявлення спаму або набір еталонних даних.

Існують такі методи виявлення фейкових новин:

– аналіз джерела повідомлення(перевірка URL адреси та доменного імені за допомогою сервісу Whois);

– дослідження вмісту та заголовку новини(зосередження уваги на поданих фактах та оцінках, перевірка присутності гучних заголовків та використання сумнівних фото та відео, що можна дослідити за допомогою сервісу Exif Data);

– вивчення діяльності автора матеріалу(визначення причини висвітлення цієї теми автором, перевірка чи не заангажованим є матеріал);

– перевірка актуальності новини(акцентування уваги на свіжому матеріалі чи повідомленні).

– оцінка правдивості інформаційного повідомлення на вебсайтах перевірки фактів(використання таких фактчекінгових ресурсів як FactCheck.org, Snopes.com задля пошуку англійською мовою та Google Fact Check Explorer задля пошуку українською відповідно).

Загалом, типовими ознаками фейкового повідомлення є: представлення думок як об'єктивних фактів; заголовок, що не відповідає змісту новини або містить надмірну емоційність; використання усталених стереотипів [21].

Існує три підходи виявлення фейкових новин:

1) На основі знань. Цей підхід базується на фактчекінгу, який передбачає використання трьох зовнішніх джерел для перевірки правдивості новини.

2) На основі стилю. Цьому підходу характерне виявлення маніпулятивних прийомів. Стильові методи бувають орієнтовані або на об'єктивність, або на обман.

3) На основі позиції. Підхід, що акцентує увагу на точку зору автора, щоб встановити правдивість первинної новини.

4) На основі розповсюдження. Цей підхід аналізує взаємозв'язки постів в соціальних мережах для того, щоб передбачити достовірність повідомлень.

Більшість експериментів було проведено із застосуванням ознак текстових повідомлень. А саме: семантичні ознаки – ознаки, що фіксують смислову нагрузку тексту, виводять шаблон значень з даних; лексичні ознаки – ознаки, що здебільшого використовуються у векторизації tf-idf для узагальнення загальної кількості унікальних слів та частоти слів; ознаки на рівні речень – мовна ознака, що класифікує будову речення, виокремлює частини мови, частини речення та будову слова; психолінгвістичні ознаки – такі ознаки, що базуються на програмному забезпеченні, включають в себе словники.

Слід зазначити, що існують такі методики виявлення дезінформації, як використання наївного метод Баєса, методу опорних векторів та нейронну мережу. Усі класифікатори, використовували вищезазначені ознаки.

Наївний метод Баєса – ймовірнісний класифікатор, що був заснований на незалежній класифікації ознак. Головна ідея застосування наївного класифікатора – розглядати кожне окреме слово в матеріалі незалежно одне від одного.

На прикладі фейкової новини [22], розглянемо як можна застосувати формулу Баєса

$$P(A|B) = \frac{P(B|A)\times P(A)}{P(B)}, \text{ де} \qquad (1.1)$$

– $P(A)$ – апріорна ймовірність події А, тобто втеча голови ОВА;

– $P(B|A)$ – ймовірність, що інформація правдива, за умови реальної втечі голови ОВА;

– $P(B|\neg A)$ – ймовірність того, що така інформація з’явиться, але голова ОВА не втік.

Загалом, для належної перевірки цієї новини треба застосувати підходи, що ми розглядали раніше. Зокрема:

1) Аналіз джерела походження інформації: портал походить з країни агресора, підтвердження на українських ресурсах або серед офіційних представників влади відсутнє;

2) Дослідження змісту та заголовку: в поданій новині присутній лише текстовий контент, фото-підтвердження події не надається, в тексті акцентується увага, що новина, була взята з іншого ресурсу, а також наводиться цитування. Наприклад: «пишут, что он покинул Харьков», тобто повідомлення подається без автора, що також ставить під сумнів автентичність новини;

3) Перевірка стилю написання: в матеріалі новини присутній маніпулятивний тон подання інформації, зокрема замість надання підтвердження події, надається побічна інформація, що не стосується первинної новини.

На рисунку 3.1 зображено сгенеровану схему, за допомогою якої ми можемо проаналізувати повідомлення різного типу.

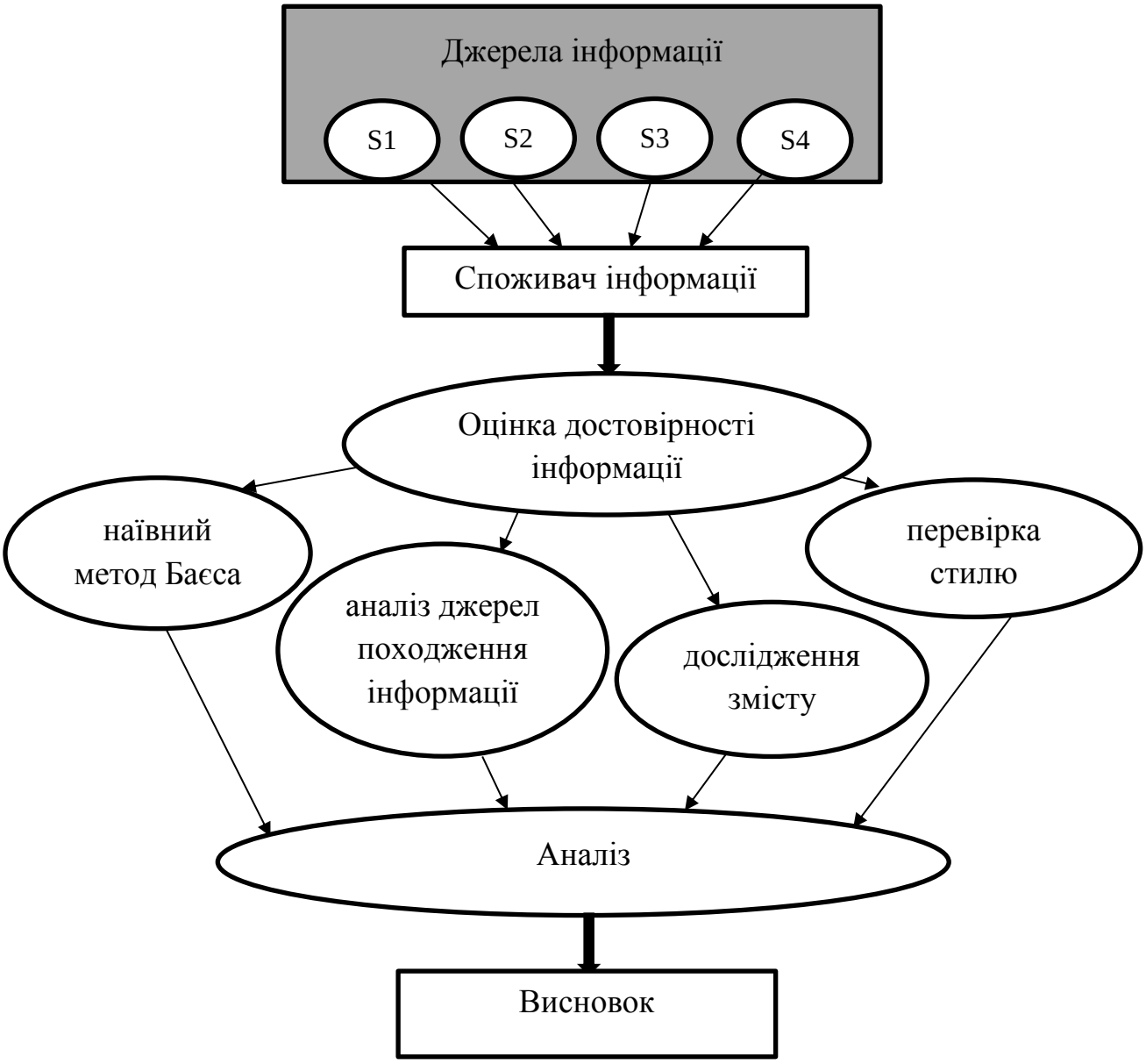

Рисунок 3.1 – Схема обробки повідомлення

Відповідно до схеми, де s1, s2, s3, s4 – джерела інформації, зображено процес обробки інформаційного потоку людиною, що не стане жертвою інформаційних впливів (на прикладі розглянутого повідомлення).

Провівши ретельний аналіз повідомлення, можемо визначити, що подана новина є підготовленою заздалегідь дезінформацією з метою навіювання паніки в суспільстві, введення в оману громадян та дискредитації влади.

Отже, підсумовуючи усе вищесказане, можемо зробити такий висновок, що коли людина має критичне мислення – вона не стане жертвою маніпуляції.

У випадку, коли вона розуміє що певна новина є неправдивою, вона вже не стане об’єктом маніпуляції.

ВИСНОВКИ

Інформаційні впливи відіграють вагому роль в формуванні поглядів суспільства. Провідні країни світу розробили свої стратегії протидії існуючим загрозам, закріплюючи це на законодавчому рівні. Особливу небезпеку створюють засоби інформаційного впливу на український інформаційний простір.

Під час виконання кваліфікаційної роботи були проаналізовані основні методи інформаційного впливу, а саме інформаційно-психологічні операції та кібернетичні атаки. В контексті інформаційного конфлікту, інформаційний простір країни став потенційним вразливим місцем. Перешкодами для нормального функціонування усіх державних структур є різного виду інформаційні атаки збоку ворога.

Актуальними питаннями є визначення основних завдань інформаційного впливу, а саме це маніпулювання думкою, дестабілізація суспільного стану, створення загроз інформаційній безпеці тощо. На сьогоднішній день існує багато методів протидії інформаційним атакам. Було розглянуто такі можливості як забезпечення кібербезпеки, вдосконалення алгоритмів фільтрації інформації, а також підвищення медіа-грамотності серед населення. Зокрема, важливим є розвиток та підтримка критичного мислення серед громадян, що дозволяє відрізняти об’єктивну інформацію від маніпуляцій та пропаганди.

В результаті дослідження даної теми в межах роботи було розглянуто стратегії, методи та запропоновано відповідний алгоритм протидії маніпулюванню думкою в інформаційному суспільстві, що є одним із завдань кваліфікаційної роботи.

Аналізуючи кваліфікаційну роботу, можемо зробити такий висновок, що є необхідність у співпраці з міжнародними партнерами у сфері кібербезпеки та обмін досвідом у протидії інформаційним загрозам. Важливою складовою є також здатність правоохоронних органів ефективно реагувати на кібернетичні атаки та здійснювати швидке реагування на появу нових загроз. Тільки комплексний підхід до проблеми може забезпечити ефективний захист інформаційної безпеки країни.

ПЕРЕЛІК ПОСИЛАНЬ

1. Зіменко О.В., Інформаційний вплив: поняття та еволюція в сучасній науковій думці. *Вісник ХДАК. Випуск 60.* 2021 URL: https://doi.org/10.31516/2410-5333.060.02
2. Мельникова-Курганова О.С., Засоби інформаційного впливу під час війни: типи, трансформація, тенденції. URL: http://surl.li/trupm
3. Жаровська, І., & Ортинська, Н. (2020). Інформаційна війна як сучасне глобалізаційне явище. *Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки*, (2 (26)), С. 56-61. URL: http://doi.org/10.23939/law2020.26.056
4. Антонюк, В. В. (2021). Інформаційна війна в структурі сучасного геополітичного протиборства: нові контексти та інтерпретації. URL: http://www.dy.nayka.com.ua/pdf/7_2021/35.pdf
5. Яковчук, В. С., Борзов Ю.О, Малець Б. І., Інформаційні війни в сучасному світі. Diss. Захист інформації в інформаційно-комунікаційних системах: збірних тез доповідей IV Всеукраїнської науково-практичної конференції молодих вчених, курсантів та студентів. – Львів, ЛДУ БЖД, 2020. URL: http://surl.li/bevva
6. Почепцов Г. Г., Від покемонів до гібридних війн: нові комунікативні технології XXI століття. К.: *Видавничий дім «Києво-Могилянська академія»*, 2017. 260 с.
7. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Дата оновлення 21.03.2023р. № 3005-IX URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
8. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.2021р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text
9. Кушко А. М. Актуальні проблеми законодавчого регулювання в сфері інформаційної безпеки. Суспільство та держава в умовах воєнного стану: виклики та перспективи, 27 квітня 2024 р. Одеса, 2024

10. Залкін С. В.; Хударковський К. І., Використання штучного інтелекту в інформаційно-психологічних операціях. Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку, 2020, С.187-188 URL: http://surl.li/truyf
11. Анісімович-Шевчук О. З., Сучасні інформаційно-психологічні впливи в системі міжнародних відносин у контексті російсько-української війни 2014-2022 років. URL: https://doi.org/10.30525/978-9934-26-262-3-6
12. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017р. № 2163-VIII. Дата оновлення 16.01.2024р. № 3549-IX URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
13. Ткачук К. О., Гамова І. В. Кібернетична війна як різновид інформаційної війни. URL: http://doi.org/10.31617/k.knute.2019-03-19.68
14. Особливості класифікації різновидів інформаційної війни. URL: http://surl.li/twypb
15. Дмитрук Я. В., Гришанович Т. О., Гринчук Л. Я., Жигаревич О. К., Кібервійна як різновид інформаційних війни. Захист кібепростору України. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2022, 4.16: 28-36. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/361/308
16. Мережеві війни. URL: http://psychologis.com.ua/Cetevye_voyny.htm
17. Вакуленко Р. В. «Огляд та аналіз методів протидії інформаційним впливам супротивника в умовах інформаційної війни.», 2016. URL: https://core.ac.uk/download/pdf/84825417.pdf
18. Протистояння інформаційним війнам та пропаганді у сучасному світі. URL: http://surl.li/twypr
19. Черниш Роман. Правовий досвід країн європейського союзу у сфері протидії поширенню фейкової інформації. *Інформаційне право*, 2019, 10: 123-128. URL: https://doi.org/10.32849/2663-5313/2019.10.21
20. Медіаспоживання українців: другий рік повномасштабної війни. Опитування ОПОРИ. URL: http://surl.li/twyja

21. Тищенко В. С., Мужанова Т. М., Дезінформація і фейкові новини: ознаки та методи виявлення в мережі інтернет. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2022, 2.18: 175-186. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/413/341
22. Голова Харківської ОДА Олег Синегубов втік із міста – паблики. URL: http://surl.li/twyrp