ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ МЕНЕДЖМЕНТУ ТА ПІДПРИЄМНИЦТВА
КАФЕДРА ДОКУМЕНТОЗНАВСТВА ТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

КВАЛІФІКАЦІЙНАРОБОТА
на тему:« ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ: ПРОТИДІЯ ВОРОЖІЙ ПРОПАГАНДІ»

на здобуття освітнього ступеня магістра

зі спеціальності 029 Інформаційна, бібліотечна та архівна справа

освітньо-професійної програми Управління інформаційно-комунікаційною діяльністю

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Володимир НОВАК

Виконав: здобувач вищої освіти
групи ДЗДМ-61
Володимир НОВАК
Керівник: Володимир Даниленко, к.філол.н., доц.
Рецензент: Світлана Стежко, к.філол.н., доц.

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут менеджменту та підприємництва
Кафедра документознавства та інформаційної діяльності

рівень вищої освіти другий «Магістр»

спеціальність 029 Інформаційна, бібліотечна та архівна справа

освітня програма: Інформаційна аналітика та зв'язки з громадськістю

форма навчання: денна

ЗАТВЕРДЖУЮ
Завідувач кафедри документознавства
та інформаційної діяльності
_____Т. М. Сидоренко
«___» _____2024 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Новака Володимира Валерійовича

1. Тема роботи: «Інформаційна безпека України: протидія ворожій пропаганді». Керівник кваліфікаційної роботи: Володимир ДАНИЛЕНКО, к.філол.н., доц. каф., затверджено наказом Державного університету інформаційно-комунікаційних технологій від «15» жовтня 2024 року № 320.
2. Строк подання студентом роботи: 15 грудня 2024 р.
3. Вихідні дані про роботу: дослідження ролі українських ютубканалів в боротьбі з російськими історичними міфами.

Об'єкт дослідження: російсько-українська інформаційна війна.

Предмет дослідження: технології протидії російській інформаційній війні.

4. Перелік питань, які потрібно розробити:

1. Теоретичні основи інформаційної безпеки.
2. Аналіз сучасного стану інформаційної безпеки України.
3. Шляхи вдосконалення системи інформаційної безпеки України.

4. Перелік ілюстративного матеріалу: презентація

5. Дата видачі завдання: «07» вересня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення тематики, вибір наукового керівника, уточнення теми	09.09.2024	виконано
2.	Розроблення та складання плану кваліфікаційної магістерської роботи	17.09.2024	виконано
3.	Підготовка 1 розділу	08.10.2024	виконано
4.	Підготовка 2 розділу	29.10.2024	виконано
5.	Підготовка 3 розділу	22.11.2024	виконано
6.	Висновки	29.11.2024	виконано
7.	Підготовка остаточного варіанту роботи	12.12.2024	виконано
8.	Написання відгуку науковим керівником	13.12.2024	виконано
9.	Оформлення та представлення роботи на кафедру та перевірка на плагіат	16.12.2024	виконано
10.	Підготовка доповіді, презентації та ілюстративного матеріалу, рецензія	18.12.2024	виконано
11.	Попередній захист роботи	20.12.2024	виконано
12.	Основний захист кваліфікаційної магістерської роботи	23.01.2025	виконано

Здобувач вищої освіти _____ Василь ЧОРНОМАЗ
Науковий керівник роботи _____ Володимир ДАНИЛЕНКО

ЗМІСТ

ВСТУП

У сучасному світі інформаційна безпека набуває надзвичайно важливого значення, особливо в умовах зростання масштабів інформаційного впливу, поширення дезінформації та пропаганди. Інформаційний простір став не лише середовищем для комунікації, а й полем для ведення гібридних війн, де вирішуються стратегічні питання національної безпеки. Для України, яка вже тривалий час перебуває в стані збройного протистояння та інформаційної агресії з боку Російської Федерації, питання протидії ворожій пропаганді є одним із ключових аспектів забезпечення державного суверенітету та цілісності.

Ворожа пропаганда є багатовекторним інструментом, який спрямований на маніпулювання суспільною думкою, підрив довіри до державних інституцій, розпалювання міжетнічних, релігійних та соціальних конфліктів. Її методи постійно вдосконалюються, включаючи використання соціальних мереж, онлайн- медіа, а також спеціально створених платформ для поширення фейкової інформації. Водночас, низький рівень інформаційної культури населення, слабкість регуляторних механізмів та недостатня координація державних органів створюють додаткові виклики для протидії цьому явищу.
Актуальність теми обумовлена не лише воєнними діями на сході України, але й систематичними спробами впливу на український інформаційний простір, які тривають вже багато років. Пропагандистські кампанії Російської Федерації мають на меті дискредитацію європейського курсу України, формування негативного іміджу держави на міжнародній арені, а також вплив на виборчі процеси та внутрішньополітичну стабільність. Це ставить перед Україною завдання створення ефективної системи протидії, яка поєднувала б технічні, правові, соціальні та освітні інструменти.

У даній магістерській роботі основна увага зосереджена на аналізі сучасних викликів інформаційної безпеки України у контексті боротьби з

ворожою пропагандою, дослідженні існуючих механізмів протидії та розробці рекомендацій щодо їх вдосконалення.

Предметом дослідження є методи та інструменти, що використовуються для протидії інформаційним загрозам.

Об'єктом є інформаційний простір України в умовах гібридної війни.

Мета роботи: полягає у визначенні ключових загроз, пов'язаних із ворожою пропагандою, оцінці ефективності державних заходів і розробці рекомендацій щодо їхнього вдосконалення.

Завдання дослідження включають:

- розкрити поняття та значення інформаційної безпеки в сучасному світі;
- виявити та проаналізувати основні загрози інформаційній безпеці України;
- дослідити нормативно-правову базу забезпечення інформаційної безпеки в Україні;
- дослідити стан та динаміку розвитку кібербезпеки;
- проаналізувати проблему дезінформації та впливу пропаганди на інформаційний простір України;
- дати оцінку ефективності державних заходів у сфері інформаційної безпеки;
- дослідити інтеграцію сучасних технологій кіберзахисту;
- визначити та проаналізувати роль міжнародної співпраці у забезпеченні інформаційної безпеки України;
- проаналізувати та надати рекомендації щодо підвищення інформаційної культури населення та боротьби з дезінформацією.

Практична значущість роботи полягає в можливості використання її результатів для вдосконалення державної політики у сфері інформаційної безпеки, формування ефективних комунікаційних стратегій, підвищення рівня інформаційної культури населення, а також посилення міжнародної співпраці у сфері протидії пропаганді.

Таким чином, дослідження має на меті зробити внесок у створення стійкої системи захисту національного інформаційного простору, що є невід’ємною частиною забезпечення безпеки та стабільності держави.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

1.1. Поняття та значення інформаційної безпеки в сучасному світі.

У сучасну епоху цифрових технологій інформація стала стратегічним ресурсом, а її безпека – критично важливим елементом стабільності й розвитку будь-якого суспільства. Інформаційна безпека охоплює комплекс заходів, спрямованих на захист інформаційних ресурсів і систем від внутрішніх та зовнішніх загроз, які можуть порушити їхню цілісність, конфіденційність і доступність. Ця сфера є ключовою не лише для держав, але й для приватного сектору та громадян, адже інформація нині впливає на політику, економіку, соціальні процеси та особисте життя.

Інформаційна безпека є ключовим елементом загальної національної безпеки в умовах інформаційного суспільства. Розвиток інформаційних технологій, глобалізація комунікацій та зростання залежності суспільства від інформаційних систем зробили питання забезпечення інформаційної безпеки пріоритетом для більшості держав. Це поняття охоплює широкий спектр аспектів, починаючи від захисту державних і корпоративних інформаційних систем до забезпечення прав людини на доступ до правдивої інформації. Інформаційна безпека визначається як стан захищеності інформації, інформаційних систем і інфраструктури від несанкціонованого доступу, використання, поширення або знищення.
Основу цього поняття складають три основні принципи:

1. **Конфіденційність** – гарантування того, що доступ до інформації мають лише уповноважені особи;
2. **Цілісність** – забезпечення точності, повноти та захисту інформації від несанкціонованих змін;
3. **Доступність** – забезпечення доступу до інформаційних ресурсів у визначений час для тих, хто має на це право;

Інформаційна безпека включає в себе такі ключові складові як захист цифрових систем і мереж, тобто кібербезпека, бо кібератаки можуть завдати шкоди державним, комерційним та приватним ресурсам. Захист від несанкціонованого використання або знищення приватних даних користувачів.

Для того, щоб протистояти кіберзлочинам, держава або організація, що займається обробкою та збереженням даних повинні бути здатні протистояти інформаційним атакам та маніпуляціям. В наш час держава повинна створити законодавчу базу для боротьби з інформаційними злочинами, такими як кіберзлочинність та поширення дезінформації.

В Україні великий відсоток населення складають пенсіонери або люди які необізнані в необхідності бути захищеними від кібератак, тому держава повинна створити базу для підвищення інформаційної культури серед населення

В сучасних умовах значення інформаційної безпеки нашої держави відіграє вкрай важливу роль, захист суверенітету, у багатьох країнах інформаційна безпека розглядається як частина національної безпеки. Сучасні загрози, зокрема кібератаки, маніпуляції громадською думкою та втручання у виборчі процеси, можуть порушити стабільність держави. Для України, яка перебуває під інформаційною агресією Російської Федерації, це питання має стратегічне значення.

Ще ключовим фактором є підтримка стабільності суспільства, так як дезінформація та пропаганда здатні створювати конфлікти в суспільстві, підривати довіру до державних інституцій та медіа. Інформаційна безпека сприяє збереженню громадянського миру та соціальної стабільності, забезпечуючи доступ до достовірної інформації. Громадяни повинні розуміти, що їх дані під захистом, Захист персональних даних і приватності є важливим аспектом інформаційної безпеки. В епоху, коли інформація про кожну людину зберігається у цифровій формі, порушення безпеки таких даних може призвести до серйозних наслідків, включаючи фінансові втрати чи порушення прав на приватність.

Для державних установ є важлива економічна безпека, зараз економіка багатьох держав базується на функціонуванні інформаційних систем. Кібератаки на фінансові установи, енергетичні системи та транспортну інфраструктуру можуть завдати значних збитків. Інформаційна безпека забезпечує стабільність і безперервність економічних процесів.

З швидким розвитком технологій, зростає кількість кібератак, тому інформаційна безпека є важливим компонентом боротьби з транснаціональними загрозами, такими як міжнародний тероризм і організована кіберзлочинність. Глобальна координація між державами в цій сфері дозволяє ефективніше протистояти таким викликам.

Таким чином інформаційна безпека є одним із ключових факторів для розроблення національної стратегії абсолютно для кожної держави світу.

Для забезпечення інформаційної безпеки необхідно розробити ефективну національну стратегію, яка б включала в себе розвиток законодавчої бази для боротьби з інформаційними злочинами, наприклад коли людину звинувачують у скоєнні кіберзлочину і всі докази вказували на неї, щоб ця людина не змогла уникнути покарання та понесла справедливе покарання. Створення спеціалізованих органів для реагування на кіберзагрози, таких як CERT-UA, інвестиції в технології захисту інформаційних систем і мереж, підвищення рівня інформаційної грамотності населення, що зменшить вразливість до дезінформації.

Україна вже зробила значні кроки в цьому напрямі, впроваджуючи національні програми з кіберзахисту та активізуючи міжнародну співпрацю. Зокрема, активний розвиток України у сфері кіберзахисту зумовив інцидент, що трапився 27 червня 2017 року, коли кілька українських компаній повідомили про проблеми з доступом до своїх комп’ютерних систем і даних. Спочатку це здавалося черговою атакою програми-вимагача, подібною до WannaCry, що мала глобальні наслідки раніше того ж року. Проте більш глибокий аналіз показав, що NotPetya була набагато складнішою і небезпечнішою.

На відміну від звичних вірусів-вимагачів, NotPetya не мала на меті вимагати викуп за відновлення доступу до файлів. Замість цього, вона використовувала шифрування, щоб безповоротно знищити дані. Це стало зрозуміло лише після того, як атака поширилася на інші країни, і компанії з різних регіонів почали відзначати подібні проблеми.

Експерти вважають, що основною мішенню атаки була Україна, де вона виявилася особливо потужною. Вірус використовував вразливості в популярному в Україні програмному забезпеченні, що дозволило йому поширюватися в різні сектори економіки, зокрема енергетику, транспорт, фінанси і державні установи. Методи атаки та технічний аналіз NotPetya використовувала кілька методів для проникнення в комп'ютерні системи.

Вірус поширювався через вразливості в бухгалтерській програмі «M.E.Doc», популярній в Україні. Це дало змогу хакерам впровадити шкідливий код, який потрапив у корпоративні мережі. Крім того, атака використовувала інструмент EternalBlue, який також застосовувався під час WannaCry. Цей інструмент експлуатував уразливості в операційних системах Windows, що дозволяло зловмисникам запускати шкідливий код без взаємодії з користувачем. Вірус був спроектований таким чином, щоб після початкового проникнення він міг швидко поширюватися через внутрішні мережі, використовуючи техніки «латентного виявлення». Це дозволило NotPetya охопити велику кількість комп’ютерів і серверів.

Масштаб і наслідки атаки NotPetya завдала значних збитків як Україні, так і іншим країнам. Хоча найбільше постраждала Україна, атака також торкнулася компаній у США, Великобританії, Німеччині та Росії. В Україні порушилося функціонування багатьох державних установ, зокрема банків, енергетичних компаній і міністерств. Багато підприємств змушені були припинити свою діяльність через знищення або блокування важливих даних. З економічної точки зору, атака принесла значні втрати. Великі українські компанії втратили доступ до даних і витратили мільйони доларів на відновлення своїх систем. Загальні економічні збитки в Україні оцінюються в

мільярди доларів. Крім того, атака порушила стабільність банківської та енергетичної інфраструктури, що могло мати серйозні наслідки для національної безпеки.

У цілому, атака показала глобальний характер кіберзагроз і підкреслила необхідність міжнародної співпраці у боротьбі з кібертероризмом.

Отже, інформаційна безпека в сучасному світі є основою стабільного розвитку держави та суспільства. Вона впливає на політичну, економічну й соціальну сфери, забезпечуючи захист національних інтересів, прав громадян та безперебійну роботу критичної інфраструктури. Для України, яка перебуває під постійним інформаційним тиском, розвиток ефективної системи інформаційної безпеки є стратегічним завданням. Це потребує комплексного підходу, що включає технічні, правові, освітні та міжнародні аспекти.

1.2. Основні загрози інформаційній безпеці України (кіберзагрози, дезінформація, втручання в інформаційний простір).

Інформаційна безпека України постійно зазнає впливу численних загроз, які ставлять під удар національну безпеку, громадську стабільність та роботу критично важливих інфраструктур. До головних викликів належать кіберзагрози, дезінформація та зовнішнє втручання в інформаційний простір. Ці явища є невід’ємною частиною гібридної війни, спрямованої проти України, і становлять серйозну проблему як для держави, так і для суспільства.

Тому зараз більш детальніше обговоримо кожну із загроз для інформаційної безпеки України.

Загалом усі загрози для інформаційної безпеки України називають кіберзагрозами, які насамперед належать до найбільш серйозних викликів для інформаційної безпеки України, оскільки можуть завдати значної шкоди критично важливій інфраструктурі, державним органам та приватному сектору. Також кіберзагрози поділяють на різні типи, а саме:

1. Кібератаки на критичну інфраструктуру.

Критична інфраструктура, така як енергетика, транспорт, фінанси, медицина та телекомунікації, часто стає основною мішенню кібератак. Яскравим прикладом є атака на енергетичні об'єкти України в грудні 2015 року, організована угрупованням "Sandworm", яка спричинила масштабне відключення електроенергії. Такі випадки показують, що дії зловмисників можуть не лише завдати серйозних економічних втрат, але й становити пряму загрозу для життя людей.

2. Використання шкідливого програмного забезпечення.

Російські хакерські угруповання, зокрема «APT28», «Gamaredon» та інші, активно використовують шкідливе програмне забезпечення для здійснення кібершпигунства, знищення даних або виведення з ладу інформаційних систем. Наприклад, вірус «NotPetya», що атакував Україну у 2017 році, спричинив мільярдні збитки не лише для українських установ, а й для міжнародних компаній.

3. Кіберзлочинність.

Також загрозу становлять організовані кіберзлочинні угруповання, які здійснюють атаки з метою викрадення даних, фінансових шахрайств та вимагання через програмне забезпечення типу ransomware.

4. Уразливість інформаційних систем.

Багато державних і приватних інформаційних систем України все ще мають недостатній рівень захисту через використання застарілих технологій, обмежене фінансування кібербезпеки та відсутність достатньої кількості кваліфікованих спеціалістів.

Другим важливим фактором, що становить небезпеку для інформаційної безпеки нашої країни є дезінформація, яка є потужним інструментом інформаційної війни, що використовується для впливу на суспільну свідомість, маніпуляції громадською думкою та підриву довіри до державних інституцій.

Серед основних цілей дезінформаційних кампаній можна виокремити наступні:

1. Підрив суверенітету держави: Створення образу України як «недієздатної країни».

2. Дискредитація органів влади та демократичних інститутів: Зменшення довіри громадян до уряду, парламенту, армії та судів.

3. Поляризація суспільства: Підбурювання до міжетнічних, міжрелігійних і політичних суперечок.

4. Вплив на міжнародну спільноту: Поширення негативного іміджу України з метою зниження підтримки з боку міжнародних партнерів.

Сьогодні, коли найактивніша частина населення проводить багато часу в інтернет просторі дезінформація поширюється багатьма різними методами, а саме через соціальні мережі, шляхом використання фейкових акаунтів, ботів і тролів для масового поширення неправдивої інформації.

Досить розповсюдженим методом поширення дезінформації залишаються звісно і підконтрольні медіа. Використання медійних ресурсів, таких як телеканали RT, Sputnik та інші, для трансляції пропагандистських повідомлень.

Також варто виокремити й створення вигаданих історій, що дискредитують державу, її інституції чи окремих осіб, так звані фейкові новини, які в свою чергу мають достатньо великий вплив дезінформації на суспільство.

Дезінформація збільшує соціальну напругу, знижує рівень інформаційної обізнаності та формує спотворене уявлення про реальний стан справ. Це веде до втрати довіри до офіційних джерел інформації і становить загрозу національній безпеці.

Втручання в інформаційний простір — це ще один вид агресії, що полягає у використанні технологій і методів для маніпулювання інформаційним середовищем.

Російські інформаційні кампанії проти України охоплюють організацію дезінформаційних акцій, маніпулювання медійними темами та створення інформаційних пасток для міжнародної аудиторії. Основною їхньою метою є змінити політичні пріоритети, посіяти розбрат у суспільстві та підірвати довіру до західних партнерів.

Соціальні мережі виступають головним інструментом для маніпуляцій. Завдяки алгоритмам платформ, таких як Facebook, Twitter чи Telegram, агресор може поширювати пропаганду серед мільйонів користувачів. Для цього активно застосовуються ботоферми, які допомагають накручувати "вподобання" або створювати «штучні» обговорення.

Окрім дезінформації, агресори активно збирають дані про урядові установи, військові об’єкти та приватний сектор через кібершпигунство. Це дозволяє отримати стратегічну інформацію, яка може бути використана для подальших атак.

Також варто приділити увагу й технологіям глибоких фейків (deepfake), які дають змогу створювати фальшиві відео та аудіозаписи, які виглядають дуже реалістично. Це створює загрозу підробки заяв офіційних осіб, що може викликати суспільне обурення або дипломатичні суперечки.

Україна в свою чергу досить активно протидіє вищезазначеним загрозам, а саме основними заходами є:

- **розвиток кібербезпеки**: Діяльність CERT-UA, створення кіберпідрозділів у державних структурах;
- **попередження дезінформації**: Використання фактчекінгових платформ, таких як StopFake, а також ініціатив із медіаграмотності;
- **міжнародна співпраця**: Участь у програмах кіберзахисту НАТО, співпраця з ЄС у сфері інформаційної безпеки;
- **підвищення інформаційної стійкості населення**: Освітні кампанії та поширення інформації про те, як розпізнавати фейки та захищати свої персональні дані.

Таким чином можна виділити основні загрози інформаційній безпеці України, такі як кіберзагрози, дезінформація та втручання в інформаційний простір, вимагають комплексного підходу до їхнього усунення. Ефективна протидія цим загрозам є основою для стабільності держави, її розвитку та збереження інформаційного суверенітету. Україні слід

продовжувати удосконалювати систему інформаційної безпеки, адаптуючи її до нових реалій і залучаючи міжнародний досвід.

1.3. Нормативно-правова база забезпечення інформаційної безпеки в Україні (аналіз законів, стратегій, міжнародних угод).

Нормативно-правова база забезпечення інформаційної безпеки в Україні охоплює закони, стратегії, концепції, міжнародні угоди, а також інші акти, які регулюють питання захисту інформаційного простору. Вона визначає, хто і як має діяти для захисту національних інформаційних ресурсів, а також організує співпрацю між державними структурами, приватним сектором та міжнародними партнерами.

Захист інформації є важливою складовою національної безпеки, оскільки інформація є стратегічним ресурсом, а її захист має прямий вплив на економічну, політичну та соціальну стабільність країни. Нормативно-правова база забезпечення інформаційної безпеки в Україні є ключовим елементом національної безпеки, оскільки ефективний захист інформаційного простору країни залежить від адекватного правового регулювання. З огляду на швидкий розвиток інформаційних технологій та нових загроз у цій сфері, Україна постійно вдосконалює законодавство, приймаючи нові закони, стратегії та міжнародні угоди.

Основою для забезпечення інформаційної безпеки є національне законодавство, яке регулює діяльність у цій сфері. На сьогодні в Україні є кілька ключових законів, що визначають правила роботи з інформацією та інформаційними системами.

Закон України «Про основи національної безпеки України» це закон, що є основою національної безпеки та визначає пріоритети в різних сферах, зокрема в інформаційній безпеці. Він розглядає інформаційну безпеку як важливу частину національної безпеки, що передбачає захист інформаційних систем, ресурсів і технологій від зовнішніх і внутрішніх загроз. Ключовою частиною

закону є концептуальні підходи до захисту від кіберзагроз та забезпечення інформаційного суверенітету.

Інший не менш важливий закон, є Закон України «Про інформацію», який регулює доступ до інформації та визначає права і обов'язки учасників інформаційних відносин. Однією з ключових його положень є те, що інформація є стратегічним ресурсом для держави, а її захист — важливою частиною національної безпеки. Закон також встановлює правила використання та обробки інформаційних ресурсів, захисту персональних даних і визначає відповідальність за порушення прав на інформацію.

Закон України «Про захист персональних даних», що забезпечує захист персональних даних громадян України, а також регулює питання збору, обробки та зберігання таких даних. Захист персональних даних є важливою складовою частиною інформаційної безпеки, оскільки зловмисне використання персональних даних може призвести до серйозних наслідків, таких як фінансові шахрайства чи втручання у приватне життя громадян.

І основний сучасний закон для збереження персональних даних користувачів є Закон України «Про кібербезпеку», закон про кібербезпеку є основним правовим актом, що регулює захист інформаційних систем і мереж від кіберзагроз. Згідно з цим законом, всі державні органи зобов'язані розробляти та впроваджувати заходи для забезпечення кібербезпеки, а також створювати системи для попередження та реагування на кіберінциденти. Закон також визначає органи, відповідальні за координацію заходів у сфері кібербезпеки, зокрема Державну службу спеціального зв'язку та захисту інформації.

Для успішного впровадження законодавчих ініціатив важливо мати чітко визначену стратегію, яка передбачає конкретні кроки щодо зміцнення інформаційної безпеки. Україна розробила «Стратегію кібербезпеки України», яка визначає ключові напрямки діяльності держави в галузі кібербезпеки на найближчі роки. Вона включає заходи щодо захисту критичної інфраструктури, боротьби з кіберзлочинністю та підвищення інформаційної обізнаності серед

населення. Окрему увагу стратегія приділяє співпраці з міжнародними партнерами для протидії глобальним кіберзагрозам. Стратегія, що окреслює основні загрози для національної безпеки та способи їх подолання є «Стратегія національної безпеки України», інформаційна безпека є ключовим елементом стратегії, оскільки загрози в інформаційній сфері можуть мати серйозні наслідки для стабільності держави, її економіки та міжнародних відносин. Та основним стратегічним документом, який визначає основні напрямки державної політики щодо захисту інформаційного простору є «Концепція інформаційної безпеки України», що охоплює такі питання, як кібербезпека, боротьба з дезінформацією, захист національної інформаційної інфраструктури та забезпечення інформаційного суверенітету.

Також, слід зазначити роботу України на міжнародній арені з питань інформаційної безпеки. Міжнародна співпраця в свою чергу є важливою складовою забезпечення інформаційної безпеки. Україна активно бере участь у низці міжнародних угод та ініціатив, спрямованих на захист інформаційних систем і боротьбу з кіберзлочинністю, а саме Конвенція Ради Європи про кіберзлочинність або Будапештська конвенція. Ця угода є ключовим документом, який визначає міжнародні правила боротьби з кіберзлочинністю. Україна є підписантом цієї конвенції і активно співпрацює з іншими країнами для забезпечення безпеки інформаційних систем.

Україна активно співпрацює з НАТО в рамках програми «Партнерство заради миру» та інших ініціатив, що спрямовані на зміцнення інформаційної безпеки. Співпраця з Альянсом дозволяє Україні впроваджувати сучасні технології і методи боротьби з кіберзагрозами, а також отримувати доступ до міжнародного досвіду в цій сфері, тому Україна уклала двосторонні угоди щ іншими країнами, що сприяють обміну інформацією та координації зусиль у сфері кібербезпеки. Ці угоди включають спільні ініціативи, спрямовані на боротьбу з кіберзлочинністю, попередження кібератак та захист критичної інфраструктури.

Незважаючи на існуючі нормативно-правові акти, Україна стикається з низкою викликів у сфері інформаційної безпеки. Це включає високий рівень кіберзлочинності, розвиток нових технологій, таких як глибокі фейки, а також постійні спроби інформаційного втручання з боку агресивних держав. Для подолання цих викликів Україні необхідно продовжувати вдосконалювати своє законодавство, забезпечувати належну підготовку кадрів у галузі кібербезпеки, а також зміцнювати міжнародне співробітництво.

Попри те, що Україна має розвинену нормативно-правову базу для забезпечення інформаційної безпеки, є кілька аспектів, які потребують подальшого вдосконалення, наприклад постійне оновлення законодавства, щоб відповідати новітнім технологіям і методам кіберзагроз, забезпечення ресурсного та кадрового забезпечення для ефективного впровадження стратегій і заходів, покращення координації між державними органами та приватним сектором, оскільки багато критичних інфраструктур належать приватним компаніям.

Підсумовуючи все вище проаналізоване, нормативно-правова база забезпечення інформаційної безпеки в Україні є важливим елементом національної безпеки, однак для її ефективного функціонування треба постійно вдосконалювати законодавчі ініціативи відповідно до змін в технологічному середовищі, активніше залучати міжнародний досвід у сфері кібербезпеки та інформаційного захисту, залучати ресурси та фахівців для створення більш ефективної інфраструктури кіберзахисту, проводити освітні кампанії для підвищення рівня інформаційної грамотності серед населення.

Забезпечення належної інформаційної безпеки є запорукою стабільності та розвитку України в умовах постійно зростаючих загроз в інформаційному середовищі.

Висновки до першого розділу

Інформаційна безпека є важливою складовою національної безпеки, оскільки ефективний захист інформаційного простору має вирішальне значення

для стабільності, розвитку та збереження суверенітету України. Сучасні загрози в інформаційній сфері, такі як кіберзлочинність, дезінформація та зовнішнє втручання, можуть серйозно вплинути на політичну, економічну та соціальну стабільність держави. Тому теоретичні основи інформаційної безпеки мають ґрунтуватися на комплексному підході, що охоплює всі аспекти захисту інформації та кібербезпеки.

Основними складовими інформаційної безпеки України є захист інформаційних систем і мереж від кіберзагроз, боротьба з дезінформацією, підтримка інформаційного суверенітету та охорона критичної інфраструктури. Для ефективного захисту потрібно не тільки технічне забезпечення, а й розробка стратегій та політик на державному рівні, спрямованих на попередження та реагування на інформаційні загрози. Важливим елементом є також оновлення законодавства, щоб відповідати сучасним викликам у цій сфері.

Нормативно-правова база є фундаментом для регулювання діяльності у сфері інформаційної безпеки. В Україні існує низка законів, стратегій та концепцій, що визначають основні принципи, механізми та структури для захисту інформаційного простору. Проте, щоб ефективно боротися з сучасними загрозами, необхідно регулярно оновлювати і адаптувати законодавство до нових технологічних викликів, зокрема у сфері кібербезпеки та захисту персональних даних.

Оскільки інформаційні загрози мають глобальний характер, міжнародна співпраця є ключовим фактором для забезпечення інформаційної безпеки України. Підписання двосторонніх і багатосторонніх угод з іншими країнами та міжнародними організаціями є важливим для обміну даними, координації зусиль і боротьби з кіберзлочинністю на міжнародному рівні. Активна участь

України в міжнародних ініціативах допомагає підвищити ефективність захисту від інформаційних загроз.

Основними загрозами для інформаційної безпеки України є кібератаки, дезінформація, маніпулювання громадською думкою та зовнішнє втручання в

інформаційний простір. Ці загрози можуть мати серйозні наслідки для стабільності держави, економіки та міжнародних відносин. Тому необхідно забезпечити не тільки технічну, але й інформаційно-політичну готовність до таких викликів.

Для ефективного забезпечення інформаційної безпеки необхідно підвищувати рівень інформаційної грамотності серед населення. Важливо сприяти розвитку критичного мислення у громадян, що дозволить їм усвідомлено реагувати на інформаційні загрози, такі як фейкові новини та маніпуляції в медіапросторі. Цей аспект є ключовим елементом стратегії національної безпеки, оскільки зміцнює внутрішню стійкість суспільства.

Для ефективного подолання сучасних загроз і забезпечення стабільності інформаційного простору України необхідно продовжувати вдосконалення системи інформаційної безпеки. Ключовими напрямками є інтеграція новітніх технологій, адаптація до змін у глобальному інформаційному середовищі, а також створення ефективної співпраці між державними структурами, приватним сектором і міжнародними партнерами. Не менш важливим є постійне навчання та підготовка фахівців у сфері кібербезпеки та інформаційної безпеки.

Теоретичні основи інформаційної безпеки України створюють міцну основу для її захисту від сучасних інформаційних загроз. Однак для ефективної реалізації цих принципів необхідно постійно оновлювати нормативно-правову базу відповідно до нових викликів, активно співпрацювати з міжнародними партнерами і підвищувати рівень інформаційної грамотності серед населення.

Це дозволить забезпечити належний захист інформаційного простору України та зберегти її інформаційний суверенітет.

РОЗДІЛ 2. АНАЛІЗ СУЧАСНОГО СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ.

2.1 Стан та динаміка розвитку кібербезпеки (кіберінциденти, роль CERT-UA).

Кібербезпека є однією з найактуальніших проблем сучасності, особливо для країн, таких як Україна, яка стикається з численними викликами через гібридні війни та швидкий розвиток технологій. Ця сфера включає в себе ряд заходів, що спрямовані на захист інформаційних систем, мереж, даних і програмного забезпечення від атак, зловмисних дій або несанкціонованого доступу.

Важливість кібербезпеки для України зумовлена як зовнішніми, так і внутрішніми загрозами, зокрема кібератаками з боку державних акторів і злочинних угруповань, які використовують технології для дестабілізації політичної та економічної ситуації в країні.

У зв'язку з величезним значенням кібербезпеки для національної безпеки та стабільності держави, Україна розпочала активний розвиток цієї галузі після початку війни з Росією в 2014 році, коли країна зазнала масштабних кібератак. Відтоді кібербезпека стала важливим пріоритетом не лише для державних органів, а й для приватного сектору, наукових установ і громадянського суспільства.

Оцінка стану та розвитку кібербезпеки в Україні дозволяє виявити досягнення, а також проблеми, з якими стикається країна, і визначити кроки для покращення захисту інформаційної інфраструктури. До 2014 року стан кібербезпеки в Україні був значно менш розвинений порівняно з багатьма західними державами. Українські органи влади та бізнес не надавали достатньої уваги захисту інформаційних систем через низький рівень обізнаності та недостатній розвиток кібернетичних технологій. Ситуація змінилася лише після початку військового конфлікту з Росією.

Перші серйозні кібератаки, які шокували країну, сталися після окупації Криму Росією та початку війни на Донбасі. У цей період відбулося багато спроб вплинути на інформаційну сферу України, включаючи кібератаки на державні і приватні установи, а також на критично важливу інфраструктуру. Особливу увагу привернули атаки на енергетичний сектор, фінансові установи та медіа.

Одним із наймасштабніших та найбільш небезпечних кіберінцидентів в Україні стала атака на енергетичну інфраструктуру, що відбулася в грудні 2015 року. Хакери, ймовірно пов'язані з Росією, здійснили кібератаку на енергетичні компанії, внаслідок чого понад 200 тисяч людей залишилися без електрики.

Атака була проведена за допомогою шкідливих програм, які дозволяли зламати системи автоматизації та управління енергетичними мережами. Цей інцидент став першим у світі зафіксованим випадком масштабного кібератакування енергетичної інфраструктури держави. Реакція України на цей інцидент була швидкою, але необхідно зазначити, що інцидент показав надзвичайну вразливість критичної інфраструктури України.

В результаті атаки були виведені з ладу декілька підстанцій та частина об'єктів енергетичних мереж.

Цей кіберінцидент став сигналом для України про необхідність значного посилення кіберзахисту енергетичних об'єктів і систем, а також зміцнення співпраці з міжнародними партнерами в галузі кібербезпеки. Інший важливий кіберінцидент стався у 2016 році, коли один із найбільших українських банків «ПриватБанк», який став жертвою великої кібератаки. Хакери, ймовірно, знову діяли з території Росії, атакуючи онлайн-системи банку, що спричинило серйозні збої в роботі платіжних систем та онлайн-банкінгу.

Через атаку були заблоковані рахунки, і клієнти не могли здійснювати платежі або знімати гроші протягом кількох годин. Попри масштаб атаки, «ПриватБанк» зміг оперативно відновити роботу завдяки ефективним засобам кіберзахисту.

Однак цей інцидент чітко продемонстрував, наскільки вразливими можуть бути фінансові установи до кібератак, які використовують складні

техніки, такі як DDoS-атаки, фішинг та віруси, здатні впливати на обробку транзакцій.

У 2017 році Україна приєдналася до Глобального партнерства з кібербезпеки, що стало важливим кроком на шляху інтеграції країни в міжнародну кіберспільноту та забезпечення належного рівня захисту своїх інформаційних систем.

На державному рівні були розроблені програми, спрямовані на покращення інформаційної безпеки в урядових установах і підвищення рівня захисту приватного сектора. Ключовим елементом розвитку кібербезпеки стали спільні зусилля з міжнародними партнерами, зокрема з Європейським Союзом та Сполученими Штатами, що дозволило модернізувати національні системи захисту від кіберзагроз і покращити здатність протистояти хакерським атакам, організованим російськими спецслужбами.

Однією з важливих платформ для співпраці України з міжнародними партнерами для розвитку кібербезпеки є НАТО, зокрема у контексті ініціативи з кібербезпеки. Після анексії Криму та початку військового конфлікту з Росією Україна звернулася до НАТО за підтримкою у боротьбі з кіберзагрозами.

Нині, досить важко недооцінити значущість та важливість ролі української команди реагування на комп’ютерні надзвичайні події CERT-UA, яка і по цей день стоїть на варті дотримання права на доступ до правдивої інформації для кожного українця, тому ми зараз більш детально з вами ознайомимося з цією командою і чим саме вона займається.

Отже, CERT-UA (Computer Emergency Response Team of Ukraine) – це українська команда реагування на комп’ютерні надзвичайні події. Вона функціонує як підрозділ, що спеціалізується на виявленні, попередженні, аналізі та реагуванні на кіберінциденти. CERT-UA є складовою Державної служби спеціального зв’язку та захисту інформації України (ДССЗЗІ) і відповідає за захист державного кіберпростору.

CERT-UA входить до міжнародної мережі CERT/CSIRT (Computer Security Incident Response Teams), яка об’єднує аналогічні організації з інших країн, що співпрацюють у сфері забезпечення кібербезпеки.

CERT-UA здійснює постійний моніторинг кіберпростору для виявлення потенційних загроз і вразливостей.

У разі виявлення кібератак команда координує заходи з ліквідації їх наслідків, надає технічну підтримку та консультує організації.

CERT-UA розробляє рекомендації для організацій та установ, щоб мінімізувати ризики кібератак.

Команда також проводить й розслідування кіберінцидентів, аналізує кібератаки, виявляє їх джерела та особливості, співпрацює з правоохоронними органами та міжнародними партнерами для виявлення винних осіб.

Після проведення даної роботи CERT-UA публікує звіти, попередження про нові кіберзагрози, проводить навчання та тренінги для організацій у сфері кіберзахисту.

CERT-UA є активним представником України на міжнародній арені, співпрацює з аналогічними організаціями за кордоном, обмінюючись досвідом і технологіями для боротьби з глобальними кіберзагрозами.

В Україні, CERT-UA забезпечує кіберзахист державних інформаційних ресурсів, запобігаючи витоку даних, блокуючи доступ до критичних систем і мінімізуючи наслідки атак.

З початком російської агресії проти України кіберкоманда відіграє критичну роль у нейтралізації хакерських атак, спрямованих на урядові системи, інфраструктуру та медіа. Команда розслідує інциденти та надає рекомендації для запобігання новим атакам.

CERT-UA співпрацює з операторами енергетики, транспорту, фінансів та інших галузей, що становлять основу економіки України. Їхні дії спрямовані на недопущення збоїв у функціонуванні важливих систем через кібератаки.

У процесі переходу України до цифрової економіки CERT-UA сприяє створенню безпечних умов для використання цифрових технологій.

Кіберкоманда регулярно інформує організації та громадян про нові загрози, надає поради щодо захисту в кіберпросторі та розвиває культуру кібербезпеки.

Приклади діяльності CERT-UA:

- **протидія кібератакам на державні системи**: CERT-UA неодноразово запобігала кібератакам, пов'язаним із російськими хакерськими угрупованнями, такими як «Sandworm» або «Gamaredon»;
- **аналіз атак на критичну інфраструктуру**: CERT-UA допомогла нейтралізувати атаки на енергетичний сектор, зокрема атаки на електромережі України в 2015-2016 роках**;**
- **попередження кіберзагроз**: Команда регулярно випускає попередження про шкідливе програмне забезпечення, фішингові кампанії та інші ризики, що можуть зачепити державні та приватні організації.

CERT-UA виконує життєво важливу функцію у забезпеченні кіберзахисту України, особливо в умовах війни. Їхня діяльність є запорукою стабільності державного управління, функціонування критичної інфраструктури та захисту інформаційного суверенітету. Завдяки міжнародній співпраці та постійному вдосконаленню технологій CERT-UA зміцнює оборону України в кіберпросторі, що є одним із ключових фронтів сучасної війни.

У 2017 році була підписана угода, що передбачає обмін інформацією щодо кіберзагроз, підготовку фахівців і розробку спільних заходів для боротьби з кіберзлочинністю. НАТО також надало Україні доступ до ресурсів, що сприяли зміцненню національного кіберзахисту та створенню центрів реагування на інциденти в кіберпросторі.

Ця співпраця передбачає регулярні тренінги для українських фахівців з кібербезпеки, що дозволяє підвищити їх кваліфікацію та ефективність боротьби з кіберзагрозами.

Участь у навчаннях НАТО надає Україні можливість перейняти досвід західних партнерів у боротьбі з кіберзлочинністю та оперативному реагуванні

на кіберінциденти. Великою проблемою кібербезпеки в україні є недостатня кількість кваліфікованих фахівців.

Із причин браку фахівців можна виділити такі основні моменти, як швидке зростання кіберзагроз.

Кібератаки, зокрема з боку державних структур, стали великою проблемою для України після анексії Криму та початку конфлікту на Донбасі.Це створило потребу в висококваліфікованих спеціалістах, здатних розробляти нові методи захисту інформаційних систем від постійно змінюваних кіберзагроз.

Кіберзлочинці використовують все складніші методи, що вимагає від фахівців постійного оновлення своїх знань і навичок. Швидкий розвиток технологій і постійні зміни в тактиках атак створюють необхідність у нових спеціалістах, які могли б оперативно реагувати на нові загрози.

В Україні спостерігається не лише дефіцит кадрів, а й обмежені можливості для забезпечення організацій достатньою кількістю кваліфікованих працівників. Це пов'язано з тим, що ринок кібербезпеки не здатний повністю задовольнити попит через обмежену доступність відповідної освіти та навчальних програм. Також слід зазначити, що в Україні наявний дефіцит освітніх програм в галузі кібербезпеки.

Для створення високоякісної освітньої програми з кібербезпеки потрібні великі фінансові витрати на закупівлю сучасного програмного забезпечення, лабораторного обладнання та підготовку викладачів, які мають відповідні навички та знання.

В Україні багато навчальних закладів, що надають освіту в цій галузі, стикаються з фінансовими труднощами, що ускладнює оновлення навчальних матеріалів та залучення висококласних спеціалістів. Зокрема, у багатьох університетах відсутні сучасні комп'ютерні класи та лабораторії, що відповідають вимогам часу. Окрім того, багато навчальних закладів не мають доступу до необхідних ліцензій на програмне забезпечення для ефективного

навчання студентів. Це призводить до того, що студенти здобувають знання, які не завжди відповідають актуальним вимогам сучасних кіберзагроз.

Соціальний статус професії має великий вплив на її привабливість. В Україні багато людей вважають престижнішими професії, що пов’язані з традиційними сферами, такими як медицина, право чи економіка. Кібербезпека ж часто сприймається як вузька спеціалізація, яка не має такого рівня соціального визнання. Це може зупиняти молодь від вибору цієї професії, адже для них важливо, як їхній вибір буде сприйнятий у суспільстві.

Стереотипи щодо професії в кібербезпеці впливають на ставлення до неї, особливо серед старших людей, які ще не звикли до нових технологічних професій. Більше того, багато хто не розуміє, чим займаються фахівці в кібербезпеці, що додатково знижує престиж цієї професії.

Тобто для покращення стану кібербезпеки в Україні треба вводити нові освітні ініціативи, збільшувати співпрацю з міжнародними партнерами, а саме США, Великобританія, Японія, Німеччина. Ключовим є те, щоб усі гілки влади, бізнес та громадські організації об'єднали зусилля для створення безпечного кіберпростору, здатного протистояти сучасним загрозам.

Лише таким чином Україна зможе гарантувати надійний захист своїх інформаційних ресурсів, забезпечити стабільність економіки та захистити національні інтереси.

2.2. Проблема дезінформації та впливу пропаганди на інформаційний простір України.

Найбільшим викликом для України і її інфомаційного простору став 2014 рік, рік кардинальних змін. Євромайдан 2014 року став важливим етапом в історії України, перетворившись із мирних протестів на потужний народний рух, що виступав за європейську інтеграцію та демократичні зміни.

Проте поряд із цими подіями країна стикнулася з серйозною проблемою, якою стала дезінформація, яка суттєво вплинула на інформаційний простір і

громадську думку. Пропагандистські кампанії, організовані як зовнішніми, так і внутрішніми силами, активно маніпулювали фактами, спотворюючи реальність і створюючи напругу серед населення.

Однією з основних загроз для України стало вторгнення пропаганди, яке намагалося маніпулювати інформаційним простором, підживлюючи страхи та непорозуміння серед різних соціальних і політичних груп.

Російська пропаганда мала величезний вплив як на внутрішнє, так і на міжнародне сприйняття подій в Україні. За допомогою медіа та соціальних мереж Росія намагалась переконати громадськість у тому, що протестувальники на Майдані є радикальними елементами, які загрожують стабільності країни.

Пропагандисти активно поширювали наративи про фашизм, насильство та анархію, спотворюючи реальні події і створюючи негативний образ протестувальників як небезпечних людей, що нібито прагнуть порушити мирний порядок.

Протягом подій на Майдані особливо гостро постала проблема маніпуляції інформацією про насильство. У реальності протестувальники часто ставали жертвами нападів з боку силових структур, що призводило до численних жертв.

Проте ці події були активно перекручені у проросійських ЗМІ, де протестувальники подавалися як радикали, що намагаються зруйнувати спокій у країні. Інформація про «антимайдан», вигадані історії про «погроми» та «бандитизм» активно розповсюджувалась з метою дискредитації протестного руху і виправдання насильства з боку силових структур.

Дезінформація мала також великий вплив на суспільство в Україні, особливо в регіонах з проросійськими настроями, таких як Схід і Південь країни. Російська пропаганда активно нагнітала образи «небезпечних націоналістів», які нібито намагаються розділити країну на основі мовних і культурних розбіжностей. Пропагандистські повідомлення, що нова влада в Україні нібито є незаконною та вороже налаштованою до російськомовних громадян, сприяли подальшій поляризації суспільства і розколу між регіонами.

Відповідно, українська влада та громадські активісти вжили низку заходів для боротьби з дезінформацією.

Було створено альтернативні медіа, які об'єднали журналістів, патріотів та волонтерів, спрямованих на розповсюдження правдивої інформації, а також на спростування фальшивих наративів. Велику роль у боротьбі з дезінформацією зіграли соціальні мережі, де активісти публікували відео, фото та новини, які допомагали розвінчувати фальшиві повідомлення.

Однак, важливою умовою для боротьби з дезінформацією була підтримка з боку міжнародної спільноти. Західні медіа та уряди активно висвітлювали події на Майдані, що дозволило сформувати більш об'єктивну картину подій, попри те, що повністю подолати вплив російської пропаганди не вдалося.

Отже, дезінформація стала однією з головних проблем під час Євромайдану, яка не лише ускладнювала внутрішню ситуацію в Україні, але й впливала на міжнародні відносини. Пропагандистські кампанії впливали на суспільство, створюючи розкол і напругу, та перешкоджали розвитку стабільної демократії в країні. Водночас ці події стали важливим уроком для України, підкреслюючи необхідність боротьби з дезінформацією та розвитком інформаційної культури для майбутнього.

Після Євромайдану та початку військової агресії Росії в 2014 році Україна зіткнулася з численними труднощами, серед яких одними з найбільших загроз стали дезінформація та пропаганда.

Протягом 2015-2022 років ці явища мали значний вплив як на внутрішню ситуацію в Україні, так і на міжнародні відносини, створюючи серйозні перешкоди для стабільності та демократичного розвитку. В умовах масштабної гібридної війни, розв'язаної Росією проти України, особливу увагу слід приділити основним аспектам дезінформаційних кампаній та їх наслідкам для інформаційного простору країни. Пропаганда як елемент Гібридної війни.

Починаючи з 2014 року, Росія активно використовувала дезінформацію як один із головних інструментів гібридної війни, намагаючись дестабілізувати ситуацію в Україні та дискредитувати її уряд.

Протягом наступних років ці методи лише посилювались, а масштаби пропагандистських кампаній ставали все більш значущими.

Основною метою російської пропаганди було не тільки маніпулювання громадською думкою в Україні, але й вплив на міжнародну спільноту, щоб створити враження, що ситуація в Україні є внутрішнім конфліктом, а не актом агресії з боку Росії.

Особливо вражаючими були масштаби використання соціальних мереж та інтернет-платформ для розповсюдження фальшивої інформації. Російські пропагандисти створювали численні фейкові акаунти, групи, а також застосовували “ботоферми» для маніпуляцій громадською думкою.

Це сприяло поширенню повідомлень, що змінювали сприйняття реальних подій, часто зокрема за допомогою ретельно створених фейкових новин. Серед тем, що часто використовувалися у пропаганді, були звинувачення України у фашизмі, насильстві та дискримінації, що створювало негативний образ української влади і народу, особливо серед російськомовних громадян України та на теренах пострадянських країн.

У період з 2015 по 2022 рік в Україні активно поширювалися фальшиві новини, які піддавали сумніву урядові реформи та трактували соціальні і економічні проблеми як наслідок політики центральної влади. Одним з найбільш поширених меседжів було звинувачення українських політиків у корупції, навіть серед тих, хто вважався реформаторами. Часто дезінформація супроводжувалася викривленням фактів щодо діяльності силових структур, зокрема Національної гвардії та Збройних сил України, що послаблювало довіру населення до влади.

Пропагандисти намагалися нав’язати думку, що «порушення прав людини» і «репресії» з боку української влади є звичайним явищем, хоча насправді йшлося про боротьбу з сепаратизмом і російською агресією. З самого початку російської агресії українська влада вжила заходів для боротьби з дезінформацією. Було створено спеціальні інформаційні платформи, такі як

«StopFake», які активно перевіряли і спростовували фальшиві новини, що поширювались у ЗМІ та соціальних мережах.

Важливу роль у цьому процесі відіграли також організації громадянського суспільства та волонтерські ініціативи, які працювали над створенням достовірної інформації та її поширенням. Посилення внутрішньої інформаційної політики, розвиток нових незалежних медіа та підтримка міжнародних ініціатив для боротьби з дезінформацією стали важливими кроками у протидії російській пропаганді.

Проте, незважаючи на ці зусилля, повністю уникнути впливу пропаганди не вдалося, і вона залишалася серйозною загрозою для України до 2022 року.

Інформаційна війна у 2022 – 2024 роках. З початку повномасштабного вторгнення Росії в Україну 24 лютого 2022 року, війна не обмежувалася лише військовими діями. Росія, маючи багатий досвід ведення інформаційної війни, продовжила активно застосовувати пропагандистські кампанії для дестабілізації не тільки в Україні, а й за її межами.

Основними цілями було маніпулювання громадською думкою, ослаблення міжнародної підтримки України та поширення фальшивих відомостей для посилення внутрішніх розбіжностей і розколу в українському суспільстві.

Одним із найбільших досягнень Росії в інформаційній війні стало вміння створювати альтернативні реальності для населення, спотворюючи факти та поширюючи пропагандистські наративи через державні і проросійські медіа, а також соціальні мережі.

Одним із головних аргументів, які Росія використовувала для виправдання свого вторгнення в Україну, було нібито необхідне «захист російськомовних громадян» і «припинення геноциду». За версією російської пропаганди, українська влада систематично атакує російськомовних громадян, зокрема на сході країни, і ця ситуація потребує негайного втручання.

Хоча ці заяви не мали реальних доказів, у сучасному медіапросторі це не завадило їх поширенню. Таким чином, Росія створювала образ «жертви», що

дозволяло їй виступати в ролі «рятівника», який захищає права своєї нації в Україні.

Ще одним важливим елементом російської дезінформаційної кампанії став наратив про «нацизм» в Україні. Російські державні ЗМІ та пропагандисти безперервно заявляли, що українська влада охоплена націоналістичними переконаннями, і націоналізм нібито став основною лінією державної політики. Варто зауважити, що цей образ був сильно спотворений.

Насправді в Україні націоналізм не має значного впливу на політику, а більшість населення підтримує європейські цінності. Проте в російських медіа цей наратив подавався як виправдання для агресії.

Через такі фальшиві повідомлення Росія формувала образ ворога, якого потрібно було знищити, що додавало агресії "морального" підґрунтя. І найголовніший наратив російської пропаганди була "теорія геноциду" щодо російськомовних громадян України.

Російська пропаганда поширювала інформацію про нібито намір української влади здійснити геноцид проти російськомовних, особливо на Донбасі. Хоча ці твердження не мали жодних доказів, вони служили для створення враження про жорстокого ворога, якому треба протистояти. Завдяки цій маніпуляції Росія не лише виправдовувала свою військову агресію, а й намагалася легітимізувати свої військові злочини на захоплених територіях.

Отже, протягом 2014–2024 років Україна стикалася з серйозними викликами в інформаційній війні.

Пропаганда і дезінформація стали основними засобами гібридної війни, які Росія використовувала для ослаблення морального духу населення, дестабілізації внутрішньої політичної ситуації та спотворення фактів на міжнародному рівні.

Відповідаючи на ці загрози, Україна розробила низку ініціатив, спрямованих на боротьбу з дезінформацією, спростування фейкових новин і захист національних інтересів. Активна співпраця з міжнародними партнерами,

використання соціальних мереж та цифрових платформ стали важливими інструментами у протидії інформаційній агресії.

Досвід, здобутий в ці роки, має стати основою для розвитку майбутньої інформаційної політики України. Враховуючи зміни в медіапросторі, важливо зосередити увагу на підвищенні медіа-грамотності громадян, зміцненні незалежності медіа та забезпеченні доступу до правдивої і об'єктивної інформації.

Боротися з дезінформацією можливо лише в умовах відкритого інформаційного простору, де громадяни здатні критично аналізувати отримувану інформацію. Україні необхідно продовжувати працювати на міжнародному рівні для збереження інформаційної незалежності та протистояння зовнішньому впливу, зокрема з боку Росії.

2.3. Оцінка ефективності державних заходів у сфері інформаційної безпеки (аналіз програм, політичних ініціатив).

Оцінка ефективності заходів держави у сфері інформаційної безпеки є ключовим елементом стратегії управління національною безпекою України. В умовах стрімкого розвитку інформаційних технологій і збільшення кіберзагроз, захист інформаційного простору стає основою для забезпечення стабільності, економічного розвитку та суверенітету країни. Тому важливо не лише розглянути теоретичні аспекти, а й оцінити реальні політичні ініціативи та програми, спрямовані на зміцнення інформаційної безпеки. Оцінка ефективності державних заходів охоплює кілька ключових аспектів: законодавчу базу, стратегії, політичні ініціативи, а також моніторинг і реалізацію практичних заходів у галузі кібербезпеки.

З початку 2010-х років Україна почала активно розробляти та впроваджувати програми та ініціативи для захисту свого інформаційного простору. Перші кроки були зроблені у контексті гібридної агресії з боку Росії, що призвело до значного посилення уваги до цієї проблеми. У результаті були

розроблені та прийняті основні стратегії та нормативно-правові акти, які визначають напрямки розвитку інформаційної безпеки на державному рівні.

У 2016 році була затверджена Стратегія кібербезпеки України, яка визначила основні пріоритети державної політики в захисті інформаційних систем та кіберпростору від загроз. Головною метою цієї стратегії є забезпечення національної безпеки в кіберпросторі, підвищення захищеності інформаційної інфраструктури, розвиток органів, що відповідають за реагування на кіберінциденти, а також захист критичної інфраструктури.

Програма реалізації стратегії включала в себе створення та впровадження національної системи реагування на кіберінциденти, коли всі державні установи отримують попередження, щоб приділити увагу до кіберзагроз, формування кіберпідрозділів у державних органах, підтримка розвитку науково-технічного потенціалу в галузі кібербезпеки, включаючи в себе допомогу від партнерів такких як НАТО, США або ЄС. В програму реалізації також входило удосконалення нормативно-правового регулювання для боротьби з кіберзлочинністю.

Однак реалізація цих заходів зіткнулася з низкою труднощів, серед яких були недостатнє фінансування, слабка координація між державними установами та приватним сектором, а також недостатній рівень підготовки фахівців.

Одним з основних документів у сфері інформаційної безпеки є Концепція забезпечення інформаційної безпеки України, яка була прийнята в 2017 році.
Цей документ пропонує комплексний підхід до захисту інформаційного простору від різних внутрішніх і зовнішніх загроз. Він охоплює проблеми, пов’язані з інформаційними війнами, боротьбою з дезінформацією, забезпеченням інформаційного суверенітету, а також безпекою в кіберпросторі. Для роботи цієї концепції виділили основні напрями, такі як формування єдиного інформаційного простору, що базується на міжнародних стандартах та безпекових протоколах, розвиток національної системи реагування на кіберзагрози, покращення захисту інформаційних ресурсів, що

використовуються державними органами та в критичних інфраструктурах та урахування впливу новітніх технологій, таких як блокчейн та штучний інтелект, на сферу інформаційної безпеки.

Однак, як і в галузі кібербезпеки, впровадження цієї концепції стикається з певними проблемами, зокрема, значним відставанням у реалізації її положень через недостатність ресурсів та проблеми з координацією між різними відомствами.

У відповідь на загрози, що виникають від дезінформації, боротьба з інформаційними атаками стала одним із пріоритетних напрямків політики України, особливо на тлі російської агресії. У 2017 році було створено Медіа-центр інформаційної безпеки та Український Центр стратегічних комунікацій, метою яких є протидія фальшивим новинам, пропаганді та маніпуляціям, що поширюються в медіапросторі.

Особлива увага була приділена розробці стратегій інформаційної безпеки для боротьби з пропагандою та маніпуляціями в соціальних мережах. Україна активно співпрацює з міжнародними партнерами, зокрема з Європейським Союзом, в рамках ініціатив, спрямованих на протидію дезінформації. Однак, через обмежені ресурси для моніторингу та оперативного реагування, ці програми стикаються з труднощами у їхній реалізації.

Правова база в свою чергу є важливою частиною забезпечення інформаційної безпеки України. Вона створює основу для координації заходів з безпеки в державних органах, визначає права і обов'язки громадян і організацій у цій сфері, а також забезпечує правові засади для боротьби з кіберзлочинністю. Законодавство України в галузі інформаційної безпеки було суттєво оновлено останнім часом, зокрема в частині боротьби з кіберзлочинністю та захисту персональних даних. У 2017 році був ухвалений Закон України «Про кібербезпеку», який встановлює правові засади для захисту інформаційних систем і критичної інфраструктури.

Цей закон передбачає створення Національного координаційного центру кібербезпеки, регулює діяльність державних органів у сфері кібербезпеки, а

також визначає права та обов'язки юридичних осіб і громадян щодо захисту інформації. Однак цей закон ще потребує вдосконалення, зокрема щодо покращення співпраці між державними органами та приватним сектором.

Один із ключових аспектів інформаційної безпеки — це захист персональних даних громадян. В Україні в 2010 році був ухвалений Закон «Про захист персональних даних», який регулює правила збору, обробки та захисту персональної інформації в усіх сферах, від державних органів до приватних компаній.

Цей закон узгоджує українське законодавство з європейськими стандартами, зокрема з GDPR (Загальний регламент захисту даних ЄС). Однак на практиці існують проблеми, зокрема відсутність належного контролю за обробкою персональних даних та недостатня правова база для боротьби з несанкціонованим доступом до таких даних.

Для оцінки ефективності державних заходів у сфері інформаційної безпеки важливо враховувати не лише правові та організаційні ініціативи, але й реальний результат їх впровадження.

Одним із основних напрямків ефективної реалізації програм є розбудова інфраструктури кібербезпеки. Створення Кіберполіції України, яка спеціалізується на боротьбі з кіберзлочинністю, стало важливим кроком у захисті інформаційного простору. Вона активно працює в напрямку запобігання кіберінцидентам, допомагаючи підприємствам і державним установам у розв’язанні проблем.

Загалом, Кіберполіція України — це спеціалізований підрозділ Національної поліції України, створений з метою боротьби з кіберзлочинністю та забезпечення захисту кіберпростору країни. Основним завданням кіберполіції є гарантування безпеки інформаційних систем і мереж, розслідування кіберзлочинів, виявлення та розслідування випадків, пов'язаних з несанкціонованим доступом до комп'ютерних систем, крадіжкою персональних даних, кіберфінансовими шахрайствами та порушеннями в сфері інформаційних технологій, моніторинг кіберпростору здійснення постійного

спостереження за Інтернетом для виявлення потенційних загроз і швидке реагування на них, інформування та навчання надання консультацій для організацій та громадян з питань безпеки в Інтернеті, а також проведення освітніх заходів для підвищення рівня кіберграмотності, міжнародна співпраця, взаємодія з міжнародними правоохоронними організаціями, такими як Інтерпол і Європол, для боротьби з глобальними кіберзлочинами.

Кіберполіція також активно працює над вдосконаленням нормативно-правової бази для боротьби з кіберзлочинністю, а також підтримує державні ініціативи щодо розвитку кібербезпеки в Україні.

Висновки до другого розділу.

Підсумовуючи, проведений аналіз сучасного стану інформаційної безпеки України можна зазначити, що останні роки питання інформаційної безпеки в Україні набуло особливої актуальності через зростання глобальних кіберзагроз та зовнішню агресію, насамперед з боку Росії. Це спонукало до розробки й ухвалення низки законодавчих актів, стратегій і концепцій, спрямованих на створення ефективної системи кіберзахисту та протидії сучасним викликам в інформаційному середовищі.

Законодавство України у сфері інформаційної безпеки зазнає постійного вдосконалення. Ухвалення таких актів, як Закон України «Про кібербезпеку» та «Про захист персональних даних», суттєво підвищило ефективність регулювання та забезпечення захисту інформаційного простору. Водночас, незважаючи на досягнутий прогрес, окремі аспекти потребують подальшого доопрацювання, зокрема в частині налагодження взаємодії між державними інституціями та приватним сектором.

Сучасні кіберзагрози не мають кордонів, тому активне залучення України до міжнародних ініціатив, таких як співпраця з Європейським Союзом та іншими міжнародними організаціями, має вирішальне значення для ефективного реагування на глобальні кіберзагрози. Україна активно співпрацює

з міжнародними партнерами, що сприяє розвитку кіберзахисту та боротьбі з кіберзлочинністю.

Україна стикається з численними викликами в сфері інформаційної безпеки, серед яких ключову роль відіграють кіберзлочинність, дезінформація та зовнішні інформаційні атаки. Основними пріоритетами є протидія фейковим новинам і маніпуляціям у медіапросторі, а також забезпечення захисту критично важливої інфраструктури від кіберзагроз.

З огляду на швидкий розвиток технологій і появу нових загроз в інформаційному середовищі, важливо активно працювати над підвищенням рівня інформаційної обізнаності населення. Це сприятиме кращому захисту особистих даних громадян і допоможе їм ефективніше розпізнавати потенційні ризики, зокрема пов’язані з поширенням фейкових новин та інформаційними маніпуляціями.

Хоча Україна досягла значного прогресу у зміцненні інформаційної безпеки, існує потреба в подальшому вдосконаленні правової та технічної бази, підвищенні рівня кіберграмотності серед громадян і посиленні співпраці з міжнародними партнерами. У цьому напрямі ключовими завданнями залишаються впровадження передових технологій та адаптація законодавства до актуальних кіберзагроз, що забезпечить ефективний захист інформаційного простору держави.

РОЗДІЛ 3. Шляхи вдосконалення системи інформаційної безпеки України.

3.1. Інтеграція сучасних технологій кіберзахисту (штучний інтелект, блокчейн тощо).

З швидким розвитком технологій зросла потреба у більш технологічних рішеннях вирішення проблем, з якими стикається кожна людина, що має доступ до інтернету. Технології шифрування та їх роль у захисті даних.

Шифрування є ключовим методом захисту інформації від несанкціонованого доступу та витоку. Використання передових шифрувальних технологій забезпечує високий рівень безпеки при передачі даних через відкриті канали зв'язку.

Сучасні підходи, такі як асиметричне шифрування та квантові алгоритми, значно ускладнюють роботу хакерів, роблячи доступ до зашифрованих даних майже неможливим без відповідного ключа. Крім того, новітні методи шифрування не лише захищають дані під час їх передачі чи зберігання, а й забезпечують цілісність інформації. Такі технології, як блокчейн, гарантують незмінність записів і транзакцій у цифрових середовищах.

З розвитком цифрових технологій і збільшенням обсягу даних, що обробляються в інтернеті, зростають можливості для злочинців, які використовують новітні технології для здійснення кібератак. Однак, разом з цими новими загрозами, з'являються й нові інструменти для боротьби з ними.

Одним з таких інструментів є Штучний Інтелект (ШІ), який активно застосовується в різних сферах кібербезпеки. ШІ має значний потенціал для поліпшення кіберзахисту завдяки своїй здатності до самонавчання та автоматизації, що дозволяє оперативно реагувати на нові загрози.

Останніми десятиліттями штучний інтелект швидко розвивається та знаходить застосування в різних галузях, від медицини до фінансів і розваг.

Однак, поряд з численними перевагами, він приносить і нові виклики, зокрема у сфері кібербезпеки. Як технологія, що має потенціал для автоматизації та підвищення ефективності, ШІ також створює нові можливості для кіберзагроз.

Хоча ШІ може бути використаний для захисту систем від атак, він також стає інструментом для зловмисників, що підвищує ризики для інформаційної безпеки. Це вимагає розуміння не лише можливих загроз, а й способів реагування на них.

Однією з основних областей, де ШІ демонструє великий потенціал, є виявлення аномалій. Ця технологія допомагає виявляти нові або непередбачувані загрози, які не були зафіксовані в базах даних відомих атак. ШІ здатний швидко виявляти будь-які відхилення від звичних моделей поведінки користувачів або систем, що дозволяє ефективніше і точніше визначати можливі загрози.

Використання методів машинного навчання дає змогу створювати моделі, які можуть обробляти великі обсяги даних, трафіку та інших цифрових слідів, для виявлення навіть найменших аномалій. Це дає змогу швидше реагувати на нові загрози та знижує ймовірність успішних атак.

Автоматизація процесів захисту ШІ може бути використаний для автоматизації різних аспектів кіберзахисту, таких як спостереження за системами, реагування на загрози та налаштування захисних заходів. Автоматизація дозволяє зменшити вплив людських помилок, що знижує ймовірність затримок чи неправильних дій при відповіді на загрози. Системи, побудовані на основі ШІ, можуть самостійно змінювати налаштування безпеки, блокувати підозрілі IP-адреси або обмежувати доступ до певних ресурсів без участі людини. Це також дозволяє швидше реагувати на інциденти безпеки та забезпечує оперативне відновлення роботи систем після атак.

Виявлення фішингових атак штучного інтелекту активно застосовується для боротьби з фішингом і соціальною інженерією. Завдяки алгоритмам машинного навчання можна автоматизувати виявлення фальшивих повідомлень,

які зловмисники створюють для крадіжки конфіденційних даних. Ці алгоритми можуть виявляти підозрілі електронні листи, посилання та інші види комунікації, що використовуються для обману користувачів. Штучний інтелект також здатен аналізувати структуру і зміст повідомлень, виявляючи ознаки фішингу, що допомагає знизити ймовірність того, що користувачі стануть жертвами шахрайських схем.

Вихід людського фактору на другий план, оскільки більшість атак спричинені людськими помилками, впровадження ШІ в кіберзахист допомагає зменшити цей ризик, оскільки системи працюють за алгоритмами, а не залежать від людських помилок. Це дозволяє значно знизити кількість несанкціонованих доступів і атак, викликаних людським фактором. Також однією з технологій захисту даних є блокчейн.

Блокчейн — це технологія збереження даних, яка структурує інформацію у вигляді послідовності блоків, пов'язаних між собою через криптографічні методи.

Однією з основних переваг цієї технології є її дистрибутивний характер та відсутність централізованого керування: кожен учасник мережі має доступ до повної копії даних, що дозволяє уникнути можливих зловживань і несанкціонованих змін.

Кожен блок у ланцюзі містить інформацію про транзакції або інші важливі дані, які не можуть бути змінені без згоди більшості учасників. Це забезпечує високу довіру та прозорість, що є критично важливим для сфер, де необхідно гарантувати цілісність і безпеку інформації.

У сучасному кіберпросторі, де атаки на інформаційні системи стають дедалі складнішими та масштабнішими, застосування технології блокчейн для забезпечення кібербезпеки набуває все більшої важливості. Блокчейн володіє кількома важливими характеристиками, які роблять його ефективним інструментом для протидії кіберзагрозам.

Дані, що зберігаються в блокчейні, не можуть бути змінені чи видалені без згоди більшості учасників мережі. Це забезпечує високий рівень захисту від маніпуляцій з боку хакерів або зловмисників.

Усі учасники мережі мають доступ до однакових даних, що дозволяє контролювати всі транзакції та процеси, що відбуваються в системі.

Блокчейн в свою чергу гарантує високий рівень захисту завдяки застосуванню криптографії. Користувачі можуть виконувати транзакції, не розкриваючи своєї особистої інформації чи інших конфіденційних даних. Також блокчейн може бути використаний для підвищення захисту від різних кібератак, зокрема фішингу, DDoS-атак, крадіжки паролів та шкідливих програм.

Блокчейн відіграє важливу роль у захисті від фішингу. Фішинг — це шахрайський метод, коли зловмисники створюють підроблені електронні листи чи веб-сайти з метою отримання конфіденційної інформації, наприклад, паролів або банківських даних. Використання блокчейн-технологій для створення захищених каналів комунікації допомагає зменшити ризики фішингу, оскільки кожен користувач може перевірити достовірність сайту чи листа за допомогою криптографії.

Розподілені атаки на мережу, коли багато комп'ютерів одночасно намагаються вивести сервер з ладу, є серйозною загрозою для компаній і урядів. Блокчейн може допомогти розподіляти навантаження серед учасників мережі, що дозволить зменшити вплив DDoS-атак. Блокчейн дає можливість інтегрувати шифрування в кібербезпекову систему, забезпечуючи захищений обмін даними між користувачами. Завдяки криптографії блокчейн дозволяє створювати надійні цифрові підписи, які підтверджують автентичність і захищають інформацію від змін.

Інтеграція блокчейн у корпоративні і урядові системи один з найбільших потенціалів блокчейну, в сфері кіберзахисту полягає в його застосуванні в корпоративних та урядових системах.

У цих секторах забезпечення інформаційної безпеки є надзвичайно важливим, оскільки дані, що зберігаються в таких організаціях, часто стають мішенями для значних кібератак.

Впровадження блокчейн-технологій може суттєво знизити ризики для компаній та урядів, а також покращити ефективність їхніх внутрішніх процесів.

Аутентифікація користувачів і контроль доступу є важливим аспектом інформаційної безпеки є правильне управління доступом до чутливих даних.

Блокчейн дозволяє розробляти системи контролю доступу, в яких користувачі автентифікуються через дистрибутивні механізми. Це забезпечує високий рівень захисту та усуває можливість централізованих вразливих точок.

Зберігання та обмін даними є одним із прикладів застосування блокчейну для зберігання чутливих даних гарантує їх цілісність і захист від зовнішніх атак.

Усі записи в блокчейні є незмінними та прозорими, що дозволяє відстежувати будь-які зміни в системі та своєчасно виявляти потенційні загрози. Найголовнішою властивістю блокчейну є захист критичної інфрастуртури.

Критична інфраструктура є основою функціонування сучасного суспільства, її захист має першочергове значення в сфері кібербезпеки, оскільки її вразливість може призвести до серйозних наслідків, таких як зупинка виробництва, порушення зв'язку чи загроза національній безпеці. Блокчейн дає змогу створювати дистрибутивні системи для моніторингу та управління критичною інфраструктурою, що покращує її стійкість до атак. Цей підхід не тільки гарантує безпечне зберігання даних про стан інфраструктури, а й захищає її від несанкціонованого доступу. Насамперед важливість захисту та безпечного зберігання даних підкреслила фахівчиня із кібербезпеки Сюзан Ландо: «Захист даних — це не розкіш, а обов’язок кожної організації, яка працює в цифровому світі» [18].

Хмарні технології набувають дедалі більшої популярності серед компаній і організацій по всьому світу. Вони дозволяють підприємствам

зберігати та обробляти значні обсяги даних без потреби у потужних фізичних серверах.

Окрім цього, хмарні технології створюють нові можливості для підвищення гнучкості бізнес-процесів, зменшення витрат і покращення ефективності. Хмарні технології передбачають зберігання та обробку даних на віддалених серверах, до яких користувачі можуть підключатися через Інтернет.

Це дозволяє орендувати серверні потужності замість того, щоб мати їх у власності.

До найбільш відомих хмарних сервісів відносяться Amazon Web Services (AWS), Microsoft Azure, Google Cloud та інші.

З точки зору безпеки хмарні технології пропонують ряд переваг, таких як централізоване управління даними, автоматичне оновлення програмного забезпечення та зберігання даних у захищених дата-центрах. Однак, незважаючи на ці переваги, хмарні технології стикаються з певними безпековими викликами, зокрема, ризиками несанкціонованого доступу, витоками даних, атаками на інфраструктуру та недостатнім контролем доступу до чутливої інформації.

Тому необхідно ретельно розглядати методи забезпечення безпеки в хмарних середовищах.

Основними загрозами для безпеки даних є несанкціонований доступ до даних. Оскільки дані зберігаються на віддалених серверах, вони можуть бути схильні до несанкціонованого доступу. Якщо організація не здійснює належний контроль за доступом або не застосовує ефективне шифрування, це може призвести до витоку конфіденційної інформації.

Дані, збережені в хмарі, можуть бути схильні до витоків через вразливості в системах захисту. Хоча хмарні провайдери прагнуть забезпечити високі стандарти безпеки, помилки користувачів або неправильно налаштовані сервіси можуть стати причиною серйозних витоків інформації.

Хмарні сервіси можуть бути піддані різним видам кібератак, таким як DDoS-атаки, крадіжка паролів, фішинг або інфікування шкідливим програмним

забезпеченням. Хоча більшість хмарних постачальників використовують механізми захисту, зловмисники можуть використовувати вразливості для порушення роботи системи чи несанкціонованого доступу до даних.

У хмарних середовищах часто спостерігається поділ відповідальності між користувачем та постачальником послуг.

Це може призвести до ситуацій, коли одна зі сторін не здійснює належного контролю за безпекою, що робить систему вразливою до атак.

Попри усіх загроз до безпеки зберігання інформації в хмарному середовищі, досить на високому рівні є розвинутими й методи захисту безпечного збереження інформації.

Зокрема, одним з основних способів захисту інформації в хмарах є її шифрування. Це гарантує, що навіть у разі витоку або несанкціонованого доступу, дані залишатимуться недоступними без відповідного ключа. Багато хмарних провайдерів включають автоматичне шифрування у свої послуги, проте користувач повинен самостійно контролювати ці налаштування. Багатофакторна аутентифікація підвищує безпеку, оскільки для доступу до даних потрібно пройти кілька етапів перевірки (наприклад, ввести пароль і код, отриманий через SMS). Використання багатофакторної аутентифікації знижує ризик несанкціонованого доступу, навіть якщо пароль був компрометований.

Постійний моніторинг активності в хмарних системах дозволяє оперативно виявляти спроби несанкціонованого доступу або аномальні дії. Аудит безпеки дає змогу ретельно перевіряти доступ до даних і забезпечує, щоб лише авторизовані особи мали доступ до конфіденційної інформації.

Регулярне створення резервних копій є важливою частиною стратегії безпеки, оскільки дозволяє відновити інформацію у разі її втрати чи пошкодження через атаки або непередбачені обставини.

Технології хмарної безпеки постійно вдосконалюються, зокрема завдяки інтеграції новітніх рішень, таких як штучний інтелект (ШІ) та машинне навчання (МН), які допомагають виявляти нові загрози та оперативно реагувати на них.

Очікується, що в майбутньому хмарні сервіси стануть ще більш захищеними завдяки впровадженню сучасних методів шифрування, автоматизації безпекових процесів та удосконаленому моніторингу. Виклики і майбутнє кіберзахисту

Попри всі досягнення, кіберзахист стикається з кількома суттєвими проблемами. Одна з основних — це швидкий розвиток кіберзагроз. Злочинці постійно удосконалюють свої методи атак, здатні обходити навіть найсучасніші системи захисту.

Це вимагає постійного оновлення та вдосконалення технологій кібербезпеки. Також існує проблема несумісності різних систем захисту.

Оскільки організації використовують різні технології безпеки, це може створювати вразливості в загальній екосистемі кіберзахисту.

Для розв'язання цієї проблеми необхідно створювати універсальні платформи і стандарти, які дозволяють ефективно інтегрувати різні засоби захисту. Не менш важливим викликом є людський фактор. Недостатня обізнаність користувачів про кіберзагрози може призвести до помилок, що знижують ефективність навіть найновітніших технологій захисту. На мою думку, досить чітко на цю деталь звернув увагу колишній хакер, а нині експерт із безпеки Кевін Мітнік: «Люди — це найслабша ланка в ланцюгу безпеки. Ви можете встановити найскладніші системи захисту, але якщо людина припуститься помилки, вся безпека руйнується» [14].

Тому важливим напрямом є підвищення рівня обізнаності і навчання основам кібербезпеки серед усіх користувачів Інтернету.

3.2 Роль міжнародної співпраці у забезпеченні інформаційної безпеки України

У сучасному глобалізованому світі інформаційна безпека стає однією з найважливіших складових національної безпеки кожної держави. Для України, яка стикається з постійними геополітичними та військовими викликами,

питання захисту інформації набуває надзвичайної важливості. Інформаційні війни, кібератаки, дезінформація та пропаганда є невід'ємною частиною гібридної війни, що ведеться проти України її агресором. В таких умовах міжнародна співпраця відіграє критичну роль у забезпеченні надійної інформаційної безпеки країни. Варто виокремити слова експерта з кібербезпеки Євгена Касперського: «Сучасні загрози настільки складні, що для захисту необхідна глобальна кооперація між країнами та компаніями», який досить чітко підкреслив важливість міжнародної співпраці в галузі кібербезпеки. [13]

У цьому контексті міжнародна співпраця в сфері інформаційної безпеки не лише надає технічну підтримку, а й виступає важливим інструментом для зміцнення стратегічних альянсів і спільної боротьби з глобальними загрозами.

Тому роль міжнародної співпраці у забезпеченні інформаційної безпеки України є незамінною.

Одним із ключових напрямків міжнародної співпраці України є активна участь у глобальних організаціях, що займаються питаннями інформаційної безпеки. До таких організацій належать Організація Об'єднаних Націй (ООН), НАТО, Європейський Союз (ЄС), а також різноманітні двосторонні та багатосторонні угоди з країнами-партнерами.

Міжнародна співпраця в сфері інформаційної безпеки включає обмін інформацією про кіберзагрози, що є важливим аспектом у боротьбі з глобальними кіберзлочинами. Платформи, такі як EUROPOL, INTERPOL та інші міжнародні механізми обміну даними, допомагають координувати дії між країнами під час великих кіберінцидентів. Це дозволяє оперативно визначати джерела атак і знижувати ймовірність їх повторення. Спільні зусилля та обмін знаннями створюють ефективний бар'єр для кібератак і мінімізують їхні наслідки.

Незважаючи на значні переваги міжнародної співпраці в сфері кібербезпеки для України, існують певні труднощі. Однією з основних є необхідність інтеграції різних кібербезпекових систем у рамках цієї співпраці, що вимагає постійної модернізації та адаптації до новітніх технологій і методів

кіберзагроз. Іншою важливою проблемою є різні рівні доступу до інформації та різні правові системи кіберсуб'єктів. У таких умовах важливо розробляти стандарти безпеки, які враховують різноманіття технічних та правових підходів.

Європейський Союз грає важливу роль у зміцненні інформаційної безпеки України, пропонуючи програми співпраці, які сприяють удосконаленню національних механізмів захисту інформації. Однією з основних ініціатив ЄС є допомога Україні в адаптації європейських стандартів у галузі кібербезпеки та захисту даних. Це передбачає надання технічної підтримки, підготовку кадрів, а також реалізацію спільних проектів у сфері розвитку інформаційної інфраструктури.

Однією з ключових ініціатив Європейського Союзу є підтримка України в розбудові та вдосконаленні національної інфраструктури кібербезпеки. ЄС надає Україні технічну підтримку для розробки систем моніторингу та захисту від кіберзагроз, сприяючи створенню національних команд оперативного реагування на кіберінциденти (CERT).

Це дає змогу Україні швидко виявляти загрози та вживати необхідних заходів для їх усунення. Технічна допомога під час інцидентів: У разі серйозних кіберінцидентів, таких як хакерські атаки на критичну інфраструктуру, ЄС надає технічну підтримку. В своєму виступі свою позицію щодо боротьби з хакерами пояснив експерт з кібербезпеки Мікко Гіппонен: «Захист від хакерів не залежить лише від технологій — це поєднання технологій, процесів і культури безпеки»[3].

Це може включати надання інструментів для виявлення та нейтралізації загроз, аналізу вразливостей і визначення джерела атаки. Європейські фахівці також можуть бути залучені до спільних команд для швидкого реагування на кібератаки, що допомагає зменшити шкоду та оперативно усунути наслідки інциденту. ЄС також активно підтримує оновлення національних органів, відповідальних за кібербезпеку, зокрема Державної служби спеціального зв'язку та захисту інформації України.

Іншим важливим напрямком допомоги ЄС є розробка правових та нормативних основ для забезпечення кібербезпеки. ЄС допомагає інтегрувати європейські стандарти та практики в українське законодавство, зокрема щодо захисту персональних даних, боротьби з кіберзлочинністю та забезпечення безпеки критичної інфраструктури. Україна вживає заходи для впровадження законодавчих ініціатив, що відповідають Загальному регламенту захисту даних (GDPR), що покращує захист персональних даних громадян.

Програмою «Східне партнерство» ЄС також надає Україні значну підтримку в зміцненні кібербезпеки, фінансуючи тренінги, симуляції кіберінцидентів та обмін досвідом між Україною та європейськими країнами. Крім того, ЄС сприяє співпраці через Агентство ЄС з кібербезпеки (ENISA), що дозволяє Україні бути в курсі останніх тенденцій та технологій у галузі кібербезпеки.

Європейський Союз активно працює над розвитком спільної кібербезпеки в регіоні, створюючи платформи для обміну інформацією між державами-членами, що дає Україні можливість долучатися до міжнародних ініціатив щодо протидії кіберзагрозам. Однією з таких ініціатив є програма «Cybersecurity Capacity Building», яка забезпечує Україну необхідними ресурсами та технологіями для підвищення рівня кіберзахисту.

Співпраця США та України в галузі кібербезпеки розпочалася після анексії Криму Росією в 2014 році та ескалації конфлікту на сході України. США одними з перших відреагували на ці виклики, надавши Україні необхідну технічну, фінансову та консультаційну підтримку для посилення її кіберзахисту. Зокрема, американські партнери брали участь у створенні та розвитку Національного центру реагування на кіберінциденти (CERT-UA) та організовували навчальні програми для українських фахівців у сфері кібербезпеки.

Основним напрямком співпраці стало удосконалення технологічної інфраструктури для ефективного протистояння кіберзагрозам. США надали Україні доступ до передових технологій для моніторингу, аналізу та захисту від

кібератак. Наприклад, у 2017 році американські фахівці допомогли виявити та нейтралізувати вірус NotPetya, один з найбільших кібернападів, що вразив українські компанії та державні установи. Вони також надали консультації та допомогу у відновленні пошкоджених систем, що дозволило значно знизити збитки та уникнути серйозніших наслідків.

Ще одним важливим аспектом співпраці є обмін інформацією щодо кіберзагроз та спільна розробка стратегій для боротьби з ними. США та Україна активно обмінюються даними про кіберзлочинність та потенційні кібератаки, що дозволяє оперативно виявляти загрози та вживати необхідних заходів для їх нейтралізації. Крім того, обидві країни співпрацюють у міжнародних організаціях, таких як Глобальна ініціатива з кібербезпеки та Європейська мережа центрів реагування на інциденти (ENISA), що сприяє зміцненню міжнародної кібербезпеки та координації дій у протидії кіберзагрозам.

Спільні кібероперації та тренування: США активно співпрацюють з Україною через спільні тренування та кібероперації, що сприяють ефективній взаємодії в протидії кіберзагрозам. Програми, що фінансуються США, включають участь українських фахівців у міжнародних кібернавчаннях та змаганнях, таких як «Cyber Storm», де проводяться тренування з реагування на масштабні кіберзагрози.

США також вкладають кошти в розвиток кіберінфраструктури України, зокрема через програми, що сприяють оновленню державних органів та приватних підприємств. Це охоплює фінансування та технічну підтримку для посилення захисту критичних інформаційних систем і створення платформ, стійких до кіберзагроз. Україна активно співпрацює з НАТО в межах програми «Партнерство заради миру», зокрема, щодо підготовки військових та цивільних фахівців у сфері кібербезпеки. Спеціалісти беруть участь у курсах, тренінгах та семінарах, які допомагають покращити захист національної кіберінфраструктури та ефективно реагувати на кіберзагрози.

Агентство США з міжнародного розвитку (USAID) надає Україні підтримку через освітні курси та програми для підвищення кваліфікації

фахівців у сфері кібербезпеки. Однією з ключових ініціатив є навчальна програма для державних установ і приватного сектору, яка допомагає створювати ефективні системи кіберзахисту. Європейський Союз активно підтримує Україну через різні проекти, зокрема «EU CyberNet», який сприяє розвитку інфраструктури кібербезпеки та проводить навчання для українських фахівців. ЄС надає технічну підтримку, організовує тренінги та відкриває можливості для участі у міжнародних конференціях і семінарах з кібербезпеки.

Технічна допомога та координація з західними партнерами для боротьби з вірусом Notpetya

Першим кроком західних партнерів після виявлення атаки NotPetya стало надання термінової технічної допомоги для аналізу та реагування на інцидент. Сполучені Штати, Великобританія та країни ЄС залучили свої кібербезпекові агентства, зокрема CISA (Cybersecurity and Infrastructure Security Agency) та GCHQ (Government Communications Headquarters) Великобританії, щоб підтримати Україну у виявленні джерела атак, поширенні шкідливого коду та оцінці масштабу збитків.

Західні фахівці також надали інструменти для моніторингу інфраструктури, що дало змогу українським організаціям оперативно виявляти зараження та вживати заходів для ізоляції систем від подальшого розповсюдження вірусу. Для цього використовувалися спеціалізовані програми та платформи для аналізу шкідливих програм, розроблені як агентствами, так і приватними компаніями на Заході.

Одним із важливих аспектів допомоги західних партнерів була спільна робота над розслідуванням атаки, що дозволило виявити джерело загрози.

Фахівці з FBI та інших американських і європейських агентств кібербезпеки брали участь у розслідуванні, що допомогло точно визначити, що вірус NotPetya був спеціально створений як частина кібервійни. Міжнародне дослідження показало, що вірус використовував вразливості в програмному забезпеченні Microsoft і M.E.Doc, через які він потрапляв до організацій. Це

дозволило українським установам вжити додаткових заходів для запобігання майбутніх атак і усунути слабкі місця в національних мережах.

Допомога західних партнерів під час кібератак на Українf є важливим чинником для забезпечення стабільності та кібербезпеки країни. Технічна підтримка, навчання, обмін інформацією, розслідування інцидентів дають змогу Україні ефективно протидіяти кіберзагрозам. Завдяки співпраці з міжнародними партнерами Україна зміцнює свою кіберінфраструктуру, запобігає новим атакам і зменшує наслідки кібератак.

3.3. Рекомендації щодо підвищення інформаційної культури населення та боротьби з дезінформацією.

Підвищення рівня інформаційної грамотності населення та боротьба з дезінформацією є надзвичайно важливими викликами сучасного суспільства. У нинішніх умовах, коли фейкові новини поширюються миттєво, а інформаційні атаки можуть суттєво впливати на суспільну думку та процеси, необхідно формувати в людей навички критичного мислення, аналізу достовірності інформації та протистояння маніпуляціям. Щоб не стати жертвою кіберзлочинців, державі необхідно дотримуватися таких рекомендацій та статегій як впровадження курсів медіаграмотності у школах, університетах і на професійних тренінгах. Курси мають включати в себе методи перевірки джерел, аналіз маніпулятивних технік у медіа та вміння розрізняти факти та думки. організація онлайн-платформ для навчання медіаграмотності, що доступні для широкої аудиторії. В сучасних умовах необхідним є інтеграція медіаграмотності у шкільній програмі, треба щоб уроки медіаграмотності включали до навчальних дисциплін, таких як громадянська освіта, історія та українська мова, створювались інтерактивних навчальних матеріалів, які дозволять учням аналізувати реальні приклади дезінформації.

Багато дорослого населення може стати жертвою кіберзлочинів, тому варто проводити публічн семінари, тренінги і вебінари для різних вікових груп.

Необхідно залучати громадські організації для організації просвітницьких заходів у громадах.

Розвиток платформ фактчекінгу є невід'ємною частиною боротьби з кіберзлочинністю підтримка і розвиток незалежних фактчекінгових організацій, таких як StopFake або VoxCheck. Створення державних та громадських ініціатив для популяризації фактчекінгу. Партнерство з медіа та стимулювання традиційних медіа до дотримання стандартів журналістики, співпраця з провідними платформами для просування матеріалів, які базуються на фактах. Державі необхідно вводити освітні компанії, проведення компаній у соціальних мережах із закликом до перевірки інформації. Законодавчі ініціативи, такі як розробка законів, що передбачають відповідальність за цілеспрямоване поширення фейків, захист журналістів-розслідувачів та фактчекерів від юридичних переслідувань, використання інфографіки та відео для популяризації ідей критичного мислення. Також необхідне створення правових та технологічних умов для боротьби з дезінформацією, а саме розробка законів, що передбачають відповідальність за цілеспрямоване поширення фейків, захист журналістів-розслідувачів та фактчекерів від юридичних переслідувань.

Важливу роль у сучасному світі де кіберпростір є невід'ємною частиною життя населення та держави є Технологічні рішення використання штучного інтелекту для виявлення фейкових новин та ботів. Розробка інструментів аналізу контенту, які допомагають користувачам швидко оцінювати достовірність інформації. Розвиток культури усвідомленого споживання для заохочення користувачів соціальних мереж перевіряти достовірність інформації, перш ніж ділитися нею з іншими та введення позначок автентичності для надійних джерел на платформах соціальних мереж. Людей треба навчити керувати своїми емоціями під час отримання провокаційних чи шокуючих новин. Потрібна розробка програм, спрямованих на зміцнення стійкості до інформаційного тиску та маніпуляцій.

Держава створює та впроваджує загальнонаціональні програми, спрямовані на розвиток медіаграмотності населення, також постійний

моніторинг інформаційного простору для виявлення та запобігання поширенню дезінформації допомагає у вирішенні проблем кібербезпеки, ініціювання проєктів, які мотивують молодь активно долучатися до боротьби з фейками та інформаційними маніпуляціями та формування волонтерських спільнот, що займаються просвітництвом та популяризацією критичного мислення, що є невід'ємною частиною сучасного суспільста.

Міжнародний досвід і співпраця.

Україна користується запозиченням світових практик у країн, які досягли успіху в боротьбі з дезінформацією, наприклад, Фінляндії, що має один із найвищих рівнів медіаграмотності у світі. Налагодження взаємодії з глобальними організаціями, такими як ЮНЕСКО, для адаптації та впровадження передових методик, обмін знаннями з країнами Європи щодо використання цифрових інструментів для боротьби з інформаційними загрозами.

В сучасному світі треба дуже швидко реагувати на кіберінциденти і адаптуватися під них у цифровому середовищі. Наприклад захист дітей і підлітків, а саме розробка освітніх програм, спрямованих на молодь, яка найбільше піддається впливу дезінформації. Створення інструментів для батьківського контролю, щоб забезпечити доступ до надійної інформації. виявлення нових форм дезінформації, дослідження того, як дезінформація поширюється через меми, візуальний контент і відео.

Просвітницькі ініціативи у громадах

Для того щоб вберегти людей від кіберзагроз необхідно проведення заходів у регіонах, що мають високий ризик інформаційного впливу із залученням місцевих лідерів до просвітницької роботи. Використання соціальних мереж

залучення лідерів думок до поширення перевіреної інформації та використання TikTok, Instagram та інших платформ для донесення ідей медіа грамотності.

Популяризація наукових досліджень з інформаційної культури.

Для популяризації наувих досліджень використовують аналіз поведінки користувачів в умовах дезінформації, вивчення реакцій людей на фейкові новини, маніпулятивні заголовки та пропагандистські матеріали. В наш час кожна людина стикається з дезінформацією в будь яких галузях, тому важливо застосування методів соціологічних опитувань, аналізу даних у соціальних мережах та експериментів для оцінки впливу дезінформації та виявлення груп населення, які найбільш схильні до впливу дезінформаційних кампаній, та розробка рекомендацій для їх захисту. Вивчення взаємозв'язку між джерелами інформації, емоційними реакціями аудиторії та її діями.

Результати досліджень необхідно поширювати та публікувати наукові статті у доступних форматах та організація конференцій і круглих столів на тему інформаційної безпеки.

Коли майже все населення України сидить в Інтернеті, багато людей не відчувають своєї відповідальності за речі які там робить, тому необхідний Розвиток особистої відповідальності за поширення інформації, етичне виховання, пояснення важливості дотримання етики у соціальних мережах та

навчання принципам цифрової гігієни. Громадян активно залучають до проектів та платформ які дозволяють людям ставати частиною боротьби з дезінформацією, організація флешмобів та акцій, які сприяють поширенню правдивої інформації.

Ці поради мають сприяти створенню ефективної системи боротьби з дезінформацією та покращенню інформаційної грамотності серед громадян.

Реалізація кожної з них потребує співпраці різних секторів та активної участі кожної людини в суспільстві.

Висновки до третього розділу.

Узагальнюючи, шляхи вдосконалення системи інформаційної безпеки України можна описати як комплексний підхід, який включає низку ключових напрямків:

1. Стратегічне управління: Потрібно розробити і впровадити єдину національну стратегію інформаційної безпеки, яка забезпечить інтеграцію зусиль державних органів, приватного сектору та громадян у боротьбі з кіберзагрозами;
2. Зміцнення законодавчої та інституційної основи: Важливо удосконалити законодавство, створити спеціалізовані органи та центри, що будуть відповідати за координацію дій у сфері кібербезпеки, а також впроваджувати ефективні механізми боротьби з кіберзлочинами;
3. Технічне оснащення та інновації: Україні слід інвестувати в новітні технології для захисту інформаційних систем, зокрема в системи моніторингу кіберзагроз та в технології криптографії, що дозволяють забезпечити високий рівень захисту інформації;
4. Навчання та підвищення обізнаності: Важливо проводити освітні програми для громадян і професіоналів, аби підвищити загальний рівень обізнаності та готовності до кіберзагроз;
5. Міжнародна співпраця: Україна повинна активно співпрацювати з іншими країнами і міжнародними організаціями, аби обмінюватися досвідом і технологіями, а також координувати дії на глобальному рівні для протидії кіберзлочинності.

Усе це разом дозволить створити більш захищену та ефективну систему інформаційної безпеки в Україні, здатну протистояти сучасним викликам і загрозам.

ВИСНОВКИ

У кваліфікаційній роботі було проведено дослідження на тему «Інформаційна безпека України: протидія ворожій пропаганді». Протягом проведення досліджень у кваліфікаційній роботі було досліджено та проаналізовано вищепоставлених завлань, а саме: розкрито поняття та значення інформаційної безпеки в сучасному світі, виявлено та проаналізувано основні загрози інформаційній безпеці України, досліджено нормативно-правову базу забезпечення інформаційної безпеки в Україні, а також стан та динаміку розвитку кібербезпеки.

Під час проведення досліджень було проаналізувано проблему дезінформації та впливу пропаганди на інформаційний простір України, дано оцінку ефективності державних заходів у сфері інформаційної безпеки, досліджено інтеграцію сучасних технологій кіберзахисту, визначено та проаналізувано роль міжнародної співпраці у забезпеченні інформаційної безпеки України та надано рекомендації щодо підвищення інформаційної культури населення та боротьби з дезінформацією.

Україна вже має деякі успіхи в боротьбі з ворожою пропагандою, зокрема через розвиток кіберзахисту, зміцнення інформаційної політики та організацію роботи медіа, які орієнтовані на правдиву і об'єктивну подачу інформації. Однак наявні інституції та заходи не є достатньо ефективними для повної протидії, і потрібно вдосконалювати механізми реагування.

Серед основних проблем в протидії ворожій пропаганді можна виділити:

- Недостатній рівень координації між державними органами, медіа та громадянським суспільством у боротьбі з дезінформацією;
- Низька обізнаність населення щодо методів маніпуляцій у медіа та соціальних мережах;
- Обмежені ресурси та технології для моніторингу і нейтралізації ворожої пропаганди, особливо в умовах масштабних інформаційних атак.

Проте, важливо приділяти увагу щодо вдосконалення системи протидії ворожій пропаганді, а саме розвитку єдиної стратегії інформаційної безпеки, яка б включала заходи для боротьби з пропагандою і маніпуляціями в медіа-просторі, зміцненню державної інформаційної політики та підтримувати незалежні медіа, що працюють в інтересах правди і демократії.

У рамках проведеного дослідження було детально розглянуто сучасні підходи до протидії інформаційним загрозам, що дозволило визначити ключові виклики у сферах кібербезпеки, протидії пропаганді та дезінформації, а також окреслити ефективні методи їхнього подолання.

Аналіз правової бази України в галузі інформаційної безпеки виявив низку недоліків, які потребують усунення для створення надійної системи захисту інформаційного простору. Також було підкреслено важливість адаптації національного законодавства до міжнародних стандартів.

Дослідження технологій боротьби з пропагандою та дезінформацією продемонструвало необхідність використання сучасних інструментів, таких як штучний інтелект, системи автоматизованого моніторингу та обробки великих обсягів даних. Ці технології здатні значно підвищити швидкість і точність реагування на загрози.

Рекомендації, розроблені в межах дослідження, спрямовані на зміцнення стійкості інформаційного простору України. Вони включають впровадження комплексного підходу до інформаційної безпеки, посилення міжнародного співробітництва, навчання громадян основам медіаграмотності та підвищення їхньої обізнаності щодо інформаційних ризиків.

Таким чином, отримані результати стали важливим підґрунтям для подальшого розвитку системи інформаційної безпеки України, враховуючи сучасні виклики та потреби цифрового суспільства.

Отже, для ефективної протидії ворожій пропаганді Україні необхідно створити комплексну та добре організовану систему інформаційної безпеки, що базується на інноваційних технологіях, законодавчих ініціативах, а також на активному залученні громадянського суспільства. Тільки так можна забезпечити стійкість до маніпуляцій, зміцнити соціальну згуртованість та захистити національні інтереси в інформаційному просторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. CERT-UA — Центр реагування на інциденти в інформаційних системах України. — [Електронний ресурс]. — Режим доступу: https://cert.gov.ua.
2. NotPetya: Кібератака, що спричинила глобальні наслідки / Imena. — [Електронний ресурс]. — Режим доступу: https://www.imena.ua/blog/notpetya-cyberattack/.
3. Гіппонен, М. Виступ на TED: «Три типи онлайн-злочинців». — [Електронний ресурс]. — Режим доступу: https://www.ted.com/talks/mikko_hypponen/ .
4. Головченко, М. О. Національна безпека України: концептуальні основи та практика забезпечення / М. О. Головченко. — К. : Видавничий дім "Ін Юре", 2017. — 312 с.
5. ДСТУ 2392–94. Інформація та документація. Базові поняття. Терміни та визначення. [Чинний від 1995-01-01]. Київ : Держстандарт України, 1994. С. 53.
6. ДСТУ 3017-95. Видання. Основні види. Терміни та визначення. [Чинний від 01.01.1996]. Київ. : Держстандарт України, 1995. – 47 с.
7. ДСТУ 4163:2020. Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів. [Чинний від 2021.09.01]. Вид. офіц. Київ : Держспоживстандарт України, 2020, 22 с.
8. Журнал "Science and Education a New Dimension". — [Електронний ресурс]. — Режим доступу: http://lsej.org.ua/12_2023/100.pdf.
9. Захист критичної інфраструктури: актуальні питання та рішення / Wezom. — [Електронний ресурс]. — Режим доступу: https://wezom.com.ua/ua/blog/zahist-kritichnoyi-infrastrukturi.
10. Ільницька, О. М. Роль інформаційної безпеки в системі національної безпеки України / О. М. Ільницька. — [Електронний ресурс]. — Режим

доступу: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf.

11. Інститут психології і прав людини. — [Електронний ресурс]. — Режим доступу: https://ippi.org.ua/sites/default/files/14_17.pdf.
12. Інформаційна безпека / Науковий журнал. — [Електронний ресурс]. — Режим доступу: https://sit.nuou.org.ua/article/view/239988/239388.
13. Касперський, Є. *Глобальна кіберзагроза: новий порядок денний для урядів та бізнесу*. — [Електронний ресурс]. — Режим доступу: https://www.kaspersky.com/.
14. Кевін Мітнік: "Люди — найслабша ланка в ланцюгу безпеки". — [Електронний ресурс]. — Режим доступу: https://www.example.com. — Дата доступу: 24 грудня 2024 року.
15. Кібезпека в Україні: шляхи розвитку та можливості / Укрінформ. — [Електронний ресурс]. — Режим доступу: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html.
16. Конвенція Ради Європи про кіберзлочинність (Конвенція Будапештська) : підписана 23 листопада 2001 року в м. Будапешт, набрала чинності 1 липня 2004 року. — [Електронний ресурс]. — Режим доступу: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
17. Концепція національної безпеки України : затверджена Указом Президента України від 26 квітня 2003 року № 404/2003. — [Електронний ресурс]. — Режим доступу: https://www.president.gov.ua/documents/4042003-527.
18. Ландо, С. Захист даних як пріоритет цифрової ери // *Кібербезпека та приватність*. — 2022. — №3. — С. 12–18.
19. Медіааналіз у сфері інформаційної безпеки / Детектор медіа. — [Електронний ресурс]. — Режим доступу: https://ms.detector.media/mediaanalitika/post/15168/2015-12-09-otsinka-efektyvnosti-diy-organiv-vlady-v-sferi-informatsiynoi-bezpeky-v-2014-15-rr/.
20. Наукова бібліотека Педагогічного університету. — [Електронний ресурс]. — Режим доступу: https://library.pp-ss.pro/index.php/ndippsn_20231212.

21. ОБСЄ. Офіційний звіт про ситуацію в Україні. — [Електронний ресурс]. — Режим доступу: https://www.osce.org/files/f/documents/0/2/175056.pdf.
22. Палій, О. В. Стратегічні основи національної безпеки України / О. В. Палій. — К. : Наукова думка, 2019. — 200 с.
23. Право і суспільство / Науковий журнал. — [Електронний ресурс]. — Режим доступу: http://pravoisuspilstvo.org.ua/archive/2012/3_2012/28.pdf.
24. Про захист персональних даних : Закон України від 20 листопада 2012 р. № 5491-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 22.12.2024).
25. Про інформацію : Закон України від 02 жовтня 1992 р. № 2658-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 22.12.2024).
26. Про основи національної безпеки України : Закон України від 16 липня 2023 р. № 3858-IX. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 22.12.2024).
27. Про основні засади забезпечення кібербезпеки : Закон України від 21 червня 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 22.12.2024).
28. Пропаганда Росії в українських містах: Херсонщина, Маріуполь, Мелітополь / Радіо Свобода. — [Електронний ресурс]. — Режим доступу: https://www.radiosvoboda.org/a/khersonshchynv-mariupol-melitopol-propahada-rosiyi/31828320.html.
29. Протистояти кіберзагрозам: спільні зусилля / Армія Інформ. — [Електронний ресурс]. — Режим доступу: https://armyinform.com.ua/2022/02/05/protystoyaty-kiberzagrozam-spilno/.
30. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам / Європейська Бізнес Асоціація. — [Електронний ресурс]. — Режим доступу: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/.

31.Стратегія національної безпеки України : затверджена Указом Президента України від 14 вересня 2015 року № 555/2015. — [Електронний ресурс]. — Режим доступу: https://www.president.gov.ua/documents/5552015-19088.

32. ЦБІС КНУ. — [Електронний ресурс]. — Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/issue/view/29.

33. Як російська пропаганда поляризує українське суспільство / УНІАН. — [Електронний ресурс]. — Режим доступу: https://www.unian.ua/society/yak-rosiyska-propaganda-polyarizuye-ukrajinske-suspilstvo-12464529.html.

34. Як технології змінюють сферу кібербезпеки / УА Генерал. — [Електронний ресурс]. — Режим доступу: https://uageneral.net/blog/it/iak-tekhnologii-zminiuiut-sferu-kiberbezpeky/.