УДК 659.4.011
UDC 659.4.011
DOI:10.33744/0365-8171-2023-114.2-297-312

ІНФОРМАЦІЙНИЙ ПРОСТІР: ФЕЙКИ ТА ДІПФЕЙКИ. ДИЗІНФОРМАЦІЯ ТА ЇЇ ВПЛИВ НА ДІЯЛЬНІСТЬ ПІДПРИЄМСТВ В СУЧАСНИХ УМОВАХ ВІЙНИ

INFORMATION SPACE: FAKES AND DEEP-FAKES. DISINFORMATION AND ITS IMPACT ON THE ACTIVITIES OF ENTERPRISES IN MODERN WAR CONDITIONS

Компанець Катерина Андріївна, *кандидат економічних наук, доцент, доцент кафедри готельно - ресторанного бізнесу, Державного торговельно економічного університету, м. Київ, Україна, e-mail: ket13@ukr.net,*

https://orcid.org/0000-0002-7189-2355

Городецький Микола Ярославович*, кандидат економічних наук, старший викладач кафедри міжнародного туризму і готельного бізнесу, Західноукраїнського національного університету. Тернопіль, Україна, e-mail: 0672083508@ukr.net,*

https://orcid.org/0000-0003-3312-5945

Гончар Тетяна Миколаївна*, старший викладач кафедри менеджменту, Національний транспортний університет, Київ, Україна, e-mail: tetgonchar@ukr.net,*

https://orcid.org/0000-0002-3724-3490

Анотація. В статті досліджено сучасний стан ведення бізнесу підприємствами в умовах інформаційного простору. Досліджено позитивний та негативний вплив інформації на діяльність підприємств. На сучасному етапі розвитку суспільства і технологій інформаційний простір став складним та динамічним середовищем з численними викликами та можливостями. Сучасний інформаційний простір вимагає уваги до багатьох питань, включаючи безпеку, прозорість, етичність та захист прав та свобод користувачів. Триває пошук ефективних стратегій та рішень для забезпечення стійкої та етичної інформаційної сфери.

В статті дається визначення дезінформації та її види. Визначено самий загрозливий з них, а саме, дипфейк. Для боротьби з цими загрозами важливо вдосконалювати технології виявлення діпфейків, розвивати кіберзахист, підвищувати інформаційну грамотність суспільства та вдосконалювати законодавство, щоб врахувати виклики, які ставлять перед нами ці технології.

Встановлені загрози та ризики кожного з видів дезінформації. Визначені шляхи подолання. Для боротьби з цими загрозами важливо вдосконалювати технології виявлення діпфейків, розвивати кіберзахист, підвищувати інформаційну грамотність суспільства та вдосконалювати законодавство, щоб врахувати виклики, які ставлять перед нами ці технології. Важливо вдосконалювати технології виявлення та блокування ботів, розвивати алгоритми для розпізнавання штучної активності в мережі, а також залучати спільноту та користувачів до підтримки боротьби з автоматизованою маніпуляцією.

Ключові слова: інформація, інформаційний простір, фейки, діпфейки, дезінформація, діяльність підприємств.

Постановка проблеми. В сучасному стані воєнних дій в Україні стає актуальне питання про діз інформацію. Наразі інформативний простір є відіграє важливу роль в в суспільстві в цілому та особливо для діяльності підприємств. Неякісна інформація може стати серйозною проблемою для діяльності підприємств, викликуючи різноманітні негативні наслідки. Неправдива або спотворена інформація може призвести до втрати довіри споживачів, клієнтів та інших зацікавлених сторін. Репутаційні проблеми можуть важко відновити, і вони можуть вплинути на відносини з клієнтами та партнерами. Неточна інформація про фінансові результати, стратегії або інші ключові аспекти бізнесу може призвести до невірного розуміння ринків та втрат інвестицій. Це може вплинути на ціну акцій, призводячи до фінансових втрат для інвесторів. Неправдива інформація може порушити закони та норми, що регулюють бізнес. Підприємство може стати об'єктом судових позовів або штрафів за розповсюдження маніпульованої інформації. Великими проблемами може буте стратегічні помилки, а саме прийняття рішень на основі неточної інформації може привезти до стратегічної помилки. Це може включати невірне визначення цільового ринку, конкурентного середовища чи ефективності певних стратегій.

На разі під час війни достовірність інформації є запорукою виживання та розвитку підприємств. Тому вивчення інформаційного простору є важливим завдання в сучасних умовах.

Аналіз і огляд останніх досліджень. В науковій літературі постійно приділяється увага інформації, як джерела якісного управління підприємством. Крім цього авторами надається наголос на маркетингові комунікації, що є провідником інформації про підприємства, товари, послуги. Можна відзначити роботи в цьому напрямку таких вчених, як: Антонюк І.[6], Демкова М. [4], Железняк К.[2], Медведева А.[6], Сидоренко Т.[1], Тягнирядно Л.[3], Федоряк Р.[1],Фігель М. [4], та інші. В наукових працях висвітлено питанні про роль інформаційного простору, але не розкрити головні загрози. Тому стає за необхідне знати не тільки переваги а і загрози інформації.

Мета дослідження. Дослідження теоретичних та практичних засад впливу інформаційного простору на діяльність підприємств.

Основна частина. Маркетингові заходи із просування туристичних послуг змінюються у відповідності до змін у навколишньому середовищі, новизни та змісту пропозицій підприємств гостинності, зростання запитів, вимог до послуг, зростання чисельності досвідчених туристів. Особливе місце маркетингу в управлінні зумовлено, передусім, маркетинговими дослідженнями, в проведенні яких в умовах інформаційної економіки зацікавлене кожне підприємство, адже в сучасних умовах ефективність роботи прямо залежить від правильних управлінських рішень, які більшою мірою спираються на інформацію, отриману в ході маркетингових досліджень. Тому саме маркетингові дослідження можуть дати можливість підприємству ефективно функціонувати відповідно до вимог ринку та потреб споживачів[1].

Спроможність досягти конкурентної переваги і зберегти її залежить від ефективності маркетингової стратегії підприємства, що зумовлена орієнтацією стратегії на створення виняткової споживацької переваги, чутливістю до умов ринку, спрямованістю на розроблення нових товарів, послуг та визнанням глобального характеру конкуренції [2]. Все це, залежить від якісної, достовірної та вчасної інформації.

Інформація виступає основним об'єктом інформаційного суспільства, і її роль сьогодні важко переоцінити. Відображаючи реальну дійсність, вона інтегрується у всі напрямки діяльності держави, суспільства, громадянина. З появою нових інформаційних технологій, основою яких є впровадження засобів обчислювальної техніки, зв'язку, систем телекомунікації, інформація стає постійним і необхідним атрибутом забезпечення діяльності держави, юридичних осіб, громадських організації та громадян. Від її якості та достовірності, оперативності одержання залежать численні рішення, що приймаються на різних рівнях – від глави держави до громадянина. [4].

Інформація стає реальною, майже фізично відчутною силою.

Поняття "інформація" використовується в усіх галузях науки, і в правовій, зокрема. Воно набуло багатозначності й інтерпретується залежно від сфери вживання[4].

Термін "інформація" може мати кілька різних визначень, залежно від контексту. Ось кілька можливих розумінь та визначень:

1. **Загальне розуміння:** У загальному сенсі "інформація" - це знання або дані, які передаються або отримуються з метою розуміння чого-небудь. Це може включати текст, числа, мультимедійні файли, ідеї тощо.
2. **В інформаційних технологіях:** У сфері IT "інформація" може вказувати на дані, які обробляються та передаються за допомогою комп'ютерних систем. Це може бути текст, аудіо, відео, графіка, тощо.
3. **Філософське розуміння:** З погляду філософії інформація може розглядатися як концепція, пов'язана з розумінням та організацією даних, яка призводить до виникнення знань.
4. **Управління:** В контексті управління "інформація" вказує на дані, які використовуються для прийняття рішень та впливу на операційні процеси в організації.

Визначення та розуміння терміну "інформація" може змінюватися в залежності від контексту, у якому він використовується.

У контексті маркетингових досліджень та аналізу, термін "інформація" має особливе значення. Маркетингові дослідження включають збір, аналіз та інтерпретацію даних з метою розуміння ринкових тенденцій, споживчих поведінок та інших аспектів, які важливі для бізнесу. Інформація в маркетингових дослідженнях може бути поділена на кілька типів:

1. **Демографічна інформація:** Це дані, що стосуються характеристик публіки, таких як вік, стать, освіта, доходи та інші фактори, які допомагають визначити цільову аудиторію продукту чи послуги.
2. **Психографічна інформація:** Описує стилі життя, інтереси, цінності та інші психологічні аспекти споживачів. Це допомагає розуміти, які мотивації впливають на їхні вибори та покупки.
3. **Поведінкова інформація:** Аналізує споживчу поведінку, включаючи звички покупців, їхні уподобання, реакцію на рекламу та інші фактори, що впливають на їхні рішення.
4. **Географічна інформація:** Враховує географічні аспекти, такі як місцезнаходження клієнтів, регіональні відмінності в попиті та інші географічні чинники.

5. **Технічна інформація:** Включає в себе технічні аспекти, такі як використання технологій, прихильність у використанні платформ та інші технічні аспекти, які можуть впливати на споживацький досвід.

Ця інформація допомагає маркетологам та бізнесам розробляти стратегії продажу, підходи до маркетингу та удосконалювати свої продукти чи послуги з урахуванням потреб та очікувань своєї цільової аудиторії. Аналіз маркетингової інформації може також допомагати визначити конкурентні переваги, ідентифікувати можливості для розвитку та зменшення ризиків у сфері бізнесу.

Але на разі інформація нобула іншої форми. За допомогою інформації можливо покращіти імідж компанії, а можливо повністю знищіти з конкурентного ринку. За допомогою інформації можливо зробити лояльних покупців прихильних до себе, а можливо просто отримати зворотній результат. Неякісна, неправдива інформація може стати серйозною проблемою для діяльності підприємства. Визначимо головні ризики підприємств при отримані і використанні дезінформації (табл..1)

Таблиця 1 – Проблеми, ризики та наслідки використання дезінформації підприємствами.

Table 1 – Problems, risks and consequences of the use of disinformation by enterprises.

Ризики	Ознаки
Репутаційні ризики	Неправдива або спотворена інформація може призвести до втрати довіри споживачів, клієнтів та інших зацікавлених сторін. Репутаційні проблеми можуть важко відновити, і вони можуть вплинути на відносини з клієнтами та партнерами.
Фінансові втрати	Неточна інформація про фінансові результати, стратегії або інші ключові аспекти бізнесу може призвести до невірного розуміння ринків та втрат інвестицій. Це може вплинути на ціну акцій, призводячи до фінансових втрат для інвесторів
Правові проблеми	Неправдива інформація може порушити закони та норми, що регулюють бізнес. Підприємство може стати об'єктом судових позовів або штрафів за розповсюдження маніпульованої інформації.
Стратегічні помилки	Прийняття рішень на основі неточної інформації може призвести до стратегічних помилок. Це може включати невірне визначення цільового ринку, конкурентного середовища чи ефективності певних стратегій
Конфлікти в команді	Якщо різні члени команди отримують різну інформацію або розуміють її по-різному, це може призвести до конфліктів внутрішньої комунікації та незгод в прийнятті стратегічних рішень.
Витрати часу на ресурси	Пошук та корекція неточної інформації може вимагати значних зусиль та ресурсів, що призводить до втрат часу та затрат на переорієнтацію.

Джерело: сформовано авторами

Щоб запобігти цим проблемам, підприємства повинні приділяти особливу увагу якості інформації, активно впроваджувати системи контролю та перевірки фактів, а також вдосконалювати процеси управління інформацією та комунікаціями всередині організації. Крім цього наразі інформація під час війни руйнує свідомість і людей (споживачів). Тому треба маркетологам звертати увагу і на те, що завдяки розумному інтелекту заявились і нові види дизінформації.

Дизінформація — це розповсюдження неправдивої або прихованої інформації з метою введення в оману або обману громадськості. Вона може набувати різних форм і виявлятися в різних сферах. Види дезінформації представлено на рис.1.

Розповсюдження дизінформації може мати серйозні наслідки для суспільства, бізнесу та політики, тому розпізнавання та протидія цьому явищу є важливим завданням. Розберемо детально кожен з видів дезінформації. Дані занесемо в таблицю 2.

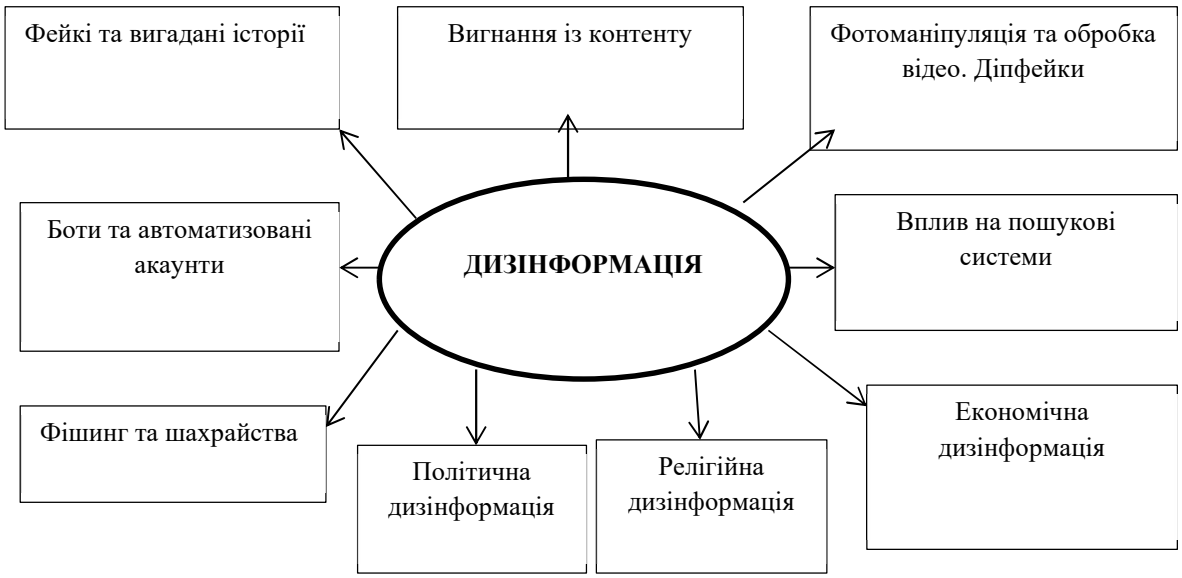

Рисунок 1 – Види дезінформації в сучасному інформаційному просторі.

Figure 1 – Types of disinformation in the modern information space.

Джерело: сформовано авторами

Таблиця 2 – Характеристика видів дезінформації
Table 2 – Characteristics of types of disinformation

Дизін форм	Харак-терис-тика	Загрози та ризики
Фейкі та вигадані історії	Створення неправдивих повідомлень, новин або історій з метою обману читачів. Це може включати як явно вигадані події, так і спотворення реальних подій	1. **Роз'яснення та довіра:** Фейки можуть підривати довіру громадськості до інформації та джерел новин. Це може вплинути на загальний рівень розуміння суспільних явищ та призводити до поширення стереотипів і неправильного розуміння подій. 2. **Репутаційні ризики:** Для осіб, брендів, компаній та організацій розповсюдження фейків може призвести до втрати репутації та довіри. Навіть одна неправдива історія може має глибокі наслідки для образу бренду чи особи. 3. **Ефективність ринків:** Фейки можуть впливати на фінансові ринки, спричинюючи коливання цін акцій або інших фінансових показників. Це може веде до втрат для інвесторів та компаній. 4. **Політичні втручання:** Фейки та дизінформація можуть бути використані для впливу на політичні процеси, вибори та формування громадської думки. Це може викликати нестабільність і підривати демократичні інституції. 5. **Кібербезпека:** Використання фейків може бути частиною кібератак або фішингових кампаній, що призводить до порушення безпеки інформації та приватності. 6. **Витрати на боротьбу з фейками:** Компанії, медіа та організації повинні витрачати значні кошти на боротьбу з фейками, виявлення неправдивої інформації та її виправлення. 7. **Вплив на соціальний мир:** Фейки можуть поглиблювати соціальні розбіжності, створювати конфлікти між групами та підривати соціальний мир. 8. **Втрата особистої інформації:** Шахраї можуть використовувати фейки для отримання особистої інформації від користувачів, що призводить до ризику крадіжки ідентичності та інших кіберзагроз.
Вигнання із контенту	Представлення інформації або цитат без врахування повного контексту, щоб змінити її значення або викликати неправильне .	1. **Неправильне розуміння ситуацій:** Вигнання із контенту може призвести до неправильного розуміння подій чи інформації, що може вплинути на прийняття рішень як на особистому, так і на організаційному рівні. 2. **Маніпуляція громадською думкою:** Подання інформації без повного контексту може бути використано для маніпуляції громадською думкою, формування стереотипів та навіть провокування соціально-політичних конфліктів. 3. **Репутаційні ризики:** Для індивідів, компаній чи організацій, вигнання із контенту може стати причиною втрати репутації, оскільки спотворена інформація може виглядати об'єктивно та правдиво. 4. **Поширення міфів та слуханок:** Вигнання із контексту може сприяти поширенню міфів та слуханок, оскільки нецільова інформація може виглядати переконливо та обманливо. 5. **Економічні наслідки:** Для бізнесу вигнання із контексту може призвести до неправильного розуміння ринкових умов, конкурентного середовища та інших факторів, що може вплинути на прийняття невірних стратегічних рішень. 6. **Поглиблення ділянок та конфліктів:** В умовах соціальної нестабільності вигнання із контексту може сприяти поглибленню конфліктів та розбіжностей між різними групами чи спільнотами.

Фотоманіпуляція та обробка відео. Діпфейки	Зміна чи обробка зображень та відео для створення фейкових сценаріїв, які можуть виглядати як реальні події	1. **Дезінформація та Маніпуляція:** • *Політика та виборчі кампанії:* Фотоманіпуляція та діпфейки можуть використовуватися для створення фальшивих заяв, інтерв'ю чи подій, що може впливати на громадську думку під час виборчих кампаній. • *Репутаційні ризики:* Індивіди та організації можуть стати жертвами фейкових відео, що призводить до втрати репутації та довіри. 2. **Безпека та Кіберзахист:** • *Шахрайства та обман:* Діпфейки можуть бути використані для шахрайства, коли зловмисники створюють фальшиві відео з метою обману користувачів та отримання конфіденційної інформації. • *Кібератаки:* Використання діпфейків може посилити кіберзагрози, оскільки фальшиві відео можуть викликати паніку та призводити до непередбачуваних наслідків. 3. **Порушення Приватності та Етики:** • *Використання особистих даних:* Діпфейки можуть використовувати зібрані в інтернеті відеоматеріали для створення вигаданих сценаріїв, що порушує приватність осіб. 4. **Юридичні Питання:** • *Правова відповідальність:* Виникнення фейкових відео може породжувати питання щодо юридичної відповідальності та наближати до необхідності розробки нових правових рамок. 5. **Суспільний Розкол:** • *Збільшення соціальних розбіжностей:* Використання діпфейків може призвести до загострення соціальних конфліктів та поглиблення розбіжностей у суспільстві.

Боти та втоматизовані акаунти	Використання автоматизованих акаунтів чи ботів для розповсюдження дизінформації та маніпуляції соціальними мережами.	1. **Розповсюдження дизінформації:** • *Соціальні мережі:* Боти можуть використовуватися для автоматизованого розповсюдження фейків та дезінформації, впливаючи на громадську думку та суспільний діалог. • *Політичні втручання:* Боти можуть бути задіяні у політичних кампаніях для створення штучної підтримки або впливу на результати виборів. 2. **Атаки на Інтернет-ресурси:** • *DDoS-атаки:* Автоматизовані акаунти можуть брати участь у розподіленому відмові в обслуговуванні (DDoS) атаках для перевантаження інтернет-ресурсів та призводження до їхнього недоступності. 3. **Шахрайства та Обман:** • *Фішинг:* Боти можуть використовуватися для автоматизованого розсилання фішингових повідомлень, спрямованих на отримання конфіденційної інформації від користувачів. 4. **Маніпуляція Ринками:** • *Фінансові ринки:* Автоматизовані акаунти можуть впливати на фінансові ринки шляхом створення штучного попиту або пропозиції, що може викликати коливання цін. 5. **Порушення Приватності:** • *Збір та обробка особистої інформації:* Боти можуть використовуватися для автоматизованого збору особистої інформації користувачів з метою надалі використовувати цю інформацію для шахрайства або неправомірних цілей. 6. **Спотворення Звітності та Оглядів:** • *Онлайн-рейтинги та відгуки:* Боти можуть бути використані для автоматизованого створення фальшивих відгуків або штучного збільшення рейтингів певних продуктів чи послуг. 7. **Поглиблення Поділів в Суспільстві:** • *Соціальні конфлікти:* Боти можуть використовуватися для розпалювання соціальних розбіжностей та конфліктів через масове розповсюдження провокацій та спірних публікацій

Вплив на пошукові системи	Спроби маніпулювати алгоритми пошукових систем для підняття неправдивих або спотворених результатів пошуку	1.**Чорна оптимізація (Black Hat SEO):** • *Неправомірні методи оптимізації:* Використання неправомірних методів, таких як надмірне використання ключових слів, приховані текстові блоки чи інші методи, які порушують правила пошукових систем. 2.**Маніпуляція Рейтингами:** • *Фейкові відгуки та рейтинги:* Створення фальшивих відгуків, штучного збільшення рейтингів або інших маніпуляцій, щоб вплинути на відображення результатів у пошукових системах. 3.**Фішинг та Мошенництво:** • *Фішингові сайти:* Створення штучних сторінок, що імітують легітимні ресурси, для збору конфіденційної інформації від користувачів. 4.**Контентний Спам:** • *Неправомірне розміщення контенту:* Автоматизоване розміщення великої кількості неправдивого або непотрібного контенту для підвищення рейтингу сторінки. 5.**Загрози Безпеці:** • *Шкідливі програми:* Пошкодження сайтів чи видача підозрілого контенту, який може стати джерелом загроз для безпеки користувачів. 6.**Вплив на Рекламні Кампанії:** • *Фальшиві кліки:* Автоматизовані акаунти, що генерують фальшиві кліки на рекламні блоки, можуть призводити до збитків для рекламодавців. 7.**Зміна Алгоритмів Пошукових Систем:** • *Несправедливі зміни алгоритмів:* Вплив на пошукові системи може здійснювати суб'єктивний вплив на ранжування результатів, що викликає недовіру та негативні наслідки для бізнесів. 8.**Поглиблення Поділів в Мережі:** • *Фільтрація та персоналізація:* Персоналізована видача може створювати "фільтровані бульбашки", які обмежують доступ до різноманітної інформації та поглиблюють поділ в суспільстві. 9.**Ідентифікація та Збір Особистої Інформації:** • *Приватні дані та слідкування:* Збирання та використання особистої інформації користувачів для наступного впливу на їхні видачі. 10. **Збільшення Залежності від Пошукових Систем:** • *Монополія та контроль:* Загроза великим компаніям, що контролюють пошуковий ринок, які можуть визначати стандарти та обмежувати конкуренцію.

Фішинг та шахрайство	Використання обманливих методів для витягування особистої чи конфіденційної інформації від осіб	1. **Крадіжка Особистої Інформації:** • *Логіни та паролі:* Атаки фішингу можуть спрямовуватися на отримання логінів та паролів, що може призвести до незаконного доступу до особистих акаунтів. 2. **Фінансові Втрати:** • *Шахрайства з банківськими реквізитами:* Фішингові атаки можуть включати в себе піддавання користувачів впливовим шахраям, що призводить до втрат грош 3. **Компрометація Корпоративної Безпеки:** • *Атаки на підприємства:* Фішинг може бути спрямованим на співробітників підприємства з метою здійснення атаки на корпоративну інфраструктуру, крадіжки конфіденційної інформації чи розповсюдження шкідливих програм. 4. **Використання для Ідентифікаційного Обману:** • *Соціальний Інжиніринг:* Шахраї можуть використовувати фішинг для отримання особистих даних та використання їх для соціального інжинірингу, щоб введені в оману особи робили непередбачувані дії. 5. **Загроза Інформаційній Безпеці:** • *Шкідливі програми:* Фішинг може бути використаним для поширення шкідливих програм, таких як віруси, троянці, різновиди рансомвару, що може завдати серйозного шкоди системам та даним. 6. **Втрата Репутації:** • *Фальшиві Сайти та Імітації Брендів:* Фішинг може включати в себе створення фальшивих веб-сайтів, які імітують офіційні ресурси популярних брендів, що може призвести до втрат репутації та довіри користувачів. 7. **Поширення Масової Дезінформації:** • *Фейкові Соціальні Мережі:* Фішинг може бути використаним для створення фейкових профілів та поширення дезінформації через соціальні мережі. 8. **Напади на Користувачів:** • *Фішингові Атаки на Користувачів:* Загроза для звичайних користувачів через спроби виведення їх в оману та використання особистої інформації в шахрайських цілях.

Політична дизінформації	Використання маніпуляцій та неправдивих заяв для впливу на громадську думку та політичні процеси	1. **Маніпуляція Громадською Думкою:** • *Фальшиві новини та інформація:* Розповсюдження фальшивих новин та спотвореної інформації для впливу на громадську думку та створення штучних переконань. 2. **Втручання в Вибори:** • *Спроби маніпулювання результатами:* Використання дезінформації для впливу на виборчий процес, створення або посилення політичних конфліктів. 3. **Збурення Суспільної Стабільності:** • *Поширення провокацій та конфліктів:* Використання дезінформації для створення або поглиблення соціальних та політичних конфліктів, що може призвести до нестабільності в суспільстві. 4. **Атаки на Інститути Демократії:** • *Підрив демократичних процесів:* Використання дезінформації для підриву демократичних процесів, навіть через спроби дискредитації виборів або інших ключових інститутів. 5. **Загрози Національній Безпеці:** • *Поширення неправдивих звітів про кризи:* Використання дезінформації для створення неправдивого образу кризи або екстрених ситуацій, що може впливати на рішення влади та реакцію громадськості. 6. **Вплив на Зовнішні Стосунки:** • *Порушення міжнародних відносин:* Використання дезінформації для впливу на сприйняття та ставлення до інших країн або міжнародних питань. 7. **Втрата Довіри до ЗМІ та Інформаційних Джерел:** • *Скептицизм щодо ЗМІ:* Постійне використання дезінформації може призводити до загального скептицизму щодо ЗМІ та інших інформаційних джерел. 8. **Використання Технологій Штучного Інтелекту:** • *Діпфейки та глибокий фейк:* Використання технологій, які створюють вигляд автентичних відео чи аудіозаписів з фіктивним вмістом. 9. **Загрози Захищеним Меншинам:** • *Дискримінація та ворожість:* Використання дезінформації для створення атмосфери дискримінації та ворожість до захищених меншин.

Релігійна дизінформація	Розповсюдження неправдивих чи спотворених інформаційних повідомлень, які стосуються релігійних питань чи вірувань.	1. **Втручання у Релігійні Вірування:** • *Спотворення священних текстів:* Можливість спотворення та викривлення текстів священних писань для підтримки певних агенд або ідеологій. 2. **Створення Конфліктів та Розбратів:** • *Поширення релігійної нетерпимості:* Дезінформація може бути використана для посилення релігійної нетерпимості, створення конфліктів між різними віросповіданнями та групами. 3. **Порушення Релігійної Гармонії:** • *Створення напруженості між вірниками:* Релігійна дезінформація може провокувати напруженість та недовіру між прихильниками різних релігій. 4. **Вплив на Релігійні Лідери та Організації:** • *Дискредитація релігійних лідерів:* Спроби дискредитації релігійних лідерів або організацій через розповсюдження неправдивих чи перекручених інформаційних матеріалів. 5. **Поширення Спрощених Стереотипів:** • *Створення стереотипів та передвищення:* Використання дезінформації для створення неправдивих стереотипів та передвищень стосовно певних релігійних груп. 6. **Маніпуляція Вірників:** • *Спроби впливу на релігійні погляди:* Використання дезінформації для маніпуляції вірниками та зміни їхніх релігійних переконань. 7. **Вплив на Релігійні Практики:** • *Спотворення релігійних обрядів та практик:* Можливість створення фальшивих або спотворених релігійних обрядів та практик для зміни сприйняття вірників. 8. **Використання Технологій для Дезінформації:** • *Використання соціальних мереж:* Розповсюдження дезінформації через соціальні мережі та інші технологічні засоби для швидкого та широкого впливу.

Економічна дизінформація	Широкомасштабна розповсюдження фейкових або прихованих економічних даних для впливу на фінансові ринки або інвестиційні рішення	1. **Маніпуляція Фінансовими Ринками:** • *Розповсюдження неправдивих фінансових новин:* Використання дезінформації для спотворення оцінок ринкової ситуації, що може призвести до необгрунтованих коливань на фінансових ринках. 2. **Псевдоекономічні Атаки:** • *Створення неправдивих економічних звітів:* Розповсюдження фальшивих економічних звітів та статистики, що може вплинути на рішення інвесторів та фінансових аналітиків. 3. **Дискредитація Фінансових Інститутів:** • *Спроби дискредитації банків та фінансових установ:* Використання дезінформації для порушення довіри до банків, фінансових установ та регуляторів. 4. **Підрив Довіри до Бізнесу:** • *Фальшиві новини про підприємства:* Розповсюдження неправдивих інформаційних матеріалів щодо фінансового стану, стратегій та планів підприємств. 5. **Втручання в Торговельні Відносини:** • *Створення штучних торговельних конфліктів:* Використання дезінформації для спровокування торговельних конфліктів та порушення економічної співпраці. 6. **Руйнування Репутації Брендів:** • *Фейкові новини про продукцію та послуги:* Спроби підірвати довіру до брендів через розповсюдження дезінформації про їхню продукцію, послуги або практики. 7. **Маніпуляція Вартості Валют:** • *Розповсюдження неправдивої інформації про валютні курси:* Використання дезінформації для впливу на валютні курси та обмінні курси. 8. **Вплив на Регуляторну Політику:** • *Ложні інформаційні кампанії для впливу на регуляторні рішення:* Використання дезінформації для впливу на регуляторні органи та прийняття політичних рішень у галузі економіки. 9. **Загрози Інвестиційній Клімату:** • *Порушення інвестиційного клімату:* Використання дезінформації для створення негативного образу країни або регіону, що може вплинути на інвестиційний клімат. 10. **Використання Технологій Штучного Інтелекту:** • *Генерація фейкових аналітичних звітів:* Використання технологій штучного інтелекту для створення вигляду автентичних, але фейкових аналітичних документів.

Джерело: сформовано авторами

Одним із важливих, ба навіть ключових, елементів повномасштабної війни росії в Україні є інформаційний фронт. Країна-терорист роками вкладала мільйони в те, щоби пропагандистська армія спотворювала інформацію й поширювала російські наративи, які викривлюють реальність. Так народилися наративи про "недодержаву", "утиски російськомовного населення", "укрофашистів". Крім того, потужною зброєю окупантів стало щоденне масштабування сотень тисяч фейків про Україну та українців[3]. Аби сіяти сумніви, росія з початку повномасштабного вторгнення, за даними "Детектор медіа", "*збільшила витрати держбюджету на державні телеканали, агенції та видання. Суми підскочили в 3,2 рази в порівнянні з аналогічним періодом минулого року. В абсолютних цифрах за три місяці 2022 року це еквівалент 217 мільйонів євро"*[3].

Саме під час війни най популярною інформаційною атакою стали діпфейки, саме вони створили паніку українців. В перші дні війни в соц. Мережах було викладено відео ролік діпфейк виступи президента України Володимира Зеленського. В якому було висловлена про інформація о сдачі Києва і про капітуляцію України. Для перегляду надаємо посилання https://bit.ly/3i9XgPd). Саме від діпфейків страждають репутації відомих та публічних людей, великих підприємств та невідь країн в цілому. Приклади таких діпфейків викладено на платформі ДІЯ.

У сучасній мережі інтернету існує велика кількість таких підроблених відео, зокрема на відеостримінговій платформі YouTube. Одним із найвідоміших діпфейків сучасної історії став ролик із виступом Барака Обами, випущений у 2018 році.

- https://www.youtube.com/watch?v=cQ54GDm1eL0

Виглядає справді досить реально, щоб повірити. Автором цього діпфейку став американский режисер Джордан Піл. У кінці ролику він демонструє, як сам записує це відео, а далі за допомогою програми накладає зображення президента. Глядач бачe кінцевий результат, де начебто Барака Обама невтішно відгукується про Дональда Трампа.

Популярним персонажем для створення діпфейків став Том Круз. Цей невимушений жарт досяг неймовірних масштабів. У соціальній мережі TikTok був створений обліковий запис @deeptomcruise, присвячений відеофейкам за участю відомого актора.

- https://www.youtube.com/watch?v=iyiOVUbsPcM

Ще один реалістичний ролик за участю Моргана Фрімена. На відео автор Бет Шувінк (Boet Schouwink) розповідає про глибоку фейкову сенгулярність голосом американського актора. Справді можна повірити.

- https://www.youtube.com/watch?v=oxXpB9pSETo [4]

Тобто, Діпфейк (дизінформація або маніпуляція інформацією з метою створення фейкового враження) може мати значний вплив на діяльність підприємств у сучасних умовах. Ось деякі аспекти, які слід враховувати:

1. **Репутаційні ризики:** Діпфейк може призвести до поширення неправдивої інформації про підприємство, що впливає на його репутацію. Це може призвести до втрати довіри споживачів, клієнтів та інших зацікавлених сторін.
2. **Фінансові наслідки:** Якщо діпфейк впливає на ринкову ціну акцій або інших фінансових показників підприємства, це може мати серйозні фінансові наслідки. Інвестори можуть реагувати на маніпульовану інформацію, що призводить до коливань на ринку.
3. **Конкурентність:** Діпфейк може використовуватися для збентеження конкурентів або спотворення ринкових умов. Це може призвести до некоректної конкуренції та втручання в ринковий порядок.
4. **Законодавчі наслідки:** Розповсюдження діпфейку може призвести до законодавчих заходів і реакцій влади. Підприємства можуть стикатися з правовими наслідками, якщо їхній бізнес або репутація стає об'єктом масштабної дезінформації.
5. **Захист інформації:** Підприємства повинні бути готові до виявлення та протидії діпфейку. Захист інформації та вживання заходів щодо виявлення та відповіді на маніпуляції є важливим елементом управління ризиками.
6. **Соціальні мережі та медіа:** Оскільки соціальні мережі та медіа є основними каналами поширення діпфейку, підприємства повинні активно взаємодіяти з цими платформами для виявлення та виправлення фейкової інформації.

Для боротьби з цими загрозами важливо вдосконалювати технології виявлення діпфейків, розвивати кіберзахист, підвищувати інформаційну грамотність суспільства та вдосконалювати

законодавство, щоб врахувати виклики, які ставлять перед нами ці технології. Усі ці аспекти підкреслюють важливість для підприємств у сучасних умовах бути готовими до виявлення та відповіді на діпфейк, а також активно взаємодіяти з різними зацікавленими сторонами для збереження репутації та довіри.

Висновки. Інформаційний простір веде не тільки до переваг ведення бізнесу, але і велику загрозу в створені негативного іміджу підприємства. Для боротьби з цими загрозами важливо вдосконалювати технології виявлення діпфейків, розвивати кіберзахист, підвищувати інформаційну грамотність суспільства та вдосконалювати законодавство, щоб врахувати виклики, які ставлять перед нами ці технології. Важливо використовувати критичне мислення при сприйнятті інформації, перевіряти джерела та забезпечувати повний контекст при поданні інформації. Навчання громадськості та підвищення інформаційної грамотності також можуть сприяти зменшенню впливу вигнання із контексту. Підтримувати високі стандарти журналістики, впроваджувати технологічні засоби виявлення дизінформації та активно залучати спільноту до боротьби з цим явищем.

Перелік посилань

1. Компанець К.А., Федоряк Р.М., Сидоренко Т.М.. Формування та практичне застосування маркетингових досліджень в діяльності підприємств готельно-ресторанного бізнесу. V Міжнародна науково-практична конференція «Сучасні тенденції розвитку фінансових та інноваційно-інвестиційних процесів в Україні» Вінницький національний технічний університет, м. Вінниця 25 лютого 2022 року [Електронний ресурс]. – Режим доступу: https://conferences.vntu.edu.ua/index.php/fiip/fiip2022/schedConf/presentations

2. Железняк К.Л., Компанець К.А. Маркетингові дослідження – інструмент стратегічного управління конкурентоспроможністю підприємства. Причорноморські економічні студії. 2019.Випуску 46. С. 83-87. [Електронний ресурс]. – Режим доступу: DOI:https://doi.org/10.32843/bses.46-14

3. Тягнирядно Л. Дезінформація, пропаганда і все, що між ними: як розпізнати і захиститися. Інформаційний журнал Директ Медія. [Електронний ресурс]. – Режим доступу: https://detector.media/withoutsection/article/201754/2022-08-10-dezinformatsiya-propaganda-i-vse-shcho-mizh-nymy-yak-rozpiznaty-i-zakhystytysya/

4. Демкова М., Фігель М. Інформація, як основа інформаційного суспільства: поняття та правове регулювання. [Електронний ресурс]. – Режим доступу: https://dl.nure.ua/pluginfile.php/468/mod_resource/content/3/content/content2.html

5. Інформаційний портал ДІЯ [Електронний ресурс]. – Режим доступу: https://osvita.diia.gov.ua/news/what-is-a-deepfeak

6. Антонюк І.Ю., Медведева А.О., Компанець К.А. Прийоми маркетингу в організації ресторанного бізнесу України під час війни. «Наука і техніка сьогодні» Випуск № 5(5) 2022. С. 78-87 [Електронний ресурс]. – Режим доступу: DOI:https://doi.org/10.52058/2786-6025-2022-5(5)-78-866

INFORMATION SPACE: FAKES AND DEEP-FAKES. DISINFORMATION AND ITS IMPACT ON THE ACTIVITIES OF ENTERPRISES IN MODERN WAR CONDITIONS

Kateryna Kompanets, Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Hotel and Restaurant Business, State University of Trade and Economics, Kyiv, Ukraine, e-mail: ket13@ukr.net, *https://orcid.org/0000-0002-7189-2355*

Mykola Horodetskyi, candidate of economic sciences, senior lecturer at the Department of International Tourism and Hotel Business, West Ukrainian National University. Ternopil, Ukraine, 0672083508@ukr.net, https://orcid.org/0000-0003-3312-5945

Tetyana Gonchar, senior lecturer at the Department of Management, National Transport University, Kyiv, Ukraine, tetgonchar@ukr.net, https://orcid.org/0000-0002-3724-3490

Abstract. The article examines the current state of business conduct by enterprises in the information space. The positive and negative impact of information on the activities of enterprises was studied. At the current stage of development of society and technology, the information space has become a complex and dynamic environment with numerous challenges and opportunities. The modern information space requires attention to many issues, including security, transparency, ethics, and protection of users' rights and freedoms. The search for effective strategies and solutions to ensure a sustainable and ethical information sphere continues.

The article defines disinformation and its types. The most threatening of them, namely, deepfake, has been determined. To combat these threats, it is important to improve deepfake detection technologies, develop cyber defenses, increase public information literacy, and improve legislation to take into account the challenges these technologies pose to us.

Threats and risks of each type of disinformation are established. Definite ways to overcome. To combat these threats, it is important to improve deepfake detection technologies, develop cyber defenses, increase public information literacy, and improve legislation to take into account the challenges these technologies pose to us. It is important to improve technologies for detecting and blocking bots, develop algorithms for recognizing artificial activity on the network, and involve the community and users in supporting the fight against automated manipulation.

Keywords: information, information space, fakes, deepfakes, disinformation, enterprise activity.

References

1. Kompanets K.A., Fedoryak R.M., Sydorenko T.M.. Formation and practical application of marketing research in the activities of hotel and restaurant business enterprises. V International scientific and practical conference "Modern trends in the development of financial and innovation-investment processes in Ukraine" Vinnytsia National Technical University, Vinnytsia February 25, 2022 [Electronic resource]. – Access mode: https://conferences.vntu.edu.ua/index.php/fiip/fiip2022/schedConf/presentations

2. Zheleznyak K.L., Kompanets K.A. Marketing research is a tool for strategic management of the company's competitiveness. Black Sea Economic Studies. 2019. Issue 46. P. 83-87. [Electronic resource]. – Mode of access: DOI:https://doi.org/10.32843/bses.46-14

3. Tyagniryadno L. Disinformation, propaganda and everything in between: how to recognize and protect yourself. Information magazine Direct Media. [Electronic resource]. – Access mode: https://detector.media/withoutsection/article/201754/2022-08-10-dezinformatsiya-propaganda-i-vse-shcho-mizh-nymy-yak-rozpiznaty-i-zakhystytysya/

4. Demkova M., Figel M. Information as the basis of the information society: concept and legal regulation. [Electronic resource]. – Access mode: https://dl.nure.ua/pluginfile.php/468/mod_resource/content/3/content/content2.html

5. Information portal DIYA [Electronic resource]. – Access mode: https://osvita.diia.gov.ua/news/what-is-a-deepfeak

6. Antonyuk I.Yu., Medvedeva A.O., Kompanets K.A. Marketing techniques in the organization of the restaurant business of Ukraine during the war. "Science and Technology Today" Issue No. 5(5) 2022. P. 78-87 [Electronic resource]. – Mode of access: DOI:https://doi.org/10.52058/2786-6025-2022-5(5)-78-86