[6] MSECB Transition Policy on Management System Certification to ISO/IEC 27001:2022. URL: https: //msecb.com/wp-content/uploads/2023 / 01 / MS-ECB-Transition-Policy-on-MS-Certification-to-ISO-IEC-27001.pdf?utm_source=sendinblue&utm_ campaign=Clients%20ISOIEC%20270012022%20 Transition%20Policy&utm_medium=email.
[7] ISO 27001 2013 vs. 2022 revision. What has changed? URL: https: // advisera. com/ 27001academy/blog/ 2022/02/09/iso-27001-iso-27002/.
[8] Pacaiova, H., Nagyova, A. Risk based thinking. New approach for modern enterprises' management, Advances in Intelligent Systems and ComputingVolume 783. 2019. pp. 524-5362019 AHFE International Conference on Human Factors, Business Management and Society, 2018 Orlando21, July 2018, through 25 July 2018, Code 215359.
[9] Susukailo V., Opirsky I., Yaremko O. Methodology of ISMS Establishment Against Modern Cybersecurity Threats. In: Klymash M., Beshley M., Luntovskyy A. (eds) Future Intent-Based Networking. Lecture Notes in Electrical Engineering, vol 831. 2022. Springer, Cham. https: // doi.org / 10.1007/ 978-3-030-92435-5_15.
[10] What is an ISO 27001 internal audit? URL: https: / /www.vanta.com/glossary/iso-27001-internal-audit.
[11] How to manage changes in an ISMS. URL: https: //advisera.com/27001academy/blog/2015/09 /14/ how-to-manage-changes-in-an-isms-according-to-iso-27001-a-12-1-2/.

DEVELOPMENT OF A METHODOLOGY FOR ASSESSING COMPLIANCE WITH ISO 27001 STANDARD

This document proposes the methodology for assessing organizations' compliance with the new version of the ISO 27001 standard, which was introduced at the end of 2022. The high significance of information security in the modern world requires companies to adapt their practices and policies to the new requirements of the standard. The authors analyze recent research in the field of ISO 27001 implementation and the shortcomings of relevant materials for compliance assessment. The methodology includes the analysis of the new standard requirements, comparing them with the current practices of organizations, identifying gaps between them, developing a plan for implementing changes, and monitoring compliance. The provided recommendations will help organizations ensure an effective transition to the new standard, minimize risks, and maintain a high level of information security. This methodology is a relevant tool for organizations seeking to adapt their practices and policies to the new version of the ISO 27001 standard and maintain the security of their information at a high level. This development takes into account the unique needs of organizations and contributes to their successful implementation of new information security practices and requirements. The purpose of this article is to help readers understand the complexity and importance of conducting an initial gap assessment prior to implementing a standard and to highlight the effectiveness of using a detailed checklist when performing a gap analysis. To support the study, a detailed analysis of literature and articles related to the implementation of the ISO 27001 standard in organizations was conducted.

Keywords: information security, cybersecurity, ISO 27-001, information security framework, information security management system, gap assessment, gap analysis.

Курій Євгеній Олегович, асистент кафедри захисту інформації Національного університету «Львівська політехніка».

Yevhenii Kurii, assistant at the Department of Information Security, "Lviv Polytechnic" National University.
E-mail: yevhenii.o.kurii@lpnu.ua.
Orcid ID: 0000-0002-3423-5655.

Сусукайло Віталій Андрійович, асистент кафедри захисту інформації Національного університету «Львівська політехніка».

Vitalii Susukailo, assistant at the Department of Information Security, "Lviv Polytechnic" National University.
E-mail: vitalii.susukailo@gmail.com.
Orcid ID: 0000-0003-4431-9964.

Опірський Іван Романович, д.т.н., професор, завідувач кафедри захисту інформації Національного університету «Львівська політехніка».

Ivan Opirskyy, Doctor of Technical Sciences, Professor, Head of the Department of Information Security, "Lviv Polytechnic" National University.
E-mail: ivan.r.opirskyi@lpnu.ua.
Orcid ID: 0000-0002-8461-8996.

DOI: 10.18372/2410-7840.25.17939
УДК 316.772.4:004

СИНТЕЗ МОДЕЛІ СОЦІАЛЬНИХ САНКЦІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ВІРТУАЛЬНИХ СПІЛЬНОТ У СОЦІАЛЬНИХ МЕРЕЖАХ В УМОВАХ АНТАГОНІСТИЧНОГО СЕРЕДОВИЩА

Сергій Євсеєв, Юрій Тимонін, Сергій Веретюк, Тетяна Войтко, Дмитро Оленюк

Швидка інтеграція віртуальних комунікацій у суспільне життя актуалізує потребу у створенні безпечного й комфортного середовища для комунікації користувачів віртуальних спільнот. Метою дослідження є підвищення рівня інформаційної безпеки соціальних віртуальних груп шляхом обґрунтування та формалізації особливостей застосування інструментів соціального контролю для управління динамікою віртуальної спільноти в інформаційному просторі. На основі моделей Моно та популяційної динаміки формалізовано процес еволюції віртуальної спільноти в умовах антагоністичного середовища, а також функціонал управління та забезпечення стійкістю віртуальної спільноти в соціальних інтернет-сервісах. Параметрами моделі визначено вплив частки деструктивних публікацій, які становлять загрозу інформаційній безпеці соціальній спільноті; глибина комунікації акторів досліджуваної спільноти з учасниками антагоністичної спільноти; показники якості контенту. У дослідженні набули подальшого розвитку компоненти соціального контролю в соціальних інтернет-сервісах та класифікація порушників інформаційної безпеки.

Ключові слова: *антагоністичне середовище, віртуальна спільнота, загроза, інформаційна безпека, санкції, соціальна мережа, соціальний контроль.*

ВСТУП

Віртуальні спільноти, які виникли внаслідок розвитку Інтернету та соціальних мереж, в епоху інформаційного суспільства забезпечують можливість спілкування і взаємодії між людьми та стали популярними майданчиками для обміну інформацією, дискусій, співпраці, розваг. Наразі соціальні мережі стали невід'ємною складовою повсякденного та професійного життя й часто користувачі надають перевагу віртуальному спілкуванню на противагу «живому». Процеси комунікації акторів у віртуальних спільнотах мають особливості, які відрізняють їх від комунікації в реальному житті, серед яких основними є такі:

1) анонімність та використання псевдонімів, оскільки частина користувачів глобальної мережі обирають залишатись інкогніто та висловлювати свої думки більш вільно, не маючи страху бути ідентифікованими;

2) асинхронність спілкування, що дозволяє здійснювати комунікацію з іншими користувачами інтернет-сервісу із певною затримкою у часі і це надає можливість обмірковувати інформацію та формулювати свою відповідь на неї;

3) розширення меж для спілкування із користувачами з різних регіонів та країн, що значною мірою впливає на обмін та поширення досвіду, ідей та поглядів, а також розширює можливості комунікацій у культурній сфері;

4) обмін мультимедійним контентом допомагає наочно передавати власні думки, та надає певне роз'яснення або підкреслює їх емоційність;

5) наявність модераторів у віртуальних спільнотах забезпечує дотримання порядку і врегулювання конфліктних ситуацій;

6) різноманітність форм комунікації акторів.

Водночас, із інтеграцією віртуальних комунікацій у суспільне життя виникає потреба у створенні безпечного й комфортного середовища для комунікації користувачів віртуальних спільнот, що стає першочерговим завданням для її власників та/або адміністраторів.

Віртуальні спільноти взаємодіють з іншими віртуальними спільнотами та досить часто стають об'єктом булінгу, дискримінації, поширення дезінформації та агресивної поведінки не тільки деяких акторів по відношенню до інших учасників, а також по відношенню до всієї віртуальної спільноти. Тим самим постає актуальне завдання – підтримка стійкості віртуальної спільноти в умовах антагоністичного зовнішнього середовища.

Важливою передумовою реалізації стратегії сталого розвитку віртуальної спільноти є розробка моделі ефективного управління віртуальною спільнотою через реалізацію компонентів соціального контролю, зокрема через ефективне застосування соціальних санкцій, під якими розуміють сукупність покарань у правовому полі держави і середовищі соціальних інтернет-сервісів (СІС), які застосовуються у випадку виявлення відхилень від загальноприйнятих норм взаємодії акторів та віртуальних спільнот з метою гарантованого дотримання в інформаційному просторі СІС стандартів [2].

Для дослідження процесу розвитку стійких віртуальних спільнот варто зважати на інформаційні ситуації, які можуть виникати в інформаційному просторі інтернет-сервісу. Fedushko S., Molodetska K., Syerov Y. [3] під інформаційною ситуацією пропонують розглядати ступінь невизначеності в інформаційному середовищі у момент прийняття рішень учасниками стійкої віртуальної спільноти за якої проявляються їх антагоністичні інтереси. Дана ситуація відображає процеси інформаційного конфлікту в інформаційному просторі соціального інтернет-сервісу та виникає через несумісні цінності, ідеології, різноспрямовані погляди та агресивну поведінку користувачів у відстоюванні власних інтересів.

Реалізація механізму моделі санкцій неможлива без застосування соціального контролю. Праця Молодецької К. [2] присвячена систематизації ключових складових соціального контролю у соціальних інтернет-сервісах. Розкриття сутності кожної з компонент дозволяє більш глибоко розуміти механізми їх реалізації. Дослідницею встановлено, що впровадження моделі соціального контролю сприятиме формуванню у стійких віртуальних спільнотах здатності до інформаційного протиборства загрозам інформаційної безпеки, які можуть потенційно виникати в інформаційному просторі соціальних інтернет-сервісів.

Mustafa Oz, Esra Nur Oz Cetindere у своїй праці [5] досліджують вплив соціальних санкцій та деіндивідуалізації на бажання акторів ділитися власними думками у соціальних інтернет-сервісах. Авторами було опитано 535 користувачів різних інтернет-сервісів і встановлено, що деіндивідуалізація значною мірою пом'якшує зв'язок між соціальними санкціями і бажанням акторів висловлювати думки.

Аналіз психологічних особливостей акторів надає можливість прогнозувати результати впроваджених соціальних санкцій на поведінку акторів щодо висловлювання власних думок в інформаційному просторі соціальних інтернет-сервісів, а деіндивідуалізація у даному контексті постає як один із ефективних інструментів вирішення даної проблеми.

Ефективності реалізації санкцій у мережах різної архітектури присвячено працю Sumit Joshi, Ahmed Saber Mahmud [6]. Вченими розроблено дві концепції – стратегічної компліментарності та зовнішніх ефектів, які перетинаються в антагоністичному середовищі й допомагають пов'язати ефективність санкцій із конкретною мережею, а безпосередньо ефективність санкцій оцінюється як ступінь зменшення частоти порушень.

Jyh-Jeng Wu, Alex S. L. Tsang у роботі [4] концентрують увагу на тому, як рівень довіри акторів віртуальної спільноти впливає на їх поведінку. На основі запропонованої моделі факторів вченими було здійснено аналіз 625 онлайн-анкет акторів віртуальних спільнот та встановлено, що залучення певної вигоди та спільної цінності мають вагомий позитивний вплив на зміцнення рівня довіри учасників, що в свою чергу впливає на рівень інституційної довіри і забезпечує постійність членів у віртуальних спільнотах, сталості її розвитку.

В умовах функціонування великої кількості віртуальних спільнот у соціальних мережах, на думку Zhang K., Lo D., Lim EP. [7], часто виникають підспільноти, які мають протилежну від інших поведінку. На їх погляд, антагоністичне середовище у соціальних мережах формується на основі наявності груп людей із протилежними смаками, утворень в середині спільнот, які не мають довіри один до одного тощо. На основі запропонованої авторами методики, яка ґрунтується на основі аналізу заданих користувачем порогових значень, виокремлюються пари підспільнот, що мають протилежну поведінку, для імплементації заходів з метою запобігання виникнення конфліктів у межах спільноти.

На переконання О. Предместнікова, В. Хотмірової серед негативних ефектів від використання соціальних мереж варто виокремлювати поширення ненависті, дискримінації та кібербулінгу [1]. Серед вищезазначеного переліку особливо небезпечним є кібербулінг, який проявляється як агресивні наміри до окремих категорій користувачів соціальних мереж та підсилюється можливістю порушників інформаційної безпеки залишатись анонімними, працювати на широкий загал та наносити терористичні напади на жертву у будь-який момент часу та за будь-яких обставин.

Метою статті є підвищення рівня інформаційної безпеки соціальних віртуальних груп шляхом

обґрунтування та формалізації особливостей застосування інструментів соціального контролю для управління динамікою віртуальної спільноти в інформаційному просторі.

ОСНОВНА ЧАСТИНА

Драйверами формування та сталого розвитку віртуальної спільноти лежать спільні інтереси, які об'єднують акторів та ефекти від функціонування спільноти у соціальних мережах.

Основним ефектом від формування та функціонування віртуальної спільноти є поширення конкретного типу інформації серед максимальної кількості її споживачів за рахунок створення і розповсюдження відповідного контенту.

Таблиця 1

Класифікація порушників інформаційної безпеки в СІС

№ з/п	Критерій	Позначення	Види порушників
1.	По відношенню до віртуальної спільноти	$relation = \bigcup_q R_q$, $q = \overline{1,2}$	- внутрішні правопорушники (R_1) – особи, які вже є членами віртуальної спільноти; - зовнішні правопорушники (R_2) – особи, які не є членами віртуальної спільноти і намагаються на неї впливати й порушувати її.
2.	За рівнем знань	$qualification = \bigcup_w Q_w$, $w = \overline{1,3}$	- особи з високим рівнем технічних знань, умінь та навичок (Q_1); - особи з середнім рівнем технічних знань, умінь та навичок (Q_2); - особи з низьким (обмеженим) рівнем технічних знань, умінь та навичок (Q_3).
3.	За рівнем наданих прав	$access = \bigcup_f A_f$, $f = \overline{1,3}$	- особи, які мають повний доступ до управління віртуальною спільнотою (A_1); - особи, які мають обмежений доступ до управління віртуальною спільнотою (A_2); - особи, які не мають права на управління віртуальною спільнотою (A_3).
4.	За мотивом порушень	$motive = \bigcup_n M_n$, $n = \overline{1,2}$	- особи, які діють з наміром (M_1); - особи, які діють без наміру (M_2)
5.	За характером дій	$nature = \bigcup_p N_p$, $p = \overline{1,3}$	- особи, які несвідомо та/або без вагомих мотивів та/або намірів здійснюють порушення (N_1); - особи, які свідомо здійснюють порушення для самоствердження та/або отримання нематеріальної вигоди (N_2); - особи, які свідомо здійснюються порушення для отримання матеріальної вигоди (N_3)
6.	За проявом дій	$privacy = \bigcup_e P_e$, $e = \overline{1,2}$	- особи, які намагаються діяти приховано та залишити свою діяльність непомітною (P_1); - особи, які відкрито демонструють свої дії (P_2)
7.	За чисельністю	$violator = \bigcup_d V_d$, $d = \overline{1,2}$	- окремі особи (V_1); - групи осіб (V_2)

Індикатором відповідних ефектів, насамперед, є рівень інформаційного забезпечення акторів та суспільства у цілому. До факторів рівня інформаційного забезпечення належать якісні (відповідність суспільній думці, яку слід сформувати у рамках спільноти; простота та доступність; своєчасність публікації; актуальність; грамотність подання; розмір повідомлень тощо) та кількісні (кількість, періодичність публікацій) характеристики контенту.

Саме ці характеристики визначають кількість переглядів контенту, тривалість взаємодії із ним, коефіцієнт конверсії, географію акторів тощо. Крім того, рівень інформаційного забезпечення у межах як віртуальної спільноти, так і суспільства в цілому залежить від кількості акторів та їх поведінки.

Особливу загрозу розвитку стійких віртуальних спільнот мають порушники інформаційної безпеки. Загалом, порушники інформаційної безпеки здійснюють навмисну або ненавмисну дію, яка суперечить інтересам окремих акторів та/або обмежує досягнення позитивних ефектів функціонування спільноти.

Актори-порушники з навмисно деструктивною поведінкою використовують методи пропаганди, поширюють дезінформацію та шкідливий контент, некоректно поводяться із іншими акторами. Для аналізу та ідентифікації осіб, що можуть становити потенційну загрозу інформаційній безпеці віртуальній спільноті, розроблено класифікацію порушників інформаційної безпеки (табл. 1).

Розроблена класифікація порушників демонструє широкий спектр осіб, які можуть становити потенційну загрозу інформаційній безпеці віртуальної спільноти: $O = \langle R, Q, A, M, N, P, V \rangle$.

З метою уникнення порушень інформаційної безпеки, необхідними є формування та формалізація системи інституціональних обмежень (формально закріплених та неформальних норм, правил, інструкцій) щодо поведінки у межах спільноти. У разі порушення цих обмежень мають запускатись регуляційні механізми спільноти (у тому числі, за ініціативою інших акторів) для усунення негативних інформаційних впливів. Імплементація таких механізмів передбачає регулювання складу акторів віртуальної спільноти, зокрема за рахунок збільшення чисельності активних акторів з продуктивною поведінкою, а також мінімізації деструктивних впливів акторів-порушників. Ключовим у виборі інструментів регулювання поведінкою акторів-порушників інформаційної безпеки є розподіл їх дій на навмисно та ненавмисно шкідливі. Кількість акторів-порушників з навмисно шкідливою поведінкою має мінімізуватись та прямувати до нуля. Що ж стосується ненавмисних порушників, то існуючі механізми регуляції віртуальної спільноти мають забезпечити їх трансформацію у активних акторів з продуктивною поведінкою. Для забезпечення максимальної ефективності регулювання поведінкою порушників інформаційної безпеки обох типів, важливим є об'єднання зусиль максимальної кількості учасників спільності соціальних мереж.

Відповідно до вище викладеної логіки запропоновано механізм соціального контролю, що сприятиме забезпеченню інформаційної безпеки та розвитку сталої віртуальної спільноти. Розглянемо ключові аспекти механізму соціального контролю:

1. Створення норм та правил $\{R_k\}$, $k = \overline{1,m}$. Важливо, щоб віртуальна спільнота мала чіткі норми та правила поведінки, які визначають, що допустимо і недопустимо для її учасників. Це може включати в себе правила щодо образливого мовлення, дискримінації, плагіату тощо;

2. Модерація та адміністрування. Віртуальні спільноти можуть мати модераторів та адміністраторів, які відповідають за виконання норм і правил $\{M_b\}$, $b = \overline{1,r}$. Вони можуть здійснювати моніторинг спільноти, видаляти або приховувати контент, який порушує правила, і накладати санкції на порушників;

3. Формування та формальне закріплення заохочень позитивної поведінки $\{P_l\}$, $l = \overline{1,g}$. Віртуальна спільнота може мати систему заохочення позитивної поведінки її учасників, зокрема нагороди, визнання членів або інші форми позитивного підкріплення;

4. Спільна відповідальність η. Учасники спільноти також повинні відчувати спільну відповідальність за її розвиток та безпеку. Це може бути здійснено через розповсюдження ідеї колекти-

вного власництва та активної участі у вирішенні конфліктів і проблем;

5. Навчання та освіта α. Важливо забезпечувати учасників спільноти навчанням та освітою щодо їх прав та обов'язків, а також щодо того, як вони можуть сприяти сталому розвитку спільноти;

6. Взаємодія з іншими спільнотами і організаціями. Віртуальна спільнота може співпрацювати з іншими спільнотами і організаціями, щоб обмінюватися досвідом, ресурсами та інформацією для спільного розвитку;

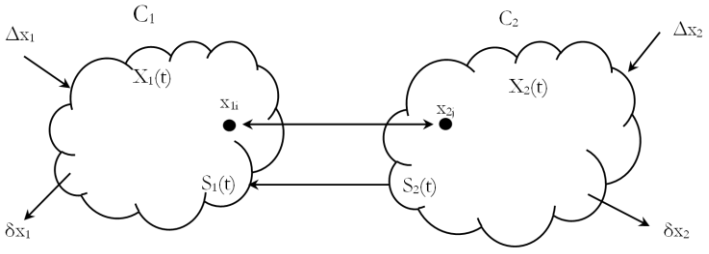
7. Моніторинг та удосконалення відповідно до змін у віртуальній спільноті та потреб її учасників.

Формалізація предмету дослідження

Предметом даного дослідження є процеси еволюції віртуальної спільноти в антагоністичному середовищі. Нехай деякий СІС перебуває у стані m_i з множини можливих $M=\{m_i\}$, $i=\overline{1,n}$, який визначає актуальний рівень інформаційної безпеки $Z_{actual}^{m_i}$. У свою чергу, такий стан СІС описується вектором параметрів PR. Внаслідок антагоністичного/конкурентного впливу на інформаційний простір СІС $U_i(COMP)$, а також під дією інструментів соціального контролю $U_j(SC)$ за час T відбуваються процеси еволюції акторів – змінюється структура віртуальних спільнот або параметри взаємодії акторів між собою. Тоді СІС переходить до заданого стану інформаційної безпеки $Z_{preset}^{k_l}$ з можливих $K=\{k_l\}$, тобто:

$$Z_{actual}^{mi}(t)\xrightarrow[Z\in\Omega(PR)]{T\to\min,\ \bigcup_j(SC),\bigcup_k(COMP)} Z_{present}^{k}(t+T),\quad F_q(U)=\bigcup_{j=0}U_j(SC). \tag{1}$$

Завдання полягає у визначенні сукупності механізмів соціального контролю у СІС $F_q(U)$, використання яких забезпечить стійке функціонування СІС в умовах дії антагоністичного середовища. На рис. представлена схема функціонування/еволюції досліджуваної віртуальної спільноти в умовах антагоністичного середовища.



Примітка: C_1 – досліджувана віртуальна спільнота; C_2 – антагоністична віртуальна спільнота; $S_1(t)$ – частка нових публікацій на задану тему у віртуальній спільноті C_1, опублікованих учасниками (акторами X_1); $X_1(t)$, $X_2(t)$ – кількість акторів у віртуальних спільнотах C_1, C_2, відповідно; $S_1(t)$ – частка публікацій у спільноті C_1; $S_2(t)$ – частка публікацій (антагоністичних) у спільноті C_2, спрямованих на C_1, опублікованих учасниками (акторами X_2); $x_{1i}\leftrightarrow x_{2j}$ – безпосередня комунікація (взаємодія) між акторами C_1 та C_2; Δx_1, Δx_2 – приріст нових акторів в C_1 та C_2, відповідно; δx_1, δx_2 – відтік акторів з C_1 та C_2, відповідно.

Розглянемо завдання формування віртуальної спільноти акторів, яка буде здатна до сталого розвитку завдяки активізації віртуальної петлі – швидкості поширення контенту в СІС, а також ефективній протидії деструктивним діям антагоністичного середовища через реалізацію комплексу заходів у вигляді соціальних санкцій. Формалізуємо процеси взаємодії акторів віртуальної спільноти у СІС у вигляді модифікованої моделі Моно, яка додатково описує взаємодію із зовнішнім середовищем, представленим конкурентним типом взаємодії, і представляє собою систему звичайних диференціальних рівнянь:

$$\begin{cases}\dfrac{dx_1}{dt}=\mu_1(S_1)x_1-D_1x_1-b_1x_1x_2-\xi S_2x_1+a_1x_1\\ \dfrac{dx_2}{dt}=a_2x_2-b_2x_1x_2\\ \dfrac{dS_1}{dt}=D_1u_{S1}(t)-\alpha_1\mu_1(S_1)x_1-D_1S_1+\xi S_2\\ \mu_1(S_1)=\dfrac{\mu_m S_1}{K_m+S_1}\end{cases}. \tag{2}$$

$S_2(t)$ – невід'ємна функція, $S_2(t_j) > S_2(t_i)$, при $t_j > t_i$, тобто частка антагоністичного контенту логічно зросте $\frac{dS_2}{dt} > 0$, для $\forall t$, де $x_1(t)$, $x_2(t)$ – кількість акторів у, відповідно, досліджуваній C_1 та антагоністичній C_2 віртуальних спільнотах; $S_1(t)$ – частка публікацій учасників досліджуваної віртуальної спільноти C_1; $D_1 x_1$ – приріст нових учасників у досліджуваній спільноті C_1; $b_1 x_1 x_2$ – відтік учасників, зумовлений взаємодією акторів досліджуваної спільноти C_1 та антагоністичної спільноти C_2; $S_2(t)$ – частка деструктивних публікацій, спрямованих на учасників досліджуваної спільноти C_1; $\xi S_2 x_1$ – відтік акторів з досліджуваної спільноти C_1 через антагоністичні публікації; $a_1 x_1$ – приріст нових акторів в спільноті C_1 через залучення безпосередньо акторами з C_1; $a_2 x_2$ – приріст нових акторів в спільноті C_2 через залучення безпосередньо акторами з C_2; $b_2 x_1 x_2$ – відтік акторів з C_1 через безпосередню комунікацію з акторами C_1; $D_1 u_{S1}$ – кероване зростання частки публікацій, що забезпечують стійкість віртуальної спільноти C_1; $\mu_1(S_1)x$ – приріст акторів в спільноті C_1 через зацікавленість часткою контенту S_1; $\alpha_1 \mu_1(S_1) x_1$ – кількість публікацій, які вплинули на формування суспільної думки акторів віртуальної спільноти C_1; $D_1 S_1$ – зменшення кількості публікацій, які не викликали зацікавленості акторів глобальної СІС та не спонукали їх стати учасниками віртуальної спільноти C_1; ξS_2 – приріст частки публікацій, обумовлений необхідністю протидіяти антагоністичному контенту; $\mu_1(S_1)$ – функція, яка описує обмежене зростання частки контенту; μ_m – максимальна швидкість появи публікацій; K_m – константа, яка чисельно дорівнює частці публікацій, за яких швидкість зростання x_1 дорівнює половині від максимально можливої.

З огляду на роль та місце соціального контролю в процесі еволюції віртуальної спільноти модель (2) дозволяє формалізувати застосування соціальних санкцій як управління динамікою соціальної спільноти у вигляді:

$$U(t) = f\left(U_S(t), \vec{\beta}, \alpha\right),$$

де $U_S(t)$ – функція управління якістю публікацій учасників віртуальної спільноти; з практичної точки зору комплекс заходів спрямованих на удосконалення форми та змісту контенту; $\vec{\beta} = \{b_1; b_2\}$ – управління випливами контенту на суспільну думку глобального СІС, з метою підвищення репутації та зацікавленості з боку інших віртуальних спільнот.

Зважаючи на високу швидкість зростання кількості акторів і віртуальних спільнот у СІС, виникнення еволюційних процесів у межах віртуальних спільнот, інтенсивність обміну інформацією між СІС і зовнішнім середовищем його функціонування – національним та світовим інформаційними просторами, використаємо для опису взаємодії акторів у СІС модель мікробіологічної системи. Публікацію контенту заданого змісту здійснюють учасники команди віртуальної спільноти у СІС, які виступають її адміністраторами. Для формалізації зовнішнього впливу доцільно використати підходи популяційної динаміки, а саме взаємообумовлений розвиток / взаємодію / конкуренцію двох видів.

ВИСНОВКИ

У роботі систематизовано та розглянуто аспекти і компоненти механізму соціального контролю щодо забезпечення сталого функціонування віртуальних спільнот в інтернет-сервісах. Параметризовано модель, яка враховує еволюцію віртуальної спільноти як систему в антагоністичному середовищі. Синтезовано функцію управління шляхом реалізації комплексу заходів соціального контролю та санкцій у вигляді функціоналу, який враховує керування контентом, контроль за комунікацією між учасниками різних віртуальних спільнот, а також комплекс заходів щодо підвищення привабливості та зацікавленості в активності у межах спільноти.

ЛІТЕРАТУРА

[1] Предместніков О., Хотмірова В. Соціальні мережі як майданчик для порушення прав людини: можливості та загрози. Scientific Collection «InterConf».

2023. С. 276-284. URL: https://archive. interconf. center/ index.php / conference-proceeding / article/ view/3485 (дата звернення : 14.09.2023).
[2] Молодецька К. В. Механізми синергетично керованої самоорганізації акторів у соціальних інтернет-сервісах. Управління розвитком. 2018. Т. 4. вип. 4. С. 1-13. URL: http://dx.doi.org/10.21511/dm. 4(4).2018.01 (дата звернення: 10.09.2023).
[3] Fedushko S., Molodetska K., Syerov Y. Decision-making approaches in the antagonistic digital communication of the online communities users. Soc Netw Anal Min. 2023. № 13(1). P. 18. doi: 10.1007/s13278-022-01021-4. Epub 2023 Jan 3. PMID: 3661-9664; PMCID: PMC9808702 (Accessed : 10.09.2023).
[4] Jyh-Jeng Wu, Alex S. L. Tsang. Factors affecting members' trust belief and behaviour intention in virtual communities. Behaviour & Information Technology. 2008. № 27. С. 2. pp. 115-125. doi: 10.1080/01449290600961910 (Accessed : 17.09.2023).
[5] Oz, Mustafa; Oz Cetindere, Esra Nur. Perceived Social Sanctions and Deindividuation: Understanding the Silencing Process on Social Media Platforms. International Journal of Communication, [S.l.]. 2023. Vol. 17. P. 22. Available at : https://ijoc.org/index.php/ijoc/article/view/20116 (Accessed: 08.09.2023).
[6] Sumit Joshi, Ahmed Saber Mahmud, Sanctions in networks. European Economic Review. 2020. Vol. 130. Available at: https: // doi. org / 10.1016 /j.euroecorev.2020.103606 (Accessed : 11.09.2023).
[7] Zhang, K., Lo, D., Lim, EP. Mining Antagonistic Communities from Social Networks. In: Zaki, M.J., Yu, J.X., Ravindran, B., Pudi, V. (eds) Advances in Knowledge Discovery and Data Mining. PAKDD 2010. Lecture Notes in Computer Science. 2010. Vol. 6118. Springer, Berlin, Heidelberg. https://doi.org/10. 1007 / 978-3-642-13657-3_10 (Accessed: 07.09. 2023).

SYNTHESIS OF THE SOCIAL SANCTIONS MODEL FOR ENSURING THE SUSTAINABILITY OF VIRTUAL COMMUNITIES IN SOCIAL NETWORKS IN THE CONDITIONS OF AN ANTAGONISTIC ENVIRONMENT

The rapid integration of virtual communications into social life actualizes the need to create a safe and comfortable environment for the communication of virtual community users. The purpose of the study is to increase the level of information security of social virtual groups by substantiating and formalizing the features of using social control tools to manage the dynamics of the virtual community in the information space. The process of the virtual community evolution in the conditions of an antagonistic environment, as well as the functionality of management and ensuring the stability of the virtual community in social Internet services were formalized on the basis of Mono model and population dynamics model. The impact of the share of destructive publications that pose a threat to information security of the social community; the depth of communication between the actors of the studied community and the participants of the antagonistic community; content quality indicators were determined as the parameters of the author's model. The components of social control in social Internet services and the classification of violators of information security were further developed.

Keywords: antagonistic environment, virtual community, threat, information security, sanctions, social network, social control.

Євсеєв Сергій Петрович, доктор технічних наук, професор, завідувач кафедри кібербезпеки Національного технічного університету «Харківський політехнічний інститут».

Serhii Yevseiev, Doctor of Technical Sciences, Professor, Head of Cyber Security Department, National Technical University "Kharkiv Polytechnic Institute".
E-mail: serhii.yevseiev@gmail.com.
Orcid ID: 0000-0003-1647-6444.

Тимонін Юрій Олександрович, кандидат технічних наук, доцент, доцент кафедри комп'ютерних технологій і моделювання систем Поліського національного університету.

Yuriy Tymonin, Candidate of Technical Sciences, Docent, Associate Professor of Computer Technology and Systems Modeling Department, Polissia National University.
E-mail: ytimonin45@gmail.com.
Orcid ID: 0000-0002-0179-5226.

Веретюк Сергій Михайлович, кандидат технічних наук, старший викладач кафедри комп'ютерних технологій і моделювання систем Поліського національного університету.

Serhiy Veretiuk, Candidate of Technical Sciences, Senior Lecturer of Computer Technology and Systems Modeling Department, Polissia National University.
E-mail: sergey.veretiuk.pnu@gmail.com.
Orcid ID: 0000-0002-7915-9991.

Войтко Тетяна Миколаївна, науковий співробітник науково-дослідного відділу Інституту інформаційно-комунікаційних технологій та кібероборони Національного університету оборони України.

Tetiana Voitko, Researcher of the Research Department, Institute of Information and Communication Technologies and Cyber Defense, National Defence University.
E-mail: t.voytko@ukr.net.
Orcid ID: 0000-0002-4326-0633.

Оленюк Дмитро Олександрович, аспірант, асистент кафедри комп'ютерних технологій і моделювання систем Поліського національного університету.

Dmytro Oleniuk, Postgraduate student, Assistant of Computer Technology and Systems Modeling Department, Polissia National University.
E-mail: omuzif@gmail.com.
Orcid ID: 0000-0002-9641-3795.

DOI: 10.18372/2410-7840.25.17940
УДК 004.056.5

ЗАСТОСУВАННЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ ТА ПОСЛІДОВНОСТЕЙ В КІБЕРБЕЗПЕЦІ, МЕТОДИ ЇХ ПОБУДОВИ ТА ОЦІНКИ ЯКОСТІ

Марія Хомік, Олег Гарасимчук

У зв'язку з бурхливим розвитком обчислювальної і вимірювальної техніки, а також із впровадженням новітніх технологій значно розширилась сфера застосування генераторів псевдовипадкових чисел та псевдовипадкових послідовностей, що ставить нові вимоги до їх проектування та методів оцінки якості. Якісні псевдовипадкові послідовності, хоча і є за своєю суттю детермінованими, володіють проте практично всіма властивостями реалізацій істинно випадкових процесів і успішно їх замінюють, оскільки формування випадкових послідовностей надзвичайно складне. У зв'язку з різноманітністю і широким спектром завдань, які потребують використання псевдовипадкових числових послідовностей, постійно розробляються і вдосконалюються нові алгоритми, методи і засоби для отримання таких послідовностей. За допомогою генераторів псевдовипадкових послідовностей можна отримувати послідовності чисел, де кожен елемент практично незалежний від інших і відповідає певному заданому закону розподілу, найбільш поширеним з яких є рівномірний закон розподілу. Завдяки своїм статистичним властивостям та швидкості генерації генератори псевдовипадкових чисел та послідовностей є важливим інструментом для багатьох сфер діяльності: імітаційного моделювання (економічні, математичні, фізичні, медичні дослідження, військова справа), розробок комп'ютерних ігор (генерація 3D-моделей, текстур та світів, а також створення різноманітності та випадковості у поведінці персонажів та подій), вимірювальної техніки. Загалом важливо відзначити, що розробники генераторів псевдовипадкових послідовностей стикаються з низкою жорстких вимог, щодо певних характеристик результатів, які вони створюють за допомогою цих генераторів. Ці вимоги можуть варіюватися залежно від конкретного призначення генератора, і в разі використання псевдовипадкових послідовностей у сферах кібербезпеки та захисту інформації, вони можуть бути особливо високими і вимогливими. Наприклад, для криптографічних застосувань вимоги є надзвичайно суворими і часом навіть протирічать одна одній. Для перевірки відповідності згенерованої послідовності заданим критеріям та вимогам необхідно провести оцінювання її якості, під час якого проводиться оцінювання за різними ознаками та параметрами. Оскільки при розробці генераторів псевдовипадкових послідовностей прагнуть досягти того, щоб вони були схожі на послідовності чисел, що розподіляються дійсно випадково, то в основі будь-якого оцінювання генераторів лежить порівняння статистичних характеристик згенерованої послідовності з характеристиками істинно випадкових послідовностей. З цією метою використовуються різноманітні тести, які дозволяють виявляти наявні статистичні закономірності і, таким чином, виявляти низьку якість згенерованих псевдовипадкових послідовностей.

***Ключові слова**: генератори псевдовипадкових чисел, генератори псевдовипадкових послідовностей, кібербезпека, генерування, тестування, оцінювання якості.*

ВСТУП

Швидкий розвиток інформаційних технологій та засобів обчислювальної техніки значно розширив сферу застосування випадкових чисел та послідовностей та підвищив вимоги, які висуваються до пристроїв їх генерування.