МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій,
обліку та фінансів

Кафедра комп'ютерних технологій
і моделювання систем

Кваліфікаційна робота
на правах рукопису

ОЛЕНЮК ДМИТРО ОЛЕКСАНДРОВИЧ

УДК 004.738.5

КВАЛІФІКАЦІЙНА РОБОТА

МОДЕЛЬ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ СИНТЕЗУ ІНФОРМАЦІЙНО-СТІЙКИХ ВІРТУАЛЬНИХ СПІЛЬНОТ У СОЦІАЛЬНИХ МЕРЕЖАХ

Спеціальність – 125 «Кібербезпека»

Галузь знань – 12 «Інформаційні технології»

Подається на здобуття другого (магістерського) рівня вищої освіти

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

_____ Дмитро ОЛЕНЮК

Керівник роботи:
Молодецька Катерина Валеріївна,
доктор технічних наук, професор

Житомир – 2023

АНОТАЦІЯ

Оленюк Д. О. Модель підтримки прийняття рішень для синтезу інформаційно-стійких віртуальних спільнот у соціальних мережах. – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття другого (магістерського) рівня вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології». – Поліський національний університет, Житомир, 2023.

У першому розділі визначено загальні відомості про віртуальні спільноти у соціальних мережах; розкрито особливості інформаційно-стійких віртуальних спільнот, а також окреслено сучасні загрози і порушників інформаційної безпеки та основні захисні механізми у соціальних мережах. Другий розділ присвячено дослідженню інформаційних ситуацій, в яких здійснюється прийняття рішень та розробленню моделі для підтримки їх прийняття адміністраторами з метою синтезу інформаційно-стійких віртуальних спільнот у соціальних мережах. У третьому розділі наведено розрахунки й експериментальні дані, що підтверджують правильність запропонованих рішень та здійснено їх порівняльний аналіз з відомими. У роботі набула подальшого розвитку модель прийняття рішень для синтезу інформаційно-стійких віртуальних спільнот у соціальних мережах, що відрізняється від відомих врахуванням стану інформаційного простору сервісів, що дозволило підвищити ефективність процесу формування спільнот, стійких до деструктивного інформаційного впливу в антагоністичних умовах взаємодії. Розроблена модель на практиці забезпечує дієвим інструментарієм прийняття рішень адміністраторів віртуальних спільнот соціальних мереж в умовах антагоністичної поведінки інформаційного середовища, який дозволяє зробити внесок у підвищення рівня інформаційної безпеки акторів у соціальних мережах.

Ключові слова: віртуальна спільнота, інформаційна безпека, соціальні мережі, сталий розвиток, стійкість.

SUMMARY

Oleniuk D. O. Decision Support Model for Synthesizing Information-Resilient Virtual Communities in Social Networks. – Qualification work on the manuscript rights.

Qualification work for the acquisition of the second (master's) level of higher education in the specialty 125 «Cybersecurity» in the field of knowledge 12 «Information Technologies». – Polissia National University, Zhytomyr, 2023.

The first chapter provides general information about virtual communities in social networks, elucidating the characteristics of information-resilient virtual communities, and outlining contemporary threats and violators of information security, along with fundamental protective mechanisms in social networks. The second chapter focuses on researching decision-making in information situations and developing a model to support administrators in synthesizing information-resilient virtual communities in social networks. The third chapter presents calculations and experimental data validating the proposed solutions, accompanied by a comparative analysis with established methods. The study advances the decision support model for synthesizing information-resilient virtual communities in social networks. It distinguishes itself by incorporating the state of the information space of services, enhancing the efficiency of community formation resistant to destructive informational influences in antagonistic interaction conditions. In practice, the developed model provides an effective decision-making tool for administrators of virtual communities in social networks facing antagonistic behaviors in the information environment, contributing to the enhancement of information security for actors in social networks.

Keywords: virtual community, information security, social networks, sustainable development of virtual communities, resilience.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Розвиток соціальних мереж в останні десятиліття призвів до збільшення кількості віртуальних спільнот, які стали поширеним інструментом для спілкування, обміну інформацією та співпраці. Через появу нових форм інформаційних загроз та зміну стратегій атак виникає необхідність для прийняття ефективних рішень адміністраторами віртуальних спільнот, які забезпечать сталий розвиток такого об’єднання і всебічний захист прав та інтересів його учасників. Специфіка віртуальних спільнот у соціальних мережах вимагає унікальних підходів до забезпечення інформаційної стійкості, враховуючи психологічні та соціальні аспекти взаємодії користувачів. Розробка моделі підтримки прийняття рішень адміністраторами віртуальних спільнот відповідно до сучасних вимог та тенденцій у сфері інформаційної безпеки сприятиме підвищенню відповідальності та ефективності дій при управлінні віртуальними спільнотами.

Метою кваліфікаційної роботи є підвищення інформаційної стійкості віртуальних спільнот у соціальних мережах за рахунок запропонованої моделі підтримки прийняття рішень.

Для досягнення поставленої мети, необхідно виконати наступні **завдання**:

- охарактеризувати загальні відомості про віртуальні спільноти у соціальних мережах;
- розкрити особливості інформаційно-стійких віртуальних спільнот;
- окреслити сучасні загрози та основні захисні механізми у соціальних мережах;
- дослідити інформаційні ситуації, в яких здійснюється прийняття рішень адміністраторами віртуальних спільнот у соціальних мережах;
- розробити модель прийняття рішень адміністраторами віртуальної спільноти у соціальних мережах;
- розробити методи порівняльної оцінки запропонованих рішень;
- здійснити порівняльний аналіз запропонованого рішення з відомими.

Об'єктом дослідження є процес підтримки прийняття рішень для синтезу інформаційно-стійких віртуальних спільнот у соціальних мережах.

Предметом дослідження є синтез інформаційно-стійких віртуальних спільнот у соціальних мережах.

Під час написання кваліфікаційної роботи було використано такі **методи дослідження**, як *аналіз* для визначення існуючих підходів до забезпечення безпеки віртуальних спільнот у соціальних мережах;, *синтез* для визначення основних компонент запропонованої моделі та рішень, які можуть приймати адміністратори віртуальних спільнот; *моделювання* для розробки моделі прийняття рішень з метою синтезу інформаційно-стійких віртуальних спільнот; *класифікації і топології* для визначення загроз і порушників інформаційної безпеки віртуальної спільноти; *експертних оцінок* для побудови матриці ризиків, а також *метод експерименту* для отримання кількісних характеристик запропонованої моделі та рішень, які можуть прийматись адміністраторами віртуальної спільноти у соціальних мережах.

Перелік публікацій автора за темою дослідження:

- Євсеєв С. П., Тимонін Ю. О., Веретюк С. М., Войтко Т. М., **Оленюк Д. О.** Синтез моделі соціальних санкцій для забезпечення стійкості віртуальних спільнот у соціальних мережах в умовах антагоністичного середовища. *Захист інформації*. 2023. Т. 25. № 3. С. 139-147. DOI: 10.18372/2410-7840.25.17939.

Наукова новизна та практичне значення отриманих результатів. Набула подальшого розвитку модель прийняття рішень для синтезу інформаційно-стійких віртуальних спільнот у соціальних мережах, що відрізняється від відомих врахуванням стану інформаційного простору сервісів, що дозволило підвищити ефективність процесу формування спільнот, стійких до деструктивного інформаційного впливу в антагоністичних умовах взаємодії.

Розроблена модель на практиці забезпечує дієвим інструментарієм прийняття рішень адміністраторів віртуальних спільнот соціальних мереж в умовах антагоністичної поведінки інформаційного середовища, який дозволяє зробити внесок у підвищення рівня інформаційної безпеки акторів у соціальних мережах.

Структура та обсяг роботи. Кваліфікаційна робота складається з анотації, вступу, трьох розділів, висновків та списку використаних джерел. Загальний обсяг кваліфікаційної роботи становить 26 сторінок та містить 3 таблиці і 5 рисунків.

РОЗДІЛ 1. АНАЛІЗ ІСНУЮЧИХ ПІДХОДІВ ДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВІРТУАЛЬНИХ СПІЛЬНОТ У СОЦІАЛЬНИХ МЕРЕЖАХ

1.1. Загальні відомості про віртуальні спільноти

«Віртуальні спільноти виникли внаслідок розвитку Інтернету та соціальних мереж і забезпечують можливість спілкування і взаємодії між людьми. Вони стали популярними майданчиками для обміну інформацією, дискусій, співпраці та розваг. Процеси комунікації акторів у віртуальних спільнотах мають свої особливості, які відрізняють їх від комунікації в реальному житті» [4, с. 140]. Розглянемо деякі з них на рис. 1.1.

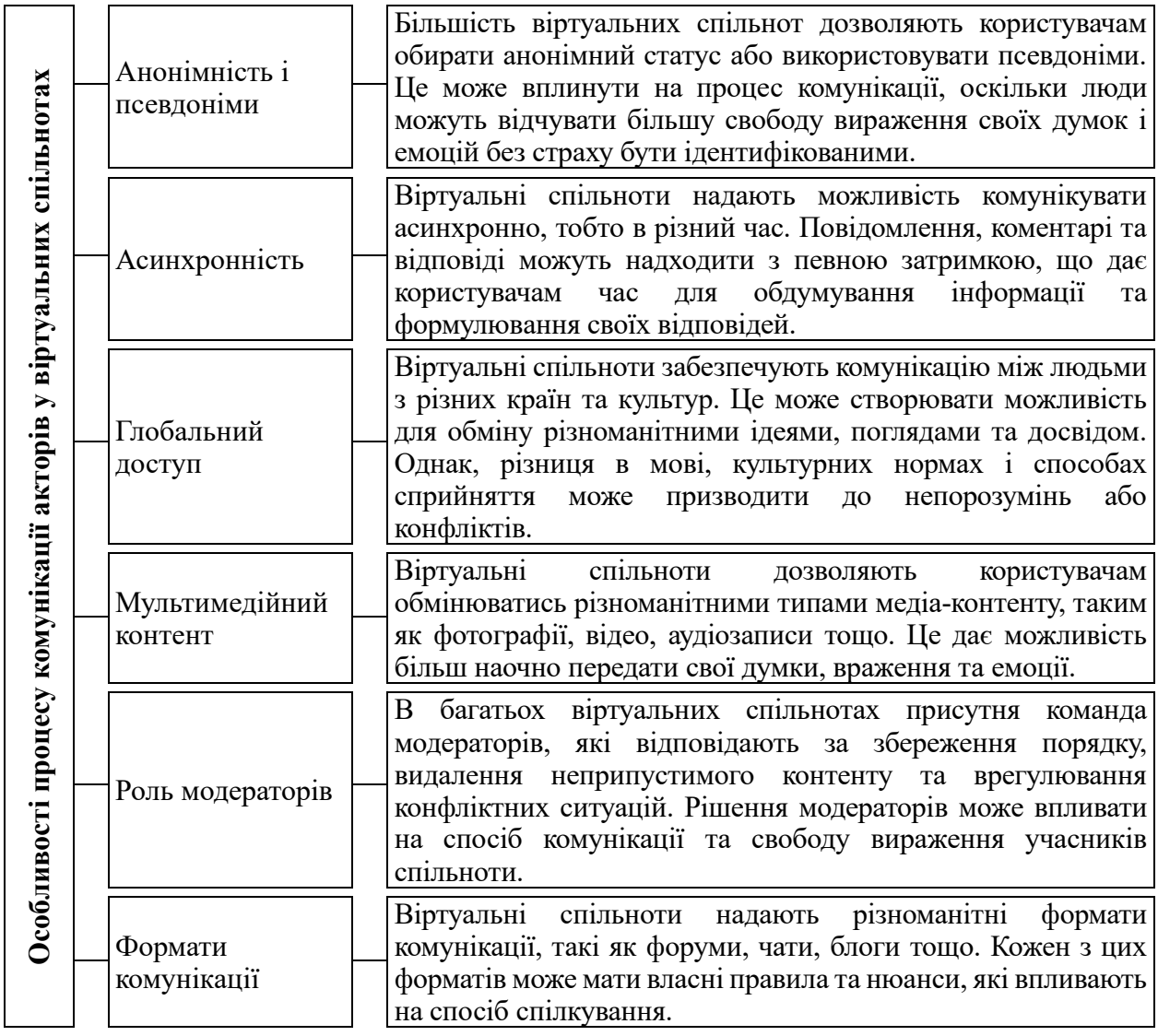

Рисунок 1.1 – Особливості процесу комунікації у віртуальних спільнотах

Джерело: Побудовано автором на основі [4, с. 140].

Загалом, віртуальні спільноти надають багато можливостей для взаємодії та обміну інформацією у процесі комунікації між акторами. Однак, їх особливості також можуть вносити виклики, пов'язані з анонімністю, масштабом та різноманітністю учасників, а також виникненням конфліктів.

1.2. Особливості інформаційно-стійких віртуальних спільнот

Згідно зі Стратегією інформаційної безпеки, затвердженої Указом Президента України № 685/2021 від 28 грудня 2021 року, «основними напрямами забезпечення інформаційної безпеки України є стійкість та взаємодія» [8].

Під інформаційною стійкістю віртуальної спільноти у соціальних мережах слід розуміти її здатність чинити опір загрозам інформаційної безпеки та відновлюватись після їх впливу, а також адаптуватись до змін в інформаційному просторі й реалізовувати власні цілі та функції. Інформаційна стійкість відрізняється від інформаційної безпеки тим, що враховує вимоги сталого розвитку в середовищі соціальної мережі. Для досягнення інформаційної стійкості віртуальна спільнота має забезпечити своєчасну готовність до реакції, реалізації механізмів захисту та подальшого відновлення від завданої шкоди стану інформаційної безпеки віртуальної спільноти у соціальних мережах.

Головною відмінністю стійкої віртуальної спільноти від інших є штучно-керований процес її виникнення, за якого інформаційний вплив на акторів даної спільноти утворює синергетичний ефект, через що відбувається самоорганізація користувачів і утворюються нові віртуальні угрупування, а зв’язки між окремими користувачами вирізняються високим рівнем сталості. Другою, не менш важливою ознакою стійкої віртуальної спільноти є те, що активність її учасників зумовлює сталий розвиток такого об’єднання користувачів соціальної мережі.

Отже, формування інформаційної стійкості віртуальної спільноти – це складний та динамічний процес, який відображає здатність протистояння інформаційним атакам і вимагає постійної готовності до реакції, ефективного захисту та постійного розвитку з боку віртуальних спільнот.

1.3. Аналіз сучасних загроз та механізмів безпеки у соціальних мережах

Спираючись на підходи, описані у роботі Молодецької К. В. [5, с. 80], доцільно використовувати фасетну систему класифікації, яка відзначається високою гнучкістю та дозволяє додавати необмежену кількість фасетів і здійснювати поділ загроз на категорії відповідно до різних критеріїв. На основі цього підходу були визначені основні класифікаційні ознаки загроз інформаційній безпеці віртуальної спільноти (табл. 1.1).

Таблиця 1.1 – Класифікація загроз інформаційної безпеки віртуальної спільноти у соціальних мережах

№ з/п	Критерій	Позначення	Види загроз
1	2	3	4
1.	По відношенню до акторів соціальної мережі	$Relatinon = \bigcup_{j} R_j$, $j = \overline{1,2}$	- внутрішні загрози R_1; - зовнішні загрози R_2;
2.	За видами суб'єктів загроз	$Subject = \bigcup_{l} S_l$, $l = \overline{1,2}$	- групи осіб S_1; - окремі особи S_2;
3.	За частотою повторюваності	$Frequency = \bigcup_{d} F_d$, $d = \overline{1,3}$	- одноразові F_1; - повторювані F_2; - продовжувані F_3;
4.	За прихованістю прояву	$Secrecy = \bigcup_{w} Sr_w$, $w = \overline{1,2}$	- латентні Sr_1; - явні Sr_2;
5.	За характером загрози по відношенню до соціальної мережі	$Character = \bigcup_{b} C_b$, $m = \overline{1,2}$	- комунікаційні C_1, які проявляються в галузі реалізації потреб акторів у продукуванні, споживанні і розповсюдженні контенту; - технологічні C_2, що полягають в порушенні функціонування і захищеності соціальної мережі;

Закінчення таблиці 1.1.

1	2	3	4
6.	Залежно від мети загрози	$Target = \bigcup_z T_z$, $n = \overline{1,4}$	- вплив на психічний і емоційний стан акторів соціальної мережі T_1; - вплив на свободу вибору акторів T_2 у прийнятті будь-яких рішень; - заклики до сепаратизму, повалення конституційного ладу, порушення територіальної цілісності T_3; - підтримка, супроводження чи активізація злочинної або терористичної діяльності T_4.
7.	За способом дії загрози у соціальних мережах	$Method = \bigcup_p M_p$, $p = \overline{1,4}$	- інформаційні впливи через соціальні мережі M_1; - несанкціонований доступ і кібератаки на аккаунти керівників віртуальної спільноти, лідерів громадської думки M_2; - розголошення інформації з обмеженим доступом у соціальних мережах M_3; - розповсюдження шкідливого програмного забезпечення у соціальних мережах M_4;
8.	За можливістю реалізації у соціальних мережах	$Possibility = \bigcup_i P_i$, $i = \overline{1,4}$	- потенційні P_1; - реальні P_2; - реалізовані P_3; - псевдореальні P_4;
9.	За рівнем впливу на акторів і віртуальні спільноти у соціальних мережах	$Impact = \bigcup_q I_q$, $q = \overline{1,2}$	- допустимі I_1; - недопустимі I_2;

Джерело: Побудовано автором на основі [5, с. 80-84].

Отже, відповідно до запропонованого підходу класифікації загроз інформаційній безпеці у соціальних мережах, формалізуємо їх у вигляді кортежної моделі $D = \langle R, S, C, T, M, F, Sr, P, I \rangle$. Дана модель є інструментом для ідентифікації та аналізу потенційних загроз, які можуть впливати на безпеку інформації у віртуальній спільноті. Своєчасне детектування таких загроз забезпечить ефективність функціонування систем забезпечення інформаційної безпеки і розробку дієвих методів протидії загрозам у соціальних мережах [5, с. 84].

Створення моделі порушника надає можливість здійснювати аналіз та ідентифікувати осіб, що можуть становити загрозу для безпеки інформації у віртуальній спільноті, встановити мотивацію, засоби атаки та наслідки їх діяльності. Розглянемо табл. 1.2, у якій відображено класифікацію порушників інформаційної безпеки.

Таблиця 1.2 – Класифікація порушників інформаційної безпеки віртуальної спільноти у соціальних мережах

№ з/п	Критерій	Позначення	Види порушників
1	2	3	4
1.	По відношенню до віртуальної спільноти	$Relation = \bigcup_{q} R_q,$ $q = \overline{1,2}$	- внутрішні правопорушники (R_1) – особи, які вже є членами віртуальної спільноти; - зовнішні правопорушники (R_2) – особи, які не є членами віртуальної спільноти і намагаються на неї впливати й порушувати її;
2.	За мотивом порушень	$Motive = \bigcup_{n} M_n,$ $n = \overline{1,2}$	- особи, які діють з наміром (M_1); - особи, які діють без наміру (M_2);
3.	За чисельністю	$Violator = \bigcup_{d} V_d,$ $d = \overline{1,2}$	- окремі особи (V_1); - групи осіб (V_2);

Закінчення таблиці 1.2.

1	2	3	4
4.	За рівнем знань	$Qualification = \bigcup_{w} Q_w,$ $w = \overline{1,3}$	- особи з високим рівнем технічних знань, умінь та навичок Q_1; - особи з середнім рівнем технічних знань, умінь та навичок Q_2; - особи з низьким обмеженим рівнем технічних знань, умінь та навичок Q_3;
5.	За рівнем наданих прав	$Access = \bigcup_{f} A_f,$ $f = \overline{1,3}$	- особи, які мають повний доступ до управління спільнотою A_1; - особи, які мають обмежений доступ до управління спільнотою A_2; - особи, які не мають права на управління спільнотою A_3;
6.	За характером дій	$Nature = \bigcup_{p} N_p,$ $p = \overline{1,3}$	- особи, які несвідомо та/або без вагомих мотивів та/або намірів здійснюють порушення N_1; - особи, які свідомо здійснюють порушення для самоствердження та/або отримання нематеріальної вигоди N_2; - особи, які свідомо здійснюються порушення для отримання матеріальної вигоди N_3;
7.	За проявом дій	$Privacy = \bigcup_{e} P_e,$ $e = \overline{1,2}$	- особи, які намагаються діяти приховано та залишити свою діяльність непомітною P_1; - особи, які відкрито демонструють свої дії P_2;

Джерело: Побудовано автором на основі [4, с. 142].

Розроблена класифікація порушників демонструє широкий спектр осіб, які можуть становити загрозу інформаційній безпеці віртуальної спільноти. Відповідно, формалізовану класифікацію загроз інформаційній безпеці варто подати у вигляді кортежної моделі $O = \langle R, Q, A, M, N, P, V \rangle$, яка дає можливість відстежувати потенційні ризики і вразливості, що можуть виникати у процесі діяльності акторів соціальної мережі та розробляти заходи для їх запобігання.

Серед основних інструментів, які протидіють загрозам інформаційної безпеки варто виокремити механізми безпеки у соціальних мережах, під якими слід розуміти технології і практики, що використовуються для захисту користувачів та їх даних від несанкціонованого доступу. Соціальні мережі містять велику кількість особистої інформації про користувачів, включаючи їх імена, адреси електронної пошти, номери телефонів, фото тощо. Дана інформація може бути використана проти її власників у шахрайських цілях, у тому числі, крадіжки цифрової особистості. Узагальнюючи основні захисні механізми, які наявні у соціальних мережах, варто виокремити основні з них:

1) *Використання паролів* здійснюється для ідентифікації власників облікових записів. Користувачі соціальних мереж повинні використовувати складні паролі, які включають не менше 12-ти символів – цифри, літери різних регістрів, спеціальні символи.

2) *Двоетапна аутентифікація* дозволяє створювати додатковий рівень безпеки облікового запису, вимагаючи від користувача введення одноразового коду під час входу або підтвердження з перевіреного пристрою, на якому здійснено вхід до аккаунту.

3) *Сповіщення про дії з обліковим записом*. Соціальні мережі пропонують своїм користувачам використання сповіщень про спроби входу у обліковий запис з невідомих пристроїв, можливість відстежувати активність облікового запису та, за потреби, тимчасового блокування аккаунту у випадку підозри його злому.

4) *Шифрування*. У соціальних мережах наявне шифрування для захисту інформації під час її зберігання на серверах для унеможливлення прочитання даних шахраями, які потенційно можуть отримати доступ до них злочинним шляхом.

5) *Відстеження активності*. У соціальних мережах наявні моніторингові механізми за допомогою яких відслідковуються підозріла активність облікових записів для активації заходів для усунення потенційних загроз витоку особистої (конфіденційної) інформації користувачів соціальних мереж.

До внутрішніх механізмів захисту віртуальних спільнот відносять:

1) *можливість скаржитись на контент* – дозволяє учасникам спільноти повідомляти адміністраторам про матеріал, який порушує правила спільноти (адміністратори можуть видалити такий контент, або вжити інших заходів – винести попередження або заблокувати користувача);

2) *цензура на контент* – дозволяє адміністраторам спільноти обмежувати поширення певного контенту, який має образливий та/або дискримінаційний характер;

3) внутрішня політика взаємодії учасників віртуальної спільноти, розроблена її адміністраторами.

Висновки до Розділу 1

Підсумовуючи вищевикладене, можна дійти таких висновків:

1) Комунікація між акторами та їх антагоністичні інтереси є одними з визначальних факторів, що впливають на розвиток віртуальних спільнот.

2) Інформаційна стійкість віртуальних спільнот у соціальних мережах є ключовим аспектом, який визначає їхню спроможність чинити опір інформаційним загрозам та адаптуватись до змін в інформаційному просторі.

3) Модель загроз та модель порушника інформаційної безпеки віртуальної спільноти дозволяють ідентифікувати потенційні ризики й аналізувати потенційних порушників, їх мотивацію, засоби атаки та наслідки діяльності для своєчасної реакції з боку адміністраторів віртуальної спільноти.

4) Захисні механізми у віртуальних спільнотах сприяють ефективному захисту особистої інформації користувачів від несанкціонованого доступу, а також унеможливлюють порушення їх особистих кордонів через внутрішню політику безпеки.

РОЗДІЛ 2. МОДЕЛІ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ СИНТЕЗУ ІНФОРМАЦІЙНО-СТІЙКИХ ВІРТУАЛЬНИХ СПІЛЬНОТ

2.1. Інформаційні ситуації, в яких здійснюється прийняття рішень адміністраторами віртуальних спільнот

Для дослідження процесу розвитку стійких віртуальних спільнот варто зважати на інформаційні ситуації, які можуть виникати в інформаційному просторі соціальної мережі. *Fedushko S.*, *Molodetska K.*, *Syerov Y.* [1] під інформаційною ситуацією пропонують розглядати ступінь невизначеності в інформаційному середовищі у момент прийняття рішень учасниками стійкої віртуальної спільноти за якої проявляються їх антагоністичні інтереси. Дана ситуація відображає процеси інформаційного конфлікту в інформаційному просторі соціальної мережі та виникає через несумісні цінності, ідеології, різноспрямовані погляди та агресивну поведінку користувачів у відстоюванні власних інтересів. Спираючись на результати досліджень у даній галузі, виділимо такі інформаційні ситуації, які можуть виникати у соціальних мережах:

«1) задано розподіл апріорних імовірностей множини станів інформаційного середовища сервісів – прийняття рішень в умовах ризику;

2) формалізовано заданий розподіл імовірностей перебування соціальних мереж у різних станах інформаційного середовища з невідомими параметрами;

3) задано системи лінійних відношень порядків на компонентах апріорного розподілу станів інформаційного середовища сервісу;

4) невідомий розподіл імовірностей на множині станів інформаційного середовища соціальної мережі;

5) антагоністичні інтереси різних віртуальних спільнот, що функціонують в інформаційному середовищі соціальної мережі, в процесі прийняття рішення щодо їх функціонування;

6) існування розмитої множини станів інформаційного середовища СІС, коли вони формалізуються якісними показниками» [1].

2.2. Розроблення моделі прийняття рішень

Спираючись на ключові дослідження у теорії прийняття рішень в умовах невизначеності та ризику відіграють важливу роль критерії Севіджа та Вальда [6]. Критерій Севіджа базується на теорії уникнення ризику та визначає стратегію прийняття рішень, де рішення обирається таким чином, щоб максимізувати очікувану корисність, враховуючи ймовірність та можливі втрати. З іншого боку, критерій Вальда фокусується на максимізації мінімального очікуваного виграшу, що означає вибір рішення, яке гарантує найбільший результат навіть у найгіршому сценарії. Аналіз та порівняння цих критеріїв в контексті конкретної ситуації дозволять здійснити обґрунтований вибір стратегії прийняття рішення, враховуючи різні аспекти невизначеності та ризику.

Розглянемо приклад прийняття рішення адміністратором щодо стратегії сталого розвитку віртуальної спільноти за умов антагоністичного протистояння в інформаційному середовищі соціальної мережі. Раціональним рішенням будемо вважати такий вибір адміністратора віртуальної спільноти R_i, $i = \overline{1,n}$, для якого буде задовольнятися умова [2]:

$$F_{i0} = \max_{R_i \in R} \min_{E_j \subset E} F_{ji}^{+}.$$

Дане рішення, прийняте адміністратором дозволяє отримати максимальний рівень виграшу у ситуації, коли відбувається загострення протистояння антагоністичних інтересів користувачів віртуальної спільноти у соціальних мережах. Однак, використання критерію максиміну (критерій Вальда) є доцільним за умови використання противником досконалих технологій інформаційного впливу на користувачів соціальної мережі у процесі інформаційної боротьби. Оскільки, рівень інформаційного впливу на користувачів зменшується за рахунок ефективних стратегічних комунікацій, тому використання критерію Вальда обмежує рівень виграшу для стійкої віртуальної спільноти через хибно прийняте рішення [1].

Тому, для досягнення максимального рівня ефекту від прийнятого рішення, доцільно скористатися критерієм мінімаксу (критерій Севіджа). Оптимальним вважатиметься рішення R_i, $i = \overline{1,n}$, для якого буде задовольнятися умова [3]:

$$\mathrm{F_{i0}} = \min_{\mathrm{R_i \in R}} \max_{\mathrm{E_j \subset E}} \mathrm{F_{ji}^{-}}.$$

«Аналіз випадків застосування цього критерію показує, що його недоліком є наступне. Якщо рішення, прийняте адміністраторами стійкої віртуальної спільноти в умовах антагоністичного протистояння у інформаційному середовищі соціальних інтернет-сервісів рішення $R_{i0} \in R$ є оптимальним за критерієм Севіджа і з множини рішень R виключити неоптимальне рішення $R_i \neq R_{i0}$, то на новій множині R^* рішення R_{i0} може не бути оптимальним» [9].

Розглянемо приклад застосування підходів до прийняття рішень з метою реалізації сталого функціонування віртуальної спільноти у соціальних мережах. Нехай, потрібно прийняти рішення з множини $R = \{R_1, R_2, \dots, R_i\}$, $i = \overline{1,n}$, які є взаємовиключними, для реалізації стратегії сталого розвитку віртуальної спільноти у соціальних мережах. При цьому інформаційний простір соціальної мережі перебуває у одному зі станів $E = \{E_1, E_2, \dots, E_j\}$, $j = \overline{1,m}$, який на момент прийняття рішення залишається невідомим. Необхідно прийняти рішення щодо зміни чисельності користувачів віртуальної спільноти. Допускаються такі варіанти рішень: R_1 – залишити чисельність користувачів незмінною; R_2 – збільшити кількість користувачів за рахунок привернення учасників віртуальних спільнот з протилежними цілями функціонування (захоплення існуючого ресурсу); R_3 – збільшити кількість користувачів за рахунок залучення нових користувачів сервісу (збільшення ресурсу); R_4 – зменшити чисельність учасників віртуальної спільноти.

При цьому в інформаційному середовищі соціальної мережі можливі такі види антагоністичного протистояння: E_1 – зіткнення користувачів між собою на підставі протилежно направлених мотивів; E_2 – зіткнення протилежно спрямованих групових мотивів віртуальних спільнот користувачів соціальної мережі, що є споживачами деякого товару чи послуги; E_3 – у інформаційному середовищі

протікають конфлікти, що ґрунтуються на економічних інтересах окремих суб'єктів економічної діяльності; E_4 – конфлікт, в якому обсяг впливу зменшується по вертикалі зверху донизу: начальник/підлеглий, вища організація/підприємство.

Нехай розглянута ситуація прийняття рішень адміністратором стійкої віртуальної спільноти у соціальних мережах описується матрицею переваг:

$$\begin{array}{c|cccc} & R_1 & R_2 & R_3 & R_4 \\ E_1 & 4 & 8 & 10 & 1 \\ E_2 & 3 & 7 & 3 & 1 \\ E_3 & 3 & 6 & 9 & 0 \\ E_4 & 2 & 4 & 9 & 2 \end{array}.$$

З метою пошуку оптимального рішення скористаємося критерієм Вальда:

$$F_1 = \min_{E_j \subset E} F_{ji}^{+} = \min\{4; 3; 3; 2\} = 2;$$

$$F_2 = \min_{E_j \subset E} F_{ji}^{+} = \min\{8; 7; 6; 4\} = 4;$$

$$F_3 = \min_{E_j \subset E} F_{ji}^{+} = \min\{10; 3; 9; 9\} = 3;$$

$$F_4 = \min_{E_j \subset E} F_{ji}^{+} = \min\{1; 1; 0; 2\} = 1;$$

$$\max_{R_i \in R} \min_{E_j \subset E} F_{ji}^{+} = \{2; 4; 3; 1\} = 4.$$

Отримані результати розрахунків показали, що оптимальним рішенням для даної ситуації є рішення R_2.

Аналогічно, для пошуку оптимального рішення скористаємося критерієм мінімаксу (критерій Севіджа). Матриця ризиків набуває наступного вигляду:

$$\begin{array}{c|cccc} & R_1 & R_2 & R_3 & R_4 \\ E_1 & 8 & 8 & 9 & 3 \\ E_2 & 4 & 5 & 3 & 2 \\ E_3 & 9 & 7 & 5 & 10 \\ E_4 & 3 & 3 & 1 & 4 \end{array}.$$

Проведемо розрахунки за критерієм Севіджа:

$$F_1 = \max_{E_j \subset E} F_{ji}^{+} = \max\{8; 4; 9; 3\} = 9;$$

$$F_2 = \max_{E_j \subset E} F_{ji}^{+} = \max\{8; 5; 7; 3\} = 8;$$

$$F_3 = \max_{E_j \subset E} F_{ji}^{+} = \max\{9; 3; 5; 1\} = 9;$$

$$F_4 = \max_{E_j \subset E} F_{ji}^{+} = \max\{3; 2; 10; 4\} = 10;$$

$$\min_{\mathrm{R_i} \in \mathrm{R}} \max_{\mathrm{E_j} \subset \mathrm{E}} \mathrm{F_{ji}^{+}} = \{9; 8; 9; 10\} = 8.$$

На основі використання критерію мінімаксу, було встановлено, що оптимальним рішення є R_2.

Порівняльний аналіз використання критеріїв Севіджа та Вальда дозволяє запропонувати модель прийняття рішень адміністраторами віртуальної спільноти у соціальних мережах в залежності від конкретних обставин та особливостей ситуації (табл. 2.1).

Таблиця 2.1. – Модель прийняття рішень адміністраторами віртуальної спільноти у соціальних мережах

	Характеристика ситуації, у якій використовується критерій
Критерій Вальда	У випадках кризових ситуацій, де необхідно максимізувати мінімальний очікуваний виграш, адміністратори можуть застосовувати критерій Вальда. Наприклад, при виявленні критичної помилки чи загрози для безпеки користувачів, важливо приймати рішення, яке максимально зменшить можливий негативний вплив, навіть якщо ймовірність такого впливу низька. Критерій Вальда може бути використаний у випадках, коли необхідно уникати великих ризиків і важливо мати гарантію максимальної вигоди в будь-якому варіанті розвитку подій.
Критерій Севіджа	Критерій Севіджа може бути ефективним при визначенні стратегій для довгострокового розвитку віртуальної спільноти. Враховуючи ймовірності та можливі втрати, адміністратори можуть обирати такі рішення, які максимізують очікувану корисність у середньому протягом тривалого періоду часу. У ситуаціях, коли спільнота знаходиться в стадії пошуку нових можливостей чи впровадження інновацій, критерій Севіджа може допомогти адміністраторам оцінити ймовірності успіху та вибрати стратегію, що максимізує потенційну користь.

Джерело: Побудовано автором на основі власних досліджень.

Висновки до Розділу 2

Інформаційні ситуації, в яких здійснюється прийняття рішень адміністраторами віртуальних спільнот, можуть бути представлені в залежності від ступеня невизначеності та ризику. Критерії Севіджа та Вальда є ефективними для прийняття рішень адміністраторами віртуальних спільнот за умов виникнення різних ситуацій в інформаційному просторі соціальної мережі. Модель прийняття рішень, яка враховує особливості інформаційного середовища соціальних мереж та антагоністичного протистояння в ньому, дозволяє адміністраторам віртуальних спільнот приймати обґрунтовані рішення, які сприятимуть її сталому розвитку.

Критерій Вальда може бути використаний у випадках, коли необхідно уникати великих ризиків і важливо мати гарантію максимальної вигоди в будь-якому варіанті розвитку подій. У ситуаціях, коли спільнота знаходиться в стадії пошуку нових можливостей чи впровадження інновацій, критерій Севіджа може допомогти адміністраторам оцінити ймовірності успіху та вибрати стратегію, що максимізує потенційну користь.

РОЗДІЛ 3. РОЗРАХУНКИ Й ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ПРАВИЛЬНІСТЬ ЗАПРОПОНОВАНИХ РІШЕНЬ

3.1. Розроблення методики порівняльної оцінки запропонованих рішень

З розвитком соціальних мереж постійно змінюються підходи до залучення користувачів у віртуальних спільнотах. Раніше, увага акцентувалась на простому обміні інформацією та дискусіях на специфічні теми, а залучення користувачів відбувалось через їх безпосередню участь у обговореннях, розміщенні повідомлень тощо. Особливу роль у механізмі підтримки зв'язку між користувачами віртуальної спільноти відігравала електронна пошта, на яку надходили повідомлення про нові події та оновлення у спільноті.

Розміщення інформації про віртуальні спільноти на різних інтернет-ресурсах, а також поширення контенту такої спільноти на сторінках її користувачів, в особистих повідомленнях друзям і знайомим, були досить ефективними способами залучення нових користувачів. І хоч зараз ці методи залишаються актуальними, однак суттєво знизилась їх ефективність, оскільки постійно зростає конкуренція за увагу користувацької аудиторії.

Однак, зі зміною смаків користувачів та підвищення рівня вимог до якості контенту, постають нові виклики для адміністраторів віртуальних спільнот, головною задачею яких стає не тільки залучення нових користувачів, а й утримання уже наявного користувацького ресурсу. Наразі, інтерактивний контент відіграє ключову роль, а його якість активізує аудиторію, надаючи їй можливість впливати на контент та взаємодіяти з іншими користувачами соціальної мережі та віртуальної спільноти, зокрема. Впровадження алгоритмів таргетованої реклами для надання користувачам індивідуалізованого контенту дає можливість зберегти інтерес аудиторії та підтримувати її активність протягом усього часу існування віртуальної спільноти, що в свою чергу відповідає принципам сталого розвитку. Використання таргетингу дозволяє підвищити ефективність рекламних кампаній і залучати більше релевантних користувачів.

Залучення інфлюенсерів, як способу ефективного привертання уваги до віртуальної спільноти наразі є дуже популярним способом збільшити активну частку користувачів. Однак, співпраця із ними вимагає залучення додаткових фінансових ресурсів, що не зовсім може підходити для усіх. Введення елементів гейміфікації (проведення конкурсів, рейтингування тощо) стимулює учасників віртуальної спільноти для взаємодії як із самою спільнотою, тобто її контентом, так і з іншими учасниками віртуального об'єднання.

Для оцінки запропонованих рішень, щодо залучення користувачів, адміністраторам віртуальних спільнот у соціальних мережах варто опиратись на такі показники, як:

– складність реалізації обраного рішення;

– ціну реалізації обраного рішення та наявний обсяг фінансового ресурсу;

– доступність і наявність потрібного обсягу ресурсного потенціалу для реалізації потенційних рішень.

На основі вищезгаданих критеріїв оцінки можна визначити, яке рішення є найбільш оптимальним для конкретної віртуальної спільноти.

3.2. Порівняльний аналіз запропонованого рішення з відомими

Для підтвердження ефективності інформаційного впливу моделі прийняття рішень для сталого розвитку віртуальної спільноти було проведено експериментальне дослідження на базі віртуальної спільноти – групи кафедри комп'ютерних технологій і моделювання систем Поліського національного університету, створеної у середовищі соціальної мережі *Facebook* (https://www.facebook.com/groups/ktims).

Адміністраторами віртуальної спільноти було реалізовано оптимальне рішення – R_2 і збільшено кількість учасників за рахунок залучення наявних користувачів соціальної мережі *Facebook*. Дане рішення було реалізовано шляхом зміни підходу до якості контенту.

Розглянемо динаміку опублікованих дописів та/або коментарів користувачами віртуальної спільноти кафедри та перегляду її дописів до реалізації експерименту – вересень 2023 р. (рис. 3.1., 3.2), та після його реалізації – жовтень 2023 р. (рис. 3.3., 3.4).

Рисунок 3.1. – Динаміка опублікованих дописів та/або коментарів користувачами віртуальної спільноти за вересень 2023 р.

Джерело: Аналітика групи у соціальній мережі *Facebook* [7].

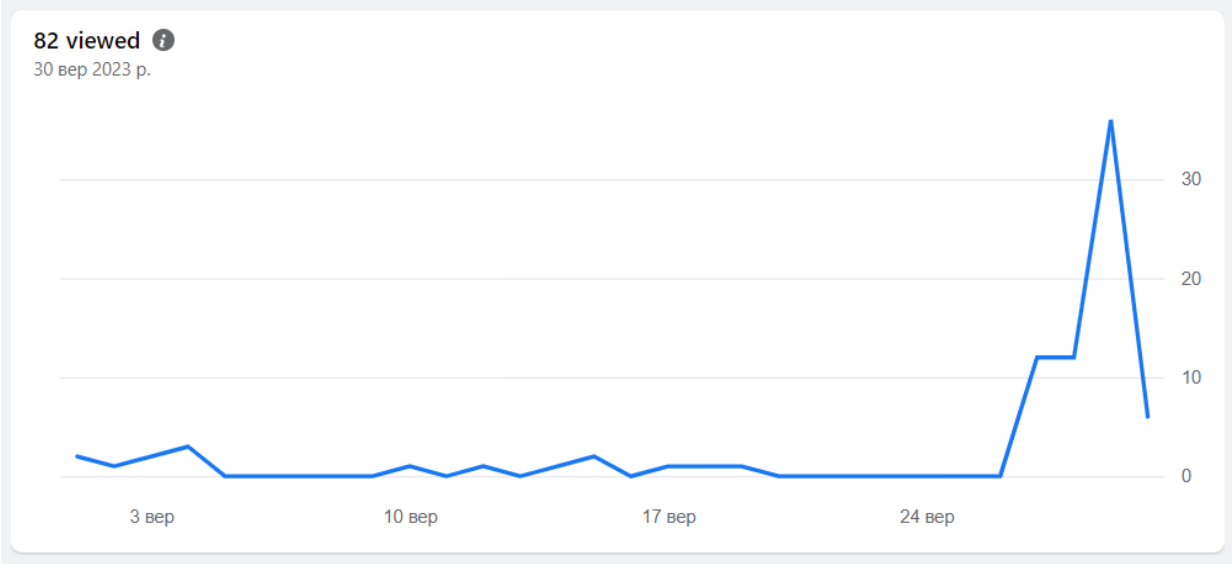

Рисунок 3.2. – Динаміка перегляду дописів віртуальної спільноти за вересень 2023 р.

Джерело: Аналітика групи у соціальній мережі *Facebook* [7].

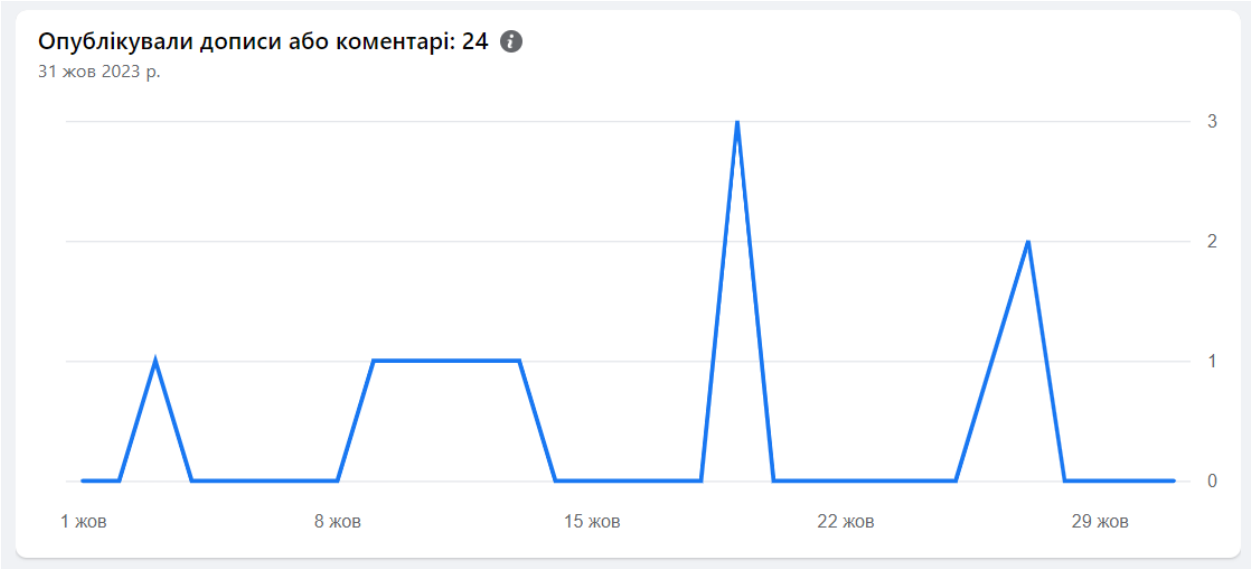

Рисунок 3.3. – Динаміка опублікованих дописів та/або коментарів користувачами віртуальної спільноти за жовтень 2023 р.

Джерело: Аналітика групи у соціальній мережі *Facebook* [7].

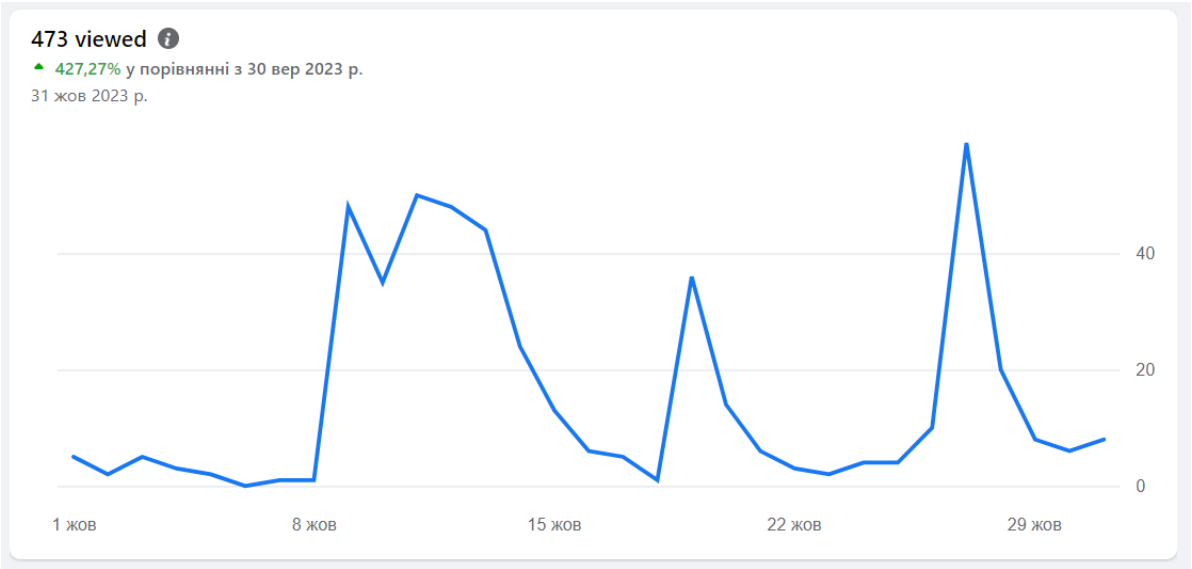

Рисунок 3.4. – Динаміка перегляду дописів віртуальної спільноти за жовтень 2023 р.

Джерело: Аналітика групи у соціальній мережі *Facebook* [7].

Аналізуючи динаміку на рис. 3.1. та 3.3., можна побачити, що реалізація обраного рішення підвищила обсяг публікаційної активності користувачів віртуальної спільноти, з 4 до 24 дописів та/або коментарів, що складає на 600% більше, ніж було до початку експерименту.

Зміна підходу до якості контенту віртуальної спільноти дозволила підвищити обсяг переглядів з 82 до 473, що станом на 31 жовтня 2023 р. на 427,27% вище у порівнянні з 30 вересня 2023 р.

Отже, можна припустити, що обране адміністраторами віртуальної спільноти рішення було вірним, а залучення користувачів відбувалось шляхом активізації інтересу аудиторії спільноти та активної взаємодії з контентом, що в свою чергу дозволило запустити механізми таргетингу, які передбачають рекомендацію контенту спільноти усім користувачам соціальної мережі *Facebook* з якими взаємодіють учасники віртуальної спільноти на базі якої було реалізовано експеримент.

Висновки до Розділу 3

Способи залучення користувачів віртуальних спільнот постійно розвиваються. Віртуальні спільноти повинні використовувати різні методи для залучення нових учасників і підвищення активності вже наявних для утримання чисельності аудиторії та підвищення її якості.

У результаті проведеного експерименту на базі віртуальної спільноти кафедри комп'ютерних технологій і моделювання систем виявлено високу ефективність впровадженого рішення R_2. За період з вересня до жовтня 2023 року спостерігалася позитивна зміна динаміки публікацій та/або коментарів на 600% та переглядів на 427,27%. Активізація взаємодії аудиторії з контентом свідчить про успішне залучення користувачів, а також сприяє ефективному таргетингу та рекомендаціям контенту на платформі соціальної мережі *Facebook*. Отримані об’єктивні показники підтверджують доцільність обраного рішення для досягнення цілей сталого розвитку віртуальної спільноти.

ВИСНОВКИ

Вивчення та розуміння динаміки й особливостей формування та подальшого розвитку стійких віртуальних спільнот у соціальних мережах є важливим аспектом розвитку інформаційної безпеки. Комунікація між акторами та їх антагоністичні інтереси впливають на розвиток цих спільнот і вимагають використання різних моделей та стратегій для забезпечення безпеки, ефективного управління й подальшого сталого розвитку цієї спільноти.

У першому розділі визначено загальні відомості про віртуальні спільноти у соціальних мережах; розкрито особливості інформаційно-стійких віртуальних спільнот, а також окреслено сучасні загрози і порушників інформаційної безпеки та основні захисні механізми у соціальних мережах.

Другий розділ присвячено дослідженню інформаційних ситуацій, в яких здійснюється прийняття рішень та розробленню моделі для підтримки їх прийняття адміністраторами з метою синтезу інформаційно-стійких віртуальних спільнот у соціальних мережах.

У третьому розділі наведено розрахунки й експериментальні дані, що підтверджують правильність запропонованих рішень та здійснено їх порівняльний аналіз з відомими.

У цілому, поставлена мета і завдання були виконані у повному обсязі. Робота містить практичні рекомендації, які були експериментально перевірені, та можуть бути корисними для адміністраторів віртуальних спільнот у соціальних мережах для формування сталого вектору їх розвитку, шляхом залучення нових користувачів та підтримання кількості наявної аудиторії, підвищення якості її взаємодії зі спільнотою та формування стійких механізмів її захисту від потенційних ризиків інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Fedushko S., Molodetska K., Syerov Y. Decision-making approaches in the antagonistic digital communication of the online communities users. *Soc Netw Anal Min*. 2023. Вип. № 13(1):18. doi: 10.1007/s13278-022-01021-4.

2. Moustakides G., Verykios V. A MaxMin approach for hiding frequent itemsets. *Data & Knowledge Engineering*. 2008. Вип. № 65(1). С. 75-89.

3. Yokoyama R., Fujiwara K., Ohkura M., Wakui, T. A revised method for robust optimal design of energy supply systems based on minimax regret criterion. *Energy Conversion And Management*. 2014. Вип. № 84. С. 196-208.

4. Євсеєв С. П., Тимонін Ю. О., Веретюк С. М., Войтко Т. М., Оленюк Д. О. Синтез моделі соціальних санкцій для забезпечення стійкості віртуальних спільнот у соціальних мережах в умовах антагоністичного середовища. *Захист інформації.* 2023. Том 25 № 3. С. 139-147. DOI: 10.18372/2410-7840.25.17939.

5. Молодецька К. В. Узагальнена класифікація загроз інформаційній безпеці держави в соціальних інтернет-сервісах. *Захист інформації.* 2016. № 23. С. 75-87.

6. Решетило В. П., Федотова Ю. В. Невизначеність та ризик: співвідношення понять та специфіка прийняття рішень. *Економіка та управління підприємствами*. 2020. Вип. №3 (77). С. 149-154.

7. Соціальна мережа Facebook. URL: https://www.facebook.com/ (дата звернення 10.12.2023).

8. Стратегія інформаційної безпеки. Затверджено Указом Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення 20.11.2023).

9. Федушко С. С., Сєров Ю. О., Трач О. Р. Методи управління веб-спільнотою в умовах психологічних, соціальних та економічних впливів на суспільство під час пандемії COVID-19 : звіт про науково-дослідну роботу. Національний університет «Львівська політехніка». 2021. 191 с.