МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ЛІНГВІСТИКИ ТА СОЦІАЛЬНИХ КОМУНІКАЦІЙ
КАФЕДРА ІСТОРІЇ ТА ДОКУМЕНТОЗНАВСТВА

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ (І. І. Тюрменко)
«_____»_____2023 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОС «МАГІСТР»

Тема: «Соціальні мережі як середовище інформаційних загроз».

Виконавець: здобувачка вищої освіти ДК 221М Божко Марина Геннадіївна

Керівник: кандидат історичних наук, доцент Божук Людмила Володимирівна

Нормоконтролер: кандидат історичних наук, доцент Халецька Леся Пилипівна

_____
(підпис)

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Факультет лінгвісти та соціальних комунікацій
Кафедра історії та документознавства
Галузь знань – 02 «Культура і мистецтво»
Спеціальність – 029 «Інформаційна, бібліотечна та архівна справа»
Освітня програма – «Документознавство та інформаційна діяльність»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ І. І. Тюрменко
«____»_____ 2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи
Божко Марини Геннадіївни

1. Тема кваліфікаційної роботи: «Соціальні мережі як середовище інформаційних загроз» затверджена наказом ректора від «19» вересня 2023 р. № 1834/ст.

2. Термін виконання роботи: з 25.09.2023 р. до 24.12.2023 р.

3. Вихідні дані до роботи: робота складається зі вступу, трьох розділів, висновків, списку використаних джерел, загальним обсягом 109 сторінок, з них обсяг основного тексту – 93 сторінки, список використаних джерел нараховує 79 позицій.

4. Зміст пояснювальної записки: Вступ. Розділ 1. Стан розроблення теми кваліфікаційної роботи у науковій літературі та джерелах. Розділ 2. Соціальні мережі як середовище інформаційного впливу та загроз. Розділ 3. Специфіка роботи з інформацією та соціальними мережами ТОВ «БАСФ Т.О.В». Висновки. Список використаних джерел. Додатки.

Перелік обов’язкового графічного (ілюстративного матеріалу): скріншот офіційного сайту ТОВ «БАСФ Т.О.В»; скріншот сторінки ТОВ «БАСФ Т.О.В» у мережі «Фейсбук»; скріншот із дописом ТОВ «БАСФ Т.О.В» у соціальній мережі «Фейсбук»; скріншот офіційних сторінок ТОВ «БАСФ Т.О.В» у соціальній мережі «Інстаграм»; допис ТОВ «БАСФ Т.О.В» у соціальній мережі «Інстаграм»; сторіс ТОВ «БАСФ Т.О.В» у соціальній мережі «Інстаграм».

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1.	Визначення та обґрунтування теми кваліфікаційної роботи	02.09.2023	
2.	Оформлення завдання на виконання кваліфікаційної роботи. Складання плану роботи. Узгодження з керівником	08.09.2023	
3.	Визначення об`єкта, предмета, мети, завдань дослідження. Підбір, опрацювання, вивчення літератури та джерел з теми дослідження	18.09.2023	
4.	Виконання індивідуальних завдань з теми роботи	22.09.2023	
5.	Написання основної частини, вступу та висновків	30.10.2023	
6.	Оформлення роботи та подання її на перше читання керівникові	02.11.2023	
7.	Опрацювання зауважень та виправлення недоліків	10.11.2023	
8.	Попередній захист кваліфікаційної роботи	30.11.2023	
9.	Проходження нормоконтролю	01.12.2023	
10.	Подання роботи на перевірку на плагіат	07.12.2023	
11.	Подання роботи на рецензування	11.12.2023	
12.	Подання остаточного варіанта на кафедру	18.12.2023	
13.	Захист роботи	25.12.2023	

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв

8. Дата видачі завдання: «08» вересня 2023 р.

Керівник кваліфікаційної роботи _____Л.В. Божук
підпис

Завдання прийняв до виконання _____ М.Г. Божко
підпис

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи ОС «Магістр» «Соціальні мережі як середовище інформаційних загроз»: 109 сторінок, 79 використаних джерела, додатки.

КОМУНІКАЦІЯ, СОЦІАЛЬНІ МЕРЕЖІ, ІНФОРМАЦІЯ, ІНФОРМАЦІЙНИЙ ВПЛИВ, ІНФОРМАЦІЙНА ЗАГРОЗА, МЕДІАГРАМОТНІСТЬ, БЕЗПЕКА КОРИСТУВАЧІВ, ІНФОРМАЦІЙНИЙ ВІДДІЛ.

Об’єкт дослідження – інформаційні загрози.

Предмет дослідження – соціальні мережі як середовище інформаційного впливу та загроз.

Мета дослідження – аналіз та узагальнення інформаційних загроз, які існують у соціальних мережах, з метою розуміння їх впливу на користувачів та розробка рекомендацій щодо забезпечення безпеки та захисту в інтернет-середовищі.

Методи дослідження. У роботі використано загальнонаукові методи, такі як: аналіз та синтез, індукції та дедукції, текстологічного аналізу, порівняння, узагальнення, бібліографічний. Також конкретно-наукові, такі як: системний, прогнозування, контент-аналіз, таблично-графічний метод.

У кваліфікаційній роботі оглянуто специфіку соціальних мереж, а також охарактеризовано інформаційні загрози та вплив цих факторів на безпеку користувачів. Проаналізовано соціальні мережі як середовище для інформаційного впливу та формування небезпек інформаційного простору.

Практичне значення дослідження полягає у тому, що основні його положення можуть бути використані при вивченні фахових дисциплін, під час підготовки до лекцій чи практичних занять, наприклад, з курсу «Соціальні комунікації», також для написання курсових та кваліфікаційних робіт. Результати дослідження мають сприяти практиці організації безпечного користування підприємствами соціальними мережами та ознайомлення працівників з базовими інформаційними загрозами.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Неможливо заперечувати, що соціальні мережі є феноменом XXI століття, але починали своє існування, як «мережа для зав'язування дружніх відносин та пошуку партнерів для романтичних стосунків». Нині ж їх аудиторія зростає стрімкими темпами, вони стали одним з основних комунікаційних каналів у розвитку ділових відносин, за їх допомогою моніторять діяльність конкурентів, покращують якість обслуговування, а також просувають свою продукцію тощо.

Соціальні мережі відіграють важливу роль у формуванні суспільних думок, переконань і цінностей, змінюють способи взаємодії організацій із клієнтами, формування брендів і спілкування з оточуючим світом. Саме тому дослідження цієї теми є досить важливими, адже можуть розкривати, зокрема, такі аспекти проблеми: як соціальні мережі впливають на масову свідомість і сприяють поширенню певних ідей, та як це впливає на суспільний розвиток.

Крім того, необхідно зазначити, що питання впливу соціальних мереж на психологічне здоров'я користувачів, включаючи такі аспекти як: стрес, депресія, залежність від соціальних мереж та ізольованість також є на часі. А, крім того, через зростання аудиторії, збільшується й цікавість до цієї теми, загалом.

Проте, вивчаючи саме інформаційний аспект впливу соціальних мереж, неможливо не зазначити, що завдяки ним відбуваються зміни в процесах політичної активності, виборів, мобілізації громадськості та організації протестів. Особливу увагу також необхідно приділяти проблемам щодо кіберзлочинів на платформах соціальних мереж, а також способам їх запобігання і боротьби. Нині значно збільшилися випадки подібної злочинної діяльності, що зачіпають не тільки організації, але і простих користувачів. Особливо актуальним питання боротьби із кіберзлочинністю та організації заходів безпеки є для великих корпорацій та компаній, які постійно перебувають під загрозою витоку інформації або персональних, службових чи конфіденційних даних, що, зокрема, й доводить важливість означеної проблеми.

Загалом, соціальні мережі можна охарактеризувати як середовище інформаційного впливу з кількох ключових аспектів.

По-перше, через розповсюдження інформації, адже саме ці мережі дозволяють користувачам легко поширювати інформацію – чи то новини, думки, відео, фотографії або інші вміст. Це створює можливість для швидкого й масового поширення інформації.

По-друге, вплив на громадську думку і формування поглядів широкого загалу через впливових користувачів, вірусні кампанії та тематичні групи. Інформація, яку користувачі бачать у своїх стрічках, може визначати їхні погляди й переконання, або безпосередньо впливати на них.

По-третє, через явище, що відоме як «фільтр бульбашок». Соціальні мережі використовують алгоритми, щоби показувати користувачам контент, який відповідає їхнім інтересам і поглядам. Це може призвести до створення «фільтру бульбашок», коли користувачі бачать лише інформацію, яка підтверджує їхні погляди, і не бачать альтернативних точок зору.

По-четверте, через роль соціальних мереж у новинах і журналістиці. Багато людей отримують новини через соціальні мережі. Журналісти використовують їх для розповсюдження статей та аналітики, і це може впливати на розуміння глобальних подій.

По-п’яте, вплив соціальних мереж на товари й послуги неможливо заперечити. Рекламодавці використовують соціальні мережі для просування товарів і послуг. Користувачі можуть впливати на інших своїми відгуками та рекомендаціями.

По-шосте, можливість мобілізації громадськості, оскільки саме соціальні мережі стали платформою для організації протестів, акцій та громадських рухів. Вони дозволяють людям об’єднуватися навколо спільних ідей та цілей.

По-сьоме, загроза для приватності, адже спільність даних у соціальних мережах може викликати проблеми з приватністю та безпекою. Інформація, якою користувачі діляться, може стати предметом зловживання або злочинності.

Зважаючи на вищезазначене, дійсно важко переоцінити інформаційний вплив сучасних соціальних платформ для суспільства, які розпочинали як середовища обміну думками та спілкування, на користувачів та компанії.

Варто додати, що соціальні мережі мають значний вплив на залучення потенційних клієнтів. Усе тому, що зацікавлена аудиторія може побачити візуалізацію діяльності підприємства, а саме фото- та відеозвіти, фінансові документи, статистичні дані. Тобто, якщо клієнт хоче переконатися у результативності компанії, то він у першу чергу зверне увагу на наявність зображень на вебпорталі підприємства.

Крім того, важливо вказати, що соціальні мережі можуть змінювати думки великих мас суспільства, навіть народів. Наприклад, вплив дезінформації та пропаганди, яка циркулює в соціальних мережах Росії, як найяскравіший серед сучасних негативних аспектів досліджуваної проблеми. Дезінформувати цілі країни тепер досить легко, у чому українці, перебуваючи у стані війни з РФ, переконалися на власному досвіді.

Усі ці фактори роблять тему загроз у соціальних мережах важливою і актуальною. Суспільство та органи влади повинні бути готові до вирішення цих проблем і встановлення відповідних регулюючих механізмів. Важливо усвідомлювати роль соціальних мереж у формуванні й поширенні інформації та вживати необхідних заходів для забезпечення збалансованого і надійного інформаційного середовища.

Зважаючи на широкий спектр важливих питань, пов’язаних із функціонуванням соціальних мереж, дослідження у цій царині є вельми актуальними та необхідними для кращого розуміння їхнього впливу на суспільство, індивідів та різні аспекти життєдіяльності сучасного соціуму.

Зв’язок з науковими програмами, планами і темами. Тема дослідження пов’язана з такими дисциплінами як «Соціальні мережі» та «Технології інформаційного впливу». Підготовка й написання кваліфікаційної роботи здійснювалася в межах проходження науково-дослідної практики у Товаристві з обмеженою відповідальністю «БАСФ Т.О.В» (далі – Товариство), що представляє

інтереси німецького концерну «BASF SE», як агентський бізнес в Україні. Виконуючи переддипломну практику, авторка магістерської роботи брала участь у документуванні виробничих процесів, а також здійснювала інформаційний супровід роботи підприємства.

Мета і завдання дослідження. Метою кваліфікаційної роботи є аналіз та узагальнення інформаційних загроз, які існують у соціальних мережах, з метою розуміння їх впливу на користувачів та розробка рекомендацій щодо забезпечення безпеки та захисту в інтернет-середовищі.

Відповідно до мети дослідження були поставлені такі **завдання:**

– проаналізувати історіографію, джерельну базу кваліфікаційної роботи та обґрунтувати застосування методів дослідження;

– дослідити соціальні мережі як середовище інформаційного впливу;

– з’ясувати сутність та типові види інформаційних загроз у соціальних мережах (на прикладі інстаграм, фейсбук та телеграм);

– вивчити існуючі практики та заходи безпеки, які використовуються для запобігання та боротьби з інформаційними загрозами в соціальних мережах(на прикладі інстаграм, фейсбук та телеграм);

– охарактеризувати структуру інформаційного відділу ТОВ «БАСФ Т.О.В»;

– розглянути політику безпеки в роботі з інформацією та соціальними мережами на підприємстві ТОВ «БАСФ Т.О.В»;

– визначити можливості та перспективи використання нових засобів роботи з інформацією та соціальними мережами ТОВ «БАСФ Т.О.В» з метою уникнення інформаційних загроз і збереження приватності.

Об’єкт дослідження – інформаційні загрози.

Предмет дослідження – соціальні мережі як середовище інформаційного впливу та загроз.

Методи дослідження. Для виконання дослідження було використано загальнонаукові та конкретно-наукові методи. До загальнонаукових методів

відносяться: аналіз та синтез; індукція та дедукція, текстологійчний аналіз, порівняння; узагальнення; бібліографічний. За допомогою методу синтезу та аналізу здійснено висвітлення проблеми інформаційного впливу як загрози в соціальних мережах. Узагальнення, як метод, було застосовано для формулювання висновків та подальших перспектив використання нових засобів у роботі із соціальними мережами ТОВ «БАСФ Т.О.В». Конкретно науковими методами, які були використані під час написання дослідження, є: системний; прогнозування; контент-аналізу вебсайту та моделювання. Важливим став емпіричний метод дослідження, а саме: спостереження, оскільки підготовка кваліфікаційної роботи частково виконана у межах проходження науково-дослідної практики.

Наукова новизна полягає в тому, що у кваліфікаційній роботі було висвітлено соціальні мережі як середовище для розвитку потенційно-небезпечних інформаційних загроз. Також було окреслено загальні засоби боротьби з ними, а на прикладі підприємства розглянуто реальні інструменти та заходи протидії, окреслено перспективи та нові можливості для захисту приватності компаній, їх працівників та користувачів інформаційно-комунікаційних технологій.

Практичне значення одержаних результатів. Практичне значення дослідження полягає у тому, що основні його положення можуть бути використані при вивченні фахових дисциплін, під час підготовки до лекцій чи практичних занять, наприклад, з курсу «Соціальні комунікації», також для написання курсових та кваліфікаційних робіт. Результати дослідження мають сприяти практиці організації безпечного користування підприємствами соціальними мережами та ознайомлення працівників із базовими інформаційними загрозами.

Особистий внесок. Кваліфікаційна робота виконана самостійно. Усі основні результати дослідження належать авторові особисто. Публікації за темою дослідження є одноосібними.

Апробація результатів. Основні положення кваліфікаційної роботи доповідалися на XXIII Міжнародній науково-практичній конференції молодих вчених і студентів «Політ. Сучасні проблеми науки» (м. Київ, 4-7 квітня 2023 р.).

Публікації. Результати кваліфікаційної роботи оприлюднені в публікації:

Божко М.Г. Соціальні мережі як середовище інформаційних загроз // Політ. Сучасні проблеми науки: матеріали XXIII Міжнар. наук.-практ. конф. молодих вчених і студентів, Київ, 4-7 квітня 2023 р. Київ: НАУ, 2023. С. 171–173.

Божко М.Г. Соціальні мережі як середовище виникнення інформаційних загроз // Тренди та перспективи розвитку мультидисциплінарних досліджень: матеріали IV Міжнар. студ. наук. конф., м. Луцьк, 1 грудня, 2023 р. / ГО «Молодіжна наукова ліга ». Вінниця: ТОВ «УКРЛОГОС Груп», 2023. С. 392–394.

Структура кваліфікаційної роботи. Робота складається зі вступу, трьох розділів з підрозділами, висновків, списку використаних джерел та додатків. Список використаних джерел налічує 79 найменувань. Загальний обсяг роботи – 109 сторінок.

РОЗДІЛ 1
СТАН РОЗРОБЛЕННЯ ТЕМИ КВАЛІФІКАЦІЙНОЇ РОБОТИ У НАУКОВІЙ ЛІТЕРАТУРІ ТА ДЖЕРЕЛАХ

1.1. Історіографія та джерельна база магістерської роботи

Дослідження щодо інформаційних загроз у соціальних мережах є важливим, оскільки цей структурний елемент системи соціуму нині відіграє визначальну роль. Основними показниками сучасного періоду розвитку суспільства є швидке зростання кількості даних, покращення інформаційних технологій, галузі інформаційно-комунікаційних систем. Зазначимо, що якісний показник розвитку інформаційної сфери та рівня інформаційної безпеки визначають роль держав у сучасному глобалізованому світі, як економічну, так і політичну, на світовій арені. Мережа «Інтернет» і все, що безпосередньо з нею пов’язане, генерує світові макротенденції, трансформує й видозмінює соціальні структури та ціннісні орієнтири як для людства загалом, так і для окремих груп суспільства.

Зміни, що відбуваються нині, були спричинені розвитком техніки, приладів та програм, що полегшили повсякденне життя, але й перемістили суспільство у сферу масового виробництва. Відбулося це явище настільки непомітно для свідомості одиниці суспільства, що важко осягнути вплив та залежність сучасної людини від техніки. Відтак актуальну проблематику інформаційних загроз у соціальних мережах було досліджено та висвітлено у кваліфікаційній роботі.

Для вивчення проблеми та всебічного її дослідження було опрацьовано значну кількість нормативно-правових актів, фахової літератури та джерел. Для зручності оперування інформацією, за допомогою проблемного підходу, опрацьовані джерела поділено на наступні групи. Перша група – нормативно-правові акти, які стосуються обраної теми. Друга група – це наукова та довідкова

література, присвячена досліджуваній проблемі. Третя група – офіційні сайти та акаунти досліджуваного товариства, а саме ТОВ «БАСФ Т.О.В» у соціальних мережах.

Як було зазначено, до першої групи джерел та літератури відносимо Закони України. Таким чином, нормативно-правовою базою даної кваліфікаційної роботи є Конституція України, Цивільний, Господарський кодекси та Закони України, Укази Президента та інші нормативні документи. Серед найважливіших можна назвати: Конституцію України [1], Кодекс законів про працю України від 01.06.1972 [2], Закон України «Про інформацію» від 02.10.1992 [5], «Про охорону праці» від 14.10.1992 [6], «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 [7], «Про Національну безпеку України» [15] від 21.06.2018, «Про захист персональних даних» [9] від 27.10.2022, «Про організацію трудових відносин в умовах воєнного стану» від 24.03.2022 [17] та ін.

В основному законі України, а саме в Конституції, у ст. 17 зазначено, що: «забезпечення економічної та інформаційної безпеки України є найважливішими функціями держави, справою всього Українського народу» [1]. Отже, усвідомлюємо, що інформаційна безпека є однією з основних складових держави, як суб'єкта на міжнародній арені. Ця теза віднайшла підтвердження в Кодексі законів про працю[2], Господарському [3] та Цивільному кодексах [4] у окремих аспектах загальнолюдських відносин, що стосуються як праці, так і суспільного життя особистості.

У Законі України «Про інформацію» від 02.10.1992 р. у статтях 5 і 6 (редакція від 27.07.2023 р.) гарантується право кожного на інформацію, що передбачає можливість «вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів» [5]. Цей Закон визначає державну інформаційну політику (ст.3), суб'єкти та об'єкти інформаційних відносин (ст.4), гарантії права на інформацію (ст.6), а також охорону права на інформацію (ст.7) та її види (ст.10) [5]. Крім того, загалом саме в

цьому нормативному акті описано основні правила поведінки з інформацією та в інформаційному скредовищі як фізичних, так і юридичних осіб. Також зазначено, що реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб [5]. Отже, норми даного закону дозволяють регламентувати відносини між користувачами в соціальних мережах та визначати, яка інформація можу бути широкодоступною [5].

Закон «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 [7] унормовує відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. У цьому Законі визначено порядок доступу до інформації, як з державних інформаційних ресурсів, так і до інформації з обмеженим доступом, перелік користувачів та їх повноваження, що представляють особливу цікавість для дослідження проблеми, оскільки часто саме витоки інформації стають першопричиною створення системи захисту та її оновлення згідно з новими викликами [7].

Також важливим для розуміння проблематики нашого дослідження є Закон «Про доступ до публічної інформації» (редакція від 08.10.2023) [10], що регламентує здійснення та забезпечення права кожного на доступ до інформації, як суб'єктів владних повноважень, так і розпорядників публічної інформації. Крім того, цей Закон забезпечує прозорість, відкритість і створення механізмів реалізації права кожного на доступ до публічної інформації, що лише полегшує її поширення в соціальних мережах, збільшуючи ризики неправдивого трактування [10].

Із вищезазначеного випливає, що проблема інформаційних загроз у соціальних мережах, як для користувачів, так і для організацій, зокрема й недержавних, в умовах сучасного глобалізованого світу є надзвичайно актуальною та регулюється на законодавчому рівні. Також вона привертає значну увагу вітчизняних та зарубіжних науковців, тому охарактеризуємо другу групу джерел, а саме наукові та довідкові видання.

У загальному плані питання щодо інформаційних загроз та впливу на користувачів соціальних мереж, характеристики цих ризиків та методів їх подолання розкривають наукові доробки таких учених: Біленчук П., Борисова Л., Неклонський І. та Собина В. [31], Бокоч Ю. [32], Гуменюк В. [34], Деркаченко Я. [35], Золотар О. [36], Кокарча Ю. [38], Кухарська Н. та Кухарський В. [40], Лисенко О. [41], Літвінчук І. [42], Нашинець-Наумова А. [46], Почепцов Г. [50], Самчинська О. та Фурашев В. [53], Семен Н. [54], Смтрич Д. [56], Юр'єва А. [59] та ін. Іноземні науковці, такі, як Брендон Дж. [61], Крістеа Л. [62], Кейворз Т. та Віттен Б. [67], Кім Дж. [68], Посетті Дж. та Ірентон К. [75], Прислан К. [76] та ін., висвітлюють загальні питання щодо дезінформації, нових ризиків сучасних медіа, кіберзагроз та ефективних засобів захисту для користувачів та організацій. Їх наукові праці були використані під час написання даного дослідження.

Так, зокрема, Лисенко О. [41] у своїй дисертації зупиняється на проблемах визначення сутності та законодавчого закріплення права особи на інформацію, її вільне поширення всередині країни й за кордоном. Дослідниця окреслює взаємовідносини між людиною, суспільством і державою в інформаційно-комунікаційному середовищі. Також нею вивчено проблему правового захисту суспільства від шкідливої інформації, сформовано основні напрямки вдосконалення законодавства щодо захисту від дії шкідливої інформації в умовах інформаційного суспільства.

Дисертація Руднєвої А. [52] комплексно описує вплив інформаційних воєн на політичну культуру сучасного українського суспільства. Науковицею розглянуто сутність, методи, джерела впливу з погляду конструктивних і деструктивних наслідків. Також Руднєва А. охарактеризувала шляхи формування фільтрів інформаційної безпеки в контексті розвитку політичної культури українського суспільства та розробила рекомендації щодо застосування результатів дослідження в суспільно-політичній практиці.

У дисертації Семен Н. [54] досліджено трактування поняття «інформаційна війна» українськими та зарубіжними вченими, охарактеризовано пропагандистські матеріали та події в Криму і в ОРДЛО, подані російськими інтернет-ресурсами, окреслено можливі шляхи боротьби української держави з російською пропагандою. Крім того, автором проаналізовано досвід роботи ЗМІ в умовах інформаційної війни.

Цікавість для нас представляє також монографія авторського колективу Біленчук П., Борисова Л., Неклонський І., Собина В. [31], у якій досліджуються питання інформаційної епохи, ролі інформації як основи для нового виду суспільства, інформаційні ресурси та правове регулювання відносин у галузі інформаційного права. Також авторами було окреслено інформаційну безпеку, як складову національної безпеки та пріоритети державної політики України в інформаційній сфері. Крім того, науковцями опрацьовано інноваційні основи захисту інформації з використанням технічних засобів.

У своїй монографії «Інформаційна безпека: питання правового регулювання» Нашинець-Наумова А. [46] вивчає питання адміністративно-правового забезпечення інформаційної безпеки корпорацій, а саме теоретичні аспекти та особливості реалізації правових форм та методів у сфері забезпечення збереженості інформації організацій. Ученою також було окреслено правові засоби забезпечення інформаційної безпеки суб'єктів господарювання.

Монографія таких науковців, як Онищенко О., Горовий В. і Попик В. [47], присвячена темі соціальних інформаційних мереж, їх змісту, особливості розвитку в системі соціальних комунікацій сучасності. Вченими досліджуються тенденції їх активізації в сучасній соціальній інформаційній системі, у розбудові вітчизняного комунікативного простору, соціальне й науково-освітнє значення, а також питання організації безпеки інформаційного простору в умовах стрімкого розвитку технологій, у тому числі й у контексті розвитку соцмереж.

У статті «Технології інформаційного впливу в умовах гібридної конфліктності» Бокоч Ю. [32] розкриває сучасні прояви інформаційної війни, як

технологїї і складової політичної комунікації, основні проблеми створення якісного інформаційного продукту та розвитку власної інформаційної сфери. Також у праці визначено сутність та значення стратегічних комунікацій у створенні дієвої системи інформаційного захисту держави.

Аналізу регулювання відносин у сфері захисту інформації з обмеженим доступом в організаціях присвячена стаття Гуменюк В. «Методи підвищення ефективності управління ризиками інформаційної безпеки підприємства» [34]. Також автором було вивчено методи підвищення ефективності управління ризиками інформаційної безпеки підприємства та вибір.

Соціальні мережі, як механізм впливу на соціальні, культурні, економічні та політичні відносини досліджує у своїй статті Деркаченко Я. [35]. Автор окреслює основні чинники використання соціальних мереж. У роботі висвітлено проблему захисту користувачів соціальних мереж від загроз, пов’язаних із неусвідомленими інформаційними впливами, формуванням штучної психічної залежності, маніпулювання суспільною свідомістю з використанням спеціальних засобів впливу.

Науковиця Кокарча Ю. [38] вивчає проблему появи та розповсюдження впливу інтернет-спільнот у соціальній сфері, надає загальну характеристику цих груп та фактори, що провокують їх появу, подає тематичні класифікації соціальних мереж.

Такі вчені, як Кухарська Н. та Кухарський В. у своїй праці визначають соціальні мережі, як феномен XXI століття, аудиторія яких зростає стрімкими темпами. Також дослідниками зазначено, що ці мережі стали одним з основних комунікаційних каналів у розвитку ділових відносин та оглянуто загрози інформаційної та економічної безпеки комерційних структур, що виникають у зв’язку з масовим поширенням сервісів соціальних мереж [40].

Самчинська О. та Фурашев В. у науковому дослідженні [53] розкривають наступні поняття: «інформаційно-психологічний вплив», «інформаційне насильство». «інформаційні маніпуляції» та «пропаганда», їх основні ознаки та

співвідношення. Автори зіставляють вищезазначені терміни, щоб отримати вірне трактування цих явищ.

Про аспекти забезпечення інформаційних прав та свобод суспільства з врахуванням захисту інформаційної безпеки держави в умовах воєнного стану, що нині є надзвичайно актуальним, йдеться у статті Смотрич Д. «Інформаційна безпека в умовах воєнного стану» [56]. Також у ній представлені типові загрози та пріоритетні напрямки захисту інформаційної безпеки.

Дослідження зарубіжних авторів Есма Емер, Сабрін Амрі та Жиля Брассар [60] стосується поширення фейкових новин, їх ідентифікації, яка досі є складною невирішеною проблемою. Крім того, науковцями зазначено, що підходи штучного інтелекту все ще нездатні подолати цю складну проблему, а ще й використовуються для обману людей шляхом створення та поширення підробленого контенту. Авторами проведено комплексний і систематичний огляд досліджень фейкових новин, а також фундаментальний огляд існуючих підходів, які використовуються для виявлення та запобігання поширенню фейкових новин.

У науковому доробку Гумінського Р. та Пелещина А. «Оцінка інформаційної загрози в процесі функціонування віртуальної спільноти» [65] запропоновано рекомендації щодо інформаційного впливу на структуру віртуальної спільноти, впливів на масову свідомість для зміни поведінки людей. Дослідниками окреслено протидії інформаційним загрозам у цих спільнотах, сформульовано та розроблено алгоритм вибору мінімальної кількості дискусій віртуальної спільноти для інформаційного впливу.

У статті Тіма Кейворта та Дуейна Віттена [67] описуються цілі та механізми дій щодо інформаційної безпеки на підприємтсвах, необхідні для їх досягнення. Наукова праця завершується рекомендаціями, які можна застосувати для забезпечення ефективного управління інформаційною безпекою в різних організаційних умовах.

Третьою групою джерел для дослідження є офіційні сайти та акаунти ТОВ «БАСФ Т.О.В» у соціальних мережах, а саме у фейсбук, інстаграм та телеграм. Товариство представлено на цих платформах декількома сторінками: в інтернеті: ТОВ «БАСФ Т.О.В» [22], «BASF Agricultural Solutions Україна» [23], «BASF SE» [24]; в інстаграмі: «BASF Agproducts» [26], «BASF Global» [27]; у фейсбуці: «BASF Agricultural Solutions UA» [28], «BASF Personal Care» [29], «BASF SE» [30].

Отже, аналіз джерел та літератури кваліфікаційної роботи показав, що нормативно-законодавча база з даної проблематики ще не є достатньо врегульованою. Наразі у науковому дискурсі є достатня кількість статей, навчальних посібників, підручників із питань, що пов'язані із соціальними мережами та інформаційним вплив, який поширюється на соціум через них, а також із питань існуючих загроз для організацій та користувачів та засобів боротьби з ними. Загалом джерельна база є достатньою для об'єктивного розкриття теми дослідження.

1.2. Методи дослідження

Використані наукові методи дослідження у кваліфікаційній роботі доцільно розподілити на загальнонаукові та конкретно-наукові. До загальнонаукових можемо віднести такі методи як: аналіз та синтез, індукції та дедукції, текстологічного аналізу, порівняння, узагальнення, бібліографічний.

При виконанні кваліфікаційної роботи необхідно було здійснити аналіз та, в подальшому, синтез проаналізованої інформації для отримання результатів дослідження. Отже, було використано методи аналізу та синтезу, оскільки вони є невід'ємними частинами та покращують загальне розуміння теми роботи, а також зумовлюють цілісність тексту. Застосування даного методу дозволило ґрунтовно виокремити та поєднати між собою різні аспекти одного явища.

Завдяки аналізу, тобто методу наукового дослідження шляхом розкладання предмета на складові, було виявлено форми взаємодії елементів цілого, а саме складових частин джерельної бази дослідження, виокремлено структурні елементи джерел та літератури. Синтез – це метод поєднання отриманих під час аналізу частин у ціле. Цей метод було застосовано для згрупування проаналізованої інформації, а також для групування літератури, кращого розуміння внутрішнього взаємозв'язку і взаємозалежності рівнів джерел. Усі отримані відомості були поєднані у історіографію, що дозволило системно поглянути на джерельну базу дослідження.

Наступними методами, що були використані для дослідження, це індукція та дедукція. Такий метод наукового пізнання, як індукція, який полягає в дослідженні руху знань від одиничного до часткового або й загального, був використаний для підведення підсумків та руху від менш загальних положень кваліфікаційної роботи до більш загальних. Крім того, цей метод був необхідний для виокремлення кожного рівня джерел. Дедукція ж дозволяє зробити висновок про певний елемент множини на підставі знання загальних властивостей усієї множини, тому цей метод застосовувався для аналізу нормативної бази, а також при характеристиці монографій та дисертацій.

Метод текстологічного аналізу – це один із групи методів, які засновані на вивченні спеціальних текстів з підручників, монографій, статей, методик та інших носіїв професійних знань. Основним призначенням цього методу було сформулювати і виокремити суть текстів для їх подальшого опрацювання. Таким чином, текстологічний аналіз став у нагоді, оскільки завдяки цьому методу було виокремлено головну думку, яку вклали автори у свої доробки, що значно полегшило аналіз їхніх праць.

Метод узагальнення використовувався для підбиття висновків проведеного дослідження та фіксації загальних ознак та властивостей кожного класу джерел та літератури. Необхідно зазначити, що в процесі узагальнення здійснюється перехід від одиничних понять до загальних, від менш загальних понять – до більш загальних, від одиничних суджень до загальних, від суджень

менш узагальнених – до більш узагальнених. Завдяки цьому методу було лаконічно, коротко та стисло підведено підсумки та окреслено основні аспекти роботи, з'ясовано основні шляхи вирішення проблем дослідження.

Бібліографічний метод як спосіб перетворення документального матеріалу на бібліографічну інформацію охоплює операції, відомі в сучасному бібліографознавстві як методи бібліографування. Цей метод було використано для складання списку використаних джерел та літератури, тобто бібліографування, при відборі даних для дослідження, а також для так званого «згортання інформації», а саме для опису джерел на підставі бібліографічного вивчення інформації. Застосування цього методу сприяло структуруванню літератури за авторами, роком написання, приналежністю джерела до певної групи джерел. Метод важливий для правильного оформлення списку літератури, оскільки унормовує його та сприяє швидкому пошуку необхідного джерела.

Наступний метод – порівняння, який є одним із найважливіших загальнонаукових методів, дозволяє співставити різні явища між собою, виокремити спільні та відмінні ознаки певної проблеми. Для використання цього методу було виокремлено однакові для порівнюваного явища категорії та визначено одиниці виміру. Таким чином, ми можемо прослідкувати схожіть процесів, які можуть здаватися протилежними на перший погляд.

У роботі метод порівняння використано для зіставлення традиційних та інноваційних технологій, що застосовуються для безпеки компанії у соціальних мережах. Необхідність даного порівняння обумовлена тим, що використання нових технологій та підходів значно впливає на забезпечення приватності та збереження інформації, яка циркулює в соціальних мережах.

Окрім загальнонаукових методів було використано також конкретно-наукові під час написання кваліфікаційної роботи. До них можемо віднести такі методи, як: системний, прогнозування, контент-аналізу вебсайту, таблично-графічний метод дослідження.

Системний підхід як метод наукового пізнання було використано для дослідження та розуміння соціальної системи, що функціонує в соціальних

мережах. Завдяки цьому підходу розглянуто систему інформаційних впливів соціальних мереж, як цілісний об’єкт, а не окремі компоненти. Також завдяки системному підходу було розлянуто наявну проблему дослідження зі складною структурою і багатьма складовими як частину більшої системи, що сприяло розумінню суті проблеми та розробці комплексних рішень.

Метод контент-аналізу було використано для вивчення вебпорталу досліджуваної організації. На основі аналізу структури сайту, рубрик, текстової та графічної частини, можна мати уявлення про основну мету діяльності установи, особливості її функціонування та напрямки роботи, рівень комунікації із клієнтами. Відповідно, застосовуючи цей метод у роботі, було досліджено офіційний вебсайт ТОВ «БАСФ Т.О.В» та сторінки у соціальних мережах «Інстаграм» і «Фейсбук», що дозволило визначити специфіку їх побудови та функціонування.

Метод прогнозування застосовується для визначення подальшого стану об’єкта дослідження. Він базується на аналізі й використанні різних даних, зв’язків та моделей, щоб передбачити майбутні події, тренди, показники або результати. Існує багато методів прогнозування, а вибір конкретного залежить від характеру дослідження і доступності даних. Відповідно, у роботі метод прогнозування використовувався для визначення майбутніх засобів для безпечного використання соціальних мереж ТОВ «БАСФ Т.О.В».

Таблично-графічний метод було використано для оформлення додатків до роботи та створення графічного представлення інформації. Сутність таблично-графічного методу полягає у систематизації і наочному поданні текстової та цифрової інформації, отриманої внаслідок збору даних, групування, проведення аналізу, синтезу нових показників, прогнозування розвитку подій та моделювання ситуації, у вигляді таблиць.

Отже, застосування методологічної бази дозволило вибудувати цілісну структуру кваліфікаційного дослідження, сформувати уявлення про подальший стан об’єкта дослідження, розробити нові заходи для захисту приватності організації ТОВ «БАСФ Т.О.В».

Таким чином, соціальні мережі є важливою складовою у розумінні процесів інформаційного впливу на організації, їхніх працівників та звичайних користувачів, а також підприємства різних галузей, що й зумовлює значну зацікавленість означеною проблематикою як вітчизняних, так і зарубіжних дослідників. Огляд наукової літератури та джерел показав, що наразі не існує єдиного підходу до визначення сутності загроз соціальних мереж як в українській, так і в зарубіжній думці. У ході опрацювання нормативної бази було визначено, що питання інформаційного впливу у соціальних мережах є недостатньо дослідженим. Відтак й надалі актуальною для досліджень залишається проблема загроз інформаційно-комунікаційних мереж. У кваліфікаційній роботі вирішено поставлені завдання завдяки підбору, поєднанню та застосуванню відповідного методологічного інструментарію. Значна частина роботи побудована на методах спостереження, опису, аналізу, синтезу, узагальнення. Гармонійне поєднання означених методів наукового дослідження у кваліфікаційній роботі забезпечило подання розгорнутих відповідей на поставлені завдання.

РОЗДІЛ 2
СОЦІАЛЬНІ МЕРЕЖІ ЯК СЕРЕДОВИЩЕ ІНФОРМАЦІЙНОГО ВПЛИВУ ТА ЗАГРОЗ

2.1. Характеристика соціальних мереж як інструменту інформаційного впливу

Інформація є головною цінністю сьогодення, оскільки людство перебуває в періоді високотехнологічних змін. Поширення відомостей за допомогою основних інструментів, а саме засобів масової інформації та комунікації, зокрема через електронні медіа, поступово створює універсальне комунікативне середовище, пов'язує значну кількість людей незалежно від відстаней та державних кордонів. Відбувається зростання кількості користувачів такого каналу комунікації, як інтернет, збільшується час, який люди проводять онлайн, а отже зростає і аудиторія соціальних мереж.

Соціальні мережі стали новим середовищем для засобів масової інформації, адже завдяки технологіям нині значно легше перенести певний вид медіа, наприклад газету, в е-формат, і тим самим, охватити більшу аудиторію та здобути нових користувачів. Сучасні мережі відрізняються від класичних ЗМІ, оскільки безпосередньо взаємодіють із читачами, прислухаються до їхніх побажань та дають «ілюзію свободи вибору». Ця ілюзія проявляється, як можливість обрати із запропонованого, до прикладу сторінку у фейсбуці, що сподобалася, але в подальшому, саме мережа буде надавати подібні варіанти до вибору на основі попередньо обраного контенту [57, с.126].

Тому необхідність ефективного нормативно-правового регулювання діяльності соціальних мереж не є перебільшеною, оскільки це вже не типові інструменти для передачі інформації, а повноцінна відокремлена структура, яка потребує законів, із чітким понятійним апаратом. Для подальшого розуміння проблематики дослідження, ґрунтуючись на законодавстві України, надамо

визначення наступним термінам: «користувачі соціальної мережі», «захист інформації», «соціальні мережі».

Так, зокрема, у Конституції України [1], ст. 34 зазначено: «Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя». Отже, громадяни можуть вільно поширювати інформацію, яка не завдає шкоди державі чи іншим особам. Із вищевказаного зрозуміло, що користування та поширення інформації може бути «в інший спосіб», тобто й за допомогою сучасних інструментів.

У Законі України «Про інформацію» [5] наявна ст. 4 про можливих «користувачів» соціальних мереж, тобто про суб'єктів (фізичні особи; юридичні особи; об'єднання громадян; суб'єкти владних повноважень) й об'єкт інформаційних відносин (інформація). Отже, можемо вважати, що суб'єкти інформаційних відносин поширюють інформацію, як об'єкт, у доступні способи, зокрема, за допомогою нових технологій. Також у ст. 10 Закону представлено види інформації за змістом: інформація про фізичну особу; інформація довідково-енциклопедичного характеру; інформація про стан довкілля (екологічна інформація); інформація про товар (роботу, послугу); науково-технічна інформація; податкова інформація; правова інформація; статистична інформація; соціологічна інформація; критична технологічна інформація; інші види інформації [5]. Подальші статті Розділу ІІ цього Закону описують ці види інформації.

Цікавість представляють норми Закону «Про захист інформації в інформаційно-комунікаційних системах» [7], де у ст. 1 подаються визначення термінів, що є важливими для нашого дослідження, а саме:

– виток інформації – результат дій, унаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

– володілець інформації – фізична або юридична особа, якій належать права на інформацію;

– захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

– комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [7].

У ст. 2 цього Закону також вказано, що об'єктом захисту є інформація та програмне забезпечення, яке призначено для обробки цієї інформації, а ст. 3 визначає, що суб'єктами відносин, пов'язаних із захистом інформації в системах, є: володільці інформації; власники системи; користувачі; спеціально уповноважений центральний орган виконавчої влади з питань захисту інформації і підпорядковані йому регіональні органи [7].

Важливим для нашого дослідження став Закон України «Про захист персональних даних» [9], адже дія цього нормативно-правового акту поширюється на діяльність, що пов'язана з обробкою персональних даних, які найчастіше користувачі публікують у соцмережах, навіть не задумуючись про небезпеки. Стаття 14 цього Закону встановлює норми саме щодо поширення персональних даних, фіксуючи, що цей процес відбувається «за згодою суб'єкта персональних даних» [9]. Зазначимо, що в соціальних мережах відсутня жодна довідка про згоду, а, власне, «згодою» є те, що особа сама реєструється в мережі, приймає політики безпеки, частіше за все не читаючи їх, і самостійно поширює свою персональну інформацію.

У Законі України «Про доступ до публічної інформації» від 13.01.2011 [10], у ст. 10 надано подається визначення терміну «публічна інформація у формі відкритих даних» як: «публічна інформація у форматі, що дозволяє її автоматизоване оброблення електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання; є дозволеною для її подальшого вільного використання та поширення». У контексті нашого дослідження було звернуто увагу та проаналізовано Закон України «Про медіа» у редакції від 02.07.2023, де визначено такі терміни:

– користувач – будь-яка фізична або юридична особа, яка використовує, отримує чи споживає медіа-сервіси для задоволення власних інформаційних потреб (без мети отримання прибутку чи ведення відповідної господарської діяльності);

– масова інформація – інформація, що поширюється з метою її доведення до необмеженого кола осіб;

– медіаграмотність – навички та знання, які надають користувачам можливість ефективно й безпечно користуватися медіа-сервісами;

– онлайн-медіа – медіа, що регулярно поширює інформацію в текстовій, аудіо-, аудіовізуальній чи іншій формі в електронному (цифровому) вигляді за допомогою мережі «Інтернет» на власному сайті, крім медіа, які віднесені цим Законом до аудіовізуальних медіа [18].

Зауважимо, що нині законодавче регулювання відбувається під час війни, тому доцільним, на нашу думку, є звернення до Закону України «Про правовий режим воєнного стану» [12]. У ст. 13, де йдеться про особливості дії нормативно-правових актів в умовах військового стану, зазначено, що певні свободи обмежуються у зв’язку з введенням воєнного стану. Також не можемо не вказати Закон «Про Національну безпеку України» [15], який визначає основи та принципи національної безпеки й оборони, цілі та основні засади державної політики, до яких і входить захист інформації та політика країни в цій сфері.

Отже, виходячи із вищезазначеного, можемо узагальнено подати трактування актуальних для нашого дослідження понять:

– користувачі соціальної мережі – це будь-яка фізична, юридична особа, об'єднання громадян чи суб'єкт владних повноважень, які поширюють дозволені види інформації, наприклад масову, публічну інформацію у формі відкритих даних чи персональну інформацію, як власну, так і за згодою суб'єкта персональних даних, у соціальних мережах на власній сторінці чи в мережі «Інтернет» через сайт або за допомогою онлайн-медіа ;

– захист інформації – це комплексний процес створення систем захисту даних, для недопущення витоку інформації та доведення її до відома фізичних чи юридичних осіб, що не мають права доступу; регулювання непоширення інформації в інтересах національної безпеки, територіальної цілісності або громадського порядку, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету й неупередженості правосуддя, а також процес пропагування серед населення медіаграмотності;

– соціальні мережі – це онлайн середовища, які за допомогою мережі «Інтернет» надають можливість для користувачів поширювати різні види інформації в різноманітних форматах, наприклад текстовому, аудіо-, відеоформаті, для необмеженої або обмеженої групи осіб, за бажанням користувача.

Крім того, для повного розуміння проблеми необхідно розглянути сутність понять: «інформаційний вплив», «інформаційна маніпуляція», «інформаційна безпека».

По-перше, розглянемо поняття «інформаційний вплив». Це явище становить загрозу демократизації суспільного життя, формуванню системи прозорої та підзвітної громадянам політичної влади. Загальна інформатизація світу змусила всіх держав відчути на собі тиск різних інформаційних впливів,

наприклад шукати відповідь на розв'язану росією пропагандистську війну доводиться не лише Україні, а й іншим державам [32, с. 79-80].

Варто зазначити, що у даному випадку мова йде не просто про інформаційний вплив, що розпорошений у часово-просторових координатах, але про безпосереднє явище в процесі комунікації в онлайн-середовищі. Зазвичай, це цілеспрямований, організований вплив, часто за допомогою маніпуляцій чи з використанням інформаційних та психологічних засобів, має чітку ціль та спрямований проти інформаційної свободи та волі особистості. Розглянемо частину цього терміну, власне слово «вплив» [53, с.57]. Під «впливом» ми вбачаємо дію, яка виконується особою чи предметом на іншу особу чи предмет. Тобто, це певний процес втручання в перебіг подій, результатом якого стають зміни, наприклад перегляд поведінки людини, її переконань, установок, намірів та інше.

Як складові подібного явища, можемо виокремити суб'єкт впливу(кому це потрібно?), об'єкт впливу (на кого він спрямований?), мету, способи, результат впливу. Суб'єктом є будь-хто, хто володіє достатніми засобами для здійснення впливу (держава, група держав, орган, організація (державна, недержавна, міжнародна), конкретна особа, група осіб), а основний об'єкт – це людина або група осіб, хоча можливий опосередкований об'єкт, яким виступають, наприклад настрої в суспільстві, соціально-психологічні процеси, ставлення до того чи іншого явища, система цінностей, діяльність конкретної держави, органу чи підприємства [53, с.59; 72, с.138]. Кінцевою метою є певна реакція, поведінка чи бездіяльність, яка відповідає основним цілям впливу. Способи – це певні інформаційні технології, способи поводження з інформацією, а також вербальні, невербальні та паралінгвістичні психологічні засоби, за допомогою яких досягається результат, тобто заплановані зміни [53, с. 59-60].

Отже, інформаційний вплив – це цілеспрямований процес, що здійснюється за допомогою використання інформаційних засобів і технологій , психологічних прийомів, з кінцевою метою, який передбачає наявність суб'єкту,

котрим може бути держава, організація чи людина, та об’єкту, яким найчастіше виступає людина чи група осіб, і кінцевого результату, тобто зміну психічного або фізичного стану людини або групи людей.

По-друге, з’ясуємо сутність поняття «інформаційна маніпуляція». У загальному значенні «маніпуляція» – це використання об’єктів із певною метою, особливими намірами, що здійснюється особою. Особливість маніпуляції в тому, що вона завжди прихована, неочевидна, оскільки під час такого впливу особа не підозрює про його здійснення та впевнена, що рішення, яке вона приймає, є її власним. Основна мета – викликати бажання до прийняття рішення, котре було нав’язано людині [51, с. 6-7].

Тобто, інформаційні маніпуляції – це цілеспрямований, прихований, суспільно-шкідливий вплив на думки, волевиявлення, переконання, поведінкові установки, свідомість особи чи групи осіб, котрий відбувається за допомогою інформаційних та психологічних засобів, поза волею особи (групи осіб) та спрямований на досягнення заздалегідь визначеного результату, а саме бажання людини здійснювати певні дії або утримуватися від них.

По-третє, для розуміння терміну «інформаційна безпека» звернемося до Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28.12.2021 № 685/2021 [20]. У документі інформаційна безпека України визначена як: «інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об’єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших

інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом» [20].

Таким чином, можемо інтерпретувати інформаційну безпеку як сукупність важливих умов функціонування суб'єктів (особи, суспільства, держави) в інформаційній сфері та суб'єктивних (правових, політичних, інформаційних, наукових, оперативно-розшукових) можливостей їх усвідомлення і контролю [46, с.10] .

Хоча інформаційна безпека є складовим компонентом проблеми інформаційного забезпечення людини, держави й суспільства, усе ж у наукових колах відсутня єдина точка зору щодо цього явища. Інформаційну безпеку також трактують, як безпеку об'єкта від інформаційних загроз або негативних впливів або непоширення відомостей про той чи інший об'єкт, що є таємницею [68, с.13]. Це явище також розглядають, як «стан захищеності інформаційного середовища, який відповідає інтересам держави, за якого забезпечується формування, використання і можливості розвитку незалежно від впливу внутрішніх та зовнішніх інформаційних загроз» [46, с. 14-15].

Таким чином, у підсумку, інформаційну безпека у науковому дискурсі узагальнено трактується як:

– стан захищеності інформаційного простору;

– процес управління загрозами та небезпеками, що забезпечує інформаційний суверенітет України;

– стан захищеності національних інтересів України в інформаційному середовищі;

– захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі;

– стан захищеності національних інтересів країни в інформаційній сфері;

– суспільні відносини, пов’язаних із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі;

– невід’ємна частина політичної, економічної, оборонної та інших складових національної безпеки [46, с.14-15; 71, с.174-175].

У науковому дискурсі поняття «соціальна мережа» представлене різними точками зору, оскільки історія її виникнення починається із галузі соціології, хоча наразі більш активно розглядається в контексті інформаційних технологій. Історично термін був введений у 1954 р. Дж. Барнсом у значенні «складного переплетення людських стосунків» [35, с.52]. Пізніше. У 1960-х рр. було опубліковано статті вчених П. Ердоса та А. Реньє про принцип формування та побудови соціальних мереж, де завдяки математичному аналізу це питання було більш детально досліджено [35, с. 52].

Найширше можемо трактувати соціальну мережу як структуру, що складається з вузлових елементів і зв’язків між ними, тобто соціальну павутину. Це трактування має назву «мережевий підхід», котрий вивчали С. Вассерман, Б. Веллман, Л. Фріман та ін. дослідники [64, с.13-14].

Існує також трактування соціальної мережі як «віртуального товариства, де відбувається обмін інформацією», хоча подібне пояснення більше підходить до терміну «інтернет». Однак, така думка також заслуговує на існування, адже сьогодні люди проводять величезну кількість часу за комп’ютером і звикли обмінюватися інформацією в електронному вигляді через соціальні мережі [38, с.454].

Наведемо також наступні дефініції терміну «соціальна мережа», що характеризують сутність цього явища:

– соціальна структура, що складається з групи вузлів, тобто об’єктів, таких як люди, групи людей, спільноти, організації, і соціальних взаємовідносин [59, с.82];

– спільнота людей, яка об’єднана загальними інтересами, спільною справою або має інші причини для спілкування між собою [47, с. 126];

– вебсервіс, що забезпечує можливість комунікації великих груп людей та їх об’єднання у віртуальні спільноти за інтересами [61];

– спеціальний підвид інтернет-ЗМІ в системі електронних засобів масової інформації, що займають безпосереднє місце в системі суб’єктів конституційного права [47, с.127].

Резюмуючи, можемо констатувати, що сутність соціальних мереж як явища активно вивчається як українськими, так і зарубіжними дослідниками. Варіативність трактувань терміну пов’язана з його багатогранністю, оскільки процеси інформатизації суспільства тривають, що, у свою чергу, зумовлює до перегляду існуючих трактувань і появи нових.

На наш погляд, соціальна мережа – це сучасний вебсервіс, канал онлайн медіа, призначений для комунікації, із широкою аудиторією користувачів, без обмежень відстанями чи кордонами, що функціонує за допомогою інформаційних технологій.

Зауважимо, що ми розглядаємо соціальні мережі, передовсім, як інструмент інформаційного впливу. На це є декілька причин, одна з головних пояснюється сутністю цих явищ, для чого було розглянуто та проаналізовано різні думки й точки зору щодо потрактування самих термінів. Інформаційний вплив, як було визначено раніше, є організованим застосуванням спеціальних інформаційних засобів і технологій із ціллю деструктивних змін у свідомості особистості, в інформаційно-технічній інфраструктурі об’єкта впливу чи фізичному стані людини. Слід додати, що інформаційний вплив можемо поділити на : інформаційно-технічний та інформаційно-психологічний.

Інформаційно-технічний вплив (ІТВ) – це вплив на інформаційно-технічну інфраструктуру об’єкта з метою забезпечення реалізації необхідних змін у її функціонуванні (зупинка роботи, несанкціонований доступ до інформації та її перекручення (спотворення), програмування на певні помилки, зниження

швидкості оброблення інформації тощо), а також вплив на фізичний стан людини [48, с.13-14]. Цей підвид впливу становить загрозу безпеці інформаційно-технічної інфраструктури (тобто машинно-технічним засобам, програмному забезпеченню, режиму захисту від несанкціонованого витоку інформації) і фізичному стану людини [48, с.14].

Інформаційно-психологічний вплив (ІПсВ) – це вплив на свідомість та підсвідомість особистості й населення з метою зміни їх поведінки і світогляду. Основними методами цього підвиду впливу є: переконання, що звернене до власного критичного сприйняття дійсності об'єктом впливу, та навіювання, котре спрямовується на суб'єктів, які некритично сприймають інформацію [48, с.15-17].

Додамо, що ознаками будь-якого інформаційного впливу є:

- організованість;
- цілеспрямованість;
- «проникнення» в думки особи або групи осіб;
- використання психологічних прийомів;
- використання спеціальних інформаційних засобів та технологій;
- внесення змін у свідомість або інформаційно-технічну структуру об'єкта [53, с.58-59].

Соціальні мережі, у свою чергу, є чудовим інструментом для інформаційного впливу, адже це середовище, що дозволяє поширювати різні дані в різноманітних форматах, наприклад текстовому, аудіо-, відеоформаті, для необмеженої або обмеженої групи осіб, без кордонів. Крім того, у соцмережах відбувається комунікація користувачів, тобто потенційних об'єктів впливу. Одночасно з тим, як інформаційні технології дозволяють особам вільно асоціюватись, реалізуючи свої соціально-політичні прагнення, права і свободи, ці ж засоби активно використовуються з метою психологічного та пропагандистського впливу. Зважаючи на комплексний характер впливу засобів нових медіа, котрими є соцмережі, вони можуть виступати як самостійним

політичним суб’єктом, так і інструментом просування інтересів владної еліти або громадянського суспільства [32,с.83]. Підтверджують цю думку й специфічні особливості соціальних мереж:

– побудовані таким чином, що їх зміст наповнюється самими користувачами;

– надають можливості не лише для спілкування та комунікації, але для споживання медіа-контенту та спектру розважальних продуктів (музика, відео, ігри та ін.);

– можливо вести економічну, політичну, рекламну та інші види діяльності;

– інформація у цілодобовій доступності, залежить лише від наявності електроенергії чи заряду акумулятора на необхідному електронному «засобі-приймачі» та доступ до інтернету [49, с.94].

Наступною причиною, чому соціальні мережі є інструментом інформаційного впливу, є їхні технологічні можливості: створення різноформатного медійного контенту лідерами думок; швидкість надходження відомостей до споживачів; вибір привабливого контенту для об’єкта впливу; пропагування ідей через джинсу, дезінформацію чи білий шум та інше. Оскільки соцмережі нині надзвичайно активно розвиваються, а про перевірку інформації користувачі часто забувають, то це ідеальний інструмент для зміни думок та світосприйняття. Крім того, ці платформи виконують низку важливих «ролей» для соціуму, а саме:

– надають можливість людям зі всього світу спілкуватися, обмінюватися інформацією та підтримувати зв’язок із друзями, родиною і колегами;

– дозволяють подолати географічні відстані та зближують людей навіть тоді, коли вони знаходяться далеко одне від одного;

– є важливим джерелом новин та інформації для багатьох людей;

– дають голос людям, незалежно від їхнього соціального статусу чи політичних переконань, що сприяє свободі слова та може сприяти обговоренню важливих суспільних питань;

– є важливим інструментом для бізнесу для просування продуктів і послуг, залучення клієнтів та спілкування з аудиторією;

– можуть сприяти об'єднанню людей для реалізації спільних цілей та боротьби за права та справедливість (дозволяють організовувати петиції, акції та кампанії національного та глобального масштабу);

– для дослідників і маркетологів соціальні мережі надають цінну інформацію про поведінку споживачів, їхні уподобання і думки [59, с.82-83].

Наступною причиною є динамічність перетворення в інформаційній сфері, зокрема, у соціальних мережах. Нові дані створюються з надзвичайною швидкість, часто неможливо відслідкувати першоджерела, потонути в «інформаційному океані» надзвичайно легко. Усе це відбувається з наступних причин:

– стрімкий розвиток інформаційної сфери та інформаційно-комунікаційних технологій;

– підвищена складність і різноманітність суспільних відносин в інформаційній сфері;

– новизна інформаційних відносин та відсутність досвіду їх правового регулювання;

– відсутність загальноприйнятих варіантів поведінки в інформаційній сфері, вироблених суспільством [61].

Слід зазначити, що функції соціальних мереж теж є однією з причин для полегшення інформаційного впливу. На думку дослідників, серед основних функцій соціальних мереж можна виокремити наступні:

– комунікаційна функція виражена в тому, що люди встановлюють контакти, обмінюються новинами, інформацією (фото, відео, аудіо-матеріали, посиланнями на сайти, коментарями, повідомленнями);

– інформаційна – потік інформації має двосторонній напрям, тому учасники спілкування виступають поперемінно й у ролі комунікатора, і в ролі реципієнта, а оскільки соцмережі часто виступають у ролі неформальних ЗМІ, то будь-який користувач може опублікувати новинне повідомлення про події;

– соціалізуюча – саморозвиток, рефлексія в системі «друзів і груп»;

– ідентифікаційна – при створенні індивідуального профілю користувач наповнює його інформацією про себе: ім'я, дата народження, сімейний статус, школа, інтереси та ін., що дозволяє здійснювати пошук анкет по заданим ознакам;

– функція формування ідентичності, коли людина схильна порівнювати себе з тими людьми, з якими в неї є більша кількість схожих рис; основний механізм, який дозволяє людині формулювати свої позиції щодо інших людей і груп [35, с. 53-54].

Наступна причина є достатньо очевидною, але важливо нею не нехтувати – це кількість користувачів. Для розуміння актуальної кількості користувачів ми скористалися інформацією зі звіту «Діджитал 2023», який наприкінці січня 2023 року підготували дослідні групи з компаній «Meltwater» та «We Are Social». У аналітичному звіті подано найбільш значущі тенденції в цифровому просторі сучасності (див. Дод. А) [21].

Першим важливим показником є глобальне населення, яке станом на січень 2022 року – це 7,91 біліона, а вже в січні 2023 року цей показник – 8,01 біліона, тобто річний темп зростання на 1,0 відсоток свідчить про те, що значно більше половини (57%) населення світу зараз проживає в містах.

Наступний показник – це глобальні користувачі мобільного зв'язку. Більше двох третин (67,1%) населення світу у 2022 році користувалося мобільним телефоном, а кількість унікальних користувачів у 2023 році – уже 68%, тобто за останній рік 95 мільйонів нових мобільних користувачів з'явилося.

Третій показник – користувачі інтернету в усьому світі: на початку 2022 року кількість користувачів в усьому світі зросла до 4,95 мільярда, а рівень

проникнення в інтернет становив 62,5% від загального населення світу. Дані показують, що кількість користувачів інтернету нині становить – 64,4%, а саме 5, 16 біліонів.

Останній показник – глобальні користувачі соціальних мереж: у січні 2022 року в усьому світі налічувалося 4,62 мільярда користувачів соціальних мереж. Ця цифра дорівнює 58,4% загального населення світу, хоча варто зазначити, що «користувачі» соціальних мереж можуть не являти собою унікальних осіб. Нині ж, у 2023 році кількість користувачів соціальних мереж у відсотковому відношенні – 59,4%, тобто це 4,76 біліонів осіб у чисельному співвідношенні.

Однак, попри стрімке зростання кількості користувачів інтернету, люди стали проводити в мережі на 5% менше часу. За даними компанії «GWI» («Глобальна Ворк Едженсі»), середньостатистичний інтернет-користувач скоротив час, який проводить у мережі, у середньому на 20 хвилин на добу (див. Дод. Б). Цей показник дуже мінливий, проте загалом відбувається його зростання. У 2013 р. він зріс на 3,8%, у 2014 р. – впав на 1%, у період 2015-2017 рр. відбулося зростання в середньому на 3% за 3 роки, тоді як 2018 р. – спад на 2,5%, 2019-2020 рр. знову зростання на 4,3% і далі ще на 0,5%, спад у 2021 р. на 4,8%, і зростання у 2022 на 1,9% [21]. І хоча дані змінюються, усе ж кількість часу, який проводять у мережі, значна.

Окрім вищезазначених причин, соціальні мережі є інструментом для інформаційного впливу, адже навіть під час навчання чи опановування нових навичок, відбуваються процеси впливу на особистість [35, с. 52]. Наприклад, за допомогою мережі користувач прослуховує тренінг, тренер надає інформацію, що базується на його досвіді, і якщо особа не ставить під сумнів жодні дані, то перебуває під інформаційним впливом. Водночас, можемо також говорити і про позитивний інформаційний вплив, а саме про необмежені горизонти для застосування соцмереж у навчальній, професійній, персональній та соціальній діяльності особистості, а саме:

– вільне володіння мережними сервісами надає можливість використання відкритих, безкоштовних і вільних електронних освітніх ресурсів для здійснення інноваційної діяльності [66, с.10-11];

– самостійне створення мережного навчального контенту;

– надання та отримання дистанційних консультацій;

– створення та участь у спільнотах за професійним напрямом і вподобаннями;

– освоєння нових концепцій інформаційно-освітнього середовища;

– опанування нових знань і формування нових навичок;

– колективна творчість та критичне мислення;

– участь користувачів у діяльності мережевої спільноти [39, с. 49-50].

Отже, загалом світ активно «йде» в онлайн-середовище, соціальні мережі стали необхідною частиною нашого повсякденного життя і впливають на різні сфери діяльності. Основними термінами, що використовувалися для пояснення процесів в соціальних мережах є: «користувачі соціальної мережі», «захист інформації», «соціальні мережі», «інформаційний вплив», «інформаційна маніпуляція», «інформаційна безпека». Проте функціонування соціальних мереж, через їх двоїсту природу, коли, з одного боку – це засіб для інформування користувачів, але з іншого – засіб для інформаційного впливу та атак, недостатньо врегульовані законодавчо, як явище інформаційного суспільства. Однак, варто зазначити, що у зв'язку з інформаційною війною, яка розгорнулася раніше за реальну, Україна має у цьому напрямі вже певні напрацювання та досвід.

2.2. Сутність та типові види інформаційних загроз у соціальних мережах (на прикладі інстаграм, фейсбук та телеграм)

Соціальні мережі є феноменом XXI століття, але починали своє існування як засіб використання «мережі для зав'язування дружніх відносин та пошуку

партнерів для романтичних стосунків». Нині ж їх аудиторія зростає стрімкими темпами, вони стали одним з основних комунікаційних каналів у розвитку ділових відносин, за їх допомогою моніторять діяльність конкурентів, покращують якість обслуговування, а також просувають свою продукцію та інше. Майже у всі сфери життя впроваджуються інформаційні технології, відбувається стрімкий розвиток телекомунікаційних систем, з'являються нові глобальні мережі, що дозволяє людині майже миттєво отримувати потрібні відомості.

Однак, інший бік цих позитивних змін – громадяни чи влада будь-якої держави можуть лише завдяки інтернету, соцмережам, каналам передавання інформації послабити або навіть зруйнувати конкуруючу державу, вивести з ладу банківську систему, певні сайти. Ще частіше ми чуємо, а нині і стикаємося з кіберзагрозами, хакерськими атаками, прихованою рекламою, від яких ми не захищені. Яскравим прикладом подібних атак є інформаційні пропагандистські кампанії росії, котрі за останні два роки стали настільки частими, що важко підрахувати їх точну кількість. Найчастіше ціллю цих атак є галузь держуправління (48%), неурядові організації та аналітичні центри (31%) [55, с.77]. Навіть найрозвиненішим країнам, за подібної ситуації, важко захиститися, якщо не усвідомити реальних і потенційних загроз, які несуть інформаційні технології, за допомогою яких чи завдяки яким працюють телекомунікаційні системи. Тобто, нашій держав теж необхідно ситематизувати і структуризувати зовнішні загрози, розробити технології захисту, використовуючи надсучасні засоби зв'язку й передачі інформації [55, с. 77].

На сьогодні, соціальні мережі є одними з найбільш відвідуваних ресурсів в глобальній мережі «Інтернет». Згідно даних дослідження, використання українцями соціальних мереж для отримання новин у 2022 році зросло до 74% від 45%, які були у 2017 році (див. Дод. А).

Звичайно, інші засоби масової інформації, такі як сайти новин, телебачення, радіо та преса не залишаються поза увагою, але кількість їх

користувачів у 2022 році складала: 42% – сайти новин, 36% – телебачення, 11% – радіо, 3% – преса. Дані 2017 року значно відрізняються: 54% – сайти новин, 77% – телебачення, 27% – радіо, 24% – преса. Соціальні мережі популярніші серед українців віком 18-35 років, новинні сайти - серед тих, кому 35-45 років, а українці старші за 46 років становлять більшість телевізійної аудиторії (див. Дод. В).

Із вищезазначеного зрозуміло, що за допомогою соцмереж аудиторія отримує новини від традиційних до альтернативних, коментує їх, тлумачить та займається поширенням із них інформації, стаючи співучасником своєрідного інформаційного процесу. Проте, виникла загроза соціальної небезпеки через застосуванням технологій штучної зміни поведінкових реакцій людини і впливу на свободу її волевиявлення, для досягнення політичних, економічних та інших переваг, оскільки соціальна мережа об'єднує в собі величезні об'єми інформаційних ресурсів, що не завжди є якісними, фільтрувати які складно[36, с.72]. Порівняно з традиційними ЗМІ, соціальні мережі дають відчуття реальної причетності до соціально-політичних процесів не лише на рівні спілкування, а й на рівні конкретних дій, участі в розв'язанні конкретних суспільних проблем [38, с.454].

Доволі велика популярність соціальних мереж, як інтернет ресурсу, постала одним із головних завдань для захисту їх користувачів від загроз, пов'язаних із неусвідомленими інформаційними впливами, кіберзагроз і формування штучної психічної залежності; маніпулювання суспільною свідомістю з використанням прихованої реклами чи спеціальних засобів впливу, що виконують чужу волю.

Для подальшого дослідження інформаційних загроз важливим є з'ясування сутності понять: «інформаційна загроза», «кіберзагроза» та «кібербезпека», «недобросовісна реклама» та «прихована реклама».

Для з'ясування сутності означених понять звернемося до нормативно-правових актів, а саме: «Про рішення Ради національної безпеки і оборони

України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» [19] та «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки», затверджених Указами Президента України [20].

У тексті рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану», затвердженого Указом Президента від 19 березня 2022 року № 152/2022 [19] зазначено, що «в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки». Тобто, інформаційні загрози нині розглядаються як небезпечні явища для національної безпеки держави, а саме для інформаційної складової. У Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28.12.2021 № 685/2021 [20] подано наступне трактування: «інформаційна загроза – потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні».

Загалом, інформаційна загроза – це явище інформаційного простору, потенційно або реально негативне, котре впливає на людину, суспільство й державу, завдаючи шкоди інформаційній безпеці.

Визначення поняття «кіберзагроза» та «кібербезпека» знаходимо в Законі України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 року, який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України в кіберпросторі [13]. У ст. 1 зазначено наступне:

– кіберзагроза – наявні та потенційно можливі явища й чинники, що створюють небезпеку життєво важливим національним інтересам України в

кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;

– кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі [13].

Таким чином, небезпечні явища, які спричиняють негативний ефект на кіберпростір держави є кіберзагрозами, а кібербезпека – захищеність інтересів держави, виявлення і подолання існуючих загроз.

З метою з'ясування сутності термінів «недобросовісна реклама» та «прихована реклама» звернемося спочатку до Закону України «Про рекламу», у якому реклама визначається як «інформація про особу, ідею та/або товар, розповсюджена за грошову чи іншу винагороду або з метою самореклами в будь-якій формі та в будь-який спосіб і призначена, щоб сформувати або підтримати в прямий (пряма реклама, телепродаж) або непрямий (спонсорство, розміщення товару (продакт-плейсмент) спосіб обізнаність споживачів реклами та їхній інтерес щодо таких особи, ідеї та/або товару» [8]. У цьому ж Законі, у ст.1 визначено, що:

– недобросовісна реклама – реклама, що вводить або може ввести в оману споживачів реклами, завдати шкоди особам, державі чи суспільству внаслідок неточності, недостовірності, двозначності, перебільшення, замовчування, порушення вимог щодо часу, місця і способу розповсюдження;

– прихована реклама – інформація про особу, ідею та/або товар, розповсюджена за грошову чи іншу винагороду в програмі аудіального чи аудіовізуального медіа, матеріалах в іншому медіа, за допомогою інших рекламних засобів, якщо така інформація слугує рекламним цілям і може ввести

в оману споживачів реклами щодо справжньої мети таких програм чи інших матеріалів [8].

Отже, недобросовісна реклама створена для викривлення інформації, позбавлення сенсів, замовчування та шкоди особам, які її споживають, а прихована – проплачена реклама, яка необхідна для введення в оману щодо певної людини, події чи ідеї.

З'ясувавши сутність понять «недобросовісна реклама» та «прихована реклама», можемо охарактеризувати проблему інформаційної загрози у соціальній мережі, наприклад, телеграм. Це один із популярних месенджерів, який широко використовується в Україні та забезпечує швидкий та безпечний обмін повідомленнями між користувачами, а також дозволяє створювати канали та групові чати для спілкування.

Сьогодні дуже легко створити сайт чи канал, який виглядає як серйозний сервер новин, але його справжньою метою буде поширення неправдивих даних або різних видів реклами з політичних, ідеологічних чи релігійних причин. Такі сайти часто поширюють різноманітні теорії змови та не дотримуються принципів роботи в інформаційному просторі. Представляючи себе суспільним медіа, які заслуговують на довіру, вони підривають довіру людей [42, с. 184].

Наприклад, на певному каналі було розміщено рекламу досить відомого магазину парфумерії та косметики, про шалені знижки до новорічних свят при оплаті товарів онлайн. В описі рекламної пропозиції було надано посилання на сайт. Клікаючи на лінк, особа потрапляла на сайт, обирала продукти та оплачувала їх в інтернеті за допомогою своєї картки. А наступного дня усвідомлювала, що всі кошти із її картки було списано. Раніше, коли оплата в інтернеті ще не стала популярною, подібний випадок був би рідкісним, проте нині це звичайний приклад шахрайства через соцмережі.

Зазначимо, що приховану рекламу або, як її ще називають «джинсу», часто використовують у політичних кампаніях. Наприклад, мають обрати мера міста і всі кандидати проводять активні рекламні заходи. Один із них вирішив

використати соцмережі, наприклад, фейсбук, де з'являється пост про благодійну пожерту для сиротинця, зроблену цим кандидатом. Прямої реклами не відбувається, описується життя дітей, вдячність дирекції, цілі на майбутнє цього дитячого будинку, але існує фото із кандидатом у мери. Людина, що читатиме цю інформацію, підсвідомо буде симпатизувати цьому кандидату, що у подальшому вплине і на її вибір. Проте, наразі ситуація змінюється, оскільки є більше можливостей для перевірки правдивих фактів. Для розповсюдження негативної новини її потрібно проплатити, а щоб видалити її з мережі – заплатити ще більше, хоча спонсори «позитивних повідомлень» готові на все для розповсюдження даних та більшого охоплення [50, с.21].

Отже, в обох ситуаціях відбувається інформаційний вплив на думки та свідомість особи. Оскільки ми досліджуємо інформаційні загрози на основі соціальних мереж таких, як фейсбук, інстаграм і телеграм, подамо їх коротку характеристику.

Фейсбук – це соціальна мережа, яка популярна в усьому світі, за винятком тих країн, де її заборонили. Засновником цієї мережі є американський єврейський юнак Марк Цукерберг. У фейсбуці можна швидко й безкоштовно зареєструватися, а потім публікувати фото і відео, знаходити друзів і однокласників, грати в ігри, вступати в співтовариства, підписуватися на цікаві сторінки й багато іншого [35, с.53].

Інстаграм – соціальна мережа, що базується на обміні світлинами і відеозаписами, дозволяє знімати фотографії та відео, застосовувати до них фільтри, а також поширювати їх через свій сервіс і ряд інших соціальних мереж [35, с.53].

Телеграм – це потужний та універсальний месенджер з елементами соцмережі, який пропонує опціональні наскрізні зашифровані чати та відеодзвінки, обмін файлами та інші функції для спілкування та організації робочих процесів [69, с.21].

Таким чином, зрозуміло, що інформаційними загрозами у соцмережах є потенційні або реальні негативні процеси (кіберзагрози та кібератаки), інформаційний вплив на громадян, суспільство загалом, державу, який завдає шкоди національним інтересам та інформаційній безпеці.

Загрози інформаційній безпеці реалізуються через порушення критичної інфраструктури, вільного обігу інформації, неправомірні дії щодо інформації, через невідповідність інформаційної політики, засобів інформування громадськості. Так, зокрема, В Гуменюк виокремлює наступні основні властивості соціальних мереж:

– наявність власних думок користувачів;

– зміна думки під впливом інших членів соціальної мережі;

– різна значимість думок (впливовість, довіри) одних користувачів для інших;

– існування «лідерів думки»;

– існування межі чутливості до зміни думки оточуючих;

– локалізація груп за інтересами, з близькими думками;

– існування зовнішніх факторів впливу (реклама, маркетингові акції) і, відповідно, зовнішніх агентів (засоби масової інформації);

– наявність «лавиноподібних» ефектів;

– вплив структурних властивостей соціальних мереж на динаміку думок, можливість утворення коаліцій [34, с. 10-12].

Загалом, усі види загроз поділяються на інформаційно-технологічні, інформаційно-комунікаційні, інформаційно-психологічні [31,с.69-70]. Також інформаційні загрози класифікуються за наступними критеріями:

– за ступенем небезпеки – особливо небезпечні, небезпечні;

– за можливістю дії – реальні, потенційні;

– за масштабами дії – національні, локальні, індивідуальні;

– за тривалістю дії – тимчасові, постійні;

– за характером впливу – прямі, безпосередні, опосередковані;

– за терміном дії – довгострокові, середньострокові, короткострокові, поточні;

– за сферою інформаційної діяльності – зовнішньополітична та внутрішньополітична сфера, воєнна, економічна, соціальна, гуманітарна, науково-технологічна та екологічна сфера [46, с. 37-38].

Погоджуємося з думкою Нашинець-Наумової А., яка поділяє загрози за сферою інформаційної діяльності. Зокрема, серед зовнішньополітичних вона визначає: інформаційний вплив іноземних політичних, економічних, військових та інформаційних структур на розробку та реалізацію стратегії зовнішньої політики; поширення за кордоном дезінформації про зовнішню політику; порушення прав громадян і юридичних осіб в інформаційній сфері за кордоном; спроби несанкціонованого доступу до інформації та впливу на інформаційні ресурси, інформаційну інфраструктуру органів виконавчої влади, що реалізують зовнішню політику та інше [46, с.40].

На противагу зовнішньополітичним загрозам, внутрішніми є, до прикладу: порушення встановленого порядку збирання, обробки, зберігання та передачі інформації в органах виконавчої влади; інформаційно-пропагандистська діяльність політичних сил, громадських об’єднань, засобів масової інформації та окремих осіб, що спотворює стратегію і тактику зовнішньополітичної діяльності; недостатня інформованість населення про зовнішньополітичну діяльність [46, с. 40-41].

Підкреслимо, що інформаційні загрози не зменшуються, і вони не мають кордонів, а фахівці з безпеки визнають збільшення частоти, впливу та швидкості атак. Традиційні загрози, такі як втрата пристроїв, внутрішні загрози, зловмисне програмне забезпечення, зломи й соціальна інженерія, уже не є чимось новим та складним, адже з кожним роком розвиваються все більш загрозливі перспективи, які мають хвилевий ефект і можуть мати катастрофічні наслідки в усьому світі [62, с. 354].

Оскільки соціальні мережі є квінтесенцією сучасних вебтехнологій, то вони містять у собі і всі загрози, властиві інтернету. Для більш детального розгляду цих загроз можемо звернути увагу на нижченаведену характеристику.

По-перше, соціальна інженерія є загрозою та найпопулярнішою тактикою для кіберзлочинців. Соцмережі дозволяють зловмисникам знайти конфіденційну інформацію, яка може бути використана для завдання майнової та моральної шкоди. Кожна людина, вступаючи в суспільні відносини, одержуючи й передаючи певну інформацію, вливається в це суспільство шляхом засвоєння і дотримання або незасвоєння норм поведінки. Тому суспільство – одна з найбільших загроз інформаційній безпеці, стверджує Золотар О. [36, с.72; 44, с.65]. Персоналізований досвід, який пропонують соціальні мережі та алгоритми пошукових систем користувачів, на основі детального аналізу даних, включно з місцем розташування та історією пошуку, призводять до створення «інформаційної бульбашки», у якій людина відчуває себе вільною, а свою думку вважає єдино вірною. Для суспільства загалом поява подібних бульбашок призводить до «фрагментації», коли масова аудиторія розформована у величезну кількість ізольованих проблемних груп населення. Соціальним інженерам легко орієнтуватися на вподобання осіб, щоб створювати повідомлення, якому людина хоче довіряти, навіть якщо закрадається підозра, що воно неправдиве; або що шукачі інформації упереджені до джерел інформації, які поділяють і підтверджують їхні погляди [73,с.9-10].

По-друге, пропаганда – відноситься до новин, створених політичними суб’єктами, щоб вводити людей в оману. Це особливий вид сфабрикованих історій, спрямованих на шкоду інтересам конкретної особи і, як правило, має політичний контекст. Останнім часом пропаганда використовується політиками й медійними організаціями для підтримки певної позиції чи погляду. Це є приховане маніпулювання громадською думкою, яке має на меті створити враження, що багато людей поділяють ту саму думку про щось. Пропаганда може бути, як в онлайн середовищі, так і в політичному, корпоративному, а ще у сфері

електронної комерції чи онлайн-сервісах [60, с.11]. Останнім часом значно поширився цей вплив, для прикладу, сторінки в соціальних мережах, підроблені під рейтингові сайти, через які певні групи людей або окремі особи привертають увагу суспільства до недостовірних подій некоректним шляхом. Недостовірні відомості розповсюджують швидко, доповнюються подробицями, які надають правдивості історіям. Також в інформаційному просторі можливо створювати псевдореальних особ, наділяючи їх вигаданою історією. Роблячи подібні вкиди фальшивої інформації, її автори враховують таку особливість мережі інтернет, як анонімність, можливість множинної дії. Фальшиві дані можуть одночасно просуватися через велику кількість сайтів, форумів, блогів, а в користувачів, котрі стикаються з однією і тією ж самою інформацією в різних місцях, складається враження, що вона є достовірною [33, с. 108].

По-третє, дезінформація також є інформаційною загрозою, адже це невід'ємна частина гібридних загроз, основною метою якої є послаблення, дезорієнтація, дестабілізація, дезорганізація політичних структур, функціонування державних і недержавних органів, їх безпека, оборона, економіка, здатність реагувати на загрози, впливати на громадську думку й моральність населення. У соціальних мережах дезінформація може поширюватися швидше й ефективніше, ніж в інших медіа, тому важливо бути обережним та розпізнавати ознаки дезінформації. Основними ознаками дезінформації в соцмережах є: неперевірені джерела; емоційне забарвлення повідомлення; неточна або викривлена інформація; надмірна спрощеність; безглузді твердження. У середовищі, створеному соцмережами, у якому особи формують думки про різні події, достатньо легко надавати різноманітну спотворену чи неправдиву інформацію, вирвану з контексту, і, таким чином, впливати на користувачів [42, с. 183-184].

По-четверте, сугестія, як процес впливу на психічну сферу людини, що знижує критичність при сприйнятті та реалізації змісту, що навіюється, теж виступає як інформаційна загроза. Відомості, отримані таким шляхом, важко

піддаються осмисленню, аналізу та корекції. Це явище відбувається за допомогою засобів сугестії, які є текстові (зміст та форма подання тексту, графіка, шрифти), мовленнєві: вербальні (фрази, слова, наголоси та інтонації), паралінгвістичні (висота, тон, тембр голосу), невербальні (міміка, жести, особливості поведінки учасників відеоряду) [51, с. 170]. Сугестивний вплив особливо дієвий у соцмережах, оскільки специфіка такого виду спілкування полягає у вільному сприйнятті інформації, що переконує самим форматом довірливого спілкування, без потреби логічних аргументів чи мотивів [51, с. 172-175]. Аналізуючи основні методи маніпулятивних технологій, доречно згадати думку Г. Почепцова [50, с. 24], який наголошує, що сьогоднішні інформаційні війни, передусім, ведуться з допомогою інтелектуального інструментарію, а соціальні мережі є безпосереднім середовищем для їхнього використання.

По-п’яте, шкідливе програмне забезпечення (ПЗ) : джерелом шкідливого ПЗ стають сайти підтримки соціальних мереж, унаслідок чого користувачі та компанії потерпають від фінансових збитків у результаті такого порушення безпеки їх комп’ютерів. Найчастішою причиною зараження шкідливим ПЗ і порушення конфіденційності є фейсбук. Інструментами вебатак кіберзлочинців є троянські програми, фальшиві антивіруси, соціальні хробаки, які використовують для власного розповсюдження списки «друзів». Проблемою сайтів багатьох соціальних мереж, зокрема, є те, що їх параметри, встановлені за замовчуванням, роблять користувачів уразливими. Ті, у кого недостатньо знань у сфері інформаційної безпеки, можуть і не підозрювати про необхідність зміни налаштувань із метою власного захисту [40, с. 38; 45, с. 211].

Наступною загрозою є крадіжка паролів і фішинг, оскільки для ідентифікації соціальні мережі використовують паролі. Щоб їх отримати зловмисники використовують фішинг, підставні сайти та інші методи. Достатньо знати послідовність символів і можна надсилати рекламу, деяку інформацію від імені інших, або спонукати одержувачів до будь-яких негативних дій, зокрема перейти за посиланням і запустити шкідливий код, а також інші (часто незаконні)

випадки. Крім того, деякі компанії використовують соціальні мережі для просування власних продуктів, а крадіжка пароля адміністратора групи дозволяє вкрасти саму групу [69, с. 22]. Зловмисники розраховують на те, що більшість користувачів для всіх своїх облікових записів використовують один і той же пароль доступу. Тоді в результаті злому користувацького запису соцмережі значно підвищується імовірність проникнення до корпоративних ресурсів від імені одного із працівників, якщо в цього працівника є звичка використовувати одні й ті ж ім'я користувача та пароль у корпоративній мережі та в зовнішній соціальній мережі [40, с. 39].

Витік інформації теж загрожує інформаційній безпеці. Соціальні мережі можуть бути використані для організації витоку важливої для компанії інформації, а також для підриву її репутації. Таку атаку можуть проводити внутрішні співробітники, незадоволені керівництвом, або спеціально впроваджені інсайдери. У соціальних мережах люди часто поводяться зовсім інакше, ніж у корпоративному комунікаційному середовищі, і цілком можливо, що шокуючі публікації та грубі репліки можуть завдати певної шкоди репутація своїх роботодавців [69, с. 22-23]. Розміри офісу, його наповнення майном, кількість працівників і активність їх телефонних переговорів, наявність клієнтів і робота з ними, корпоративний стиль – усе це є непрямою вказівкою на розміри і прибутковість компанії. І про все це можна довідатися з інформації, викладеної її працівниками на особистих сторінках у соціальних мережах [40, с. 39].

Вебатаки теж популярна нині загроза в інформаційному просторі для користувачів. Оскільки соціальні мережі є вебдодатками, вони можуть використовуватися хакерами для організації атак на вразливі місця в браузерах. Інструментами для таких атак можуть бути троянські додатки, підроблені антивіруси, соціальні хробаки, які використовуються для поширення власних списків друзів та інше. Їх головна мета – потрапити в інформаційну систему відвідувача соціальної мережі та закріпитися в ній [69, с. 22-23].

Ріст трафіку, особливо перегляду джерел відео та спілкування в соціальних мережах створює значне навантаження на інтернет-канал і сповільнює роботу мережевих програм, необхідних для ведення бізнесу. Для перегляду одного лише відео в режимі онлайн вимагається від мережі певна пропускна здатність. У випадку, коли десятки й сотні користувачів одночасно дивляться відео, пропускна здатність мережі, необхідна для роботи мережевих програм неминуче падає. Вихід із ситуації – обмежити доступ до відеотрафіку тих категорій працівників, для яких перегляд відео не допоможе у виконанні посадових обов'язків [40, с. 39; 69, с. 23].

Явища кіберприниження та кіберзалякування, залежність від соцмереж, впливають на ментальне здоров'я. Велика кількість часу, яку багато людей проводять у соціальних мережах, призводить до цифрової залежності. Це може негативно впливати на продуктивність, фізичне та психічне здоров'я, а також реальні відносини. На наш погляд, залежність розвивається тому, що робота в соціальних мережах впливає на центр задоволення в мозку. Бажання повторного отримання цих емоцій змушує проводити час онлайн. Крім того, людина отримує багато інформації дрібними порціями за короткий проміжок часу й до зручності, швидкості та доступності соцмереж звикає швидко [43, с. 157]. Використання соціальних мереж може призвести до порушень ментального здоров'я, таких як депресія, тривожність і почуття низької самооцінки. Перегляд ідеалізованих життів інших користувачів може сприяти почуттю невдоволеності своїм власним життям [40, с. 39].

Останньою загрозою зазначимо втрату особистого часу, що впливає на відносини, відчуття зовнішнього тиску, адже витрачання багато часу на соціальні мережі може призвести до втрати часу, який можна було б витратити на більш корисні або продуктивні справи. Також мережі можуть мати вплив на відносини між людьми. Наприклад, поява заздрощів або ревнощів може пошкодити дружбу або родинні зв'язки. Крім того, багато користувачів відчувають тиск створювати ідеальний імідж у соціальних мережах. Це може призвести до надмірної ретуші

фотографій, показу лише позитивних моментів і життя в ідеалізованому світі [40, с. 39; 69, с. 22].

Погоджуємося з точкою зору В. Петрик В. та М. Присяжнюк М, які у своєму навчальному посібнику «Сугестивні технології маніпулятивного впливу» зазначають, що особлива дієвість інформаційних загроз у соціальних мережах існує через наступні явища:

– сенсаційність і терміновість, які забезпечують шум і необхідний рівень нервозності, що підриває психологічний захист (використовується для відволікання уваги від тієї чи іншої події);

– дроблення, коли маніпулятор представляє замість цілісної проблеми її маленький шматочок, дробить на частини – так, щоб не було можливості осмислити дані в повному обсязі;

– тоталітаризм джерела повідомлень, як важлива умова успіху маніпуляції, який усуває незгодні джерела інформації та думок;

– тоталітаризм рішень, який навіюється аудиторією та альтернативи якому немає;

– змішання інформації та думок, як прийом маніпуляції, коли людина, яка приготувалася дізнатися факти, майже неспроможна захистити себе від думок, які нав'язуються їй разом із фактами;

– прикриття авторитетом, коли на підтримку ідеологічного, політичного або іншого твердження маніпулятора залучається авторитет, який навіть не пов'язаний із цим твердження в даній сфері [51, с. 44-46].

Отже, одне із завдань соціальних мереж – давати найсолодшу ілюзію свободи, запроторити всіх користувачів до клітки, решітки в якій невидимі, і навчити їх любити цю ілюзію, навчити користувачів вірити в те, що вони вільні у своїх думках. Тобто, з одного боку, є позитивне комунікаційне явище, яке забезпечує інформування суспільства, а з іншого, є середовищем для потужних інформаційних атак та подачі відвертої дезінформації та пропаганди. Для досягнення цілей за основу беруться спеціальні маніпулятивні технології та

бойові технології інформаційних війн. Інформаційні загрози в соціальних мережах є потужним інструментом, але як для компаній, так і для звичайних користувачів є можливість мінімізувати загрози. Властивості соцмереж, такі як наявність власних думок користувачів, зміна думки під впливом інших членів соціальної мережі, різна значимість думок (впливовість, довіри) та інші, створюють ідеальні умови для інформаційних загроз. Видами таких явищ є: соціальна інженерія, пропаганда, дезінформація, сугестія, шкідливе програмне забезпечення, крадіжка паролів і фішинг, витік інформації, вебатаки, ріст трафіку, втрату особистого часу.

2.3. Заходи безпеки, практика боротьби та запобігання інформаційним загрозам у соціальних мережах (на прикладі інстаграм, фейсбук та телеграм)

Соціальні мережі є частиною стрибка у світ нових технологій, платформою, що постійно розвивається, має глобальне охоплення і вплив на поведінку людей. На початкових етапах розвитку, ці інформаційні ресурси виконували більш соціальну роль, проти нині охоплюють і процеси пошуку інформації, аналізу відомостей, і, навпаки, дезінформування чи пропаганду. Кардинальні зміни, що відбулися і продовжуються в інформаційному середовищі, перетворюють соціальні мережі на поле болю. Цим процесам сприяють також виняткові характеристики мереж, такі як глобальне охоплення, висока доступність, низька вартість, величезний обсяг і швидкість обміну інформацією, а також певною мірою анонімність користувачів [42, с. 185]. Свою роль тут відіграє динамічний розвиток технологій, який робить усі ці дії простішими та ефективнішими. Програмно-технічне забезпечення дозволяє чи навіть замінює людей, а розвиток мультимедійних технологій робить контент соцмереж усе привабливішим.

Частою причиною інформаційних загроз, які виникають у соцмережах, є сурогатні матеріали, котрі поширюють пропаганду, дезіформацію чи створені для сугестивного впливу. Яскравим прикладом є діяльність журналістів у росії, коли головна роль сучасних медіа – інформування суспільства – замінена поширенням неякісного, неправдивого контенту, котрий викликає деградацію свідомості особистостей [54, с. 121].

Слід зазначити, що популярність соціальних мереж буде лише зростати, і при цьому можемо виділити наступні тенденції:

– зменшення «соціальності» мереж, відсівання «непотрібних» членів груп;

– використання корпораціями явище зниження рівня «соціальності» в мережах, оскільки це дозволить краще й ефективніше організувати обслуговування клієнтів;

– збільшення рівня небезпеки соціальних мереж у зв'язку з тим, що бізнеси та компанії усвідомлюватимуть значимість використання інформаційного середовища (внутрішніх і зовнішніх соцмереж);

– створення політик взаємодії із соцмережами, формалізація цього процесу, включення до нових правил роботи з мережами взаємодію співробітників один з одним;

– становлення такого явища, як «мобільність» невід'ємним для соціального спілкування з допомогою мережевих ресурсів, особливо для працівників компаній, які регулюють використання соцмереж у робочі години;

– користування спільними ресурсами соцмереж уже не буде класифікуватися, як спілкування електронною поштою [43, с. 158].

Зважаючи на вищевказані тенденції, питання запобігання інформаційним загрозам та убезпечення від них стає все актуальнішим. Тому участь держави є необхідною для правового регулювання заходів захисту та протидії загрозам, зокрема, законодавчого закріплення права особи на інформацію та захист від негативного впливу шкідливої інформації, трансформації моделі взаємовідносин

між органами державної влади та ЗМІ, створення національних систем і мереж інформації. Вирішення проблеми правового захисту від інформації, яка негативно впливає на здоров'я людей, є одним із пріоритетних завдань державної політики, що вимагає вдосконалення існуючих сьогодні нормативно-правових актів [41, с. 176-187].

Частково було модернізовано та оптимізовано інформаційну політику нашої держави, адже вторгнення російського агресора в лютому 2022 року змусило приймати нагальні рішення. В умовах розв'язання проти України відкритої інформаційної агресії, Руднєва М. у своєму дисертаційному дослідженні пропонує три рівні заходів запобігання інформаційним загрозам: геополітичний рівень, що полягає у викритті агресора в інформаційному полі, обмеження інтенсивності атак та сили нападів, які спрямовані на створення нестабільної ситуації; державний рівень складається наступних частин: захисту системи державного управління, інформаційної інфраструктури, політико-культурного простору; суспільний рівень, який має на меті забезпечення та захист стабільності й безперервності розвитку суспільно-політичних відносин [52, с.17].

На геополітичному, державному та суспільному рівні найбільш часто використовують сугестивний вплив на вище державне та військове керівництво, управлінські структури. Як протидія, після усвідомлення державою необхідності в користування цими ж мережами, є використовувати їхні переваги, щоб створити систему забезпечення своєчасного інформування громадян, а також дбати про якість інформаційного контенту. У перспективі заходами, що убезпечать від цього є: достатня кількості числа підготовлених спеціалістів для організації контрзаходів, координація дій державних та приватних інституцій для протистояння негативним впливам [43, с. 157; 59, с. 82].

На геополітичному рівні необхідними заходами, що будуть запобігати небезпекам від інформаційних загроз є:

– створення нормативно-правової бази, яка стосується інформаційного середовища та регламентує обмін інформацією в соцмережах;

– активна роль та участь органів управління держави, а також громадських організацій, об'єднань та груп в інформаціних процесах соціального середовища, налагодження ефективної зворотньої комунікації між ключовими суб'єктами, що на меті має збалансування інформаційних масивів якісною, достовірною, суспільно значущою інформацією;

– утворення державних інформаційних структур, які призначені будуть для вироблення даних, що формують та поширюють достовірні та правдиві думки всіх користувачів соціальними комунікаціями, у тому числі й мережевими;

– формування процедури роботи з прогнозування ситуативного майбутнього, реалій, які можуть настати в інформаційному просторі, та розроблення новітніх методик запобігання та протидії негативним процесам чи явищам, аргументація для нейтралізації негативних проявів у сфері інформаційної безпеки [46, с. 32-45; 77, с. 268-269].

Нині зловживання та зломи, разом зі складнішими проблемами, стаються все частіше, а вторгнення та атаки, спрямовані на зрив обслуговування користувачів або незаконне розголошення інформації є одвічними загрозами. Протистояти інформаційним загрозам мають ретельно продумані програми захисту даних, а також розроблені внутрішні системи та процедури. Загалом, на законодавчому рівні розрізняють дві групи заходів безпеки щодо інформаційних загроз: заходи, які спрямовані на підтримку суспільством негативного бачення та ставлення до порушень, й осіб, що спричиняють ці проблемні ситуації інформаційної безпеки (заходи обмежувальної спрямованості); направляючі й координуючі заходи, які спрямовані на покращення рівня освіти в суспільстві, обізнаності в галузі інформаційної безпеки, які, у майбутньому, допоможуть у розробленні та поширенні засобів забезпечення інформаційної безпеки (заходи творчої спрямованості) [37; 51, с. 156].

Зазначимо, що найважчим, але й найважливішим на законодавчому рівні є створити механізм, який дозволяє узгодити процес розробки законів із реаліями і прогресом інформаційних технологій. На наш погляд, важливо, щоб закони не надто сильно відставали від реального стану речей, однак, погоджуємося, що вони й не можуть випереджати життя. Необхідно також забезпечити медіаінформаційну грамотність користувачів, що полягає в поєднанні традиційних концептів «медіаграмотності» та «інформаційної грамотності». Можемо визначити це явище, як комбінований набір компетенцій (знань, навичок і відносин), необхідних на сьогоднішній день для життя і роботи, в основі якого лежать свободи слова та інформації, що дає змогу громадянам зрозуміти функції засобів масової інформації та інших постачальників інформації, критично оцінювати їх зміст, а також ухвалювати обґрунтовані рішення, будучи як користувачами, так і виробниками інформації та медіа контенту [39, с. 49].

Розглянемо детальніше також існуючі рівні захисту інформаційних ресурсів від загроз:

– фізичний рівень захисту передбачає організацію та забезпечення захисту в матеріально-технічному плані, тобто використання інформаційних технологій, а також управлінських технологій;

– програмно-технічний рівень містить у собі такі процеси, як ідентифікація користувача соцмережі, перевірка існування цієї особи (дійсності користувача), керування доступом до мережевої сторінки, створення протоколу дій користувача та аудит діяльності, криптографія, екранування, забезпечення високої доступності;

– рівень управління розрахований на процедури керування, координування та контролю будь-яких організаційних, технологічних і технічних заходів на всіх етапах управління з боку єдиної системи забезпечення інформаційної безпеки органів державного управління;

– на технологічному рівні передбачається здійснення та реалізація політики інформаційної безпеки за допомогою використання комплексу сучасних автоматизованих інформаційних технологій;

– на рівні користувача має бути реалізовано політики щодо безпеки в інформаційному середовищі, які мають метою зменшити вплив рефлексії на суб'єктів державного управління, унеможливити інформаційний вплив із боку соціального середовища;

– мережевий рівень необхідний для введення в дію політик, що створені для регулювання інформаційного простору, у форматі, який має поєднувати й координувати дії державних органів, що мають одну мету;

– на процедурному рівні передбачено вживання заходів, виконавцями котрих є люди, і серед яких ми можемо виділити наступні: управління персоналом, фізичний захист, підтримання працездатності користувачів, реагування на порушення режиму безпеки інформаційного середовища, планування робіт [46, с. 64-71].

Сучасні умови змушують впроваджувати ефективні методи для підтримки інформаційної безпеки в середовищі соцмереж, щоб справитися із новим спектром загроз [40, с. 39]. Заходи, на думку науковців-практиків, які можуть бути застосовані для захисту інформації та забезпечення безпеки, також можуть поділятися на такі дві групи: захист інформаційних систем від пошкодження та інформації від витоку та перехоплення; захист психіки особового складу від цілеспрямованого інформаційно-психологічного впливу [56, с. 125].

Ці заходи мають здійснюватися комплексно, на основі нових наукових розробок і програмних продуктів. Перша група заходів складається з:

– захисту військових об'єктів, а саме комп'ютерної техніки, що використовується для військових цілей, від пошкодження вогнем або іншої механічної шкоди, навмисного виведення з ладу;

– створення системи захисту від віддалених вторгнень, кібератак, зокрема, завдяки програмним продуктам, які дозволяють убезпечитися від вторгнень;

– захист інформації, яка не має потрапити в соцмережі, а саме конфіденційної, таємної, службової, комерційної та персональної, яка становить державну або військову таємницю, від витоків та розкрадання;

– радіоелектронний захист, що виконується з допомогою радіоелектронних систем та програм;

– використання технічного обладнання, тобто комп'ютерів і програмного забезпечення, які не мають проблем у їх кодах, не є пошкодженими;

– створення засобів електронної розвідки, що використовує електронні мережі для отримання інформації;

– дезінформування противника з допомогою соцмереж та даних, що публікуються;

– захист систем зв'язку через створення програм та процедур для уникнення новітніх загроз[56, с. 124-125].

Друга група заходів включає:

– унеможливлення навмисного, спрямованого, методичного та постійного психологічного впливу на психіку користувачів;

– корегування інформації, яка транслюється потенційним супротивником, її фактчекінг [56, с. 125].

Розробка та впровадження комплексу цих заходів потребує створення окремих підрозділів, що працюють у сфері інформаційної безпеки. Крім того, необхідно законодавчо узгодити комплексні дії для захисту від інформаційних небезпек у різних державних та громадських інституціях.

Серед основних засобів захисту від інформаційних загроз у компаніях, що користуються соціальними мережами, виокремлюють наступні:

– організаційні, коли керівництво організацій має: провести пояснюючу та просвітницьку роботу з працівниками, наприклад, у вигляді

тренінгу, що включатиме загальні пояснення явища інформаційних загроз, дій для убезпечення себе та компанії; покращити дисципліну та відчуття відповідальності за володіння комерційною інформацією. Втілення в дійсність цих заходів передбачає значний об'єм методичної роботи, а саме: написання, узгодження і доведення до відома працівників локальних нормативних актів, регламентів або інструкцій, впровадження доступу до комерційної таємниці;

– технічні засоби, які включають комплекс засобів для моніторингу, аналізу і фільтрації вхідного і вихідного трафіку користувачів; процес аналізу, що відбувається в реальному часі, дає можливість переглянути окремі фактори ризику, забезпечуючи цим своєчасний захист діяльності працівників організації в соціальних мережах зокрема, і в інтернеті в цілому [40, с. 39];

– вибірковий контроль, як засіб захисту, що передбачає використання соцмереж та проводиться як превентивна міра в організації від витоку даних і для впевненості керівництва в тому, що працівники не порушують прийняті обмеження на розповсюдження інформації; управління компаній має залишати за собою право слідкувати за діями свої підлеглих на сайтах соціальних мереж, наприклад, може бути встановлено заборону на здійснення завантаження на сайти соціальних мереж текстових файлів, фотографій і відеозаписів, що дасть змогу знизити ризик витоку даних і збереже репутацію компанії [40, с. 39-40];

– робота з використанням кеш-пам'яті, яку проводять для зниження впливу соцмереж на пропускну здатність інтернет-каналу; необхідно обрати для цього найпопулярніші сайти, щоб здійснити кешування даних. Після подібної процедури, першим етапом якої є завантаження із мережі файлів даних, зберігання відбуватиметься на локальному сервері компанії, що, у свою чергу, знизить використання трафіку та часу реакції на запити користувачів. Крім того, працівники можуть, не зменшуючи пропускну здатність локальної мережі організації, отримати доступ до сторінки в соцмережах [40, с. 39-40].

Отже, керівництво будь-якої компанії має усвідомити необхідність підтримки режиму безпеки і виділення на ці цілі значних ресурсів. Оскільки саме

люди підпадають під інформаційний вплив, то слід усвідомити ту ступінь залежності від соцмереж і спрямувати зусилля для створення системи захисту.

Розглянемо також методи захисту від інформаційних загроз, досліджених у попередньому підрозділі, а саме від:

– соціальної інженерії, де основним способом захиститися з боку людини є уважність та обережність, а з технічного боку – наявність антивірусних програм. Необхідно звертати увагу на адресу відправника листа та сайт, на який особа переходить, а також контактні телефони та реквізити компанії. Важливо не працювати із даними в незахищеному від поглядів місці та використовувати різні паролі для доступу до особистої та корпоративної пошти, соцмереж і банківських додатків;

– пропаганда, дезінформація та сугестія – явища, які дуже схожі, яким дуже важко протидіяти, але основні рекомендації наступні: аналізувати й думати над інформацією, щоб зменшити її емоційне навантаження та забарвлення; робити висновки з отриманої інформації самостійно, аналізуючи правдивість фактів; спростовувати наративи, перевіряти правдивість фактів; унормувати нове інформаційне законодавство; використовувати технічні рішення (використання штучного інтелекту); фінансувати суспільні медіа для поширення необхідної інформації; зробити обов'язковою якісну журналістику та когнітивну протидію інформаційним загрозам [69, с. 25];

– шкідливе програмне забезпечення (ПЗ) та вебатаки, протидія яким – антивіруси, оскільки людині виявити самостійно подібні загрози майже неможливо, тому необхідно вміюти працювати в режимі реального часу, блокуючи завантаження шкідливих кодів, а для компаній ще й також часті розсилки для персоналу про інтернет-загрози;

– крадіжка паролів і фішинг – дотримання всіх стандартних правил стосовно паролів, тобто створення окремого паролю для різних соцмереж, використання спеціальних знаків та чисел без прив'язки до особистих даних, у

тому числі періодична заміна паролю, використання DLP-систем та інтегрованих у антивірусні програми репутаційних технологій;

– витік інформації, який можна недопустити, використовуючи політики роботи в інформаційному середовищі, але в разі явища, що вже сталося, варто працювати з DLP-системами та продуктами для аналізу публікацій в інтернеті [69, с. 24-25];

– ріст трафіку, де рішенням є обмежити доступ до відеотрафіку тих користувачів, для яких перегляд відео не допоможе у виконанні посадових обов'язків, обмежити можливість використання робочої техніки для власних цілей;

– кіберприниження та кіберзалякування, втрата особистого часу – рішенням є звернення до правоохоронних органів із доказами кіберцькування , а також обмеження доступу до власних сторінок, похід до психолога; вирішення проблеми втрати часу – створення таймінгу свого дня [40, с. 39].

Отже, засоби захисту від інформаційних загроз дуже різноманітні, наприклад, організаціям для цього потрібно використовувати системний підхід до управління і піклуватися про безпеку, особливо в кризових, конфліктних і нестабільних ситуаціях, коли необхідно серйозно віднестися до проблеми забезпечення інформаційної, особистої безпеки й економічної безпеки організації загалом. Користувачі більше мають покладатися на власний досвід та розвивати свою медіаінформаційну грамотність. Загалом, для звичайних користувачів соціальних мереж методами захисту від загроз є: сильний пароль, двоетапна перевірка інформації, обмеження витоку особистої інформації, антивірусні програми та налаштування безпеки. Проте, найнеобхідніше – це розуміти власну відповідальність, аналізувати отриману інформацію, не втрачати уважність, і приймати заходи для захисту свого облікового запису та особистої інформації в інтернеті.

Таким чином, можемо стверджувати, що суспільство активно використовує соціальні мережі, які стали необхідною частиною нашого повсякденного життя і впливають на різні сфери діяльності. Визначено, що соцмережі є позитивним комунікаційним явищем, яке забезпечує інформування суспільства, але є і середовищем для потужних інформаційних атак та подачі відвертої дезінформації та пропаганди. Інформаційні загрози в соціальних мережах є потужним інструментом, а властивості соцмереж, такі як наявність власних думок користувачів, зміна думки під впливом інших членів соціальної мережі, різна значимість думок (впливовість, довіри) одних користувачів для інших, існування «лідерів думки» та інші, створюють ідеальні умови для інформаційних загроз. Видами таких явищ є: соціальна інженерія, пропаганда, дезінформація, сугестія, шкідливе програмне забезпечення, крадіжка паролів і фішинг, витік інформації, вебатаки, ріст трафіку, втрату особистого часу. Захистом від подібних явищ є наявність антивірусного програмного забезпечення з технологічної точки зору, а також розвиток медіаінформаційної грамотності населення, обізнаності щодо небезпек соцмереж, надійні паролі, аналіз та двоетапна перевірка інформації, фактчекінг.

РОЗДІЛ 3
СПЕЦИФІКА РОБОТИ З ІНФОРМАЦІЄЮ ТА СОЦІАЛЬНИМИ МЕРЕЖАМИ ТОВ «БАСФ Т.О.В»

3.1. Загальна характеристика інформаційного відділу ТОВ «БАСФ Т.О.В»

Інформаційний відділ є надзвичайно важливим для великих концернів і корпорацій. Він відіграє центральну роль у багатьох аспектах бізнесу й має безпосередній вплив на успішність компанії. Представництво німецького концерну «BASF SE» в Україні, яке має назву ТОВ «БАСФ Т.О.В» (далі – Товариство) чудово усвідомлює наявні ризики, а враховуючи історію концерну, має досвід у створенні надійної інформаційно-технічної бази для подолання сучасних викликів інформаційній безпеці.

Товариство, відкрите в 1992 році в Києві, стало однією з перших місій великих західних концернів в Україні, а саме концерну «BASF SE» – німецької хімічної компанії зі штаб-квартирою в Людвіґсгафені (Рейнланд-Пфальц). Розглянемо детальніше історичне становлення концерну.

BASF SE є одним із найбільших у світі виробників хімічного спрямування, котрий створює широкий спектр продуктів: пластик, фарбу, косметику, харчові добавки, технічні та будівельні хімікати, засоби агрохімічного захисту рослин тощо [24].

Назва концерну походить від його першої назви «Badische Anilin- und Soda-Fabrik» («Баденська анілінова та содова фабрика»). З роками продукція компанії неодноразово розширювалася та змінювалася, тому залишили тільки абревіатуру, яка нині є зареєстрованою торговою маркою. Свою історію концерн почав, коли в 1856 англійський хімік Вільям Перкін отримав із кам'яновугільної смоли перший синтетичний барвник – рожевий анілін, цінність якого одразу зрозуміли підприємці.

І вже в 1865 році німецький підприємець Фрідріх Енґельгорн відкрив у Мангеймі фабрику з виробництва порошкових продуктів: аніліну, соди та кислот. Однак невдовзі завод довелося переносити: місцева влада побоювалася, що забруднення повітря негативно вплине на імідж міста, тому фабрику було перевезено на інший берег річки Рейн, до Людвіґсгафена [24].

Фабрика стала містоутворюючим підприємством, завдяки їй маленьке містечко набуло стрімкого економічного розвитку. Гейнріхом Каро в 1876 році був синтезований барвник «метиленовий синій», на нього компанія отримала перший у Німеччині патент. Розроблені барвники відігравали важливу роль не лише в текстильній ґалузі, наприклад, німецький мікробіолог Роберт Кох у своїх дослідженнях туберкульозу за допомогою метиленового синього підфарбовував бацили, роблячи їх видимими [22]. У 1880 році компанія придбала права на виробництво щойно синтезованого індиго – найважливішого на ті часи натурального барвника. У проміжку з 1877 року по 1900 рік у Німеччині було зареєстровано 528 патентів, що належали BASF SE [24].

Для виробництва антрахінонсульфонової кислоти фабрика вимагала значних кількостей олеуму, але наявні методи виробництва були надзвичайно дорогими. Працівник BASF Рудольф Кніч розробив принципово новий метод отримання олеуму, завдяки чому фабрика стала найбільшим виробником сульфатної кислоти. В 1926 році фахівцями компанії було розроблено перше добриво – нітрофоска [29].

У 1925 році BASF об’єдналася з компаніями «Bayer», «Hoechst AG» і трьома іншими компаніями, щоб сформувати синдикат корпорацій-виробників фарбувальних матеріалів. Між 1933 і 1945 роками конгломерат відіграє центральну роль в економіці Німеччини. Під час Другої світової війни компанія розробила отруйний газ, що використовувався в концтаборах та на примусових працях. Кілька директорів і топменеджерів були засуджені за військові злочини і злочини проти людства [24].

Хімічні заводи в Людвігсхафені та сусідньому Оппау мали стратегічне значення для війни, бо їхня продукція широко використовувалася німецькими військовими (наприклад, синтетичний каучук і бензин). У результаті заводи стали головними мішенями для повітряних нальотів. Протягом війни союзні бомбардувальники атакували заводи 65 разів. Обстріл проходив з осені 1943 і завдав значної шкоди. Виробництво практично припинилося до кінця 1944 року.

У зв'язку з браком робочих-чоловіків під час війни, для роботи на заводах були мобілізовані жінки, а пізніше – військовополонені та іноземні цивільні особи. У липні 1945 року американська військова адміністрація конфіскувала всі активи конгломерату. У тому ж році Комісія Союзників ухвалила, що організація має бути розпущена. Людвігсхафен та Оппау перейшли під юрисдикцію французької влади [24].

Після тривалих переговорів «Баденська анілінова та содова фабрика» була знову заснована 30 січня 1952 року як одна з п'яти наступників конгломерату. У 1960 році було розширене виробництво за кордоном – побудовано заводи в Аргентині, Австралії, Бельгії, Бразилії, Франції, Великій Британії, Індії, Італії, Японії, Мексиці, Іспанії та США. Після зміни корпоративної стратегії в 1965 році, був зроблений акцент на більш високовартісні продукти, такі як ізоляційні матеріали, фармацевтичні препарати, пестициди й добрива. Після возз'єднання Німеччини, 25 жовтня 1990 було розширено виробництво у Шварцхайде (Східна Німеччина) [22; 23].

Після початку повномасштабного вторгнення у 2022 році, концерн заявив, що суворо засуджує напад на Україну, розпочатий за наказом російського уряду. Команда з управління кризовими ситуаціями продовжує надавати підтримку співробітникам в Україні. Щоб допомогти людям в Україні, концерн надав 1 млн євро екстреної допомоги до німецького Червоного Хреста наприкінці лютого 2022 року [27].

Додатково, співробітники з усього світу зібрали понад 2,1 млн євро у квітні 2022 року для підтримки колег з України, і компанією було подвоєно цю суму для

надання допомоги українським біженцям. Як було оголошено, концерн припинив укладання нових угод у Росії та Білорусі з 3 березня 2022 року через загарбницьку війну проти України, розпочату за наказом російського уряду [26]. Крім того, на початку липня 2022 року концерн припинив решту своєї діяльності в Росії та Білорусі. У січні 2023 року компанія заявила про те, що її спільне підприємство «Wintershall Dea» з розвідки нафти та газу залишило ринок Росії через вторгнення до України. З 2007 року вся діяльність BASF SE в Україні ведеться через ТОВ «БАСФ Т.О.В» [27].

ТОВ «БАСФ Т.О.В» є уповноваженим представником концерну в Україні. Основна мета ТОВ «БАСФ Т.О.В» вказана на логотипі концерну: «Ми створюємо хімію». Концерн BASF присутній на українському ринку з 1992 року, і понад 30 років пропонує клієнтам інноваційні та екологічні рішення на основі досягнень хімічної науки. Регіональні представництва працюють по всіх регіонах країни. Відділ захисту рослин обслуговує також клієнтів у Молдові та на Кавказі.

Здійснюючи свою діяльність в Україні, компанія керується принципами соціальної відповідальності та сталого розвитку, реалізує соціальні ініціативи, підтримує розвиток освіти та беремо участь у культурних проєктах [28].

Товариство «БАСФ Т.О.В» веде свою діяльність згідно із Законом України «Про товариства з обмеженою та додатковою відповідальністю» від 06.02.2018 року [14], де заначено правовий статус товариств з обмеженою відповідальністю. У ТОВ «БАСФ Т.О.В» основним установчим документом є «Статут», який включає відомості про повне та скорочене (за наявності) найменування, органи управління, порядок прийняття рішень, а також інші відомості, які не суперечать законодавству (ст. 11 Закону України «Про товариства з обмеженою та додатковою відповідальністю» від 06.02.2018). Товариство керується корпоративним договором, де визначено яким чином учасники можуть реалізовувати свої права та повноваження в письмовій формі, як і вказує ст. 7 Закону України «Про товариства з обмеженою та додатковою відповідальністю» в редакції від 01.01.2023 [14].

Особливу увагу в ТОВ «БАСФ Т.О.В» приділяють охороні праці та життя і здоров'я робітників, дотримуючись інструкцій та регламентів від концерну «BASF SE» та законодавства України, а саме Закону «Про охорону праці» від 14.10.1992 [6], котрий визначає основні положення щодо права працівників на охорону їх життя і здоров'я в процесі трудової діяльності. У Товаристві наявний відділ охорони праці, очільником якого є керівник, до обов'язків якого, які визначено в ст. 13 вищезазначеного Закону, крім іншого, безпосередньо входить: розробка й реалізація комплексних заходів для підвищення існуючого рівня охорони праці; виконання необхідних профілактичних заходів відповідно до обставин, що змінюються (наприклад, під час коронавірусної інфекції офісним працівникам надавали корпоративне таксі для поїздок до/з офісу та засоби захисту, такі як антисептики, маски, додаткові ліки, можливість зробити тест на інфекцію за рахунок страхування і медичне страхування у випадках хвороби). Проте, відповідальність за безпечність і належний технічний стан обладнання та засобів виробництва, що передаються працівнику для виконання дистанційної роботи, покладено на інформаційний відділ Товариства, а не відділ охорони праці.

Підкреслимо також, що діловодство, як паперове, так і електронне в Товаристві є двомовним. Обов'язково дотримуються норми Закону України «Про забезпечення функціонування української мови як державної» від 25.04.2019 [16]. Особливу увагу приділяють виконанню ст. 19 цього Закону про застосування державної мови для укладення міжнародних двосторонніх договорів, оскільки ТОВ «БАСФ Т.О.В» є представником концерну «BASF SE».

Також Товариство дотримується Закону «Про зайнятість населення» від 05.07.2012 [11], особливо ст. 8 про професійне навчання. Будь-якому працівнику обов'язково надається професійна підготовка, перепідготовка, наприклад, у разі нової посади, підвищення кваліфікації, стажування.

Крім того, нині діяльність Товариства організовується відповідно до Закону України «Про організацію трудових відносин в умовах воєнного стану» від

24.03.2022 [17]. Наприклад, Товариство виконує норми ст. 2 про особливості укладення трудового договору на період дії воєнного стану, оскільки для будь-якої категорії працівників наразі є випробувальний термін. Також, на початку війни, через евакуацію деяких працівників в іншу місцевість, Товариство надає їм можливість дистанційного виконання обов'язків і укладає строкові договори з особами, що виконують ті частини роботи, які неможливо зробити дистанційно.

Наявність на підприємстві інформаційної служби, відділу чи департаменту є необхідним для існування та ефективної роботи. Відсутність подібної структурної ланки ставить під питання функціонування будь-яких інших відділів компанії. Неможливо переоцінити важливість створених інформаційним відділом процедур роботи з інформацією, соціальними мережами, програмами для виконання службових обов'язків працівників. Однак, для ефективного виконання інформаційної службою своїх обов'язків, організації мають усвідомлювати важливість детальної структуризації подібних служб.

Концерн «BASF SE» має загальну структуру для інформаційного відділу, незалежно від розміщення офісів компанії. Основними обов'язками інформаційного відділу ТОВ «БАСФ Т.О.В» є:

– управління даними й інформацією: інформаційний відділ забезпечує зберігання, обробку й захист даних та інформації компанії. Це включає в себе корпоративні дані, фінансову інформацію, дані клієнтів та постачальників. Доцільне управління цією інформацією є критичним для бізнес-процесів і стратегічного планування;

– інформаційна безпека: захист конфіденційної інформації від витоку та кібератак є надзвичайно важливою задачею. Інформаційний відділ розробляє та впроваджує стратегії кібербезпеки, забезпечуючи захист від потенційних загроз;

– інфраструктура та технології: інформаційний відділ відповідає за розробку, підтримку та модернізацію інформаційної інфраструктури та

технологічних рішень компанії. Це включає в себе сервери, мережі, програмне забезпечення та обліковий запис співробітників;

– аналітика та прийняття рішень: відділ забезпечує доступ до даних та аналітичних інструментів, які допомагають управлінському складу приймати інформовані рішення. Аналітика дозволяє виявляти тенденції, прогнозувати попит та визначати стратегічні напрями розвитку; комунікації і зв'язок: інформаційний відділ забезпечує зв'язок і комунікацію як внутрішньо, так і зовнішньо. Внутрішні комунікації допомагають співробітникам спілкуватися та співпрацювати, а зовнішні комунікації служать для взаємодії з клієнтами, партнерами та громадськістю;

– підтримка бізнес-процесів: інформаційний відділ розробляє програмне забезпечення та інформаційні системи, які сприяють автоматизації та оптимізації бізнес-процесів, що знижує витрати і підвищує продуктивність;

– стратегічне планування: відділ бере участь у стратегічному плануванні компанії, допомагаючи визначити, які інформаційні ресурси та технології потрібні для досягнення бізнес-цілей;

– інновації і дослідження: відділ може бути центром для інновацій та досліджень у галузі інформаційних технологій. Це допомагає компанії залишатися конкурентоспроможною на ринку [27; 30].

Структура інформаційного відділу ТОВ «БАСФ Т.О.В» є стандартизованою для концерну «BASF SE», проте сучасні виклики в Україні зробили її дещо специфічною та залежною від багатьох факторів. Схематично структура інформаційного відділу зображена в Додатку Г. Проте, загалом, структура інформаційного відділу складається із рівнів:

– керівництво: знаходиться в головному офісі в Німеччині, відповідає за стратегічне планування, розробку політики інформаційної безпеки, а також координацію діяльності відділів;

– інфраструктура і технічна підтримка: ця група включає в себе системних адміністраторів, інженерів із мереж та технічних підтримки, які

відповідають за налагодження і підтримку інформаційних систем та мереж компанії (різні для кожного регіону);

– розробка програмного забезпечення: цей підрозділ відповідає за розробку та підтримку корпоративних програмних додатків та систем;

– безпека інформації: важливою частиною інформаційного відділу є забезпечення безпеки інформації, що включає в себе впровадження заходів із кібербезпеки, контроль доступу та обробку даних;

– аналітика і документація: інформаційний відділ має аналітиків даних, які вивчають та аналізують інформацію для прийняття рішень організації. Також ця група веде документацію та забезпечує зберігання інформації;

– підтримка користувачів: Інформаційний відділ має службу технічної підтримки для співробітників компанії, яка надає допомогу щодо роботи з комп'ютерами та програмним забезпеченням;

– стратегія та розвиток: Ця група включає аналітиків, які розробляють стратегії інформаційних технологій для підтримки бізнес-цілей компанії (знаходиться в головному офісі – Німеччина);

– управління проєктами: відділ має професіоналів з управління проєктами, які відповідають за впровадження нових інформаційних проєктів та систем [24; 30].

Отже, інформаційний відділ є необхідним елементом інфраструктури ТОВ «БАСФ Т.О.В», оскільки він допомагає забезпечити ефективне управління даними, безпеку інформації, технологічну підтримку та стратегічне планування, що, у свою чергу, сприяє стабільності й розвитку компанії.

Щодо питання особливостей роботи з інформацією та соціальними мережами в ТОВ «БАСФ Т.О.В» діють інструкції від головного офісу концерну «BASF SE». Робота з інформацією та соціальними мережами має свої особливості, особливо враховуючи те, що «BASF SE» є великим міжнародним концерном у хімічній промисловості. Охарактеризуємо основні із цих особливостей:

– конфіденційність і безпека інформації: у зв’язку зі специфікою хімічної промисловості, компанія має важливу потребу в забезпеченні конфіденційності своїх даних та інформації про продукцію, дослідження та розробку. Тому вживаються ретельні заходи з кібербезпеки та контролю доступу до інформації;

– дослідження і розробка: як хімічний концерн, «BASF SE» здійснює значні дослідження і розробку нових хімічних продуктів. Робота з інформацією та даними в цій галузі може включати в себе велику кількість технічних даних та вимагати високого рівня аналітики;

– регулювання і стандарти: у хімічній промисловості діють високі стандарти безпеки та регулювання. Інформаційні системи на підприємстві повинні відповідати цим стандартам і вимогам;

– управління ланцюжком постачання: концерн «BASF SE» має складний ланцюжок постачання, де інформаційні системи використовуються для відстеження та управління цим ланцюжком. Це включає в себе контроль за запасами, логістикою та обігом товарів;

– співпраця та комунікація: співпраця між різними відділами та міжнародними підрозділами «BASF SE» є важливою. Соціальні мережі та інформаційні системи використовуються для спрощення комунікації та спільної роботи на різних рівнях компанії;

– використання аналізу великих обсягів даних (Big Data) та аналітики: більшість великих корпорацій, включаючи «BASF SE», використовують аналіз великих обсягів даних (Big Data) для прийняття рішень та оптимізації бізнес-процесів. Інформаційні системи грають ключову роль у зборі, обробці та аналізі цих даних;

– стратегія та інновації: інформаційний відділ сприяє розробці та впровадженню стратегічних напрямків розвитку, включаючи інновації в галузі хімії та технологій.

Отже, завдяки великому обсягу інформації, складній технологічній інфраструктурі та вимогам до безпеки, інформаційний відділ на підприємстві, такому як ТОВ «БАСФ Т.О.В», має велике значення для ефективної роботи компанії та досягнення її бізнес-цілей. Структура інформаційного відділу передбачає наявність таких підрозділів: керівництво; інфраструктура і технічна підтримка; розробка програмного забезпечення; безпека інформації; аналітика і документація; стратегія та розвиток; управління проєктами. Робота з інформацією регулюється інструкціями концерну «BASF SE». Основними особливостями під час подібної діяльності є: конфіденційність і безпека інформації; дослідження і розробка; регулювання і стандарти; управління ланцюжком постачання; співпраця та комунікація; використання аналізу великих обсягів даних та аналітики; стратегія та інновації.

3.2. Політика безпеки у роботі з інформацією та соціальними мережами ТОВ «БАСФ Т.О.В»

У сучасних умовах у діяльності підприємств вагоме значення має її інформаційна складова. Усе частіше висловлюється та підтверджується думка про те, що найкращих результатів досягатимуть ті підприємства, які матимуть змогу контролювати інформаційні потоки, щільність і об’єми яких постійно зростатимуть. Інформація стає найдорожчим та найважливішим ресурсом суб’єкту господарювання. Розвиток інформаційних технологій, у тому числі зорієнтованих на інтернет, як інструментарію обробки й поширення інформації, вимагає їх використовувати в більшості видах діяльності підприємства. А динаміка зростання кількості користувачів інтернет, збільшення зони покриття територій, де є доступ до сервісів інтернет, рівень комп’ютерної грамотності та інформаційної культури населення сприяє впровадженню сучасних рішень щодо обробки інформаційних потоків на підприємствах.

Одним із ресурсів поширення інформації та здійснення бізнес- комунікацій в інтернет є комп’ютерні соціальні мережі. У соціальних мережах зареєстровано

сотні мільйони користувачів, через мережі розповсюджується різноманітна інформація, у базах даних соціальних мереж зберігаються величезні масиви інформації, а їх власники отримують мільярдні прибутки.

Стає зрозумілим, що такий потенціал необхідно використовувати. Тому стає завдання визначення способів і методів використання соціальних мереж у діяльності підприємств, особливостей управління інформацією, що стосується діяльності суб'єкту господарювання, з використанням сервісів, які підтримуються соціальними мережами. Тема використання комп'ютерних соціальних мереж для поширення інформації в підприємницькій діяльності освітлена публікаціями, що розкривають технологію роботи з конкретною соціальною мережею або присвячуються окремим сервісам, що підтримуються соціальними мережами.

Сучасні корпорації, компанії та організації переосмислюють та переформатовують технологічні процеси через швидке зростання інформаційних технологій, яке також спричиняє розвиток проблем безпеки в усьому світі. Цифрова ера вимагає від організацій створення нових підходів до інформаційних загроз, використання нових процедур для подолання викликів інформаційній безпеці [62, с.352].

Процедури безпеки повинні бути розроблені, реалізовані та оновлені відповідно до бізнес-операцій та процесів. Поки процеси взаємопов'язані й інформаційний потік слідує бізнес-ланцюжку, дизайн системи безпеки повинен об'єднати всі зв'язані системи. Як тільки вразливі місця проникають у систему, бізнес-ланцюжок розкривається. Компанії повинні зайняти позицію досить швидко, щоби пом'якшити наслідки вразливості. Оскільки ІТ-середовища «стають усе більш складними, уникнення інцидентів інформаційної безпеки потребують співпраці не лише в технологічній сфері, а й у стратегічній, процесній та організаційній сферах» [78, с. 35-40].

У цьому відношенні впровадження технологій безсумнівно є перевагою в захисті даних під час комунікацій. Нове шкідливе програмне забезпечення

з’являється і зростає з року в рік і завдання полягає в розробці точного методу виявлення та розпізнавання загроз. У більшості випадків, проблема стійкості до небезпек відноситься до старих операційних систем. Операційні системи повинні працювати на останній версії, працювати на телефонах, мобільних пристроях. Враховуючи, що кібератаки продовжують зростати, щодня збираються дані для фундаментального аналізу спаму, тенденцій зловмисного програмного забезпечення електронної пошти, фішингу, програм-вимагачів. І все-таки, здається, одна з найбільш значних вразливостей усіх систем безпеки – сам користувач [62, с. 355-356; 70, с. 57].

Для запобігання загрозам інформаційного середовища та кіберзлочинності, важливо визначити політику безпеки, найбільш адекватні рішення в рамках проактивного підходу, починаючи з характеристик бізнес-процесів і специфіки галузей. Загалом, інформаційна безпека починається з розуміння бізнес-операцій і розширення можливостей нових технологій. Організації по всьому світу виділяють усе більше коштів для інформаційної безпеки, але використовують технології, ніби для побудови паркану навколо себе самих, включаючи свої дані, системи та персонал. Проблема полягає в тому, що будуючи подібний захист, не враховується специфіка інтернету й соціальних мереж, як вільного середовища, де поширення даних відбувається з надзвичайною швидкістю. Тобто, компанії будують периметр, який більше не є статичним і стабільним, і паркан більше неможливий, адже більшість сьогоднішнього бізнесу здійснюється за межами «захисного паркану» [69, с. 26; 79, с.331].

Крім того, враховуючи небезпеки інформаційного простору, продовжуються активні заклики до боротьби з кіберзлочинністю від організацій. Крок за кроком таке ставлення сприяє кращій профілактиці, передбачаючи можливі небезпеки. Тобто, невеликі заходи сприяють зменшенню потенціалу майбутніх атак, спрямованих на знищення репутації компанії та довіри зацікавлених сторін [72, с. 138].

Профілактичним заходом, який компанії могли б прийняти, було б детальне дослідження, яке рекомендовано проводити організаціям для документування причин, перебігу та наслідків порушення правил організації. Цей тип аналізу вважається важливим етапом для подолання кіберзлочинності, який обговорюють та рекомендують багато дослідників [67, с. 167].

Наразі атаки організацій в інформаційному середовищі проводяться щодня, підходи до знищення систем безпеки розвиваються, і найчастішими суб'єктами загрози є кіберзлочинці, за ними йдуть незловмисні інсайдери й хакери. Ці кіберактори здійснюють із метою отримання фінансової вигоди, крадіжки інтелектуальної власності та доступу до секретних даних, інформації, що дозволяє ідентифікувати особу, порушення безпеки послуг [66, с. 12].

Наведемо, як приклад, поширення фейків на соціальних платформах, як загрозу інформаційній безпеці компанії. Фейкові новини створюються та поширюються підставними обліковими записами з подібними, до сторінок реальної людини, атрибутами та структурою в мережі, такими як соціальні боти. Боти (скорочення від програмних роботів) існують із перших днів комп'ютерів. Соціальний бот – це комп'ютерний алгоритм, який автоматично створює контент і взаємодіє з людьми в соціальних мережах, намагаючись імітувати та, можливо, змінити їхню поведінку. Хоча вони призначені для надання корисних послуг, вони можуть бути шкідливими, наприклад, коли сприяють поширенню неперевіреної інформації або чуток [60, с. 23; 65].

Однак, важливо зазначити, що боти – це просто інструменти, створені та підтримувані людьми для певних прихованих цілей. Соціальні боти, як правило, підключаються до справжніх користувачів і намагаються поводитися як люди, маючи менше слів і підписників у соціальних мережах. Небезпека для компаній криється в тому, що технології штучного інтелекту дозволяють імітувати голос, записувати відео й поширювати його в просторах інтернету. Спочатку бот отримує доступ до акаунтів, пише повідомлення і спілкується з користувачем. Нічого не підозрюючи, людина поширює в розмові фото, записує голосові

повідомлення, ділиться новинами свого життя. Потім відбувається передача цієї інформацію до осіб, що створили цього бота, і вони визначають її цінність. Наприклад, працівник поділився інформацією про клієнта, з яким працює компанія, і здається, що це не надто цінні дані, проте насправді все не зовсім так. Використовуючи фото співробітника, яке він поширив у розмові з ботом, голосі повідомлення, якщо вони були записані, або текстові повідомлення, за допомогою штучного інтелекту створюється відео з розмовою цього працівника. І, через акаунт людини, що піддала небезпеці свою інформацію, відбувається поширення цього запису до клієнта, де працівник, у режимі реального часу просить, наприклад, надіслати певні відомості на нову е-пошту. Штучний інтелект небезпечний ще тим, що дуже швидко вчиться, тому наразі можливі навіть відеодзвінки в реальному часі, без певного скрипта розмови, коли технології самі обирають, яким чином і що сказати.

Тим не менш, лише певному відсотку кібератак можна запобігти, виявити та заблокувати за допомогою ресурсів компанії. Тобто, коли йдеться про кібербезпеку, завжди є місце для вдосконалення. Тримати хакерів подалі – велика відповідальність для компаній [62, с. 358; 71, с. 174-182].

Отже, інформаційна безпека продовжує бути головною проблемою для керівників компаній. Загроза тероризму, зростаюча залежність від інтернету, глобалізація та нові державні постанови, які вимагають від компаній, які працюють як на території України, так і закордоном, захисту даних, посилили усвідомлення необхідності ефективного корпоративного управління інформаційною безпекою.

Історично компанії дотримувалися технічно орієнтованої стратегії інформаційної безпеки, яка наголошувала на головній ролі технологій у розробці ефективних рішень безпеки [60, с. 2-3].

Оскільки безпека вважається технічною проблемою, групу інформаційної безпеки в організаціях, які дотримуються цієї стратегії, як правило, позиціонують як технічну функцію низького рівня, що працює незалежно від

бізнесу. Відсутність інтеграції між групами безпеки та бізнесу можуть призвести до того, що політика безпеки та бюджети не відображатимуть потреби бізнесу [37, с. 3-4].

У подібному випадку безпека, як явище, є реактивною, інвестиційні рішення обумовлюються короткостроковими пріоритетами, а не добре продуманими стратегічними пріоритетами. Сучасна точка зору полягає в тому, що ефективна стратегія інформаційної безпеки має бути збалансованою, підкреслюючи важливість технології та, при розробці та впровадженні рішень безпеки, соціально-організаційний контекст організації [60, с. 3; 76, с.130- 131].

Раціональним рішенням для підприємства є створення внутрішніх корпоративних соціальних мереж на базі сервісів найбільш популярних соціальних мереж в інтернеті. Провідні аналітичні агентства вже кілька років обговорюють перспективність впровадження корпоративних соціальних мереж. Подібний механізм особливо актуальний для великих підприємств, а ще більш – для міжнародної корпорації, що має величезне число співробітників і подібні по профілю підрозділи в ряді країн. Менеджери або аналітики, що працюють у тому або іншому регіоні, вирішують аналогічні завдання, зустрічаються з такими ж проблемами й часом не спілкуються і не передають свій досвід, хоча формально мають можливість написати один одному по електронній пошті, але відсутність формального знайомства, культурні бар'єри заважають налагодити вільне плідне співробітництво [58, с.8-10].

Товариство «БАСФ Т.О.В», як представник німецького концерну, теж надає перевагу складним технологіям і технічно компетентним фахівцям із безпеки, здатним застосовувати різні технології для захисту інформаційних активів. Крім того, технологія, а не люди, використовуються як основа для пояснення випадків порушення безпеки.

Стратегія безпеки Товариства наголошує на важливості інтеграції безпеки в основні аспекти бізнесу та врахування людського фактора при розробці ефективних програм безпеки. Тобто, стратегія є керованою бізнесом і таким

чином гарантує, що безпека стане інтегрованою в структуру організації та сприйматиметься як важливе питання основного бізнесу. Хоча технологія все ще важлива, вона є лише частиною загального рішення, яке також має включати соціально-організаційні елементи бізнесу. Тому ефективна стратегія інформаційної безпеки повинна включати два ключові елементи, першим із яких є технічна компетентність.

Разом з тим, наразі обговорення професійних питань у соціальних мережах наштовхується на перешкоди корпоративної політики концерну «BASF SE», а отже й ТОВ «БАСФ Т.О.В». Оскільки це велике підприємство, то бажано, щоб співробітники одержували доступ до соціального капіталу, який міститься в подібних мережах, але при цьому компанія вважає необхідним мати можливість контролювати коректність контенту, що публікується, з погляду корпоративної безпеки.

Основна проблема, з якою зіштовхуються керівники служби безпеки, полягає в тому, щоб збалансувати потребу в забезпеченні бізнесу та захистити інформаційні активи. Наприклад, якщо відділу маркетингу потрібно надати доступ до даних клієнта через портативні пристрої, яка цінність надання цих даних у порівнянні з необхідністю захисту цінних даних клієнта від несанкціонованого доступу чи крадіжки? Гіпотетично ризики можна було б усунути, заблокувавши сервери та заборонивши доступ до корпоративних даних. Хоча цей варіант ефективно захистить корпоративні дані, він також завадить бізнес-операціям. Отже, керівництво Товариства дійшло висновку, що ефективна стратегія інформаційної безпеки має бути керована бізнесом, водночас забезпечуючи захист інформації активів, забезпечуючи при цьому бізнес.

Тому було створено та прийнято Політику безпеки у роботі з інформацією та соціальними мережами ТОВ «БАСФ Т.О.В». ІТ-політика ТОВ «БАСФ Т.О.В» стосується всіх співробітників, стажерів, осіб, які виконують свою роботу в офісах або за їх межами. Отже, дія цієї Політики поширюється на:

– осіб, які виконують завдання в режимі віддаленої роботи або домашнього офісу;

– осіб, які виконують завдання для Товариства на підставі цивільно-правових договорів;

– будь-яких інших осіб, які працюють у ТОВ «БАСФ Т.О.В», незалежно від правових підстав для цієї співпраці;

– будь-яких осіб, які використовують ІТ-системи та ІТ-обладнання ТОВ «БАСФ Т.О.В» (далі – Компанія).

Вищезгадана Політика визначає терміни «ІТ-системи» та «ІТ-обладнання» як:

– ІТ обладнання – це будь-який ІТ пристрій, на який Компанія має юридичне право власності, і довірений Компанією співробітнику для виключного використання з метою виконання завдань для Компанії, зокрема: комп’ютери та мобільні телефони, монітори, принтери та інше;

– ІТ системи – це будь-які системи, до яких можна отримати доступ за допомогою ІТ-обладнання, встановлених на таке обладнання або доступних із нього, включаючи, зокрема, (але не обмежуючись) програмне забезпечення, інтернет, бази даних та бази даних клієнтів, надані співробітнику Компанією або створені на основі даних, наданих Компанією.

Усі ІТ-системи та ІТ-обладнання призначені для використання в робочих цілях виключно в інтересах Компанії та не повинні використовуватися співробітниками в приватних цілях. Заборонено використовувати будь-які дані Компанії для непов’язаних із роботою цілей. Усюди, де це технічно можливо, працівник повинен позначити приватне листування в поштовому додатку, позначивши повідомлення як «Приватне/Особисте». Роботодавець може, з метою контролю за роботою працівника, на вимогу операційного або адміністративного керівника та за явною згодою Правління Компанії здійснити перевірку робочої кореспонденції на ІТ-обладнанні, при цьому будь-яка приватна кореспонденція працівника не підлягає перевірці.

Основні положення цієї Політики стосуються саме використання працівниками даних, які вони отримують під час роботи, та технічного обладнання. Розглянемо детальніше ключові аспекти ІТ-політики Компанії.

Співробітники зобов'язані використовувати ІТ-обладнання та ІТ-системи належним та відповідальним чином, у відповідності до їх цільового призначення та інтересів Компанії. Зокрема, працівники зобов'язані належним чином піклуватися про ввірене їм ІТ-обладнання та уникати використання ІТ-систем у спосіб, що порушує чинні правові норми, інтереси або правила безпеки Компанії або способом, який суперечить правилам соціальної поведінки.

Співробітники зобов'язані забезпечити резервне копіювання своїх даних. Кожен співробітник має доступ до програмного забезпечення, що забезпечує резервне копіювання даних у хмару. Резервні копії спільних/ мережевих дисків створюються ІТ-організацією.

Працівники несуть відповідальність за збереження конфіденційності та цілісності матеріалів та інформації у всіх ІТ-системах, до яких вони мають доступ. Вони не мають права копіювати або видаляти будь-яке програмне забезпечення, а також заборонено видаляти бізнес важливі файли або дані без попередньої письмової згоди від Правління Компанії. У разі порушення даного пункту, працівник несе дисциплінарну відповідальність.

Компанія надає можливість співробітникам використовувати електронну пошту як засіб ділового спілкування. Фахівець, який відправляє повідомлення електронною поштою, зобов'язаний стежити за тим, щоби будь-які повідомлення відправлялися таким чином, щоб вони були доставлені вірним адресатам. Зміст електронних листів має бути ввічливим і професійним за тоном.

Особливу увагу в цій Політиці приділено електронному листуванню. При використанні електронної пошти, працівники повинні враховувати наступні речі:

– активність на дискусійних форумах може призвести до розкриття адреси електронної пошти необмеженій кількості одержувачів у різних країнах, деякі з яких можуть бути абсолютно невідомі;

– працівники повинні пам’ятати про відповідальність, що випливає з авторських прав, захисту персональних даних і захисту особистих прав адресата.

Для уникнення непорозумінь можливі наступні дії співробітників, що пов’язані з використанням електронної пошти, ІТ-систем Компанії і ІТ-обладнання, будуть вважатися серйозним порушенням цієї ІТ-політики:

– надсилання електронних листів, текстових повідомлень, MMS або електронних повідомлень, що містять порнографічний, нецензурний або сексуальний характер однозначний вміст зображення чи документи або такі, що порушують людську гідність чи інші особисті права будь-яким іншим способом;

– надсилання образливих, вульгарних або інших недоречних електронних листів чи електронних чи текстових повідомлень;

– надсилання електронних листів або текстових повідомлень дискримінаційного характеру, що стосуються статі, сексуального характеру, орієнтації, раси, кольору шкіри, національності, етнічного походження, віку, інвалідності, релігійних чи політичних переконань;

– надсилання електронних листів або текстових повідомлень, що містять переслідування;

– використання електронної пошти в особистих цілях способом, що виходить за межі ІТ-політики;

– надсилання електронних листів або інших повідомлень, які призводять або можуть призвести до встановлення договірних відносин між Компанією і третіми особами, якщо співробітник не був уповноважений на це Компанією.

Важливо також наголосити, що Політика вимагає від працівників не полишати ввірений їм комп’ютер ніде без відповідного нагляду або заходів безпеки. У разі крадіжки або пошкодження з вини співробітника або в результаті недбалості працівника, Роботодавець може обтяжити працівника витратами, понесеними через втрату або пошкодження обладнання.

Отже, для забезпечення високого рівня безпеки необхідно створити стратегію інформаційної безпеки компанії, яка буде базуватися на важливості інтеграції безпеки в основні аспекти бізнесу та враховувати людський фактор. На основі стратегії створюється політика безпеки. Товариство «БАСФ Т.О.В» у роботі з інформацією та соціальними мережами керується власною Політикою безпеки. Політика безпеки Товариства є керованою бізнесом і таким чином гарантує, що безпека інтегрована в структуру організації та є питанням основного бізнесу. Особливу увагу в цьому документі приділено саме листуванню через електронну пошту, а також використанню IT-система та IT-обладнання компанії.

3.3. Можливості та перспективи використання нових засобів у роботі з соціальними мережами ТОВ «БАСФ Т.О.В»

Соціальні мережі можуть і повинні відігравати важливу роль у діяльності підприємств. Сьогодні людський капітал поступово заміщає основні матеріальні засоби як фактор оцінки вартості організації. Робота все більше стає спільною, а середовище розробки – більш складним. Впроваджуються схеми управління організацією, для яких соціальні мережі є важливим механізмом використання колективного досвіду, надають масу корисної інформації, а також дозволяють донести до широкої аудиторії інформацію про підприємство, причому зі зворотним зв’язком. Соціальні мережі – це унікальний інструмент для пошуку потрібних співробітників, засіб підтримки професійних співтовариств і об’єднання людей по інтересах, доступ до корисних посилань, що дають швидкий спосіб оцінки інформації.

Однак, нові можливості несуть у собі й нові ризики, особливо ризики кіберпростору. Кібератаки вважаються різноманітними та складними соціальними подіями та постійною загрозою. Своєчасне виявлення створює труднощі для компаній, оскільки багато загроз містяться в комп’ютерних платформах. У цьому відношенні машинне навчання та інтелектуальний аналіз

даних є технологіями, які контролюватимуть уразливість організацій шляхом аналізу подій в інформаційному просторі, забезпечуючи автоматичний захист у реальному часі. Використовуючи аналітичні моделі, технологія машинного навчання постійно вдосконалюється, вивчаючи нові процеси та можливості для знаходження прихованих даних, навіть не програмуючи комп'ютери [75, с. 56-72; 76, с. 135].

Для ландшафту кібербезпеки упровадження машинного навчання може сприяти розробці широкого спектру рішень і прогнозуванню небезпек. Сьогодні програмне забезпечення для кібербезпеки послідовно допомагає компаніям, будучи гнучким і простим у реалізації: забезпечує абсолютний моніторинг трафіку в мережі; пропонує видимість використання криптографії організацією шляхом вивчення проблем безпеки та формулювання рекомендацій для впровадження. Завдяки цьому його легко та швидко впровадити, надаючи підтримку в створенні політик проти зловмисного програмного забезпечення, вірусів, блокування доступу, фішингу чи невідповідних матеріалів [74].

Більшість кібератак відбувається від внутрішніх і зовнішніх загроз. Людське мислення повинно повністю усвідомлювати наслідки неадекватного управління використовуваного програмного забезпечення. Співробітники повинні володіти базовими знаннями щодо пакету безпеки в інтернеті, надійної зміни пароля, постійно оновлювати програмне забезпечення, бути поінформованим про порушення безпеки, захист від крадіжки особистих даних. Враховувати вплив інформації необхідно кожному співробітнику, оскільки це надає можливість попередити загрозу, не видати найбільш затребувані дані хакерам, захистити інформацію компанії [63, с. 2; 68, с. 13].

Одним із ресурсів поширення інформації та здійснення бізнес- комунікацій в інтернет є комп'ютерні соціальні мережі. У соціальних мережах зареєстровано сотні мільйони користувачів, через мережі розповсюджується різноманітна інформація, у базах даних соціальних мереж зберігаються величезні масиви інформації, а їх власники отримують мільярдні прибутки[45, с. 210-211].

Товариство «БАСФ Т.О.В» використовує соціальні мережі для різних цілей, включаючи сприяння бренду, взаємодію з клієнтами, рекрутинг та інше. Стратегії та цілі, які переслідує компанія, користуючись соцмережами можуть змінюватися в часі, тому розглянемо загальні аспекти використання подібних мереж, такі як:

– бренд і спілкування: Товариство використовує соціальні мережі для підтримки свого бренду та встановлення відкритого спілкування з аудиторією. Публікації можуть стосуватися інновацій, сталого розвитку, діяльності компанії та інших важливих питань;

– маркетинг та реклама: соціальні мережі є платформою для розміщення рекламних кампаній, які можуть включати в себе відео, графічний контент, промо-акції та інші форми маркетингового впливу;

– залучення клієнтів та партнерів: компанія може використовувати соціальні мережі для спілкування з клієнтами, відповіді на їх питання, збору відгуків та взаємодії з партнерами;

– інфлюенс-маркетинг: залучення інфлюенсерів для співпраці допомагає ТОВ «БАСФ Т.О.В» привертати увагу відповідної аудиторії та демонструвати застосування своїх продуктів у конкретних галузях;

– освіта та інформаційна діяльність: компанія використовує соціальні мережі для надання освітнього контенту, поділу інформації про нові технології та інновації в галузі хімії;

– рекрутинг та емплойер брендінг: Товариство може використовувати соціальні мережі для рекрутингу нового персоналу, а також для підвищення свого привабливості як роботодавця;

– сталість та екологічна відповідальність: за допомогою соціальних мереж, компанія підкреслює свої зобов’язання до сталого розвитку та екологічної відповідальності;

– взаємодія зі спільнотами та стейкхолдерами: спілкування з різними групами, такими як наукова спільнота, громадські організації, регулятори та інші

стейкхолдери, може сприяти позитивним взаєминам та підтримці різноманітних ініціатив.

Залежно від стратегії та мети компанії, використання соціальних мереж може включати в себе різноманітні методи та інструменти для досягнення бізнес-цілей. Важливо постійно вдосконалювати та адаптувати стратегії відповідно до змін у галузі та очікувань аудиторії.

Використання нових засобів у роботі із соціальними мережами відкриває широкі можливості для різних сфер, включаючи бізнес, маркетинг, науку, громадські відносини та інші. Перспективи та можливості використання нових інструментів Товариством «БАСФ Т.О.В» у цьому контексті є наступними:

– аналітика та великі дані: використання інструментів аналітики дозволяє виявляти та розуміти тренди в соціальних мережах. Великі дані дозволяють аналізувати великі обсяги інформації, що надходить із соціальних платформ, щоб робити здорові бізнес-рішення та прогнозувати поведінку користувачів та клієнтів;

– соціальний маркетинг: інструменти соціального маркетингу дозволяють компаніям ефективно взаємодіяти з аудиторією, побудовувати бренд, вивчати реакції на продукти та послуги, а також запускати рекламні кампанії, спрямовані на конкретних користувачів;

– взаємодія з клієнтами: використання засобів автоматизованої взаємодії дозволяє компаніям відповідати на питання та вирішувати проблеми клієнтів у реальному часі, що покращує якість обслуговування;

– організація подій: соціальні мережі дозволяють легко організовувати та рекламувати події. Вони стають потужним інструментом для мобілізації аудиторії та залучення учасників;

– громадське обговорення та зв’язки: соціальні мережі використовуються для спілкування та обговорення різних суспільних та політичних питань. Це може стати інструментом для будівництва спільнот та активізації громадської участі;

– персоналізований контент: використання алгоритмів та штучного інтелекту дозволяє створювати персоналізований контент для користувачів, що збільшує ефективність комунікації між співробітниками компанії;

– захист від кіберзагроз: засоби безпеки та моніторингу дозволяють виявляти та запобігати кіберзагрозам через соціальні мережі, такі як фішинг, шахрайство, дезінформація та інше.

Отже, використання нових технологій у сфері соціальних мереж відкриває багато можливостей для покращення ефективності бізнесу, спілкування та інновацій. Однак важливо враховувати етичні аспекти та забезпечувати захист приватності користувачів та працівників під час використання цих інструментів.

Наразі багато компаній використовують штучний інтелект (ШІ), щоб покращити свої стратегії роботи із соціальними мережами, і Товариство «БАСФ Т.О.В» не виключає для себе подібної можливості. Технології штучного інтелекту можуть забезпечувати ефективність, персоналізацію та аналіз даних на основі різних аспектів управління соціальними мережами. Ось кілька способів, якими компанія зможе використовувати штучний інтелект у своїй взаємодії із соціальними мережами:

– рекомендація щодо вмісту: алгоритми ШІ аналізують поведінку та вподобання користувачів, щоб рекомендувати персоналізований контент. Це допомагає компаніям адаптувати свої публікації в соціальних мережах до інтересів своєї аудиторії, підвищуючи залучення;

– чат-боти та віртуальні помічники: компанії використовують чат-боти та віртуальних помічників на основі штучного інтелекту для автоматизації взаємодії з клієнтами на платформах соціальних мереж. Ці інструменти можуть відповідати на поширені запитання, надавати підтримку та керувати користувачами різними процесами;

– соціальне прослуховування: інструменти штучного інтелекту можуть відстежувати платформи соціальних мереж на предмет згадок брендів, галузевих тенденцій і настроїв клієнтів. Це дає компаніям змогу отримати цінну

інформацію про те, що люди говорять про їхній бренд і конкурентів, що дозволяє активно залучати їх;

– прогнозна аналітика: ШІ може аналізувати історичні дані, щоб прогнозувати майбутні тенденції та поведінку користувачів. Це важливо для компаній, які прагнуть передбачити зміни ринку, оптимізувати стратегії контенту та випередити своїх конкурентів;

– націлювання реклами та персоналізація: алгоритми штучного інтелекту аналізують дані користувачів, щоб оптимізувати націлювання реклами на платформах соціальних мереж. Це гарантує показ реклами найрелевантнішій аудиторії, збільшуючи ймовірність переходів. AI також може персоналізувати контент на основі вподобань користувача;

– моніторинг соціальних мереж для захисту бренду: інструменти штучного інтелекту можуть визначати потенційні загрози репутації компанії, відстежуючи соціальні мережі на предмет негативних згадок, відгуків або тенденцій. Це дозволяє компаніям оперативно вирішувати проблеми та захищати імідж свого бренду;

– автоматизоване звітування: ШІ може автоматизувати процес збору та аналізу показників соціальних мереж. Це спрощує звітність і дозволяє компаніям ефективніше відстежувати ефективність своїх кампаній у соціальних мережах;

– аналіз зображень і відео: технології розпізнавання зображень і відео на основі штучного інтелекту допомагають компаніям контролювати візуальний вміст у соціальних мережах. Це може включати ідентифікацію логотипів брендів, аналіз настроїв зображень і виявлення невідповідного або несанкціонованого використання візуальних ресурсів;

– інфлюенсерський маркетинг: Інструменти штучного інтелекту допомагають компаніям визначати відповідних впливових осіб, аналізуючи такі дані, як демографічні показники аудиторії, рівень залученості та довіра до впливових осіб. Це забезпечує кращі збіги між брендами та впливовими особами;

– безпека даних і виявлення шахрайства: штучний інтелект використовується для підвищення безпеки облікових записів у соціальних мережах шляхом виявлення підозрілих дій, запобігання несанкціонованому доступу та виявлення шахрайської поведінки, наприклад підроблених облікових записів або взаємодії з ботами;

– обробка природної мови або збір фідбеку (NLP): НЛП дозволяє компаніям ефективніше розуміти коментарі та повідомлення користувачів у соціальних мережах і реагувати на них. Це допомагає отримувати інформацію з неструктурованих текстових даних і полегшує аналіз настроїв.

Інтеграція штучного інтелекту в стратегії соціальних мереж дозволяє компаніям оптимізувати свої процеси, ефективніше взаємодіяти зі своєю аудиторією та приймати рішення на основі даних для кращої загальної ефективності в соціальних мережах. Оскільки технології продовжують розвиватися, роль штучного інтелекту в управлінні соціальними медіа, ймовірно, буде розвиватися та розширюватися.

Необхідно також зазначити, що є можливості використання нових засобів роботи з інформацією та соціальними мережами для уникнення інформаційних загроз і збереження приватності. Це стає дедалі важливішим завданням для компаній та користувачів. Ось деякі стратегії та засоби, які можна використовувати:

– шифрування даних: використання шифрування для захисту конфіденційної інформації від несанкціонованого доступу. Це може включати шифрування електронної пошти, зберігання файлів та зв'язку в соціальних мережах;

– двофакторна аутентифікація: встановлення двофакторної аутентифікації для зміцнення захисту облікових записів у соціальних мережах та інших сервісах. Це додає додатковий шар безпеки;

– політики користування даними: розробка та виконання строгих політик користування даними як внутрішніх, так і щодо спільноти. Компанії

повинні докладати зусиль для забезпечення того, що дані користувачів обробляються відповідно до встановлених стандартів;

– системи управління ідентифікацією та доступом (IAM): застосування систем IAM для контролю доступу до інформації та ресурсів. Це включає в себе обмеження доступу до даних лише тим користувачам, які мають відповідні права;

– моніторинг та аналіз заходів безпеки: використання інструментів моніторингу та аналізу для постійного відслідковування подій інформаційної безпеки, виявлення аномалій та вчасного реагування на потенційні загрози;

– освіта та тренінг персоналу: проведення навчання з питань інформаційної безпеки для персоналу, яке включає усвідомлення ризиків, правила безпеки та процедури реагування на інциденти;

– блокування небажаних джерел: використання систем блокування рекламних та шкідливих вмістів для зменшення ризику взлому та інших інформаційних атак через соціальні мережі;

– контроль доступу та правила конфіденційності: встановлення чітких правил конфіденційності та обмеження доступу до конфіденційної інформації. Це може включати регулярне оновлення доступів та ревізії прав доступу;

– використання технологій AI для виявлення загроз: використання технологій штучного інтелекту для виявлення аномальної активності та потенційних загроз в реальному часі;

– резервне копіювання та відновлення даних: проведення регулярного резервного копіювання важливих даних та визначення стратегій відновлення для випадку втрати інформації;

– використання енкрипції передачі даних: використання енкрипції для захисту конфіденційної інформації, яка передається через соціальні мережі та інші канали зв’язку.

Отже, раховуючи постійний розвиток технологій та зростання кількості загроз, компанії повинні постійно підтримувати та оновлювати свої стратегії

забезпечення інформаційної безпеки, щоб ефективно захищати дані та зберігати приватність користувачів.

Отже, зрозуміло, що соціальні мережі стали необхідним інструментом для компаній у віртуальному світі, де взаємодія та спілкування грають ключову роль в успіху бізнесу. Основними перспективами від використання соцмереж для Товариства з обмеженою відповідальністю «БАСФ Т.О,В» є: використання аналітики та великих даних; соціального маркетингу; взаємодії з клієнтами; організації подій; громадського обговорення та зв'язків; створення персоналізованого контенту; захист від кіберзагроз. Новітні можливості, які має змогу використовувати компанія, базуються на технологіях штучного інтелекту і включають у себе: створення рекомендацій щодо вмісту контенту публікацій; використання чат-ботів та віртуальних помічників; соціальне прослуховування; прогнозну аналітику; націлювання реклами та персоналізацію; моніторинг соціальних мереж для захисту бренду; автоматизоване звітування; аналіз зображень і відео; інфлюенсерський маркетинг; безпеку даних і виявлення шахрайства; обробку природної мови або збір фідбеку. Для запобігання та захисту від інформаційних загроз можливо використовувати наступні методи: шифрування даних; двофакторна аутентифікація; політики користування даними; системи управління ідентифікацією та доступом; моніторинг та аналіз заходів безпеки; блокування небажаних джерел; контроль доступу та правила конфіденційності та інші.

Таким чином, через великий обсяг інформації та складну технологічну інфраструктуру, вимоги безпеки, інформаційний відділ ТОВ «БАСФ Т.О.В» надзвичайно важливий для ефективної роботи компанії та досягнення її бізнес-цілей. Структура інформаційного відділу передбачає наявність таких підрозділів: керівництво; інфраструктура і технічна підтримка; розробка програмного забезпечення; безпека інформації; аналітика і документація; стратегія та розвиток; управління проєктами. Процедури безпеки в поводженні з інформацією повинні бути розроблені, реалізовані та оновлені відповідно до

бізнес-операцій та процесів. Стратегія безпеки Товариства наголошує на важливості інтеграції безпеки в основні аспекти бізнесу. Тому, для забезпечення високого рівня безпеки, на основі стратегії створюється політика безпеки у роботі з інформацією та соціальними мережами. Особливу увагу в цьому документі приділено саме листуванню через електронну пошту, а також використанню IT-система та IT-обладнання компанії. Оскільки соціальні мережі є інструментом для компаній у віртуальному світі, основними перспективами від їхнього використання для Товариства з обмеженою відповідальністю «БАСФ Т.О,В» є: використання аналітики та великих даних; соціального маркетингу; взаємодії з клієнтами; організації подій; громадського обговорення та зв'язків; створення персоналізованого контенту; захист від кіберзагроз. Новітні можливості, які має змогу використовувати компанія, базуються на технологіях штучного інтелекту і включають у себе: створення рекомендацій щодо вмісту контенту публікацій; використання чат-ботів та віртуальних помічників; соціальне прослуховування; прогнозну аналітику; націлювання реклами та персоналізацію; моніторинг соціальних мереж для захисту бренду; автоматизоване звітування; аналіз зображень і відео; інфлюенсерський маркетинг; безпеку даних і виявлення шахрайства; обробку природної мови або збір фідбеку. Сучасні методи для захисту від інформаційних загроз і збереження приватності включають: моніторинг та аналіз заходів безпеки; контроль доступу та правила конфіденційності; блокування небажаних джерел; освіта та тренінг персоналу; використання технологій AI для виявлення загроз; використання енкрипції передачі даних та інші.

ВИСНОВКИ

Соціальні мережі, як новий вид інформаційно-комунікаційних каналів, стрімко розвиваються. В інформаційному середовищі вони надають можливості для швидкої передачі даних у різних форматах, наприклад, текстовому, аудіовізуальному, відеоформаті та інших, поширення контенту для великих соціальних груп, збору інформації про вподобання суспільства, висловлення думок за допомогою зручного інструментарію, маркетингу та реклами товарів чи послуг та ін. Зі збільшенням популярності соцмереж зростають і інформаційні загрози та небезпеки цього виду комунікаційних каналів, усе частіше користувачі стикаються із соціальною інженерією, кібератаками, дезіформацією та іншим. Тому нами було досліджено явище соціальних мереж як середовище та причину загроз, а також як вирішення проблем за допомогою наявних технологій.

Відповідно до поставленої мети у кваліфікаційній роботі проаналізовано історіографію, джерельну базу для дослідження обраної проблематики про соціальні мережі, як важливу складову для розуміння процесів інформаційного впливу на організації, їхніх працівників та звичайних користувачів, а також підприємства різних галузей. Було обґрунтовано застосовані методи дослідження, за допомогою використання яких вдалося досягти визначеної в дослідженні мети. Аналіз наукових джерел, дозволив зробити висновок, що проблематиці дослідження присвячено достатню кількість наукових робіт, проте актуальним залишається вивчення інформаційних загроз у соціальних мережах, адже ця тема недостатньо висвітлена як у роботах вітчизняних науковців. Отже, наразі не існує єдиного підходу до визначення сутності загроз соціальних мереж як в українській, так і в зарубіжній думці.

Досліджено соціальні мережі як середовище інформаційного впливу, із чого можемо зробити висновок, що соціальні мережі існують як онлайн середовища, де користувачі поширюють інформацію для необмежених за кількістю чи кордонами соціальних груп, обираючи певний її формат, до прикладу, текстовий, аудіо чи відео, за допомогою мережі «Інтернет». Визначено,

що інформаційний вплив, як явище інформаційного поля, є небезпечним для соціального життя не лише окремих груп, але для світової спільноти, що змушує шукати засоби протидії. Інформаційний вплив, зо відбувається в онлайн-середовищі, має чітку ціль та спрямований проти інформаційної свободи та волі особистості, часто здійснюється за допомогою маніпуляцій та технологій. Соціальні мережі спростили можливості для інформаційного впливу завдяки таким особливостям, як наповнення змісту користувачами, можливість вести політичну, рекламну чи ін. види діяльності, цілодобова доступність інформації, а також технічним характеристикам: створення різноформатного медійного контенту лідерами думок; швидкість надходження відомостей до споживачів; пропагування ідей через дезінформацію та інше. Саме тому їх використання як інструмента та середовища інформаційного впливу є надзвичайно зручним.

З'ясовано сутність інформаційних загроз у соціальних мережах та типові види цих небезпек інформаційного простору. Отже, інформаційною загрозою вважаємо явище, що потенційно чи реально здатне призвести до негативного ефекту для людини, спричинене інформаційним впливом на особистість, суспільство й державу. Цей вид небезпеки потребує особливих умов для існування, а саме інформаційного середовища, динамічного та нерегульованого. Метою цих загроз на рівні соціальної одиниці є нанесення шкоди інформаційній безпеці людини, її матеріальному становищу, викрадення персональних даних, психологічний вплив; на рівні держави – унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей, національної безпеки та оборони. Інформаційні загрози поділяють на інформаційно-технологічні, інформаційно-комунікаційні, інформаційно-психологічні, а також за наступними критеріями: за ступенем небезпеки на особливо небезпечні та небезпечні; за можливістю дії на реальні, потенційні; за масштабами дії – національні, локальні, індивідуальні; за тривалістю дії – тимчасові, постійні; за характером впливу – прямі, безпосередні, опосередковані; за терміном дії – довгострокові, середньострокові, короткострокові, поточні; за сферою інформаційної діяльності, де виокремлюємо зовнішньо- та

внутрішньополітичну сферу, воєнну, економічну, соціальну, гуманітарну, науково-технологічну та екологічну сфери. Властивості соцмереж, такі як наявність власних думок користувачів, зміна думки під впливом інших членів соціальної мережі, різна значимість думок (впливовість, довіри) одних користувачів для інших, існування «лідерів думки» та інші, створюють ідеальні умови для інформаційних загроз. Видами таких явищ є: соціальна інженерія, пропаганда, дезінформація, сугестія, шкідливе програмне забезпечення, крадіжка паролів і фішинг, витік інформації, вебатаки, ріст трафіку, втрату особистого часу. Інформаційні загрози в соціальних мережах є потужним інструментом, від якого відмовитися в цифровому суспільстві неможливо, але, як для компаній, так і для звичайних користувачів є можливість мінімізувати загрози.

Вивчено існуючі практики та заходи безпеки, що використовуються для запобігання та боротьби з інформаційними загрозами. Небезпечність соціальних мереж зростатиме через такі тенденції: соціальні мережі стають менш «соціальними», відсіваючи «непотрібних» членів; корпорації використовують це середовище для ефективнішого обслуговування клієнтів; бізнес усвідомлює значимість використання внутрішніх і зовнішніх мереж; відбувається формалізація компаніями політик використання соціальних мереж; мобільність стає невід'ємною рисою соціального спілкування, особливо для службовців тих компаній, у яких забороняється використання соціальних мереж у робочий час. Тобто, зміни, які нині відбуваються в соціальних мережах, лише посилюють необхідність застосування методів боротьби із цими небезпеками. Участь держави є необхідною умовою для правового регулювання заходів захисту та протидії загрозам, зокрема, законодавчого закріплення права особи на інформацію та захист від негативного впливу шкідливої інформації, трансформації моделі взаємовідносин між органами державної влади та ЗМІ, створення національних систем і мереж інформації. В умовах розв'язання проти України відкритої інформаційної агресії, можемо розділити на три загальні рівні заходи запобігання інформаційним загрозам: геополітичний – спрямований на

викриття інформаційного агресора й обмеження інтенсивності та сили його нападу; державний – включає захист системи державного управління, інформаційної інфраструктури, політико-культурного простору; суспільний – спрямований на захист стабільності й безперервності розвитку суспільно-політичних відносин. Визначено, що існує потреба в створенні механізму узгодження законодавства із реаліями і прогресом інформаційних технологій. Хоча закони не можуть випереджати життя, але необхідно зменшити відставання від реального стану речей. Існують різноманітні засоби захисту від інформаційних загроз, наприклад, компанії використовують системний підхід до управління та безпеки, поінформованість працівників, особливо в кризових, конфліктних і нестабільних ситуаціях. Звичайні користувачі мають використовувати: сильний пароль, двоетапну перевірку інформації, обмеження витоку особистої інформації, антивірусні програми та налаштування безпеки.

Було охарактеризовано структуру інформаційного відділу ТОВ «БАСФ Т.О.В», який відіграє важливу роль для великих концернів і корпорацій. Інформаційний відділ регулює або впливає на багато аспектів бізнесу й має безпосередній вплив на успішність компанії. Основними причинами центральної ролі цього відділу для функціонування Товариства «БАСФ Т.О.В» є: великий обсяг інформації, складна технологічна інфраструктура та вимоги до безпеки. Структурно, цей відділ компанії налічує такі підрозділи: керівництво; інфраструктура і технічна підтримка; розробка програмного забезпечення; безпека інформації; аналітика і документація; стратегія та розвиток; управління проєктами. Робота з інформацією регулюється інструкціями концерну «BASF SE». Основними особливостями під час подібної діяльності є: конфіденційність і безпека інформації; дослідження і розробка; регулювання і стандарти; управління ланцюжком постачання; співпраця та комунікація; використання аналізу великих обсягів даних та аналітики; стратегія та інновації.

Розглянуто політику безпеки в роботі з інформацією та соціальними мережами на підприємстві ТОВ «БАСФ Т.О.В». Визначено, що процедури безпеки у роботі з соцмережами повинні бути розроблені, реалізовані та оновлені

відповідно до бізнес-операцій та процесів. Поки процеси взаємопов'язані й інформаційний потік слідує бізнес-ланцюжку, дизайн системи безпеки повинен об'єднати всі зв'язані системи. Стратегія безпеки Товариства наголошує на важливості інтеграції безпеки в основні аспекти бізнесу та врахування людського фактора при розробці ефективних програм для захисту та використання працівниками. Беручи за основу стратегію безпеки, Товариство вводить у дію «Політику у роботі з інформацією та соціальними мережами». Політика безпеки Товариства є інтегрованою в структуру організації, а значну увагу в цьому документі приділено листуванню через електронну пошту, а також використанню IT-система та IT-обладнання компанії.

Визначено можливості та перспективи використання нових засобів роботи з інформацією та соціальними мережами ТОВ «БАСФ Т.О.В» з метою уникнення інформаційних загроз і збереження приватності. Необхідно зазначити, що подібні можливості використання нових засобів роботи з інформацією та соціальними мережами є актуальними для використання компанією, оскільки соціальні мережі можуть і повинні відігравати важливу роль у діяльності підприємств. До таких засобів належать: шифрування даних; двофакторна аутентифікація; політики користування даними; системи управління ідентифікацією та доступом; моніторинг та аналіз заходів безпеки; блокування небажаних джерел; освіта та тренінг персоналу; контроль доступу та правила конфіденційності; використання технологій AI для виявлення загроз; резервне копіювання та відновлення даних; використання енкрипції передачі даних. Основними перспективами від використання соцмереж для Товариства з обмеженою відповідальністю «БАСФ Т.О,В» є: використання аналітики та великих даних; соціального маркетингу; взаємодії з клієнтами; організації подій; громадського обговорення та зв'язків; створення персоналізованого контенту; захист від кіберзагроз. Загалом, новітні можливості, які має змогу використовувати компанія, базуються на технологіях штучного інтелекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Законодавчі та нормативно-правові акти

1. Конституція України : Основний Закон України від 28.06.1996. Поточна редакція 01.01.2020. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр/ed20200101#Text (дата звернення: 11.11.2023).

2. Кодекс законів про працю України. Від 01.06.1972. Поточна редакція 01.10.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/322-08#Text (дата звернення: 11.11.2023).

3. Господарський кодекс України. Від 16.01.2003. Поточна редакція 08.10.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/main/436-15#Text (дата звернення: 11.11.2023).

4. Цивільний кодекс України. Від 16.01.2003. Поточна редакція 05.10.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/main/435-15#Text (дата звернення: 11.11.2023).

5. Про інформацію : Закон України від 02.10.1992. Поточна редакція 27.07.2023. База даних «Законодавство України». URL:https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 11.11.2023).

6. Про охорону праці : Закон України від 14.10.1992. Поточна редакція 01.10.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/main/2694-12#Text (дата звернення: 11.11.2023).

7. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994. Поточна редакція 01.07.2022. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 11.11.2023).

8. Про рекламу : Закон України від 03.07.1996. Поточна редакція 02.10.2023. База даних «Законодавство України». URL:

https://zakon.rada.gov.ua/laws/main/270/96-%D0%B2%D1%80#Text (дата звернення: 11.11.2023).

9. Про захист персональних даних : Закон України від 01.06.2010. Поточна редакція 27.10.2022. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/main/2297-17#Text (дата звернення: 11.11.2023).

10. Про доступ до публічної інформації : Закон України від 13.01.2011. Поточна редакція 08.10.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/main/2939-17#Text (дата звернення: 11.11.2023).

11. Про зайнятість населення : Закон України від 05.07.2012. Поточна редакція 14.10.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/5067-17#Text (дата звернення: 11.11.2023).

12. Про правовий режим воєнного стану : Закон України від 12.05.2015. Поточна редакція 19.10.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення: 11.11.2023).

13. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. Поточна редакція 17.08.2022. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 11.11.2023).

14. Про товариства з обмеженою та додатковою відповідальністю : Закон України від 06.02.2018. Поточна редакція 01.01.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/main/2275-19#Text (дата звернення: 11.11.2023).

15. Про національну безпеку України : Закон України від 21.06.2018. Поточна редакція 31.03.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/main/2469-19#Text (дата звернення: 11.11.2023).

16. Про забезпечення функціонування української мови як державної : Закон України від 25.04.2019. Поточна редакція 27.10.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/main/2704-19#Text (дата звернення: 11.11.2023).

17. Про організацію трудових відносин в умовах воєнного стану : Закон України від 24.03.2022. Поточна редакція 19.07.2022. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/main/2136-20#Text (дата звернення: 11.11.2023).

18. Про медіа : Закон України від 13.12.2022. Поточна редакція 02.07.2023. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/main/2849-20#Text (дата звернення: 11.11.2023).

19. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»: Указ Президента України від 19 березня 2022 року № 152/2022. Поточна редакція 19.03.2022. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/152/2022#Text (дата звернення: 11.11.2023).

20. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 № 685/2021. Поточна редакція 28.12.2021. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 11.11.2023).

Офіційні сайти/портали підприємств, установ, організацій та їхні офіційні сторінки/блоги у соціальних мережах

21. Офіційний вебсайт «We are social». Спецзвіт «Digital 2023». URL: https://wearesocial.com/uk/blog/2023/01/digital-2023 (дата звернення: 16.11.2023).

22. Офіційний сайт ТОВ «БАСФ Т.О.В». URL: https://www.basf.com/ua/uk.html (дата звернення: 16.11.2023).

23. Офіційний сайт «BASF Agricultural Solutions Україна». URL: https://www.agro.basf.ua/uk/ (дата звернення: 16.11.2023).

24. Офіційний сайт «BASF SE». URL: https://www.basf.com/global/de/who-we-are/organization.html (дата звернення: 16.11.2023).

25. Офіційний сайт «USAID-Internews»: «Українські медіа, ставлення та довіра у 2022 р.». URL: https://internews.in.ua/wp-content/uploads/2022/11/Ukrainski-media-stavlennia-ta-dovira-2022.pdf (дата звернення: 16.11.2023).

26. Офіційна сторінка «BASF Agproducts» в інстаграмі. URL: https://instagram.com/basf_agproducts?igshid=OGQ5ZDc2ODk2ZA (дата звернення: 16.11.2023).

27. Офіційна сторінка «BASF Global» в інстаграмі. URL: https://instagram.com/basf_global?igshid=OGQ5ZDc2ODk2ZA (дата звернення: 16.11.2023).

28. Офіційна сторінка «BASF Agricultural Solutions UA» у фейсбуці. URL: https://www.facebook.com/BASFAgriculturalSolutionsUA (дата звернення: 16.11.2023).

29. Офіційна сторінка «BASF Personal Care» у фейсбуці. URL: https://www.facebook.com/BASF.PersonalCare (дата звернення: 16.11.2023).

30. Офіційна сторінка «BASF SE» у фейсбуці. URL: https://www.facebook.com/basf (дата звернення: 16.11.2023).

Наукові, довідкові, навчальні видання

31. Біленчук П., Борисова Л., Неклонський І, Собина В. Правові засади інформаційної безпеки України: монографія. Харків: Київський ун-т права; Нац. ун-т цивільного захисту України, 2018. 289 с. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/8484/1/Монография%20Борисова.pdf (дата звернення: 20.11.2023).

32. Бокоч Ю. Технології інформаційного впливу в умовах гібридної конфліктності. *Вісник Маріупольського державного університету.* 2017. № 19. С. 79–85. URL: https://cyberleninka.ru/article/n/tehnologiyi-informatsiynogo-vplivu-v-umovah-gibridnoyi-konfliktnosti/viewer (дата звернення: 20.11.2023).

33. Бржевська З., Гайдур Г., Аносов А. Вплив на достовірність інформації як загроза для інформаційного простору. *Кібербезпека: освіта, наука, техніка.* 2018. № 2. С. 106–112. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/32/73 (дата звернення: 20.11.2023).

34. Гуменюк В. Методи підвищення ефективності управління ризиками інформаційної безпеки підприємства. *Тернопільський національний технічний університет імені Івана Пулюя.* Тернопіль, 2019. URL: https://elartu.tntu.edu.ua/handle/lib/30728 (дата звернення: 20.11.2023).

35. Деркаченко Я. Соціальні мережі як середовище для технологій маніпулятивного впливу. *Сучасний захист інформації*. 2016. № 1. С. 51–59. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/531/493 (дата звернення: 20.11.2023).

36. Золотар О. Загрози інформаційній безпеці людини. *Правова інформатика.* 2014. № 2(42). С. 70–79. URL: https://ippi.org.ua/sites/default/files/14zooibl.pdf (дата звернення: 20.11.2023).

37. Іванова В. Інформаційна безпека як підсистема в системі економічної безпеки підприємства. *Управління фінансово-економічною безпекою: інформаційно-аналітичне забезпечення та конкурентна розвідка.* 2013. URL: http://eprints.kname.edu.ua/38599/1/67-71.pdf (дата звернення: 20.11.2023).

38. Кокарча Ю. Інтернет-спільноти в системі суспільно-політичних відносин. *Науковий часопис Національного педагогічного університету імені М. П. Драгоманова*. 2014. Спецвипуск. С. 451–456. URL: http://enpuir.npu.edu.ua/handle/123456789/14047 (дата звернення: 20.11.2023).

39. Коневщинська О., Литвинова С. Електронні соціальні мережі як складник сучасних соціальних медіа. *Інформаційні технології і засоби навчання*. 2016. № 5. С. 42–54. URL: http://nbuv.gov.ua/UJRN/ITZN_2016_55 _5_6 (дата звернення: 20.11.2023).

40. Кухарська Н., Кухарський В. Вплив соціальних мереж на корпоративну інформаційну та економічну безпеку. *Науковий часопис Львівського національного університету ім. Івана Франка*. 2015. С. 37–40. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/3740/kukharskanp kukharskyivm.pdf (дата звернення: 20.11.2023).

41. Лисенко О. Правовий захист суспільства від шкідливої інформації: автореф. дис. ... канд. юридичних наук: 12.00.07. Харків, 2011. 226 с. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/0b29a7e8-305e-45b1-b537-9ab3236f7a0d/content (дата звернення: 20.11.2023).

42. Літвінчук І. Дезінформація в соціальних мережах: алгоритми протидії. *Вчені записки ТНУ ім. В. І. Вернадського*. 2023. № 34 (73). С. 181 – 186. URL: https://www.philol.vernadskyjournals.in.ua/journals/2023/1_2023/part_2/29.pdf (дата звернення: 20.11.2023).

43. Лобовікова О. Соціальні мережі як феномен інформаційного суспільства. *Вісник Львівського університету*. 2011. № 5. С. 154 – 160. URL: http://nbuv.gov.ua/UJRN/Vlnu_sociology_2011_5_20 (дата звернення: 20.11.2023).

44. Мазуренко В., Штовба С. Огляд моделей аналізу соціальних мереж. *Вісник Вінницького політехнічного інституту «ВНТУ»*. 2015. Вип. 2. С. 62–74. URL: https://www.researchgate.net/publication/279535422_OGLAD_MODELEJ_ANALIZU_SOCIALNIH_MEREZ (дата звернення: 20.11.2023).

45. Маркіна І., Гарічев Ю. Інформаційна безпека підприємства та організаційні заходи її забезпечення. *Українськии журнал прикладної економіки*. 2019. № 4. С. 209–215. URL: https://www.dnu.dp.ua/docs/ndc/dissertations/K08.051.19/autoreferat_5bb2 b747a54ef.pdf (дата звернення: 20.11.2023).

46. Нашинець-Наумова А. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с. URL: https://elibrary.kubg.edu.ua/id/eprint/18860/1/A_Nashinets-Naumova_mono-grafia_1_FPMV.pdf1 (дата звернення: 20.11.2023).

47. Онищенко О., Горовий В., Попик В. Соціальні мережі як чинник розвитку громадянського суспільства. *НАН України, Нац. б-ка України ім. В.І.*

Вернадського : монографія. Київ: НБУВ, 2013. 220 с. URL: http://irbis-nbuv.gov.ua/everlib/item/er-0003166 (дата звернення: 20.11.2023).

48. Остроухов В., Петрик В., Присяжнюк М. Інформаційна безпека (соціально-правові аспекти): підручник. Київ: Ліра-К, 2021. 776 с. URL: https://lira-k.com.ua/preview/12867.pdf (дата звернення: 20.11.2023).

49. Поліщук О. Вплив соціальних інтернет-мереж на формування «Я». *Актуальні проблеми філософії та соціології*. Одеса. 2017. Вип. 16. С. 93–96. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/11688/ Polishchuk%20% D0%90.%20S..pdf?sequence=1 (дата звернення: 20.11.2023).

50. Почепцов Г. Смислові та інформаційні війни. *Інформаційне суспільство*. 2013. № 18. С. 21–27. URL: http://nbuv.gov.ua/UJRN/is_2013_18_6 (дата звернення: 20.11.2023).

51. Петрик В., Присяжнюк М. Сугестивні технології маніпулятивного впливу: навч. посіб. Київ: ЗАТ "ВІПОЛ", 2011. 248 с. URL: https://duikt.edu.ua/uploads/l_1353_77641912.pdf (дата звернення: 20.11.2023).

52. Руднєва А. Інформаційні війни як фактор впливу на політичну культуру в сучасній Україні: автореф. дис. ... канд. політичних наук: 23.00.03. Київ, 2014. 229 с. URL: http://enpuir.npu.edu.ua/handle/123456789/7133 (дата звернення: 20.11.2023).

53. Самчинська О., Фурашев В. Інформаційне насильство, інформаційна маніпуляція та пропаганда: поняття, ознаки та співвідношення. *Інформація і право*. 2021. № 1(36). URL: http://il.ippi.org.ua/article/view/238183/236824 (дата звернення: 20.11.2023).

54. Семен Н. Російські інтернет-ресурси як чинник інформаційної війни проти україни (на прикладі сайтів «Правда.ру» та «Российский диалог»): автореф. дис. … канд. наук із соц. комунікацій: 27.00.01. Дніпро, 2018. 247 с. URL: https://www.dnu.dp.ua/docs/ndc/dissertations/K08.051.19/autoreferat_5bb2 b747a54ef.pdf (дата звернення: 20.11.2023).

55. Слінько Т. Сучасні загрози інформаційній безпеці країни та шляхи їх подолання. *Український часопис конституційного права.* 2021. № 4. С. 77–84.

URL: https://www.constjournal.com/pub/4-2021/suchasni-zahrozy-informatsiyniy-bezpetsi-krainy-shliakhy-ikh-podolannia/ (дата звернення: 20.11.2023).

56. Смотрич Д. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського національного університету*. 2023. № 77. С. 121–127. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/284104/278250 (дата звернення: 20.11.2023).

57. Чалабієва М. Поняття соціальних мереж як особливого виду електронних засобів масової інформації. *Молодий вчений.* 2019. № 8. С. 125–129. URL: https://molodyivchenyi.ua/index.php/journal/article/view/2282/2267 (дата звернення: 20.11.2023).

58. Чернозубкін І., Цюцюпа С. Особливості управління інформацією суб'єкту господарювання з використанням комп'ютерних соціальних мереж. *Вчені записки Університету «КРОК».* Київ.: КРОК, 2012. № 31. С. 170–177.

59. Юр'єва А. Вплив соціальних мереж на суспільство. *Масова комунікація: історія, сьогодення, перспективи*. 2015. № 7-8 (6). С. 81–83. URL: https://evnuir.vnu.edu.ua/bitstream/123456789/10267/1/Yurieva.pdf (дата звернення: 20.11.2023).

60. Aimeur E., Amril S., Brassard G. Fake news, disinformation and misinformation in social media: a review. *Social Network Analysis and Mining.* 2023. Vol. 13, no. 30. P. 1–36. URL: https://link.springer.com/article/10.1007/s13278-023-01028-5 (date of access: 25.11.2023).

61. Brandon J. Here's The Real Problem With Social Media. *Forbes.* 2022. URL: https://www.forbes.com/sites/johnbbrandon/2022/12/14/heres-the-real-problem-with-social-media/?sh=23c046933cf8 (date of access: 25.11.2023).

62. Cristea L. Current security threats in the national and international context. *Journal of Accounting and Management Information Systems.* 2020. Vol. 19, no. 2. P. 351–378. URL: https://EconPapers.repec.org/RePEc:ami:journl:v:19:y :2020 : i:2:p:351-378 (date of access: 25.11.2023).

63. Luigi Gallo L., Botta A., Ventre G. Identifying threats in a large company's inbox. *Machine Learning and Artificial Intelligence for Data*

Communication Networks. 2019. P. 1–7. URL: https://doi.org/10.1145/3359992.3366637 (date of access: 25.11.2023).

64. Gritzalis D., Kandias M., Stavrouv., Mitrou L. History of Information: The case of Privacy and Security in Social Media. *Legal Publications*. 2014. P. 1–25. URL: https://www.infosec.aueb.gr/Publications/INFOHIST-2014%20Legal%20Publications.pdf (date of access: 25.11.2023).

65. Huminskiy R., Peleshchyshynb A. An Assessment of Informational Threat in the Functioning Process of Virtual Community. *Cybernetic Letters.* 2014. URL: http://www.cybletter.cz/files/AnAssessmentOfInformationalThreatInTheFunctioningProcessOfVirtualCommunity.pdf (date of access: 25.11.2023).

66. Jacquemard T., Monaghan D., O'Connor N. The Convergence of Virtual Reality and Social Networks: Threats to Privacy and Autonomy. *Science and Engineering Ethics*. 2016. Vol. 22. P. 1–29. URL: https://link.springer.com/article/10.1007/s11948-014-9621-1 (date of access: 25.11.2023).

67. Kayworth T., Whitten B. Effective Information Security Requires a Balance of Social and Technology Factors. *MIS Quarterly Executive*. 2010. Vol. 9, no. 3. P. 163–176. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2058035 (date of access: 25.11.2023).

68. Kim J. Online Social Media Networking and Assessing Its Security Risks. *International Journal of Security and Its Applications*. 2012. Vol. 6, no. 3. P. 11–18. URL: onl_ine_sns-libre.pdf (date of access: 25.11.2023).

69. Kirichenko L., Radivilova T., Carlsson A. Detecting cyber threats through social network analysis: short survey. *SocioEconomic Challenges.* 2017. Vol. 1, no. 1. P. 20–34. URL: https://arxiv.org/abs/1805.06680 (date of access: 25.11.2023).

70. Lemieux V. Two Approaches to Managing Information Risks. *Information Management Journal.* 2004. Vol. 38, no. 5. P. 56–62. URL: https://www.proquest.com/openview/3f70dad0eeca7f62fab9f224ac710ef6/1?pq-origsite=gscholar&cbl=47365 (date of access: 25.11.2023).

71. Loch K., Carr H., Warkentin M. Threats to Information Systems: Today`s Reality, Yesterday's Understanding. *MIS Quarterly.* 1992. Vol. 16, no. 2. P. 173–186. URL: https://www.jstor.org/stable/249574 (date of access: 25.11.2023).

72. Molodetska K, Tymonin Y. System-dynamic models of destructive informational influence in social networking services. *International Journal of 3D Printing Technologies and Digital Industry.* 2019. Vol. 3, no. 2. P. 137–146. URL: https://dergipark.org.tr/en/pub/ij3dptdi/issue/48431/554224 (date of access: 25.11.2023).

73. Parcu P. New digital threats to media pluralism in the information age. *Competition and Regulation in Network Industries.* 2020. Vol. 21, no. 2. P. 65–218. URL: https://journals.sagepub.com/doi/epub/10.1177/1783591719886101 (date of access: 25.11.2023).

74. Pietrantonio F., Botta A., Ventre G., Gallo L., Zinno S., Mancuso L., Presta R. Investigating Gaze Behavior in Phishing Email Identification. 7th Network Traffic Measurement and Analysis Conference (TMA). Naples, 2023. URL: https://ieeexplore.ieee.org/document/10199095 (date of access: 25.11.2023).

75. Posetti J., Ireton C. Journalism, Fake News & Disinformation. Paris: UNESCO, 2018. 122 p. URL: https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf (date of access: 25.11.2023).

76. Prislan K. Efficiency of Corporate Security Systems in Managing Information Threats: An Overview of the Current Situation. *Journal of Criminal Justice and Security.* 2016. No 2. P. 128–147. URL: https://www.researchgate.net/profile/KajaPrislan/publication/301626234_Efficiency_of_Corporate_Security_Systems_in_Managing_Information_Threats_An_Overview_of_the_Current_Situation/links/571e50c908aead26e71a8710/Efficiency-of-Corporate -Security-Systems-in-Managing-Information-Threats-An-Overview-of-the-CurrentSituation.pdf (date of access: 25.11.2023).

77. Siponen M., Willison R. Information security management standards: Problems and solutions. *Information & Management*. 2009. Vol. 46, no. 5. P. 267–270. URL: https://doi.org/10.1108/MIP-04-2013-0056 (date of access: 25.11.2023).

78. Swanson M., Guttman B. Generally Accepted Principles and Practices for Securing Information Technology Systems. USA: NIST, 1996. 60 p. URL: https://creangel.com/papers/Principlesand%20Practicesfor%20securing.pdf (date of access: 25.11.2023).

79. Tsimonis G., Dimitriadis S. Brand strategies in social media. *Marketing Intelligence & Planning.* Vol. 32, no. 3. P. 328–344. URL: https://www.sciencedirect.com/science/article/abs/pii/S0378720609000561 (date of access: 25.11.2023).

ДОДАТКИ

ДОДАТОК А

КІЛЬКІСТЬ КОРИСТУВАЧІВ СОЦІАЛЬНИХ МЕРЕЖ, 2022-2023 РІК (%)

Рисунок А.2.1 – Кількість користувачів соціальних мереж, 2022-2023 рік (%) [21]

ДОДАТОК Б

ЩОДЕННЕ ВИКОРИСТАННЯ ІНТЕРНЕТУ (%)

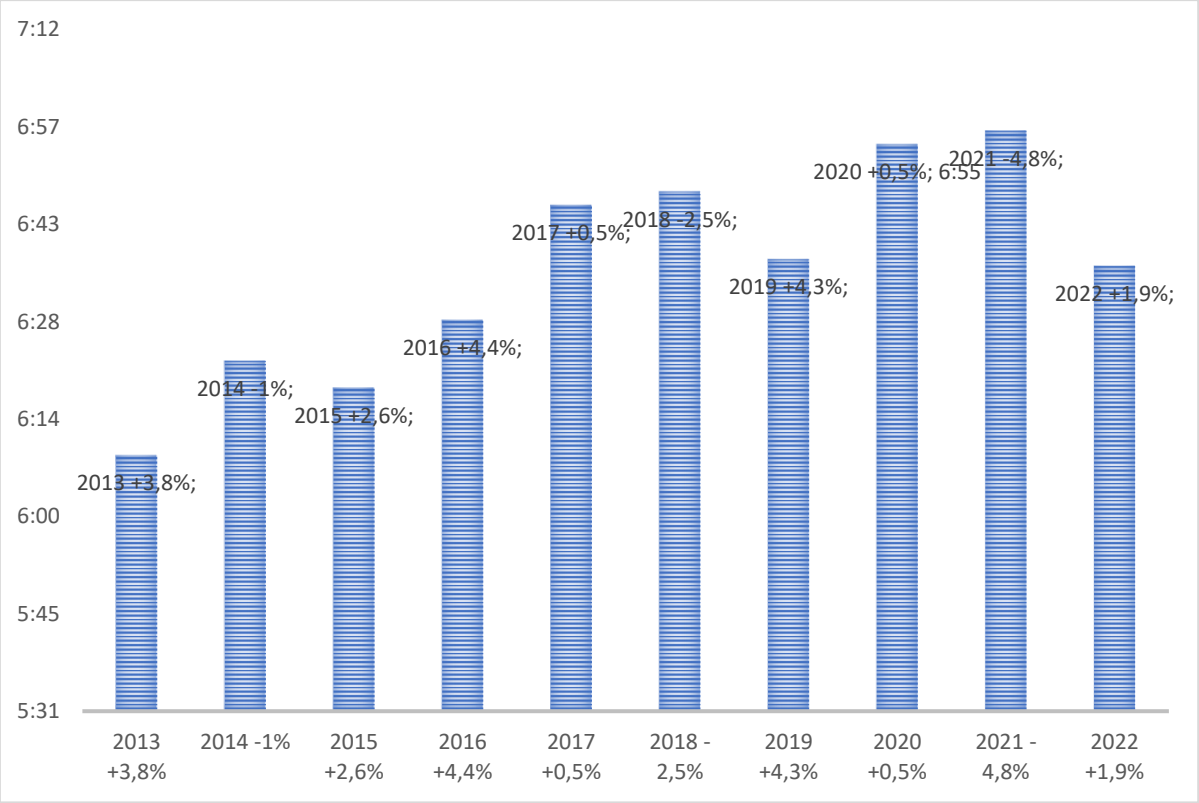

Рисунок Б.2.1 – Щоденне використання інтернету (%) [21]

ДОДАТОК В

ЗАСОБИ МАСОВОЇ ІНФОРМАЦІЇ, ЯКИМИ КОРИСТУЮТЬСЯ УКРАЇНЦІ ДЛЯ ОТРИМАННЯ НОВИН З 2017 Р. ПО 2022 Р. (%)

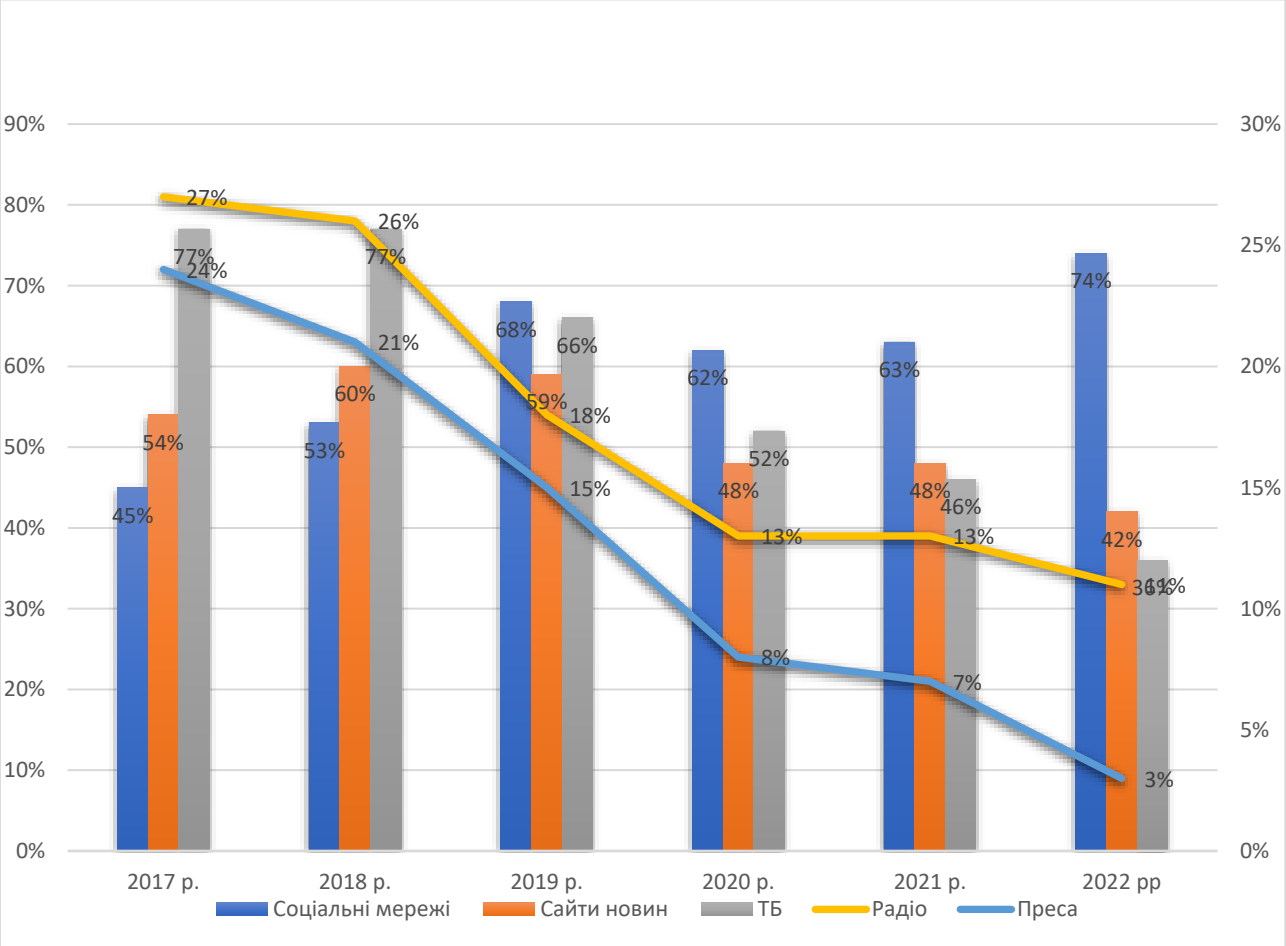

Рисунок В.2.2 – Засоби масової інформації, якими користуються українці для отримання новин з 2017 р. по 2022 р. (%) [25]

ДОДАТОК Г

СТРУКТУРА ІНФОРМАЦІЙНОГО ВІДДІЛУ ТОВ «БАСФ Т.О.В»

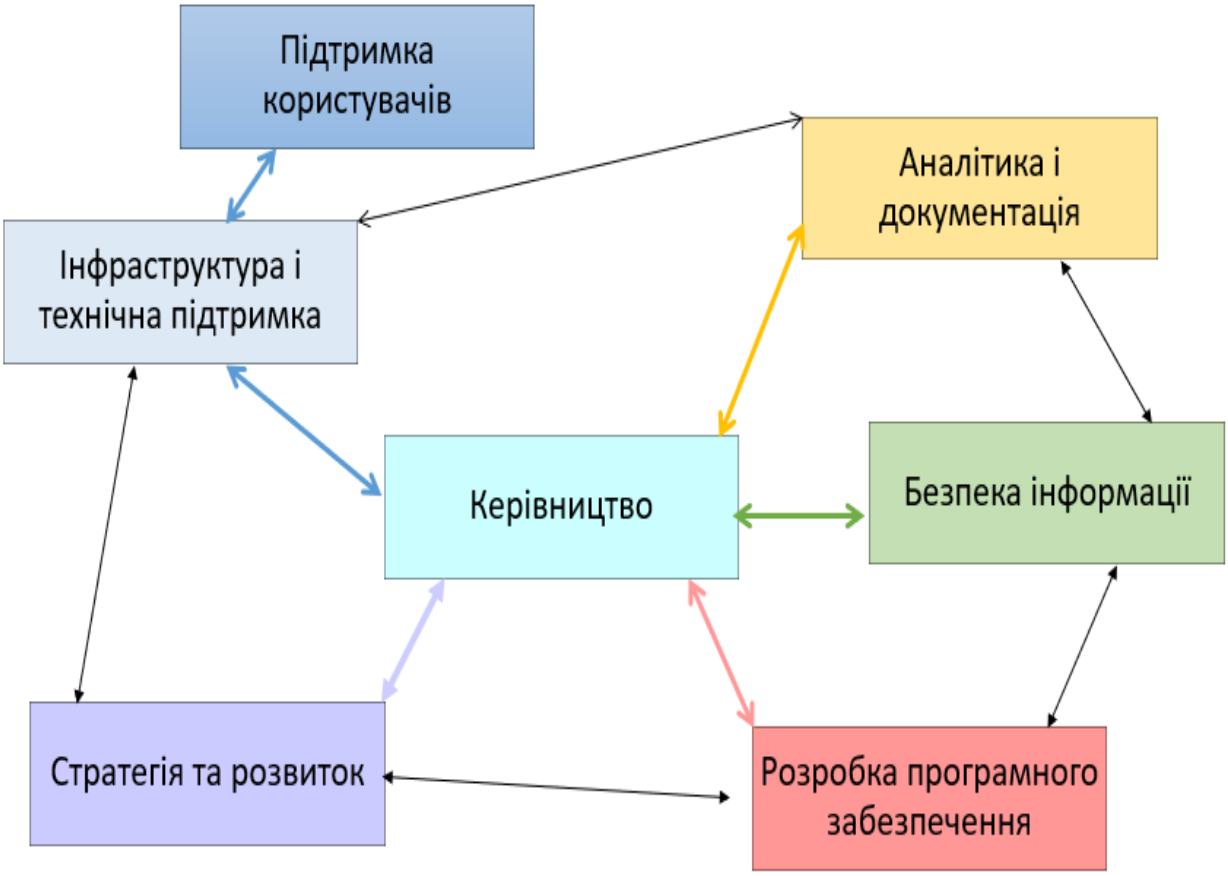

Рисунок Г.3.1. – Структура інформаційного відділу ТОВ «БАСФ Т.О.В»