РОЛЬ РЕЗИЛЬЄНТНОСТІ ВІРТУАЛЬНИХ СПІЛЬНОТ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ

Колесник В.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Актуальність. Віртуальні спільноти (ВС) у соціальних інтернет-сервісах стали стратегічним ресурсом інформаційної та кібербезпеки, оскільки на рівні політики безпеки вони виконують функції суспільної «архітектури взаємодії», сенсорної мережі раннього попередження та механізму колективної адаптації. Резильєнтні ВС знижують системний ризик втрати керованості інформаційним простором і забезпечують безперервність критичних комунікацій між державними, корпоративними та громадянськими акторами [1]. Їхня стійкість перетворює технічні збої на керовані інформаційні події та зменшує сукупні суспільні витрати на подолання криз завдяки швидшому відновленню і соціальному навчанню.

Таким чином, резильєнтність ВС підсилює конфіденційність, цілісність і доступність на рівні екосистеми та зміцнює демократичну стійкість у тривалих гібридних загрозах [1]. Вони формують «суспільний рівень безпеки»: акумулюють знання, транслюють норми та забезпечують стійкість комунікацій у кризах. Резильєнтність ВС визначає спроможність державних, корпоративних і громадянських акторів зберігати керованість інформаційного простору й забезпечувати безперервність критичних комунікацій під тиском гібридних загроз.

Стан на сьогодні та наявні обмеження. Актуальні дослідження [1-3,5], показують: резильєнтні ВС стримують поширення маніпуляцій, зменшують наслідки атак та підтримують колективну адаптацію. Водночас зберігаються системні обмеження: розрив між платформеним врядуванням і публічною політикою; дефіцит прозорості/даних; фрагментованість підходів між безпекою, комунікаціями та кризовим менеджментом; низька інституціалізація взаємодії громад із SOC/CSIRT/урядом.

Мета доповіді. Дослідити внесок резильєнтності ВС у інформаційну та кібербезпеку через трансформацію віртуальних спільнот з неформальних мереж учасників у інститути суспільної безпеки – із визначеними ролями, нормами та процедурами підзвітності, співврядуванням з платформами й державними акторами, функціями раннього попередження, підтримки взаємодії та безперервності критичних комунікацій.

Основний зміст доповіді. У фокусі аналізу перебуває внесок резильєнтності віртуальних спільнот у формування стратегічно керованого інформаційного простору та у зміцнення кібербезпеки без надмірної централізації. Резильєнтність у цьому контексті слід розуміти як здатність спільнот підтримувати ефективну взаємодію, забезпечувати

спостережуваність подій, адаптуватися до збурень і відновлювати функції комунікації, залишаючись прийнятними для різних аудиторій [1]. Саме ця властивість перетворює спільноти з розрізнених мереж учасників на елементи інфраструктури суспільної безпеки, які працюють у взаємодії з державою, платформами та професійними безпековими інститутами.

Ключовим ефектом є консолідація архітектури взаємодії. На макрорівні вона виступає запобіжником інформаційних криз: визначає готовність суспільства сприймати офіційні повідомлення, коригувати помилкові уявлення та підтримувати узгодженість рішень у ситуаціях невизначеності. Резильєнтні спільноти утримують культуру обговорення та прозорі процедури виправлення помилок, тому окремі інциденти не масштабуються у кризи інституцій.

Не менш важливим є внесок у суспільну спостережуваність і раннє попередження. Резильєнтні спільноти діють як розподілена сенсорна мережа: вони виявляють аномалії, сигналізують про нові патерни маніпуляцій і забезпечують циркуляцію валідованих сигналів між різними сегментами простору [4, 6]. Це зменшує інформаційну асиметрію між атакувальником і захисником, зміщуючи систему з реактивного на проактивний режим управління ризиками.

У підсумку знижується непередбачуваність, а рішення можуть прийматися раніше, з меншими транзакційними витратами.

Резильєнтність водночас посилює адаптивну спроможність [1, 4]. У резильєнтних спільнотах збурення стають джерелом навчання, а не тільки втрат: виробляються норми реагування, акумулюється прикладне знання, з'являються надійні механізми апеляції та відновлення репутації. Підтримка узгоджених процедур і передбачуваних правил зменшує конфлікт між модерацією та свободою вираження, забезпечуючи прийнятність політик для більшості зацікавлених сторін. Цей дисциплінований процес створює умови для стабільної координації між спільнотами, платформами та публічною політикою.

Окремо слід наголосити на зв'язку комунікацій і кіберзахисту. Коли канали комунікації стійкі, а ланцюги взаємодії підтримані, технічні інциденти не перетворюються на кризи узгодженості: інформаційні потоки переключаються на резервні маршрути, інститути зберігають голос, а аудиторії – доступ до перевірених повідомлень [5]. Таким чином резильєнтність спільнот пом'якшує системний вплив технічних атак, дозволяючи безпековим підрозділам концентруватися на усуненні кореневих причин, а не на компенсації репутаційних наслідків.

На довшому горизонті резильєнтні спільноти зміцнюють демократичну стійкість і суспільну єдність. Зниження поляризації, підвищення медіаграмотності та нормалізація етичних стандартів спілкування зменшують ефективність операцій впливу й підривають економіку маніпулятивних

кампаній. Сукупний ефект проявляється у зниженні агрегованих суспільних витрат на подолання криз: менше ресурсів витрачається на виправлення дезінформації, коротшими стають «вікна уразливості», швидше відновлюється звична траєкторія суспільних та економічних процесів.

Внесок резильєнтності віртуальних спільнот у інформаційну та кібербезпеки полягає у стабілізації взаємодії, підвищенні спостережуваності й передбачуваності простору, узгодженості правил взаємодії в онлайні, а також у поєднанні комунікацій із технічним кіберзахистом. Саме ці властивості забезпечують керованість інформаційної екосистеми під час тривалих гібридних загроз і роблять можливими узгоджені дії державних, корпоративних та громадянських акторів без вдавання до надмірної цензури чи централізації.

Практичне значення. Резильєнтні ВС – це системоутворювальний чинник безпеки: вони стабілізують взаємодію, забезпечують суспільну спостережуваність, зменшують витрати на подолання криз, узгоджують правила, пов'язують комунікації з кіберзахистом і підсилюють державні та корпоративні спроможності. Як наслідок створюються умови для підвищення національної та корпоративної стійкості без запровадження надмірного контролю чи централізованого втручання.

Список літератури

1. Kolesnyk V., Molodetska K., Fedushko S. From Connectivity to Security: Ensuring Cyber Resilience in Socio-technical Systems with Social Networking Services // Developments in Information and Knowledge Management Systems for Business Applications. – Cham : Springer, 2025. – (Studies in Systems, Decision and Control ; vol. 578). – P. 121–147. – DOI: 10.1007/978-3-031-80935-4_7.

2. Mannocci L., Mazza M., Monreale A., Tesconi M., Cresci S. Detection and Characterization of Coordinated Online Behavior: A Survey. – arXiv preprint, 2024. – DOI: 10.48550/arXiv.2408.01257. – [Електронний ресурс]. – Режим доступу: https://arxiv.org/abs/2408.01257 (дата звернення: 06.11.2025).

3. Xie L., Pinto J., Zhong B. Building community resilience on social media to help recover from the COVID-19 pandemic // Computers in Human Behavior. – 2022. – Vol. 134. – Art. 107294. – DOI: 10.1016/j.chb.2022.107294.

4. Garcia D., Mavrodiev P., Schweitzer F. Social Resilience in Online Communities: The Autopsy of Friendster // Proceedings of the 2013 Conference on Online Social Networks (COSN'13). – Boston : ACM, 2013. – P. 39–50. – DOI: 10.1145/2512938.2512946.

5. Fedushko S., Molodetska K., Syerov Y. Analytical method to improve the decision-making criteria approach in managing digital social channels // Heliyon. – 2023. – Vol. 9, Iss. 6. – e16828. – DOI: 10.1016/j.heliyon.2023.e16828.

6. Aref S., та ін. Robust Markov stability for community detection at a scale. – arXiv preprint, 2025. – [Електронний ресурс]. – Режим доступу: https://arxiv.org/abs/2504.11621 (дата звернення: 06.11.2025).