УДК 004.056.5:004.77
DOI: 10.31673/2409-7292.2024.040015

Лаптєв О. А., Колесник В. В., Ровда В. В., Половінкін М. І.

МЕТОД ПІДВИЩЕННЯ ЗАХИСТУ ОСОБИСТИХ ДАНИХ ЗА РАХУНОК СИНТЕЗУ РЕЗИЛЬЄНТНИХ ВІРТУАЛЬНИХ СПІЛЬНОТ

В сучасному інформаційному середовищі віртуальні спільноти відіграють важливу роль у забезпеченні обміну інформацією, знаннями та ідеями, сприяючи соціальній взаємодії та розвитку цифрових платформ. Їхній успіх залежить від здатності адаптуватися до змінних умов, зберігати стабільність і функціональність, що робить питання резильєнтності таких спільнот особливо актуальним. Розробка науково обґрунтованих методів підвищення резильєнтності віртуальних спільнот є важливим завданням, яке вимагає міждисциплінарного підходу. Дане дослідження зосереджене на аналізі ключових факторів, які визначають стійкість віртуальних спільнот у соціальних інтернет-сервісах. Зокрема, розглянуто роль технологічних інновацій, інклюзивності, управлінських практик та впливу зовнішніх і внутрішніх факторів. Окрему увагу приділено інтеграції автоматизованих інструментів і ручних методів модерації, що забезпечують ефективне управління поведінкою користувачів, контролювання контенту та підтримку позитивної динаміки спільноти. У ході дослідження акцентується на важливості інклюзивного підходу, що передбачає активне залучення різних соціальних груп для забезпечення різноманітності та гармонійного розвитку віртуальних середовищ. Проаналізовано перспективи використання новітніх технологій, таких як штучний інтелект, для моніторингу, аналізу та підтримки здорової екосистеми віртуальних спільнот. Запропоновані рекомендації орієнтовані на підвищення ефективності функціонування спільнот шляхом активного залучення користувачів, створення інноваційних управлінських практик та впровадження технологічних рішень для забезпечення стабільності і стійкості до викликів.

Ключові слова: резильєнтність, віртуальні спільноти, модерація, соціальна згуртованість, адаптивність, інклюзивність, кібербезпека, загрози.

Вступ

На сучасний момент віртуальні спільноти, які формуються на платформах соціальних інтернет-сервісів, є одним із ключових елементів сучасної інформаційної системи. Вони забезпечують ефективний обмін інформацією, знаннями та сприяють формуванню соціального капіталу. Однак ці спільноти зазнають впливу численних загроз, серед яких інформаційні атаки до яких відносяться: дезінформація, когнітивна війна, кіберзагрози, тролінг, а також внутрішні конфлікти між учасниками. Ці негативні чинники можуть суттєво підривати довіру до віртуальної спільноти та платформи, знижувати рівень функціональності та кіберстійкості, що ставить під питання її здатність протистояти впливу зовнішніх та внутрішніх загроз.

Система стратегічних інформаційних комунікацій значно змінилася за останні десятиліття, і диверсифікація каналів комунікації стала невід'ємною частиною цього процесу. Віртуальні платформи створили новий інформаційний простір, де користувачі (актори), одночасно із споживанням контенту, стали його авторами, що значно ускладнює трафік інформаційних потоків. Цій фактор створює нові виклики для забезпечення інформаційної безпеки. У новій реальності одну з ключових ролей відіграють когнітивні та семантичні війни, де головними цілями є вплив на сприйняття реальності користувачами на змістовні акценти та поведінку великих груп людей. Відсутність ефективних методів протидії інформаційним впливам, що є складовою інформаційної війні у рамках її когнітивної складової, підвищує вразливість суспільства перед сучасними інформаційнимизагрозами.

Методи впливу постійно змінюються і вдосконалюються, агентами впливу стають не тільки журналісти та засоби масової інформації в цілому, а письменники, режисери, діячі культури та мистецтва, лідери думок, конструктори уваги [1,2], що ускладнює протидію традиційними інструментами. Одним з перспективних напрямків протидії інформаційним впливам е розвивток та будівля резильєнтної віртуальної спільноти, яка може адаптуватися до нових умов і зберігати свою функціональність, попри тиск інформаційних загроз зі зовнішнього середовища.

Під резильєнтністю віртуальної спільноти Shaw J., Brewer L., та Veinot T. розуміють її здатність адаптуватися та розвиватися, незважаючи на виклики чи загрози [3, 4]. Дослідження резильєнтності дозволяє виявити механізми, які сприяють стійкості та адаптивності таких спільнот. Аналіз характеристик, структури та факторів, що визначають резильєнтність, є необхідним для формування цілісного уявлення про можливості підвищення ефективності функціонування віртуальних спільнот в умовах динамічного інформаційного середовища. З практичної точки зору, вирішення цієї проблеми сприятиме розробленню рекомендацій для ефективного управління спільнотами, що може бути корисним адміністраторам соціальних інтернет сервісах, організаціям, які прагнуть оптимізувати свою взаємодію з аудиторією, а також розробникам інструментів моніторингу та модерації онлайн-комунікацій.

Таким чином, вивчення та аналіз характеристик, структури та факторів, що впливають на формування резильєнтності віртуальних спільнот є актуальним напрямком досліджень, результати якого можуть сприяти підвищенню рівня безпеки та сталому розвитку інформаційного простору. Існує об’єктивне протиріччя між науковими підходами та практичними викликами. З одного боку, наука розробляє нові методології для підвищення резильєнтності віртуальних спільнот, з іншого боку, практична реалізація цих підходів стикається з труднощами, спричиненими динамічними змінами інформаційних впливів та проєктів впливу, відсутністю ефективних інструментів для їх нейтралізації, а технологічний розвиток та зміна інформаційних практик вимагають постійного вдосконалення стратегій протидії інформаційним загрозам.

Критичний аналіз останніх досліджень і публікацій [5-7] показав, що перспективний напрямок досліджень полягає у побудові резильєнтних спільнот шляхом інтеграції технологічних інновацій, гнучких управлінських стратегій та розвитку соціальної згуртованості серед учасників. Важливо враховувати культурні та соціальні фактори, що сприяють підвищенню соціальної згуртованості, а також активно використовувати новітні технології для моніторингу та захисту інформаційного простору. Культурні особливості можуть визначати рівень взаємодії та підтримки у віртуальних спільнотах, що впливає на здатність спільнот ефективно реагувати на інформаційні загрози [8-11]. Створення таких резильєнтних спільнот дозволить забезпечити сталий розвиток інформаційного середовища, яке буде здатне ефективно протистояти зовнішнім загрозам та сприяти формуванню міцних соціальних зв’язків.

Аналіз літературних джерел та формулювання проблеми

Віртуальні спільноти стають все більш значущими в сучасному суспільстві, з причини розвитку веб-платформ, популярності соціальних інтернет сервісів та діджиталізації. Дослідження свідчать, що сильне почуття спільноти є ключовим фактором для підвищення залученості користувачів та стійкості віртуальних середовищ [12]. Hong Z. і Shi Q. у своєму дослідженні [13] відзначають, що зацікавленість у віртуальній спільноті значно посилює залученість користувачів, що є необхідним для сталого розвитку цих спільнот. Як зазначають Kasperiūnienė J. та Ivanova I. [14], це залучення додатково підтримується розвитком соціального капіталу, які підкреслюють, що віртуальні спільноти сприяють комунікації та спільним інтересам, тим самим зміцнюючи зв’язки у спільноті. Проте недослідженим у даних роботах виступає фактор перенесення зв’язків між акторами всередині віртуальної спільноти в реальний світ, адже автори не описують процеси взаємодії у випадках, якщо два і більше учасників спільноти знайомі між собою у реальності.

Крім того, структури управління у віртуальних спільнотах відіграють ключову роль у їх стійкості. Tchernichovski, O. описує в своїй роботі [15] наступне, що віртуальні спільноти застосовують різні методи управління, включаючи адміністрування, модерацію контенту, пряме втручання в діяльність акаунтів користувачів, публічні та приватні обговорення, модерація користувачів, для вирішення викликів та підвищення успішності спільноти. Його ідеї доповнюють Frey S. та Sumner R. у своїй статті [6], шо дана управлінська частина може

призвести до кращої модерації та підвищення ефективності спільноти та її резильєнтності. Ефективне управління корелює з успіхом спільноти, особливо в умовах функціонування великих груп [7]. Встановлення чітких правил та настанов є важливим для створення спільної атмосфери всередині віртуальної спільноти, де учасники відчувають свою цінність та залученість. Проте жорстка модерація може призвести до відчуття постійного нагляду адміністраторів групи та обмеження свободи волі, що є негативним чинником для підвищення резильєнтності групи. Проте автори даних робіт не описали, як згадані у їхніх дослідженням методи управління працюють на практиці у різних соціальних інтернет сервісах та з різними віковими групами.

Технологічні інновації відіграють важливу роль у формуванні та підтримують функціональність віртуальних спільнот. Згідно з недавнім дослідженням Wang Y., [8], технологічний прогрес сприяє обміну інформацією та покращує якість досліджень у віртуальних академічних спільнотах, що може мати вплив на економіку країни. У даному дослідженні Lv S., [8], підкреслює важливість залучення нових користувачів і підтримки наявних, щоб забезпечити стійке зростання цих спільнот. Недоліком даних робіт виступає те, що не описані методи та засоби залучення нових користувачів у існуючі віртуальні спільноти, та перспективи застосування вже існуючих технологій для обміну інформацією між ними.

Крім того, інклюзивність віртуальних спільнот є життєво важливою для їхньої резильєнтності. Shaw, J. зазначає у своїй праці [9], що маргіналізовані групи повинні бути включені в процеси проєктування та управління програмами віртуальної допомоги, щоб уникнути соціальних розривів. Проте автор не зауважив, що гіпер інклюзивність до певних окремих груп, може зменшити зацікавленість основної маси акторів всередині спільноти, тому варто перспективним залишається дослідження, щодо балансу між різними підгрупами всередині спільноти.

Отже, проведений аналіз підтверджує, що резильєнтність віртуальних спільнот залежить від комбінації таких факторів як залученість користувачів, ефективне управління, технологічні інновації та інклюзивність. Ці фактори працюють синергетично для створення середовищ, де члени можуть процвітати, обмінюватися знаннями та підтримувати один одного, що в кінцевому результаті призводить до сталого та міцного розвитку віртуальних спільнот.

Таким чином, на підставі проведеного аналізу, результатів вивчення наукових публікацій за темою досліджень, патентів, монографій та практичних розробок встановлено, що існує об’єктивне протиріччя між науковими підходами та практичними викликами. З одного боку, наука розробляє нові методології для підвищення резильєнтності віртуальних спільнот, з іншого боку, практична реалізація цих підходів стикається з труднощами, спричиненими динамічними змінами інформаційних впливів та проєктів впливу, відсутністю ефективних інструментів для їх нейтралізації, а технологічний розвиток та зміна інформаційних практик вимагають постійного вдосконалення стратегій протидії інформаційним загрозам.

Тому встановлення й уточнення впливу факторів, які запускають процеси резильєнтності у віртуальних спільнотах, є актуальним науковим завданням в рамках вирішення проблеми синтезу резильєнтних віртуальних спільнот.

Мета роботи та цілі дослідження

Метою статті є адаптація методу підвищення захисту особистих даних за рахунок синтезу резильєнтних віртуальних спільнот. Виявлення ключових факторів, що сприяють формуванню резильєнтних віртуальних спільнот у соціальних інтернет-сервісах для створення передумов сталого розвитку інформаційного простору.

Виклад основного матеріалу

У інформаційному просторі віртуальні спільноти в соціальних інтернет-сервісах відіграють важливу роль, об’єднуючи акторів із різноманітними інтересами та забезпечуючи

обмін інформацією, знаннями та досвідом. Однак, стрімкий розвиток цифрових технологій та зростання кількості загроз в інформаційному просторі актуалізують проблему забезпечення кіберстійкості (резильєнтності) таких спільнот. Резильєнтність віртуальних спільнот є їхньою здатністю підтримувати функціональність та сталість за умов впливу стресових факторів, включно з інформаційними атаками, дезінформацією та внутрішніми конфліктами між учасниками.

Резильєнтні віртуальні спільноти характеризуються здатністю адаптуватися до змін і протистояти негативним впливам як ззовні, так і зсередини. Ці спільноти не лише здатні зберігати свою функціональність під час криз або атак, але й використовують такі ситуації для зміцнення внутрішніх зв'язків і підвищення власної стійкості. Основними характеристиками резильєнтних віртуальних спільнот є наступні:

1) стійкість до зовнішні загроз;
2) адаптивність до змін;
3) соціальна згуртованість;
4) гнучкі механізми модерації;
5) інклюзивність та підтримка різноманітності;
6) анонімність користувачів;
7) схильність до самоорганізації.

Структура резильєнтної віртуальної спільноти є багаторівневою системою взаємодій (Рис.1), яка забезпечує ефективну координацію та підтримку сталості спільноти в умовах внутрішніх і зовнішніх загроз. У такій спільноті чітко розподілені ролі, визначені правила взаємодії та впроваджені механізми моніторингу й модерації, що допомагає підтримувати соціальну згуртованість та захищати спільноту від дестабілізації. Одним з головних елементів структури такої спільноти виступає рольова ієрархія (Табл.1)

Рис. 1. Ієрархія взаємодій у віртуальних спільнотах

Модерація є ключовим механізмом для забезпечення стійкості віртуальних спільнот. Вона відіграє вирішальну роль у підтримці порядку, мінімізації конфліктів і захисті учасників від зовнішніх загроз. Успішні методи модерації повинні поєднувати соціальні та технологічні аспекти, забезпечуючи баланс між свободою взаємодії та безпекою. Автоматизація модерації в великих спільнотах стала невід'ємною частиною забезпечення стійкості. Алгоритми на

основі штучного інтелекту дозволяють швидко виявляти порушення правил, зокрема ненависницькі висловлювання, спам і дезінформацію. Попри автоматизацію, роль людської модерації залишається важливою. Модератори можуть більш гнучко реагувати на складні або неоднозначні ситуації, коли автоматичні системи можуть допустити помилки. Людський контроль дозволяє підтримувати індивідуальний підхід у вирішенні конфліктів та управлінні взаємодіями.

Таблиця 1

Рольова ієрархія резильєнтних віртуальних спільнот

Роль	Функції	Ознаки	Вплив на резильєнтність спільноти
Адміністратори та власники спільноти	Встановлення загальної політики, стратегічне управління, контроль інфраструктури	Вплив на політику, право прийняття стратегічних рішень, взаємодія з модераторами	Забезпечують основи функціонування спільноти, стратегічні рішення можуть суттєво впливати на її стійкість
Модератори	Оперативне дотримання правил, моніторинг контенту, втручання у випадку порушень	Здатність видаляти контент, попереджати та блокувати порушників, тісна взаємодія з адміністраторами	Оперативне втручання у порушення правил сприяє підтримці порядку і стійкості у спільноті
Лідери думок	Неформальне лідерство, сприяння позитивному середовищу та активній участі	Високий рівень залученості, авторитет серед учасників, вплив на загальну атмосферу спільноти	Формують позитивну атмосферу, стимулюють взаємодію учасників, сприяють зміцненню соціальних зв'язків
Рядові учасники	Участь у спільноті, створення контенту, дотримання правил	Дотримання правил, створення контенту, участь у дискусіях, взаємодія з іншими учасниками	Активна участь у спільноті та дотримання правил сприяють збереженню стабільності та розвитку спільноти

Висновки

У роботі доведено, що резильєнтність віртуальних спільнот є багатокомпонентним явищем, яка базується на кількох важливих чинниках. По-перше, ефективне стратегічне управління забезпечує стабільність через встановлення чітких правил та процедур. Адміністратори та модератори відіграють ключову роль у підтримці порядку, швидко реагуючи на загрози і порушення. Другим важливим елементом є гнучкість модераційних систем. Адаптований метод захисту особистих даних за рахунок синтезу резильєнтних віртуальних спільнот та ппоєднання автоматизованої та ручної модерації дозволяє підвищити захист інформації. Досягти балансу між швидкістю реагування та індивідуальним підходом до вирішення конфліктів. Наведені аалгоритмі можуть ефективно виявляти порушення правил, а людська модерація дозволяє уникати надмірної автоматизації, що може призвести до неправомірних санкцій.

Доведено, що соціальна згуртованість є невід'ємною складовою резильєнтності. Учасники, які мають довіру один до одного і відчувають себе частиною спільноти, здатні ефективно співпрацювати і саморегулюватися, що зменшує навантаження на модераторів. Згуртовані спільноти швидше адаптуються до змін і можуть відновлюватися після внутрішніх конфліктів або зовнішніх загроз. Інклюзивність, яка передбачає залучення різних груп користувачів, також є критичною для стійкості спільноти. Забезпечення того, що кожен учасник може висловити свою думку і відчути себе важливою частиною спільноти, знижує ймовірність конфліктів і сприяє позитивній атмосфері взаємодії.

Подальші дослідження повинні зосередитися на ролі технологічних інновацій у забезпеченні резильєнтності віртуальних спільнот. Також важливо вивчити нові підходи до

комбінованої модерації, які б поєднували автоматизовані алгоритми і людський фактор, а також дослідити вплив соціальних факторів на стійкість спільнот різних масштабів і культурних контекстів.

Перелік посилань

1.Кива В. Ю., Суднiков Є. О., Войтко О. В. Методи розвідки кіберпростору. Сучасні інформаційні технології у сфері безпеки та оборони. 2018. 33(3) стр.45-52 DOI:10.33099/2311-7249/2018-33-3-45-52

2.Особливості забезпечення національної безпеки у високотехнологічному суспільстві [Електронний ресурс]. Режим доступу до ресурсу : http://www.kbuapa.kharkov.ua.

3.Закон України Про основні засади забезпечення кібербезпеки України. Відомості Верховної Ради (ВВР), 2017, № 45, ст.403 https://zakon.rada.gov.ua/laws/show/2163-19#Text

4. Жилін Артем, Ніколаєнко Богдан, Бакалинський Олександр. Підвищення захищеності державних інформаційних ресурсів за рахунок застосування платформи threat intelligence. Захист інформації.2021. Том 23, №3. Стр136-146 DOI: 10.18372/2410-7840.23.16401

6.What is a Threat Intelligence Platform (TIP)? 2018. [Електронний ресурс] – https://www.anomali. com/ resources/what-is-a-tip.

7. Постанова КМУ “Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури” від 19 червня 2019 р. № 518. [Електрон-ний ресурс] – https://zakon.rada.gov.ua/laws /show/518-2019-% D 0%BF#Text.

8. S.Yevseiev, O. Laptiev, O.Korol, S.Pohasii, S.Milevskyi, R. Khmelevsky. Analysis of information security threat assessment of the objects of information activity. International independent scientific journal. Poland. Vol. 1, №34, 2021, pp.33 – 39. ISSN 3547-2340

9. Лаптєв О.А., Бучик С.С., Савченко В.А., Наконечний В.С. , Михальчук І.І, Шестак Я.В., Виявлення та блокування повільних ddos-атак за допомогою прогнозування поведінки користувача. Наукоємні технології. Інформаційні технології, кібербезпека. Том 55 № 3 .2022. С.184-192. DOI: 10.18372/2310-5461.55.16908

10. Serhii Yevseiev, Khazail Rzayev, Oleksandr Laptiev, Ruslan Hasanov, Oleksandr Milov, Bahar Asgarova, Jale Camalova, Serhii Pohasii. Development of a hardware cryptosystem based on a random number generator with two types of entropy sources. Eastern-European journal of enterprise technologies. Vol.5№9 (119), 2022 P. 6–16. ISSN (print) 1729 - 3774. ISSN (on-line) 1729-4061. https://doi.org/ 10.15587/1729-4061.2022.265774 Scopus.

11. Олександр Лаптєв, Віталій Савченко, Віталій Пономаренко, Сергій. Копитко, Іван Пархоменко. Удосконалення методу підвищення завадостійкості систем виявлення сигналів засобів негласного здобуття інформації. Захист інформації. Том 24 № 3 (2022): Захист інформації. С.128-136. https://jrnl.nau.edu.ua/index.php/ZI/issue/view/906

12. Barabash O.V., Open’ko P.V., Kopiika O.V., Shevchenko H.V. and Dakhno N.B. Target Programming with Multicriterial Restrictions Application to the Defense Budget Optimization. Advances in Military Technology. 2019. Vol. 14, No. 2, pp. 213 – 229.

13. Lukova-Chuiko, N., Herasymenko, O., Toliupa, S., ...Laptieva, T., Laptiev, O. The method detection of radio signals by estimating the parameters signals of eversible Gaussian propagation 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 - Proceedings, 2021, P. 67–70

14. Yevseiev, S., Laptiev, O., Lazarenko, S., Korchenko, A., & Manzhul, I. (2021). Modeling the protection of personal data from trust and the amount of information on social networks. Eureka: Physics and Engineering, (1), 24-31. https://doi.org/10.21303/2461-4262.2021.001615

15. Lukova-Chuiko, N., Herasymenko, O., Toliupa, S., LaptievA, T., Laptiev, O. The method detection of radio signals by estimating the parameters signals of eversible Gaussian propagation. Conference Paper. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 - Proceedings, 2021, pp. 67–70.

Надійшла 26.10.2024