

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

Колесник Вадим Валентинович

(прізвище, ім'я, по батькові здобувача освіти)

УДК 004.738.5:316.35

## КВАЛІФІКАЦІЙНА РОБОТА

Синтез резильєнтних віртуальних спільнот в соціальних інтернет-сервісах  
(тема роботи)

125 Кібербезпека та захист інформації  
(шифр і назва спеціальності)

Подається на здобуття освітнього ступеня магістр

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

В. В. Колесник

(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи  
Веретюк С. М.

(прізвище, ім'я, по батькові)

К. Т. Н., доцент

(науковий ступінь, вчене звання)

**Висновок кафедри**

---

за результатами попереднього захисту:

---

**Протокол засідання кафедри**

---

№ \_\_\_\_\_ від «\_\_\_\_\_» \_\_\_\_\_ 20\_\_\_\_ р.

**Завідувач кафедри**

---

(науковий ступінь, вчене звання)

---

(підпис)

---

(прізвище, ім'я, по батькові)

«\_\_\_\_\_» \_\_\_\_\_ 20\_\_\_\_ р.

**Результати захисту кваліфікаційної роботи**

Здобувач вищої освіти \_\_\_\_\_ захистив (ла)  
(прізвище, ім'я, по батькові)

кваліфікаційну роботу з оцінкою:

сума балів за 100-бальною шкалою \_\_\_\_\_

за шкалою ECTS \_\_\_\_\_

за національною шкалою \_\_\_\_\_

**Секретар ЕК**

---

(науковий ступінь, вчене звання)

---

(підпис)

---

(прізвище, ім'я, по батькові)

## АНОТАЦІЯ

Колесник В. В. Синтез резильєнтних віртуальних спільнот в соціальних інтернет-сервісах. – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття освітнього ступеня магістр за спеціальністю 125 – кібербезпека. – Поліський національний університет, Житомир, 2024.

Кваліфікаційна робота присвячена синтезу резильєнтних віртуальних спільнот в соціальних інтернет-сервісах. Для досягнення мети роботи у теоретичній частині проведено аналіз стану проблем забезпечення резильєнтності, ролі та місця у забезпеченні інформаційної безпеки віртуальної спільноти, проведено аналіз методів вимірювання та моделювання резильєнтності. Здійснено систематизацію факторів, які впливають на резильєнтність. У роботі набув подальшого розвитку метод оцінювання резильєнтності віртуальної спільноти в соціальних інтернет-сервісах. Використано сценарне моделювання для опису потенційного розвитку кризових ситуацій для інформаційної безпеки віртуальних спільнот. Проведено експериментальне дослідження методу синтезу резильєнтних віртуальних спільнот та здійснено оцінювання ефективності покращеного методу підвищення інформаційної безпеки віртуальної спільноти в соціальних інтернет-сервісах.

Робота містить 37 сторінок, 15 рисунків, 1 таблицю, 31 літературне джерело.

Ключові слова: Резильєнтність, віртуальні спільноти, соціальні інтернет-сервіси, інформаційна безпека, синтез.

## SUMMARY

Kolesnyk V. V. Synthesis of Resilient Virtual Communities in Social Internet Services. – Qualification work on the rights of the manuscript.

Qualification work for the master's degree in specialty 125 – cybersecurity. - Polissia National University, Zhytomyr, 2024.

The qualification work is devoted to the synthesis of resilient virtual communities in social internet services. To achieve the research objective, the theoretical part analyzes the current challenges of ensuring resilience, the role and significance of virtual communities in information security, as well as methods for measuring and modeling resilience. A systematization of factors influencing resilience is presented.

During the research, a mathematical method for assessing the resilience of virtual communities in social internet services has been further developed. Scenario-based modeling is employed to describe potential crisis developments affecting the information security of virtual communities. An experimental study of the synthesis method for resilient virtual communities has been conducted, along with an evaluation of the effectiveness of the improved mathematical method for enhancing the information security of virtual communities in social internet services.

The work comprises 37 pages, 15 figures, 1 table, and 31 references.

Keywords: Resilience, virtual communities, social internet services, information security, synthesis.

## ЗМІСТ

|                                                                                                                          |           |
|--------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>ВСТУП .....</b>                                                                                                       | <b>6</b>  |
| <b>РОЗДІЛ 1 АНАЛІЗ СТАНУ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ .....</b>                                                  | <b>7</b>  |
| 1.1 Аналіз ролі і місця резильєнтності віртуальної спільноти у забезпеченні інформаційної безпеки.....                   | 7         |
| 1.2 Аналіз методів вимірювання та моделювання резильєнтності .....                                                       | 10        |
| 1.3 Систематизація факторів, які впливають на резильєнтність .....                                                       | 13        |
| Висновки до першого розділу .....                                                                                        | 15        |
| <b>РОЗДІЛ 2 РОЗРОБЛЕННЯ МЕТОДУ СИНТЕЗУ РЕЗИЛЬЄНТНОЇ ВІРТУАЛЬНОЇ СПІЛЬНОТИ.....</b>                                       | <b>16</b> |
| 2.1 Подальший розвиток методу оцінки резильєнтності віртуальної спільноти у соціальних інтернет-сервісах .....           | 16        |
| 2.2 Сценарне моделювання впливу загроз віртуальним спільнотам.....                                                       | 21        |
| Висновки до другого розділу .....                                                                                        | 23        |
| <b>РОЗДІЛ 3 ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ МЕТОДУ СИНТЕЗУ РЕЗИЛЬЄНТНИХ ВІРТУАЛЬНИХ СПІЛЬНОТ .....</b>                      | <b>24</b> |
| 3.1 Дослідження впливу резильєнтності на інформаційну безпеку віртуальної спільноти в соціальних інтернет-сервісах ..... | 24        |
| 3.2 Оцінка ефективності покращеного методу підвищення інформаційної безпеки віртуальної спільноти .....                  | 28        |
| Висновки до третього розділу .....                                                                                       | 31        |
| <b>ВИСНОВКИ.....</b>                                                                                                     | <b>32</b> |
| <b>СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ .....</b>                                                                              | <b>33</b> |
| <b>ДОДАТКИ .....</b>                                                                                                     | <b>36</b> |
| Додаток А .....                                                                                                          | 36        |

## ВСТУП

**Актуальність теми.** Синтез резильєнтних віртуальних спільнот в соціальних інтернет-сервісах має важливе значення у забезпечення інформаційної безпеки. В умовах інформаційних та когнітивних війн, постає проблема швидкої адаптації віртуальних спільнот, з метою підвищення ступеня інформаційної безпеки. Діджиталізація процесів нашого життя зумовлює постійний розвиток соціальних інтернет-сервісів, ріст користувачів та створенню нових віртуальних спільнот. Існуючі методи вимірювання та моделювання резильєнтності не враховують всього спектру факторів, які мають на неї вплив.

**Метою роботи** є підвищення інформаційної безпеки в соціальних інтернет-сервісах шляхом синтезу резильєнтних віртуальних спільнот.

**Об'єктом дослідження** є процес функціонування віртуальних спільнот в соціальних інтернет сервісах.

**Предметом дослідження** є методи синтезу резильєнтних віртуальних спільнот в соціальних інтернет-сервісах.

**Наукова новизна** роботи полягає у тому, що набув подальшого розвитку метод синтезу резильєнтних віртуальних спільнот у соціальних інтернет-сервісах, який відрізняється від відомих врахуванням соціального, технічного, організаційного, комунікаційного та інформаційного доменів, що дозволило підвищити рівень їх інформаційної безпеки.

За темою кваліфікаційної роботи було опубліковано наукову публікацію (статтю):

– Лаптев, О. А., Колесник, В. В., Ровда, В. В., & Половінкін, М. І. (2024). Метод підвищення захисту особистих даних за рахунок синтезу резильєнтних віртуальних спільнот. Сучасний захист інформації, 4(60), 152–157.

## **РОЗДІЛ 1 АНАЛІЗ СТАНУ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ**

### **1.1 Аналіз ролі і місця резильєнтності віртуальної спільноти у забезпеченні інформаційної безпеки**

Синтез резильєнтних віртуальних спільнот у соціальних інтернет-сервісах має велике значення, особливо в умовах повномасштабної війни Росії проти України та підкреслює їх критичну роль у сприянні соціальній єдності, обміну ресурсами та емоційній підтримці населення. Інформаційна та когнітивна війна зумовила необхідність швидкої адаптації спільнот до віртуальних середовищ, використовуючи цифрові інструменти для підтримки зв'язків та сприяння колективним діям.

Віртуальна спільнота – це об'єднання акторів у віртуальному просторі, де люди зі спільними інтересами та цілями об'єднуються для взаємодії, комунікації та співпраці [1]. Дані спільноти використовують веб платформи для сприяння соціальним зв'язкам та обміну інформацією, часто перевершуючи географічні межі міста, країни чи навіть материка. Таким чином, віртуальні спільноти виконують різноманітні функції, включаючи соціальну підтримку, обмін інформацією та спільне вирішення проблем. Віртуальні спільноти є наслідком еволюції соціальних комунікацій, що характеризується формуванням онлайн груп, де індивіди зі спільними інтересами, цілями або баченням, беруть участь у комунікації та співпраці[1]. Ці спільноти можуть мати різні форми, включаючи форуми, групи в соціальних інтернет-сервісах та платформи, кожна з яких сприяє унікальній динаміці та взаємодії між учасниками. Особливість віртуальних спільнот полягає в їх здатності створювати відчуття належності та сприяти соціальним зв'язкам, навіть за відсутності взаємодії у реальному світі.

Кожна віртуально спільнота в соціальних інтернет-сервісах має певну кількість акторів та зв'язків між ними. Зв'язки можуть бути перенесені з реального світу та створені безпосередньо у віртуальній спільноті. Структуру віртуальної спільноти можна показати у вигляді графової моделі (Рис. 1.1).

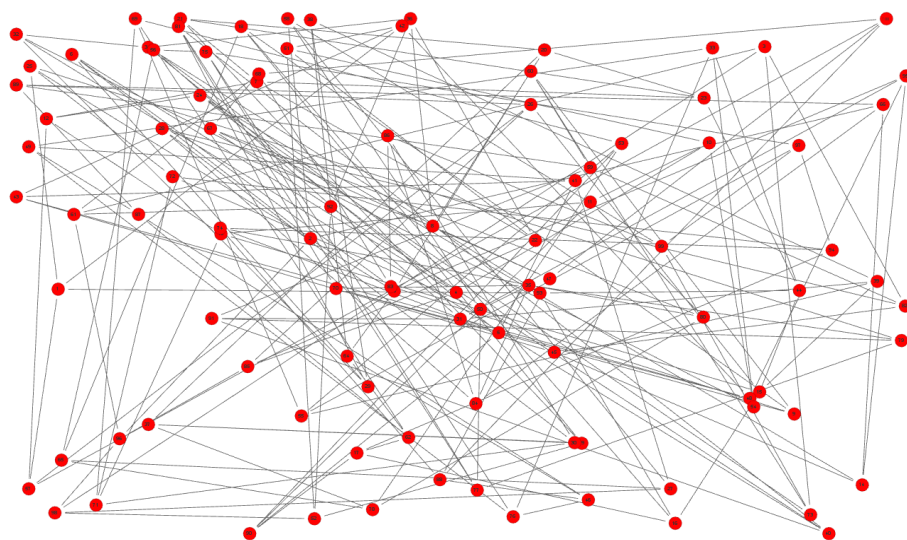


Рис. 1.1 – Графова модель віртуальної спільноти

Щільність зв'язків вказує на потенційну здатність спільноти зберігати функціональність під час кризи, але вона також є вразливістю. Ідентифікація ключових вузлів допомагає визначити, які учасники можуть сприяти відновленню чи адаптації (Рис. 1.2). Розірвані зв'язки або ізольовані вузли свідчать про групи, які менш інтегровані й можуть стати джерелом ризиків для загальної стабільності.

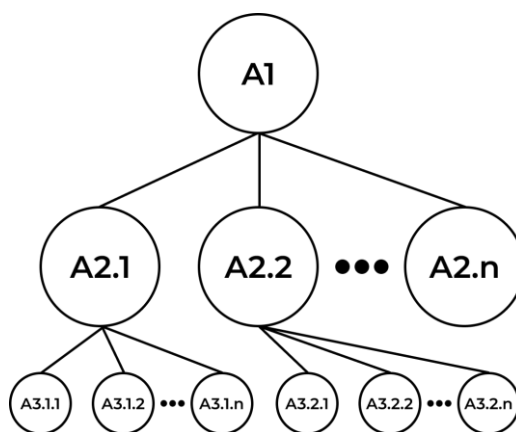


Рис. 1.2– Модель взаємозв'язків у віртуальній спільноті

На Рис. 1.2 представлено моделі зв'язків має ризик виникнення каскадного ефекту. У разі настання кризи, існує ризик, що певні актори покинуть віртуальну спільноту, забравши з собою акторів, на яких мають безпосередній вплив, визначений вагою зв'язків між ними. Віртуальні спільноти керуються принципом самоорганізації зв'язків між акторами, їх створенням та знищенням [2]. Віртуальні спільнотам властивий розвиток без чіткої ієрархії чи формального управління. Роль самоорганізації у резильєнтності постає у допоміжній здатності відновлюватися

після кризових ситуацій, за рахунок пришвидшення процесу збору ресурсів, пошуків і локалізації уражених ділянок системи. У динамічному цифровому середовищі, де загрози можуть включати технічні збої, зовнішні атаки або внутрішні конфлікти, самоорганізація стає фундаментальним механізмом для виживання і сталого розвитку спільноти [2].

Резильєнтність у віртуальній спільноті в соціальних інтернет-сервісах визначається її здатністю протистояти зовнішнім та внутрішнім загрозам, адаптуватися до змін, підтримувати стабільність та функціонування в умовах кризових ситуацій [3]. Одним із основних методів підвищення резильєнтності віртуальних спільнот під час війни між Росією та Україною стало використання соціальних інтернет-сервісів, соціальних медіа, месенджерів та онлайн-платформ для сприяння комунікації і координації серед населення. соціальні інтернет-сервіси можуть посилювати ефективність окремих осіб і спільнот, надаючи простір для організації відповідей на кризові ситуації та поширення критично важливої інформації [4]. Наприклад, під час війни між Росією та Україною платформи, такі як Facebook, Instagram, Discord та Telegram, відіграли ключову роль у поширенні оновлень у реальному часі, мобілізації підтримки та зміцненні солідарності серед людей. Ці платформи слугують не лише каналами для обміну інформацією, а й просторами для емоційної підтримки, де люди можуть ділитися своїм досвідом і стратегіями подолання труднощів, що сприяє зміцненню зв'язків у спільноті [3].

Ключовою властивістю резильєнтної віртуальної спільноти є здатність відновлюватися після атак, збоїв, змін у складі учасників або навіть змін у технологічній платформі. Аспектами резильєнтності у віртуальній спільноті є:

- стійкість до внутрішніх та зовнішніх загроз;
- адаптивність;
- відновлення функціональності;
- забезпечення наявності мінімальної точки відновлення системи;
- стабільність соціальних зв'язків.

Роль резильєнтності у віртуальних спільнотах підкреслюється їхньою здатністю сприяти колективним діям та мобілізації ресурсів під час реагування на

кризи та відновленні після них. Віртуальні спільноти стали важливими мережами для збору коштів та ініціатив підтримки, що дозволяє окремим особам робити внесок у гуманітарні зусилля та допомагати тим, хто цього потребує[5]. Такий перехід до цифрового збору коштів і залучення спільнот набули значущості під час криз, дозволяючи спільнотам адаптуватися та ефективно реагувати на виклики, спричинені війною. Крім того, створення віртуальних спільнот сприяє обміну знаннями та спільному вирішенню проблем, що є важливими для побудови резильєнтності в умовах негараздів [6].

Резильєнтність також визначають фактори технологічних інновацій, модерації всередині віртуальної спільноти та соціальної згуртованості [7]. Роль технічної частини системи спільноти має не менше значення, ніж соціальна. Забезпечення інтероперабельності у технічній та соціальній частині віртуальної спільноти підвищують її загальну резильєнтність [6-8].

## **1.2 Аналіз методів вимірювання та моделювання резильєнтності**

Резильєнтність віртуальних спільнот характеризує їхню здатність протистояти соціальним, технічним та інформаційним загрозам, зберігати функціональність під час кризи та швидко відновлюватися після збоїв [8]. Розуміння цієї властивості важливе для побудови довготривалої стабільності, підтримки довіри та взаємодії між користувачами. Загалом існує два типи резильєнтності у віртуальних спільнотах: жорстка резильєнтність (Hard Resilience) та м'яка резильєнтність (Soft resilience)[9-10].

У контексті віртуальних спільнот в соціальних інтернет-сервісах жорстка резильєнтність присутня під час реалізації технічних засобів, а саме:

- Багаторівнева автентифікація;
- шифрування даних та каналів комунікацій;
- резервні копії;
- зберігання конфіденційності.

М'яка резильєнтність відображається у соціальних факторах віртуальної спільноти:

- Згуртованість віртуальної спільноти;
- адаптивність платформи;
- швидке реагування на кризові ситуації;
- можливість своєчасного оновлення політик безпеки.

Резильєнтність є критичною характеристикою комплексних систем, яка дозволяє їм не лише знижувати втрати під час криз, але й покращувати свою стійкість завдяки адаптації до отриманого досвіду [11]. Кожній віртуальній спільноті властивий свій рівень резильєнтності, від низького до високого. Резильєнтність, як невід'ємна властивість системи, завжди присутня та впливає на час, який потрібний на відновлення до початкового стану, перед настанням кризи (Рис. 1.3)

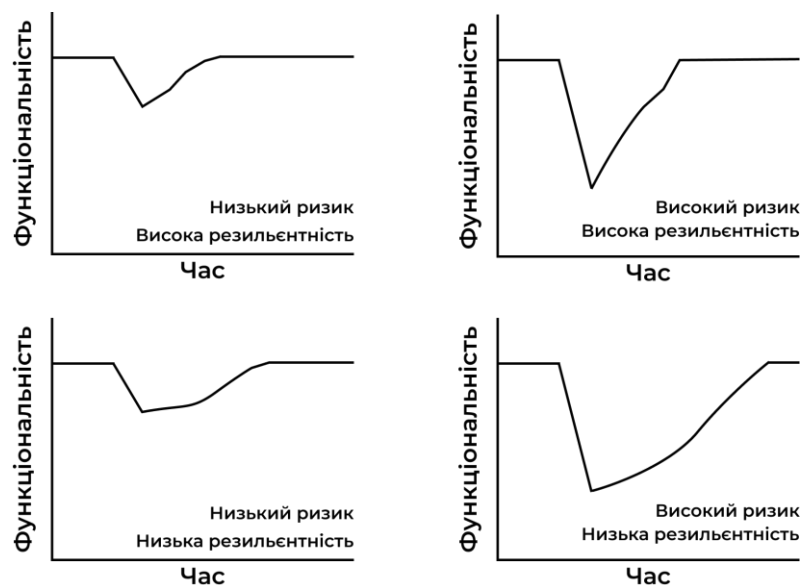


Рис. 1.3 – Час, потрібний на відновлення за різних комбінацій ризиків та резильєнтності

Дані для графіків, представлених на Рис. 1.3, взято на основі дослідження І. Лінкова[11]. Графік ілюструє чотири сценарії, які виникають в залежності від поєднання рівнів ризику та резильєнтності. У залежності від комбінацій, змінюється час, потрібний на відновлення функціональності віртуальної спільноти.

Телескопічна модель використовується для оцінки ризиків резильєнтності[12] системи. З метою вимірювання резильєнтності віртуальної спільноти в соціальних інтернет-сервісах дану модель можна використовувати на трьох рівнях (Рис.1.4).

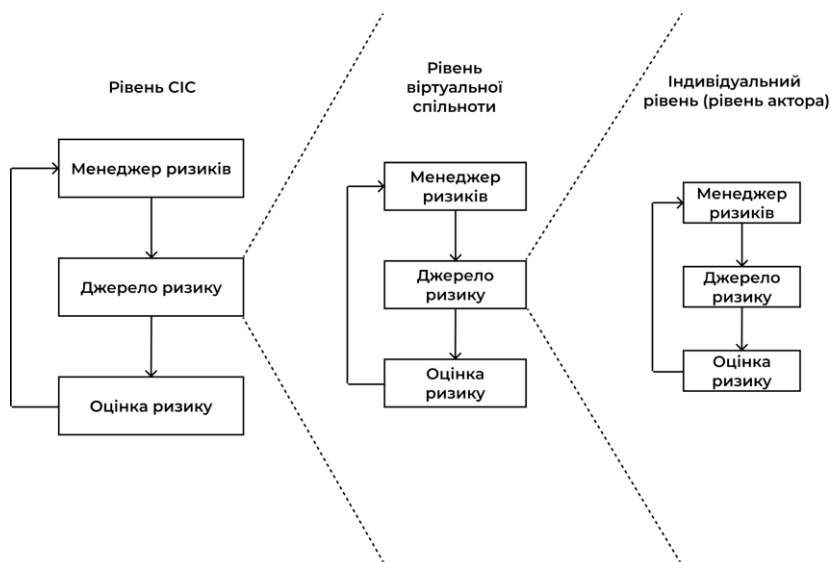


Рис. 1.4 – Телескопічна модель віртуальної спільноти

Глобальний рівень призначений для ризиків усієї віртуальної спільноти під час кризи. Груповий рівень відповідає за взаємодію між акторами у групах, чатах тощо. Індивідуальний рівень існує для менеджменту поведінки та дій окремого актора.

Модель життєздатної системи (Viable Systems Model) забезпечує структуру для аналізу управління платформою[12]. У соціальних інтернет-сервісах, дана модель показує, як система забезпечує стабільність, адаптацію та контроль у взаємодії з середовищем, яке складається з поточних і майбутніх умов (Рис.1.5).

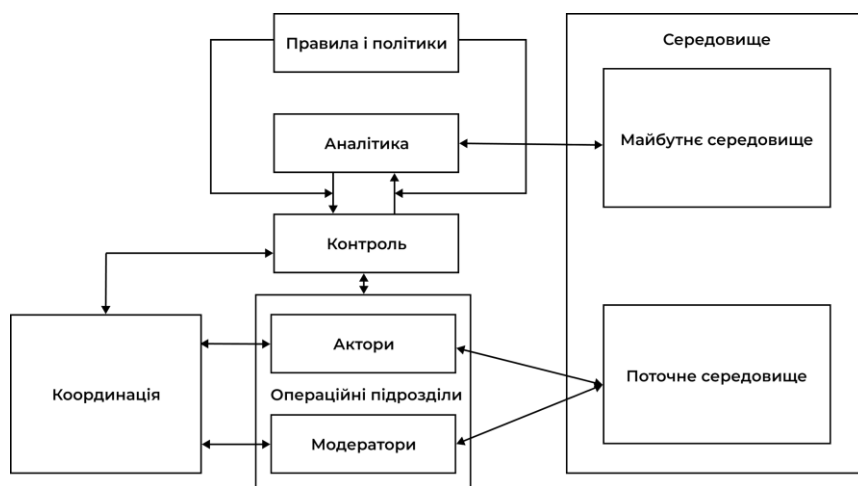


Рис. 1.5 – Модель життєздатної системи віртуальної спільноти

На рис. 1.5 представлена модель використовується для управління всією віртуальною спільнотою. Вона не підходить для здійснення управління на мікрорівні (рівні актора) та на макрорівні (рівень соціальних інтернет-сервісів).

### 1.3 Систематизація факторів, які впливають на резильєнтність

Кожна віртуальна спільнота є комплексною системою. Систематизувати віртуальну спільноту запропоновано за допомогою доменного підходу, враховуючи 5 доменів і їх піддомени. Домен розглядається як область, яка моделюється для інтеграції знань і принципів, необхідних для керування складними системами [13]. У процесі дослідження факторів резильєнтності віртуальних спільнот у соціальних інтернет-сервісах важливо розглянути кожний її аспект та визначити вплив на загальну систему (Рис. 1.3).

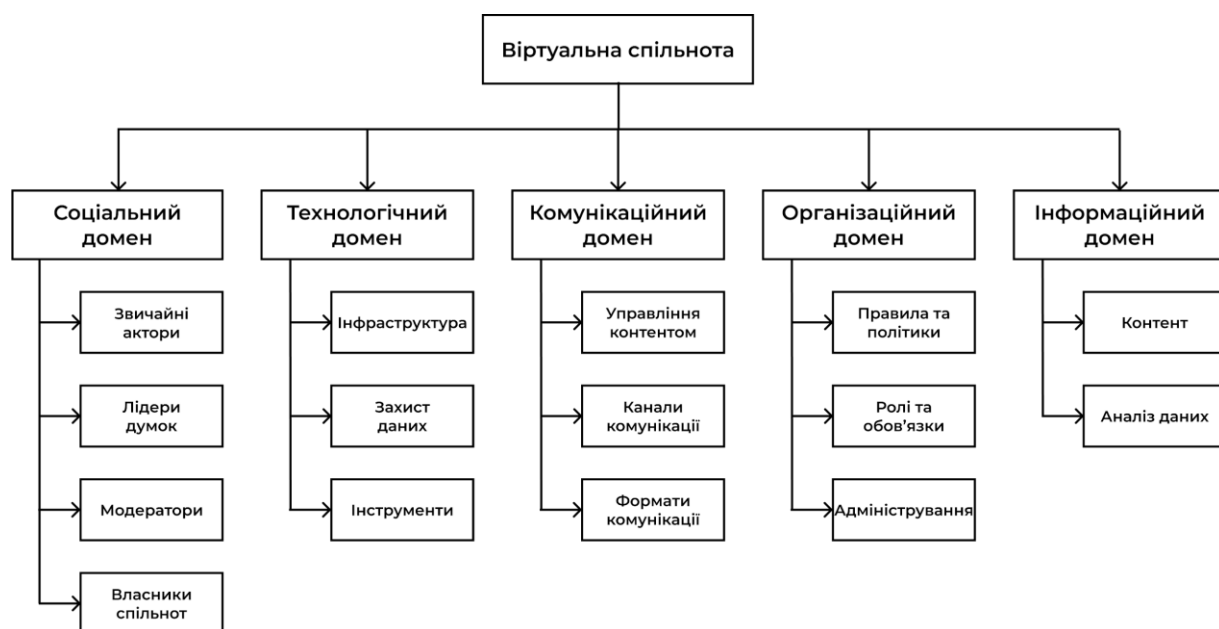


Рис. 1.6 – Доменний підхід систематизації віртуальної спільноти

Кожен домен структури віртуальної спільноти здійснює позитивний або негативний вплив на резильєнтність (Таблиця А.1). Завжди існує ризик реалізації певної загрози для кожного компонента віртуальної спільноти. Тому важливо враховувати наслідки для резильєнтності віртуальної спільноти в соціальних інтернет-сервісах від її складових компонентів. Як і в будь-якій системі, яка має певну кількість акторів і не є закритою, постійно відбувається зміна ролей та ступенів впливу в ієрархії акторів віртуальної спільноти [7]. Дані зміни несуть ризики для резильєнтності різного ступеня, в залежності від впливу одного актора на інших та ваги його зв'язків у віртуальній спільноті.

Резильєнтність у віртуальній спільноті має три основних компонента: адсорбційну здатність, адаптивність та відновлювальну здатність[9]. Абсорбційна

здатність описує наскільки віртуальна спільнота здатна поглинати наслідки деструктивних подій. Адаптивність впливає на атрибути віртуальної спільноти, а саме на змінювання правил, структури, процесів тощо у відповідь на кризові ситуації. Відновлювальна здатність відповідає за швидкість та ефективність (як правило, розуміють вартість відновлення) повернення віртуальної спільноти до нормального функціонування, яке було до настання кризової ситуації.

До метрик оцінки резильєнтності віртуальної спільноти можна віднести:

- Час відновлення після кризової ситуації;
- рівень відновлення;
- абсорбційна здатність.

Час відновлення є однією з ключових метрик для оцінки резильєнтності віртуальних спільнот. Він відображає період, необхідний для повернення спільноти або платформи до нормального функціонування після кризи [10]. У контексті віртуальних спільнот це включає час, потрібний для відновлення доступу до соціальних інтернет-сервісів після технічного збою, стабілізації дискусій після конфлікту між користувачами, або усунення негативних наслідків, таких як поширення фейкових новин чи кібербулінгу. Успішне скорочення цього часу демонструє здатність платформи ефективно реагувати на загрози.

Рівень відновлення вимірює, наскільки повноцінно віртуальна спільнота або соціальний інтернет-сервіс відновлюється після кризи, у порівнянні з початковим станом [10]. Це включає як якісні, так і кількісні показники. Наприклад, частку користувачів, які повернулися до активності після інциденту, відновлення довіри до соціальних інтернет-сервісів або повернення до нормальної взаємодії між акторами віртуальної спільноти. Високий рівень відновлення означає, що платформа не тільки повернула свої основні функції, але й змогла відновити довіру акторів, утримати активну аудиторію та забезпечити стабільне середовище для взаємодії.

Абсорбційна здатність оцінює спроможність віртуальної спільноти або соціального інтернет-сервісу поглинати негативний вплив кризової ситуації без істотного зниження функціональності [9-12]. Ця метрика характеризує, наскільки

система здатна продовжувати працювати під час кризи, навіть якщо її продуктивність або якість обслуговування частково знижуються. Наприклад, у випадку масового поширення шкідливого контенту система з високою абсорбційною ефективністю буде здатна швидко ідентифікувати та видалити такий контент, мінімізуючи його вплив на користувачів і загальну динаміку віртуальної спільноти. Абсорбційна здатність також враховує, наскільки ресурси (наприклад, модератори або алгоритми) використовуються для нейтралізації впливу кризи, без потреби в екстреній зупинці роботи платформи.

### **Висновки до першого розділу**

Визначено поняття резильєнтності віртуальних спільнот та окреслено її основні аспекти: захисні механізми, реакція на загрози, адаптивність, стабільність соціальних зв'язків і ефективність підтримки.

Наведено приклад співвідношення рівнів ризику та резильєнтності віртуальної спільноти під час настання кризової ситуації. Представлена графова модель віртуальної спільноти. Описано методи моделювання та вимірювання резильєнтності віртуальних спільнот у соціальних інтернет-сервісах, а також проведено їх систематизацію за допомогою доменного підходу.

Актуальність дослідження зумовлена значущістю віртуальних спільнот у соціальних інтернет-сервісах для соціальної згуртованості, обміну ресурсами та підтримки в кризових умовах, зокрема під час війни. Формування резильєнтних спільнот забезпечує ефективну комунікацію, координацію дій і стабільність в умовах викликів, сприяючи інформаційній безпеці в динамічному середовищі.

## РОЗДІЛ 2 РОЗРОБЛЕННЯ МЕТОДУ СИНТЕЗУ РЕЗИЛЬЄНТНОЇ ВІРТУАЛЬНОЇ СПІЛЬНОТИ

### 2.1 Подальший розвиток методу оцінки резильєнтності віртуальної спільноти у соціальних інтернет-сервісах

З метою поглибленого дослідження резильєнтності віртуальної спільноти в соціальних інтернет-сервісах, варто визначити та обґрунтувати фактори, що її забезпечують. Резильєнтність є комплексною властивістю віртуальної спільноти. Вона складається з великої кількості компонентів, кількість яких переважно визначає напрямок діяльності віртуальної спільноти, або її розміри і кількість зв'язків між акторами.

Розроблення моделі віртуальної спільноти вимагає ґрунтовного розуміння факторів резильєнтності, які є основою цих спільнот. Соціальний домен є фундаментальним елементом у зміцненні резильєнтності віртуальних спільнот. Він сприяє індивідуальному внеску та посилює соціальну підтримку у віртуальних спільнотах [14] Розвиток соціальної підтримки як у реальних, так і у віртуальних середовищах є вирішальним для підтримання резильєнтності спільнот[15]. Здатність розвивати соціальні відносини та мережі у цих спільнотах не лише забезпечує емоційну підтримку, але й підсилює обмін ресурсами, що є надзвичайно важливим у періоди криз.

Кожен домен віртуальної спільноти виконує специфічну функцію, впливаючи на резильєнтність системи та протистоїть викликам (Таблиця 2.1).

Таблиця 2.1 – Ролі та виклики доменів віртуальної спільноти

| Домен         | Роль у системі                                                                | Основні виклики                                                 |
|---------------|-------------------------------------------------------------------------------|-----------------------------------------------------------------|
| Соціальний    | Формування зв'язків між акторами, підтримка соціальної згуртованості          | Розірвані зв'язки, зниження довіри, переманювання акторів, боти |
| Технологічний | Інфраструктура для функціонування соціальних інтернет-сервісів, безпека даних | Технічні збої, кібератаки                                       |
| Комунікаційни | Забезпечення взаємодії через канали                                           | Неправильний вибір каналів,                                     |

|                |                                                        |                                                                                      |
|----------------|--------------------------------------------------------|--------------------------------------------------------------------------------------|
| й              | зв'язку, форматування інформації                       | деструктивний контент, проблеми з доступом до каналів зв'язку                        |
| Організаційний | Регуляція правил та політик, управління ролями акторів | Перевищення повноважень, неправильний розподіл ролей, недотримання правил та політик |
| Інформаційний  | Створення та розповсюдження контенту                   | Дезінформація, втрата довіри до даних                                                |

У даному дослідженні [16], віртуальна спільнота розглядається як соціо-технічна система. Резильєнтність створюється за рахунок соціального та технічного доменів. Доцільно врахувати також організацій, комунікаційний та інформаційний домен. Вплив на резильєнтність соціального домену можна зобразити за допомогою рівняння динаміки соціальних зв'язків  $\frac{dS(t)}{dt}$  обчисливши інтегральний показник відношення зв'язків до одиниці часу.

$$\frac{dS(t)}{dt} = \lambda N(t) - \mu S(t), \quad (2.1)$$

де  $S(t)$  – кількість активних соціальних зв'язків у момент часу  $t$  (од.);

$N(t)$  – кількість учасників спільноти у момент часу  $t$  (од.);

$\lambda$  – швидкість утворення нових зв'язків ( $\frac{\text{к-сть утворених зв'язків}}{\text{годину}}$ );

$\mu$  – швидкість розриву зв'язків ( $\frac{\text{к-сть розірваних зв'язків}}{\text{годину}}$ ).

$\lambda N(t)$  – описує зростання кількості зв'язків завдяки новим учасникам;

$\mu S(t)$  – враховує зникнення зв'язків через пасивність або вихід учасників.

Якщо  $\lambda > \mu$ , соціальний домен сприяє зростанню резильєнтності, збільшуючи згуртованість спільноти. У випадку, коли  $\mu > \lambda$ , соціальні зв'язки поступово слабшають, що знижує здатність до координації та підтримки, послаблюючи резильєнтність віртуальної спільноти.

Технічний домен відповідає за доступність акторів до віртуальної спільноти у соціальних інтернет-сервісах. Рівняння доступності можна зобразити у вигляді

інтегрального показника, наступним чином в межах  $\frac{dA(t)}{dt}$  від  $[0;1]$ , де 0 – відсутність доступу, 1 – повна доступність:

$$\frac{dA(t)}{dt} = \eta(1 - A(t)) - \theta A(t) + \kappa(L(t) - A(t)), \quad (2.2)$$

де  $A(t)$  – рівень доступності платформи у момент часу  $t$ ;

$\eta$  – швидкість відновлення після технічного збою (год.);

$\theta$  – швидкість виникнення технічних збоїв (год.);

$\kappa$  – ступінь адаптивності системи до змінних навантажень ( $\frac{\kappa\text{-сть запитів}}{\text{годину}}$ );

$\eta(1-A(t))$  – відновлення доступності після збою;

$\theta A(t)$  – зниження доступності через технічні проблеми;

$\kappa(L(t)-A(t))$  – адаптація системи до навантаження  $L(t)$ ;

$L(t)$  – поточний рівень запитів користувачів, лежить в межах  $[0;1]$ , де 0 – запити відсутні, 1 – кількість запитів перевищила пропускну здатність сервера.

Поведінка системи здатна змінюватися залежно від параметрів:

- система з високою швидкістю відновлення ( $\eta \gg \theta$ ). Навіть за частих збоїв платформа швидко відновлює свою функціональність, що значно підвищує її резильєнтність;

- система з низьким рівнем адаптації ( $\kappa \approx 0$ ). Система не здатна ефективно реагувати на зростання навантаження  $L(t)$ , що призводить до тривалих перебоїв у роботі. Помітно знижує резильєнтність;

- перевантаження системи ( $L(t) \gg 1$ ). Значне збільшення запитів користувачів без достатньої адаптації ( $\kappa$ ) здатне викликати колапс технічного домену, коли  $A(t) \rightarrow 0$ .

На технологічний домен також впливає період активності акторів віртуальної спільноти. В залежності від цільової аудиторії, пік активності має властивість коливатися. Якщо навантаження  $L(t)$  змінюється періодично (наприклад, денний і нічний цикл активності акторів), то його зміну можна змоделювати наступним чином:

$$L(t) = L_0 + L_1 \sin(\omega t), \quad (2.3)$$

де  $L_0$  — середнє навантаження ( $\frac{\text{К-сть запитів (24 години)}}{24}$ );

$L_1$  — амплітуда коливань ( $\frac{\text{К-сть запитів}}{\text{годину}}$ );

$\omega$  — частота коливань.

Організаційний домен відповідає за дотримання правил та політик віртуальної спільноти в соціальних інтернет-сервісах, її структуру та визначає ролі акторів. Для моделювання динаміки рівня дотримання правил організаційного домену потрібно врахувати три ключових параметра:

1.  $C(t)$  — рівень дотримання правил, лежить в межах  $[0;1]$ , де 0 — абсолютне недотримання правил, 1 — повне дотримання правил;

2.  $\alpha$  — ефективність управління ( $\frac{\text{К-сть локалізованих правопорушень}}{\text{годину}}$ );

3.  $\beta$  — частота порушень ( $\frac{\text{К-сть порушень}}{\text{годину}}$ ).

Рівняння має г вигляд:

$$\frac{dC(t)}{dt} = \alpha(1 - C(t)) - \beta C(t), \quad (2.4)$$

де  $\alpha(1-C(t))$  — зусилля модераторів та адміністраторів для покращення дотримання правил;

$\beta C(t)$  — зменшення стабільності через порушення правил.

Якщо  $\alpha > \beta$ , рівень дотримання правил зростає з часом, досягаючи стабільного стану. У разі  $\beta > \alpha$ , система деградує і рівень дотримання правил падає. Вплив організаційного домену на резильєнтність віртуальної спільноти в соціальних інтернет-сервісах збільшується, залежно від кількості акторів спільноти. Модераторам та адміністраторам стає складно контролювати велику кількість акторів, та своєчасно реагувати на порушення.

$$\frac{dC(t)}{dt} = \frac{\alpha_0(M + \sigma A)}{1 + \kappa N(t)} (1 - C(t)) - \beta_0 U C(t), \quad (2.5)$$

де  $M$ ,  $A$ ,  $U$  — кількість модераторів, адміністраторів і акторів відповідно (одиниць);  $N(t)$  — кількість учасників ( $M+A+U$ ) у момент часу  $t$ ;

$\alpha_0$  – базова ефективність модерації,  $(\frac{\text{к-сть локалізованих правопорушень}}{\text{годину}})$ ;

$\beta_0$  – базова частота порушень звичайних акторів (U),  $(\frac{\text{к-сть порушень } U}{\text{годину}})$ ;

$\sigma$  – коефіцієнт впливу адміністраторів (A) на загальну ефективність управління;

$\kappa$  – коефіцієнт, що показує, як зростання учасників знижує ефективність управління.

Через інформаційний домен забезпечується створення, розповсюдження та перевірка контенту. В умовах кризи чи інформаційних атак резильєнтність інформаційного домену визначає здатність спільноти до адаптації та стабільності. Математично організаційний домен можна зобразити наступним чином:

$$\frac{dI(t)}{dt} = C(t) + \gamma I(t) - \delta F(t), \quad (2.6)$$

де  $I(t)$  – кількість перевіреної інформації в системі у момент часу  $t$  (к-сть од., контент);

$C(t)$  – рівень створення нового контенту  $(\frac{\text{к-сть контенту}}{\text{годину}})$ ;

$F(t)$  – обсяг фейкового контенту (к-сть од., фейковий контент);

$\gamma$  – швидкість перевірки контенту,  $(\frac{\text{загальна к-сть перевіреного контенту}}{\text{годину}})$ ;

$\delta$  – швидкість поширення фейкової інформації  $(\frac{\text{к-сть фейкового контенту}}{\text{годину}})$ ;

$C(t)$  – новий контент, який створюється учасниками (включає перевірений і неперевірений контент),  $(\frac{\text{Контент}}{\text{годину}})$ ;

Комунікаційний домен визначає, наскільки ефективно відбувається обмін інформацією між акторами віртуальної спільноти. Він включає в себе канали зв'язку, формати передачі інформації, механізми модерації контенту і доступність до інструментів взаємодії. Резильєнтність комунікаційного домену забезпечує злагоджену роботу всієї спільноти, особливо під час криз чи зовнішніх атак. Представити математичну модель комунікаційного домену можна наступним чином:

$$\frac{dM(t)}{dt} = \zeta(1 - M(t)) - \xi \frac{L(t)}{N(t)} M(t), \quad (2.7)$$

де  $M(t)$  – рівень ефективності комунікації у момент часу  $t$ , лежить в межах  $[0;1]$ , 0 – комунікації немає, 1 – постійна комунікація;

$\zeta$  – швидкість покращення комунікації через налаштування каналів,  $(\frac{\text{К-сть каналів}}{\text{годину}})$ ;

$\xi$  – зниження ефективності через перевантаження каналів  $(\frac{\text{К-сть запитів на 1 канал}}{\text{годину}})$ ;

$N(t)$  – кількість акторів, що активно використовують канали зв'язку (к-сть од.);

$L(t)$  – рівень навантаження на комунікаційну інфраструктуру;

$\zeta(1-M(t))$  – зростання ефективності завдяки налаштуванню каналів.

$\xi \frac{L(t)}{N(t)} M(t)$  – зниження ефективності через перевантаження.

Сумарну резильєнтність  $R(t)$  віртуальної спільноти описано як інтеграції впливів усіх доменів, у вигляді інтегральної безрозмірної величини:

$$R(t) = \prod_{i=1}^n [X_i(t)]^{w_i}, \quad (2.8)$$

де  $X_i(t)$  — значення резильєнтності кожного домену в момент часу  $t$ ;

$w_i$  — вагові коефіцієнти важливості доменів;

$n$  — кількість доменів.

Така модель дозволяє оцінити загальну резильєнтність віртуальної спільноти в соціальних інтернет-сервісах та виявити "вузькі місця", які потребують уваги, за допомогою використання доменного підходу.

## 2.2 Сценарне моделювання впливу загроз віртуальним спільнотам

Існує велика кількість потенційних сценаріїв впливу на віртуальні спільноти. Здійснювати даний вплив можна з різними цілями, наприклад:

- знищення віртуальної спільноти;
- крадіжка даних;
- переманювання акторів;
- нав'язування фальшивих цілей;
- перевірка потенційних атак на вразливості тощо.

Описані можливі комбінації ризиків та резильєнтності на Рис. 1.3 дозволяють створити 4 потенційні сценарії впливу на віртуальну спільноту у соціальних інтернет-сервісах.

Ідеальний сценарій (низький ризик – висока резильєнтність). Можлива реалізація сценарію, коли віртуальна спільнота функціонує у стабільному середовищі, технологічна інфраструктура не пошкоджена, соціальні зв'язки акторів є згуртованими. Можливі загрози швидко нейтралізуються, відновлення функціонування віртуальної спільноти проходить за мінімальний час. Більшість акторів можливо не помітить збоїв у функціонування віртуальної спільноти.

Сценарій стабільної адаптації (високий ризик – висока резильєнтність). Віртуальна спільнота під час такого сценарію стикається з серйозними загрозами для подальшого функціонування (можливі кібератаки, інформаційні загрози, виклики довіри акторів тощо). Помітні збої, проблеми з доступом, зниження активності та продуктивності віртуальної спільноти, соціального інтернет-сервісу, або їх комбінації. За рахунок високої резильєнтності можливо швидко повернутися на рівень докризового функціонування та здійснити абсорбцію такого впливу.

Сценарій поступової деградації (низький ризик – низька резильєнтність). Проблема даного сценарію в тому, що для функціонування віртуальної спільноти не існує серйозних викликів, які могли б спричинити кризи, після яких неможливо здійснити відновлення до попереднього рівня, але і рівень резильєнтності залишається мінімальним. Прикладами таких спільнот можуть бути невеликі об'єднання акторів, які не мають достатньої інфраструктури, між ними слабкі соціальні зв'язки, не здійснюється достатнє управління і тд. Відповідь – такі спільноти просто не цікаві для здійснення різних впливів на них та не несуть в собі потенційного впливу на інші спільноти, платформи, економіку тощо. Із часом вони поступово самі деградують до того рівня, що перестануть функціонувати.

Критичний колапс (високий ризик – низька резильєнтність). Віртуальна спільнота приймає серйозні виклики для свого функціонування. Низька резильєнтність викликає помітне зниження активності акторів, потенційну втрату

ключових акторів спільноти. Як наслідок, віртуальна спільнота здатна швидко припинити своє існування.

Кожний домен віртуальної спільноти здійснює позитивний або негативний вплив на резильєнтність, в залежності від того, які дії стосовно нього виконуються. Існувати віртуальна спільнота без одного і більше доменів не може. Для цього важлива наявність та працездатність усіх 5 доменів. Допускається відсутність, або проблеми з функціонуванням піддоменів.

Важливим фактором підвищення резильєнтності соціального домену віртуальної спільноти в соціальному інтернет-сервісі на протидію різним сценаріям впливу є забезпечення відчуття спільноти та єдності між акторами[17]. Вплив на технологічний домен віртуальної спільноти можна здійснити як зовні так із середини з використанням інформаційних технологій, інфраструктури чи циркулюючими даними в системі[18].

### **Висновки до другого розділу**

Набув подальшого розвитку метод оцінки резильєнтності віртуальної спільноти, який враховує соціальний, технічний, організаційний, комунікаційний та інформаційний домен. Описані властивості та вплив на резильєнтність кожного домену, що дозволяє підвищити ефективність забезпечення інформаційної безпеки віртуальних спільнот в соціальних інтернет-сервісах.

За допомогою сценарного моделювання, описано чотири потенційних сценаріїв впливу на віртуальну спільноту в соціальних інтернет-сервісах. Детально розписано їх позитивний та негативний вплив на резильєнтність. Наведено приклади таких віртуальних спільнот.

## РОЗДІЛ 3 ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ МЕТОДУ СИНТЕЗУ РЕЗИЛЬЄНТНИХ ВІРТУАЛЬНИХ СПІЛЬНОТ

### 3.1 Дослідження впливу резильєнтності на інформаційну безпеку віртуальної спільноти в соціальних інтернет-сервісах

Для дослідження впливу резильєнтності можна створити модель віртуальної спільноти за допомогою мультиагентного програмного середовища NetLogo, яка буде імітувати соціальну взаємодію та активність, створювати нові зв'язки, розривати старі, додавати та видаляти акторів (Рис. 3.1). Кожен актор має принаймні один зв'язок, максимального обмеження по кількості зв'язків немає. Таким чином можна зобразити лідерів думок, які мають більше зв'язків, у порівнянні із звичайними акторами.

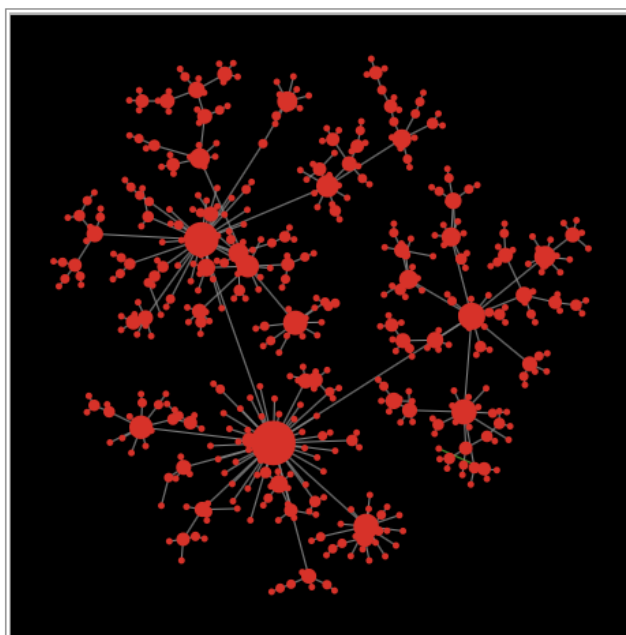


Рис. 3.1 – NetLogo. Приклад віртуальної спільноти

Для симуляції настання кризи, потрібно кожному акторові (вузол) у даній симуляції задати випадкове значення резильєнтності у межах  $[0.3;0.6]$ . Такий діапазон значень є середнім показником і дозволяє проводити симуляцію типової віртуальної спільноти у соціальних інтернет-сервісах. Значення, яке знаходиться у діапазоні  $[0;0.3)$ , вважається низьким показником резильєнтності. У разі значення резильєнтності  $(0.6;1)$  - то його доцільно вважати високим показником. Початок тестування впливу резильєнтності показано на Рис. 3.2 .

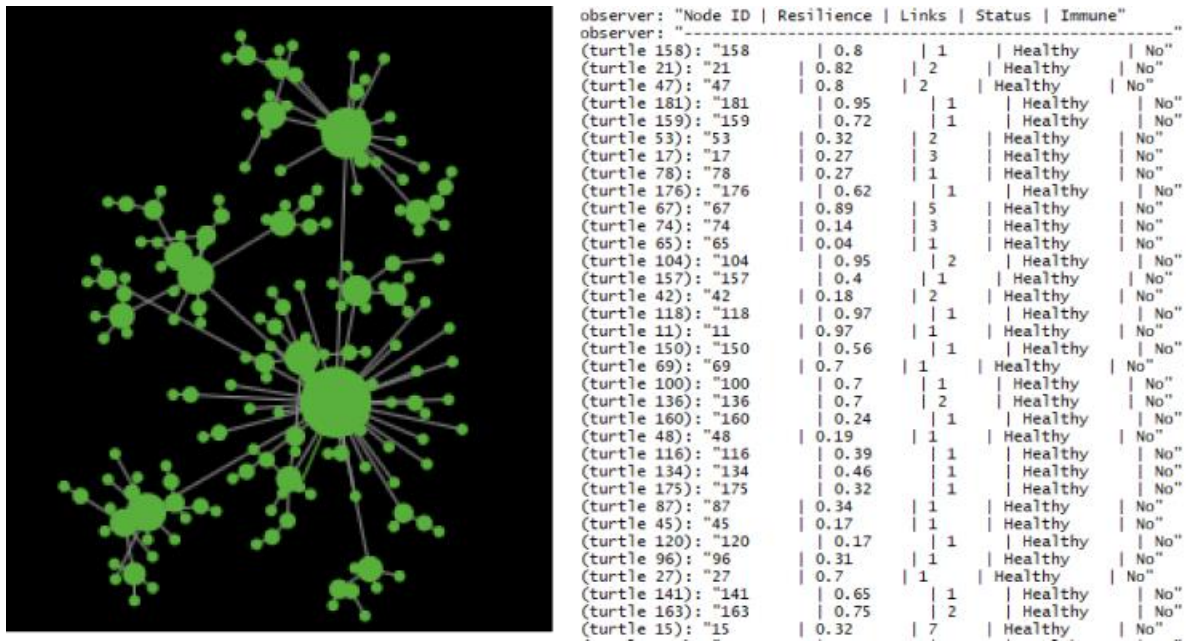


Рис. 3.2 – Початковий стан віртуальної спільноти

На Рис. 3.2 показано також таблиця властивостей для кожного вузла(актора), а саме:

1. Node ID – порядковий номер кожного вузла;
2. Resilience – обрахований інтегральний показник резильєнтності конкретного вузла;
3. Links – кількість зв'язків, які має один вузол;
4. Status – здоровий (Healthy), або заражений(Infected);
5. Immune – так або ні (Yes/No). Показник, який змінюється, якщо вузол пройшов процес кризи і завершилася абсорбція її впливу. Після чого показник No змінюється на Yes та резильєнтність цього вузла (актора) підвищується. Також він з більшим шансом повторно не може бути зараженим тим же типом атаки.

Для кращого візуального зображення, вузли (актори), які мають більшу кількість зв'язків, ніж інші, пропорційно збільшуються у розмірах. Якщо вузол (актор) зеленого кольору, то це означає, що він ще не піддавався впливу кризи, якщо червоний – криза зачепила його і він знаходиться під її впливом, синій – він зміг побороти вплив кризи та пройшов етап абсорбції.

У даній симуляції кожен вузол (актор) має випадкове значення резильєнтності, але більшість значень лежить в межах [0.3:0.6]. Такий розподіл

здійснено завдяки покращеному методу оцінки резильєнтності віртуальної спільноти у соціальних інтернет-сервісах.

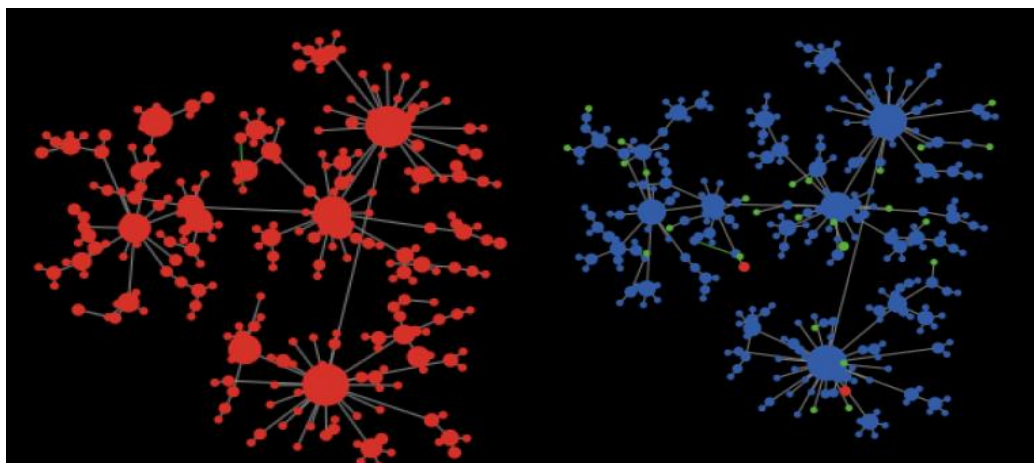
З метою подальшої симуляції, запущено процес кризи. Актори починають це відчувати і їхні значення резильєнтності та стан змінюється (Рис. 3.3). Якщо заражено актора, який має більший показник резильєнтності, ніж його сусід, з яким він має зв'язок, то резильєнтність їх обох поступово зменшується.



Рис. 3.2 – Початок кризи у віртуальній спільноті

Великі вузли імітують лідерів думок. Тобто акторів, які мають більший вплив, у порівнянні з рештою. Якщо на них здійснюється вплив, то ймовірність зараження його оточення підвищується до 95%. Існує два можливих варіанта перебігу подій (Рис. 3.3):

1. Віртуальна спільнота впоралася і подолала кризу;
2. Віртуальна спільнота перетнула точку неповернення і вплив кризи зруйнував її.



Варіант 1

Варіант 2

Рис. 3.3 – Варіанти перебігу подій

У досліджуваному випадку віртуальна спільнота змогла подолати кризу і підвищити свій рівень резильєнтності по відношенню до аналогічних впливів. Детальні показники резильєнтності кожного актора зображені на Рис. 3.4 .

| observer: "Node ID   Resilience   Links   Status   Immune" |      |    |         |      |  |
|------------------------------------------------------------|------|----|---------|------|--|
| observer: "                                                |      |    |         |      |  |
| turtle 90): "90                                            | 0.95 | 3  | Healthy | Yes" |  |
| turtle 141): "141                                          | 0.95 | 1  | Healthy | Yes" |  |
| turtle 255): "255                                          | 0.95 | 1  | Healthy | Yes" |  |
| turtle 29): "29                                            | 0.95 | 2  | Healthy | Yes" |  |
| turtle 217): "217                                          | 0.95 | 2  | Healthy | Yes" |  |
| turtle 49): "49                                            | 0.95 | 1  | Healthy | Yes" |  |
| turtle 103): "103                                          | 0.95 | 2  | Healthy | Yes" |  |
| turtle 7): "7                                              | 0.95 | 5  | Healthy | Yes" |  |
| turtle 208): "208                                          | 0.95 | 1  | Healthy | Yes" |  |
| turtle 88): "88                                            | 0.95 | 3  | Healthy | Yes" |  |
| turtle 148): "148                                          | 0.95 | 2  | Healthy | Yes" |  |
| turtle 173): "173                                          | 0.95 | 1  | Healthy | Yes" |  |
| turtle 36): "36                                            | 0.95 | 2  | Healthy | Yes" |  |
| turtle 25): "25                                            | 0.95 | 1  | Healthy | Yes" |  |
| turtle 54): "54                                            | 0.95 | 6  | Healthy | Yes" |  |
| turtle 72): "72                                            | 0.95 | 2  | Healthy | Yes" |  |
| turtle 13): "13                                            | 0.95 | 5  | Healthy | Yes" |  |
| turtle 99): "99                                            | 0.95 | 1  | Healthy | Yes" |  |
| turtle 135): "135                                          | 0.95 | 1  | Healthy | Yes" |  |
| turtle 26): "26                                            | 0.95 | 3  | Healthy | Yes" |  |
| turtle 46): "46                                            | 0.95 | 2  | Healthy | Yes" |  |
| turtle 297): "297                                          | 0.77 | 1  | Healthy | No"  |  |
| turtle 41): "41                                            | 0.95 | 1  | Healthy | Yes" |  |
| turtle 155): "155                                          | 0.95 | 1  | Healthy | Yes" |  |
| turtle 129): "129                                          | 0.95 | 1  | Healthy | Yes" |  |
| turtle 82): "82                                            | 0.95 | 1  | Healthy | Yes" |  |
| turtle 115): "115                                          | 0.95 | 1  | Healthy | Yes" |  |
| turtle 263): "263                                          | 0.95 | 1  | Healthy | Yes" |  |
| turtle 117): "117                                          | 0.95 | 2  | Healthy | Yes" |  |
| turtle 85): "85                                            | 0.95 | 1  | Healthy | Yes" |  |
| turtle 144): "144                                          | 0.95 | 2  | Healthy | Yes" |  |
| turtle 258): "258                                          | 0.95 | 1  | Healthy | Yes" |  |
| turtle 110): "110                                          | 0.95 | 2  | Healthy | Yes" |  |
| turtle 266): "266                                          | 0.95 | 1  | Healthy | Yes" |  |
| turtle 1): "1                                              | 0.95 | 29 | Healthy | Yes" |  |
| turtle 244): "244                                          | 0.95 | 1  | Healthy | Yes" |  |
| turtle 183): "183                                          | 0.95 | 1  | Healthy | Yes" |  |
| turtle 205): "205                                          | 0.95 | 1  | Healthy | No"  |  |

Рис. 3.4 – Результати успішного подолання впливу на віртуальну спільноту

Завдяки резильєнтності змодельована віртуальна спільнота мала можливість впоратися із настанням кризової ситуації та подолати її, тим самим підвищивши свою ефективність, абсорбційну здатність та адаптивність до аналогічних загроз.

### 3.2 Оцінка ефективності покращеного методу підвищення інформаційної безпеки віртуальної спільноти

З метою проведення оцінки ефективності покращеного методу було використано змодельовану віртуальну спільноту у середовищі NetLogo (Рис. 3.5).

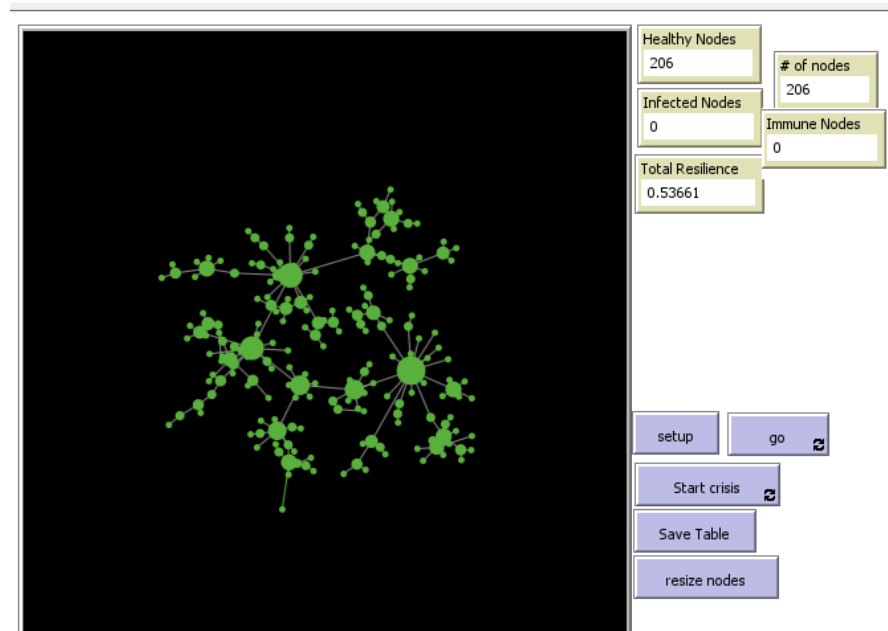


Рис. 3.5 – Початкова резильєнтність віртуальної спільноти

Показник Total Resilience = 0,53661. Він вимірюється автоматично під час настання кожного наступного тіка. Обчислення відбувається згідно описаних формул у підрозділі 2.1 кваліфікаційної роботи. Кожен актор (вузол) має індивідуальну резильєнтність, яка визначається випадково, але також врахований нормальний розподіл показника, який лежить у межах  $[0.4; 0.6]$ . Таким чином, індивідуальна резильєнтність акторів визначається у межах  $(0; 1)$ . Згідно формули 2.1 для соціального домену, важливим чинником впливу на резильєнтність є кількість зв'язків та їхня швидкість утворення і розірвання.

Врахована також умова, якщо сусідні актори, з якими він має зв'язок, мають вищий показник резильєнтності, ніж сам актор, то його показник збільшується, прямо пропорційно кількості зв'язків. Така сама залежність здійснюється, якщо сусідні актори мають нижчий рівень. Тоді резильєнтність основного актора зменшується. Це правило не працює у випадку, коли актори мають лише один зв'язок, тоді їхня резильєнтність залишається сталою.

Наступним етапом було моделювання настання кризи всередині віртуальної спільноти, шляхом поширення фейкової інформації всередині віртуальної спільноти (Рис. 3.6). Зараження акторів здійснювалося випадково. У випадку зараження, індивідуальна резильєнтність поступово знижувалася.

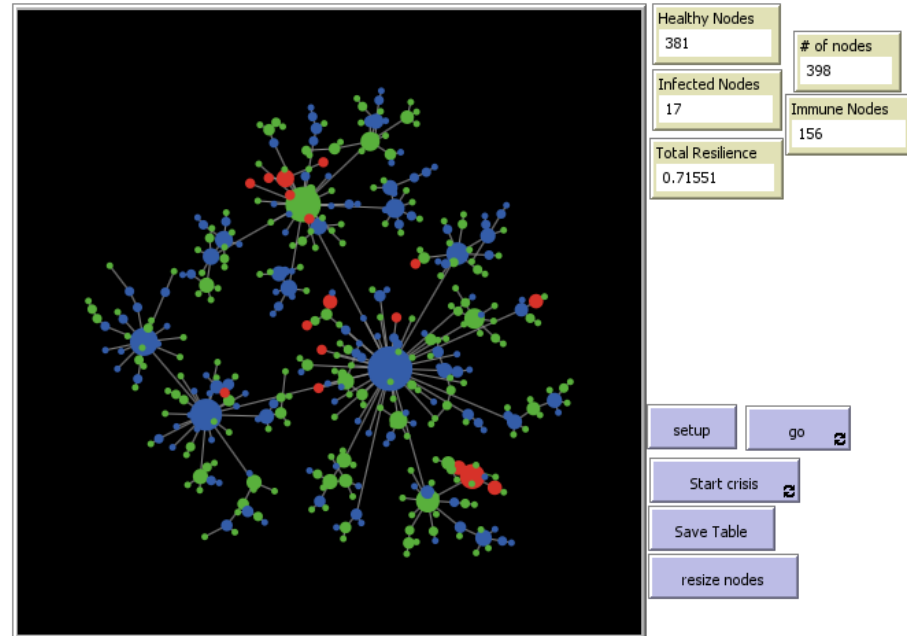


Рис. 3.6 – Вплив кризової ситуації

На Рис. 3.6 представлено успішне подолання кризової ситуації. Загальна резильєнтність модельованої віртуальної спільноти (Total Resilience) підвищилася до 0,71551, що є високим показником. Такий перебіг подій можливий за раніше визначених початкових умов. Запропонований доменний підхід (Рис. 1.6) розділяє соціальний домен, на звичайних акторів, лідерів думок, модераторів та власників спільнот. Якщо здійснювати вплив на лідерів думок, тобто акторів системи, які мають більшу кількість зв'язків та вплив на резильєнтність оточуючих, звичайних акторів, то існує ймовірність, що віртуальна спільнота не буде здатна подолати кризу (Рис. 3.7).

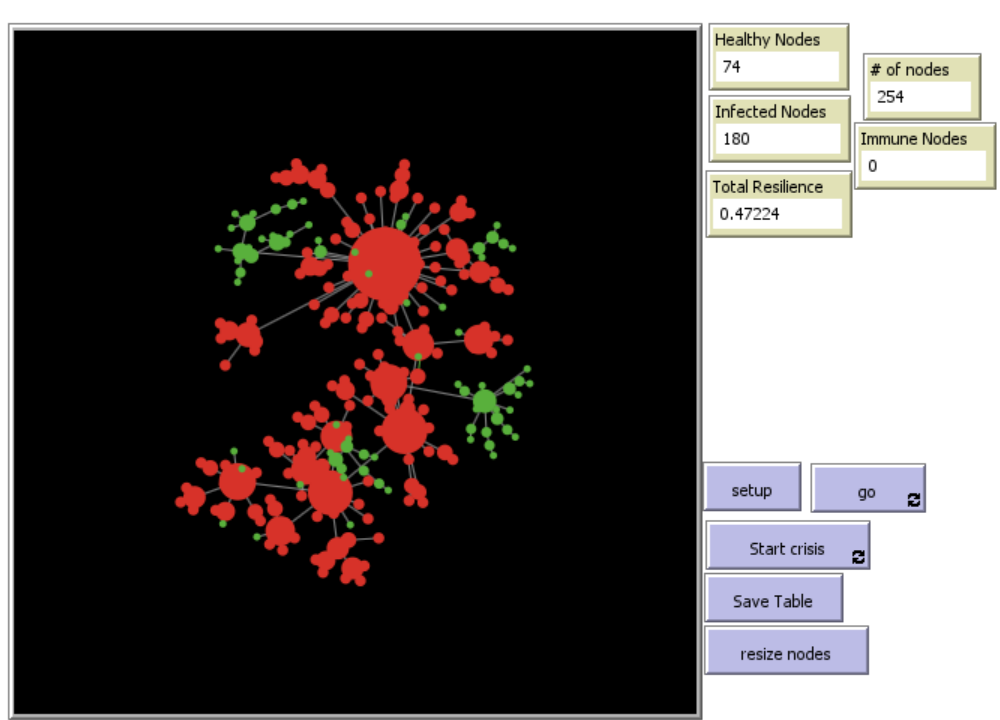


Рис. 3.7 – Розповсюдження фейкових нових, через лідерів думок

У такому випадку поширення фейкових нових здійснюється швидше, ніж шляхом поширення через випадкових акторів. Резильєнтність віртуальної спільноти знижується та наближається до точки неповернення (до 0). Якщо відтворити таку симуляцію, то можна побачити, що резильєнтність наближається до 0 (Рис. 3.8).

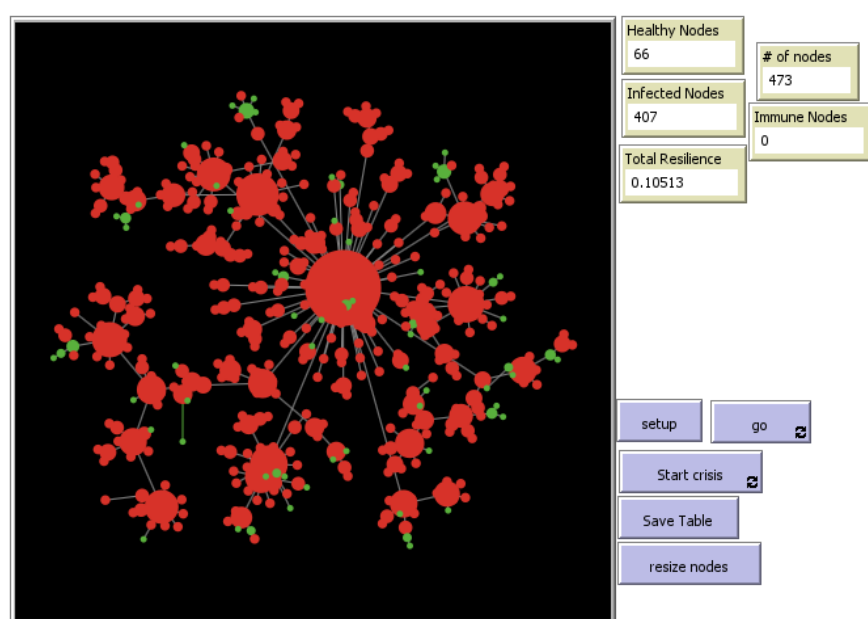


Рис. 3.8 – Віртуальна спільнота не пережила кризу

У такому випадку (Рис. 3.8) віртуальна спільнота не змогла впоратись з кризовою ситуацією. Її резильєнтність (Total Resilience) дорівнює 0,10513. При

такому значенні існує ймовірність на відновлення, але заражено 86% всіх акторів модельованої віртуальної спільноти, включно з усіма лідерами думок (вузли з найбільшою кількістю зв'язків), що в свою чергу не дозволяє власними силами подолати кризову ситуацію.

Таким чином, модельована віртуальна спільнота та потенційні варіанти перебігу кризових ситуацій показують, що резильєнтність є динамічним показником, який потрібно оцінювати у три періоди:

1. Перед настанням кризової ситуації.
2. У процесі кризи.
3. Після закінчення (успішного подолання чи невдачі).

На основі проведеного дослідження, оцінка ефективності покращеного методу є вдалою. За рахунок врахування піддоменів та факторів, описаних у підрозділі 2.1, можливо змодельовати віртуальну спільноту та здійснювати вплив на визначені домени(піддомени). Статистика, яка виводиться у реальному часі, дозволяє вести постійний моніторинг перебігу подій.

### **Висновки до третього розділу**

У середовищі NetLogo проведено дослідження впливу резильєнтності на інформаційну безпеку віртуальної спільноти в соціальних інтернет-сервісах. Описано впливи на акторів та їх взаємозв'язки між собою. Наведено два варіанта перебіга подій, коли віртуальна спільнота здатна подолати кризову ситуацію та ні.

Проведено оцінку ефективності запропонованого покращення методу, на базі врахування п'яти доменів. Проведено симуляції кризових ситуації та оцінку їхнього впливу на резильєнтність віртуальної спільноти. Описані причини і наслідки.

## ВИСНОВКИ

У кваліфікаційній роботі описано актуальність синтезу резильєнтних віртуальних спільнот в соціальних інтернет-сервісах, основною метою якої є оцінка ефективності покращеного методу для підвищення ступені інформаційної безпеки віртуальних спільнот у соціальних інтернет-сервісах. Проведено аналіз стану проблеми забезпечення резильєнтності, її ролі та місця у забезпеченні інформаційної безпеки віртуальної спільноти. Проаналізовано методи вимірювання та аналізу резильєнтності у системах. Проведено систематизацію факторів, які впливають на резильєнтність.

У процесі розроблення методу синтезу резильєнтної віртуальної спільноти покращено уже існуючий метод оцінки резильєнтності, врахувавши соціальний, технічний, організаційний, інформаційний та комунікаційний домен. За допомогою диференціальних рівнянь описано методи вимірювання резильєнтності кожного домена та віртуальної спільноти загалом. Проаналізовані потенційні загрози та їх вплив на резильєнтність за допомогою сценарного моделювання.

Проведено експериментальне дослідження методу синтезу резильєнтних віртуальних спільнот та їх вплив на власну інформаційну безпеку. За допомогою середовища NetLogo здійснено моделювання кризових ситуацій за різних початкових умов та перебігу подій. Здійснено оцінку ефективності покращеного методу.

На практиці, дана робота здатна стати доповненням до уже існуючих досліджень, у сфері резильєнтності, та мати місце у подальших дослідженнях у сфері інформаційної безпеки. Запропоноване покращення методу оцінки має більшу точність та містить фактори впливу, які до цього не враховувалися. У майбутньому дану роботу можливо розширити, з метою поглибленого дослідження резильєнтності віртуальних спільнот у конкретних випадках та соціальних інтернет-сервісах, подіях державного та глобального рівня. Це дозволить підвищити ступінь інформаційної безпеки акторів віртуальних спільнот та зменшити деструктивний вплив на процеси їх життя.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ridings C. M. Defining "Virtual Community" // *Virtual Technologies: Concepts, Methodologies, Tools, and Applications*. Hershey, PA : IGI Global, 2008. С. 8–14.
2. Молодецька-Гринчук К. В. Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах : автореф. дис. ... докт. техн. наук : 21.05.01. Житомир, 2018. 368 с.
3. Bernacchi V., LeBaron V., Porter K., Zoellner J., DeGuzman P. Barriers and facilitators to resilience for rural cancer survivors during COVID-19 // *Public Health Nursing*. 2023. Т. 40, № 5. С. 595–602. DOI: <https://doi.org/10.1111/phn.13200>.
4. Dahal L., Idris M., Bravo V. "It helped us, and it hurt us": The role of social media in shaping agency and action among youth in post-disaster Nepal // *Journal of Contingencies and Crisis Management*. 2020. Т. 29, № 2. С. 217–225. DOI: <https://doi.org/10.1111/1468-5973.12329>.
5. Parra L., Movono A., Scheyvens R., Auckram S. Pacific approaches to fundraising in the digital age: COVID-19, resilience and community relational economic practices // *Asia Pacific Viewpoint*. 2023. Т. 64, № 2. С. 222–238. DOI: <https://doi.org/10.1111/apv.12372>.
6. Haas A., Abonneau D., Borzillo S., Guillaume L. Afraid of engagement? Towards an understanding of engagement in virtual communities of practice // *Knowledge Management Research & Practice*. 2020. Т. 19, № 2. С. 169–180. DOI: <https://doi.org/10.1080/14778238.2020.1745704>.
7. Лаптев, О. А., Колесник, В. В., Ровда, В. В., & Половінкін, М. І. (2024). Метод підвищення захисту особистих даних за рахунок синтезу резильєнтних віртуальних спільнот. *Сучасний захист інформації*, 4(60), 152–157.
8. Proag V. Assessing and Measuring Resilience // *Procedia Economics and Finance*. 2014. Т. 18. С. 222–229. DOI: [https://doi.org/10.1016/S2212-5671\(14\)00934-4](https://doi.org/10.1016/S2212-5671(14)00934-4).

9. Platt S., Brown D., Hughes M. Measuring resilience and recovery // International Journal of Disaster Risk Reduction. 2016. T. 19. C. 447–460. DOI: <https://doi.org/10.1016/j.ijdr.2016.05.006>.
10. Erol O., Henry D., Sauser B. Exploring Resilience Measurement Methodologies // INCOSE International Symposium. 2010. T. 20. C. 302–322. DOI: <https://doi.org/10.1002/j.2334-5837.2010.tb01072.x>.
11. Linkov I., Bridges T., Creutzig F. та ін. Changing the resilience paradigm // Nature Climate Change. 2014. T. 4. C. 407–409. DOI: <https://doi.org/10.1038/nclimate2227>.
12. Wreathall J. Developing Models for Measuring Resilience. Dublin, Ohio, 2006.
13. Wang J. W., Wang H. F., Ding J. L., Furuta K., Kanno T., Ip W. H., Zhang W. J. On domain modelling of the service system with its application to enterprise information systems // Enterprise Information Systems. 2013. T. 10, № 1. C. 1–16. DOI: <https://doi.org/10.1080/17517575.2013.810784>.
14. Huang K., Chengalur-Smith I. N. A social capital perspective to understand individual contribution of social support in healthcare virtual support communities // Proceedings of the 47th Hawaii International Conference on System Sciences. 2014. C. 3489–3498. DOI: <https://doi.org/10.1109/hicss.2014.435>.
15. Ryan S. Information systems and healthcare XXXVI: Building and maintaining social capital—evidence from the field // Communications of the Association for Information Systems. 2010. T. 27. DOI: <https://doi.org/10.17705/1cais.02718>.
16. De Moor A., Weigand H. Formalizing the evolution of virtual communities // Information Systems. 2007. T. 32, № 2. C. 223–247. DOI: <https://doi.org/10.1016/j.is.2005.09.002>
17. Zhao H., Shi Q. Accessing the Impact Mechanism of Sense of Virtual Community on User Engagement // Frontiers in Psychology. 2022. T. 13. DOI: <https://doi.org/10.3389/fpsyg.2022.907606>
18. Hummel J., Lechner U. Social profiles of virtual communities // Proceedings of the 35th Annual Hawaii International Conference on System Sciences. Big Island, HI, USA, 2002. C. 2245–2254. DOI: 10.1109/HICSS.2002.994154.

19. Hryshchuk R., Molodetska K., Syerov Y. Method of improving the information security of virtual communities in social networking services // *Environmental Systems and Decisions*. 2024. С. 1–8.
20. Грищук Р., Молодецька К. Концепція синергетичного управління процесами взаємодії агентів у соціальних інтернет-сервісах // *Безпека інформації*. 2015. Т. 21, № 2. С. 123–130.
21. Молодецька-Гринчук К. В. Метод побудови профілів інформаційної безпеки акторів соціальних інтернет-сервісів // 2017.
22. Lomicka L. Creating and sustaining virtual language communities // *Foreign Language Annals*. 2020. Т. 53, № 2. С. 306–313.
23. Rachmad Y. E. *Resilience Building Theory*. 2022.
24. Rachmad, Y. E. *Communication Resilience Theory*. 2022
25. Walker B. Resilience: What it is and is not // *Ecology and Society*. 2020. Т. 25, № 2. С. 11.
26. Herrman H., Stewart D. E., Diaz-Granados N., Berger E. L., Jackson B., Yuen T. What is resilience? // *The Canadian Journal of Psychiatry*. 2011. Т. 56, № 5. С. 258–265.
27. Wu G., Feder A., Cohen H., Kim J. J., Calderon S., Charney D. S., Mathé A. A. Understanding resilience // *Frontiers in Behavioral Neuroscience*. 2013. Т. 7. С. 10.
28. Egeland B., Carlson E., Sroufe L. A. Resilience as process // *Development and Psychopathology*. 1993. Т. 5, № 4. С. 517–528.
29. Stocker J. *Resilience Conceptualised through Transformation: A Framework for Interdisciplinary Application*. Tigray: War in a Digital Black Hole, 2024. С. 53.
30. Paton D., Johnston D. *Disaster Resilience: An Integrated Approach*. Springfield, IL: Charles C Thomas Publisher, 2017.
31. Chang S. E., Shinozuka M. Measuring improvements in the disaster resilience of communities // *Earthquake Spectra*. 2004. Т. 20, № 3. С. 739–755.

## ДОДАТКИ

### Додаток А

Таблиця А.1 – Вплив компонентів віртуальної спільноти на її резильєнтність

| Домен         | Піддомен          | Позитивний вплив                                                              | Негативний вплив                                                          |
|---------------|-------------------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Соціальний    | Звичайні актори   | Підтримання активності і залученості, створення бази для соціальних зв'язків. | Пасивність або відсутність залучення знижує рівень активності спільноти.  |
|               | Лідери думок      | Формування колективної думки, мотивація учасників.                            | Залежність від їхнього впливу, відсутність децентралізованого управління. |
|               | Модератори        | Контроль над дотриманням правил учасниками.                                   | Можливе зловживання владою.                                               |
|               | Власники спільнот | Визначення стратегії та напрямку діяльності спільноти.                        | Надмірне втручання в діяльність віртуальної спільноти.                    |
| Технологічний | Інфраструктура    | Забезпечення працездатності платформи та доступу учасникам.                   | Збої, нестабільність у доступі або відсутність доступу.                   |
|               | Захист даних      | Підвищення довіри учасників, шляхом забезпечення конфіденційності даних.      | Витік або викрадення даних.                                               |
|               | Інструменти       | Полегшення управління та модерування.                                         | Складність у використанні.<br>Відсутність інструкцій.                     |

## Продовження таблиці А.1

|                |                      |                                                                                       |                                                                                  |
|----------------|----------------------|---------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Комунікаційний | Управління контентом | Перевірений контент знижує рівень дезінформації.                                      | Поширення деструктивного та шкідливого контенту.                                 |
|                | Канали комунікації   | Забезпечення різноманітності взаємодії, підвищення доступності інформації.            | Недостатня різноманітність здатна обмежити доступність до інформації.            |
|                | Формати комунікації  | Враховують потреби учасників. Підвищують залученість у життя віртуальної спільноти.   | Обмеження у форматах здатне негативно вплинути на активність учасників.          |
| Організаційний | Правила та політики  | Сприяння стабільності, згуртованості та довірі між учасниками.                        | Надмірні обмеження спричиняють конфлікти та відчуження учасників.                |
|                | Ролі та обов'язки    | Розподіл ролей сприяє швидкому реагуванню на загрози, забезпечує ефективне управління | Нечіткість ролей викликає хаос та конфлікти в управлінні.                        |
|                | Адміністрування      | Забезпечує стабільність платформи та швидке вирішення проблем.                        | Недостатнє адміністрування призводить до хаосу і втрати контролю над спільнотою. |
| Інформаційний  | Контент              | Якісний контент утримує учасників, забезпечуючи цінність спільноти.                   | Низькоякісний або недостовірний контент викликає втрату довіри.                  |
|                | Аналіз даних         | Дозволяє проактивно виявляти ризики та адаптуватися до змін.                          | Неправильний аналіз призводить до прийняття невірних рішень, що знижує стійкість |