Головня О. С., к.пед.н.,
доцент кафедри комп'ютерної інженерії та кібербезпеки
Бродський Ю. Б., к.т.н., доц.,
доцент кафедри комп'ютерної інженерії та кібербезпеки
Державний університет «Житомирська політехніка»

ІНФОРМАЦІЙНА БЕЗПЕКА ТА КІБЕРБЕЗПЕКА: СОЦІАЛЬНИЙ ВИМІР

Небезпекові явища часто мають комплексний характер і можуть поєднувати фактори різної природи (геофізичної, екологічної, політичної, економічної, соціальної, інформаційної тощо). Водночас, вчасне виявлення небезпекових явищ та потенційних катастроф можливе у разі належного спостереження та аналізу [1]. Усі небезпекові явища мають тією чи іншою мірою виражену соціальну складову, оскільки ключові управлінські рішення, врешті решт, приймаються людьми. Цей зв'язок особливо помітний у галузях інформаційної та кібернетичної безпеки.

Кібернетична безпека розглядає такі об'єкти впливу, як системи збору даних, канали інтерактивної взаємодії, а також органи й канали управління. Тим часом, інформаційна безпека має справу з базами даних, інформаційними потоками та персоналом [2]. Таким чином, безпека кіберпростору є складовою безпеки інформаційного простору, і ці поняття варто розглядати поряд, як тісно пов'язані між собою.

У низці публікацій досліджено соціальну складову інформаційних систем, зокрема інформаційні процеси всередині соціальних мереж [3], агенто-орієнтоване моделювання інформаційних систем [4] та інформаційних операцій [5], системи забезпечення інформаційної безпеки держави у соціальних Інтернет-сервісах [6] та ін.

Метою даної роботи є виокремлення основних соціальних аспектів інформаційної безпеки та кібербезпеки, окреслення напрямів для подальших досліджень цих аспектів.

Можна окреслити два основні напрями для вивчення:

1) небезпекові соціальні явища у кібернетичному просторі (пов'язані з *поведінкою користувачів* інформаційних систем, умисними та неумисними порушеннями безпеки цими користувачами);

2) небезпекові соціальні явища в інформаційному просторі (пов'язані з *інформацією та реакцією на неї* індивідів та соціальних груп).

Перший напрям стосується різноманітних контейнерів, що містять дані, та каналів між ними (операційні системи, комп'ютерні мережі, онлайн-сервіси). Другий напрям пов'язаний з взаємодією користувачів з метою обміну інформацією за допомогою інформаційних технологій (соціальні мережі, сервіси миттєвого обміну повідомленнями, електронні засоби масової інформації тощо).

Небезпекові соціальні явища у кібернетичному просторі. Ефект від належного адміністрування комп'ютерних систем та мереж може суттєво знижуватися, коли користувачі цих систем та мереж не дотримуються правил безпеки (наприклад, допускаючи вхід інших осіб під власними реквізитами). Роз'яснення користувачам основ інформаційної безпеки є важливим, проте його недостатньо, аби мінімізувати людський фактор як одну з вразливостей цих систем. Напрям для розвитку ми вбачаємо у моніторингу та аналізі (зокрема, й через анонімні опитування) того, як саме користувачі застосовують запропоновані їм безпекові механізми, з якими труднощами вони зустрічаються, які заходи видаються їм надмірними та незручними, які обхідні шляхи вони застосовують. Очікувано, тут можуть мати місце як загальні патерни поведінки, так і особливості, притаманні окремим соціальним групам. Результатом мають стати моделі, засоби та рекомендації, що дали б змогу виявити потенційно загрозливі явища, врахувати потреби щодо безпеки та доступності у конкретній організації чи спільноті під час адміністрування комп'ютерних систем та мереж.

Небезпекові соціальні явища в інформаційному просторі. Важливо здійснити виокремлення та систематизацію передвісників соціальних процесів та явищ, які є небезпековими чи мають потенціал перерости в небезпекові (публікації маніпулятивного характеру, фейки, діяльність ботів, кібербулінг, кібершахрайство, поширення теорій змови тощо). Систематизація передвісників повинна враховувати можливі цілі інформаційного впливу.

Наступним кроком є аналіз наявних інструментів для автоматизації виявлення потенційних передвісників, а також моделювання й розроблення нових інструментів. Особливу роль вбачаємо у міждисциплінарних дослідженнях, пов'язаних, з одного боку, з аналізом небезпекових соціальних явищ з точки зору комп'ютерних наук, а з іншого – залученням експертної думки та результатів досліджень у галузі суспільних наук. Варто наголосити, що метою досліджень соціальних аспектів інформаційної безпеки не повинно бути створення інструментів та моделей, спрямованих на надмірний контроль над інформаційним полем. Йдеться як про інформаційний простір у державах з недемократичними політичними режимами, так і про намагання витіснити з інформаційного простору будь-які висловлювання, що порушують суспільний спокій (наприклад, спекулятивне застосування терміну "мова ненависті"). Подібні наміри самі по собі сприяють появі небезпекових соціальних явищ замість того, аби попереджати про них чи боротися з ними.

Висновки. Дослідження соціального виміру інформаційної безпеки та кібербезпеки на основі міждисциплінарного підходу є важливою складовою попередження про небезпекові явища. Доцільним є вивчення соціальних аспектів, які стосуються і безпеки комп'ютерних систем та мереж, і обміну інформацією за допомогою цих систем та мереж. Подальші дослідження варто спрямувати на виокремлення та систематизацію передвісників небезпекових соціальних процесів та явищ.

Список використаних джерел

1. O. Maevsky, V. Artemchuk, Yu. Brodsky, L. Makarenko, Yu. Shpylovyi. A conceptual approach to the development of software tools for the analysis and synthesis of geophysical monitoring systems models. – Studies in Systems, Decision and Control. – Springer, 2021, pp. 333-345. URL: https://www.springerprofessional.de/en/a-conceptual-approach-to-the-development-of-software-tools-for-t/18988478
2. В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа, Інформаційна та кібербезпека: соціотехнічний аспект. За ред. В. Б. Толубка. – Київ: ДУТ, 2015, 288 с.
3. О. С. Онищенко, В. М. Горовий, В. І . Попик. Соціальні мережі як інструмент взаємовпливу влади та громадянського суспільства: Монографія. – НАН України, Нац. б-ка України ім. В. І. Вернадського. – К ., 2014 . – 260 с.
4. J. Epstein, Generative Social Science: Studies in Agent-Based Computational Modeling. — Princeton: Princeton University Press, 2012, 384 p.
5. В. Горбулін, О. Додонов, Д. Ланде, Інформаційні операції та безпека суспільства: загрози, протидія, моделювання. Монографія. Київ: Інтертехнологія, 2009, 164 с.
6. Р. Грищук, К. Молодецька-Гринчук. Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних Інтернет-сервісах. – Захист інформації, Т. 19, №4, 2017, с. 254-262.