УДК 004.056

В. М. Островська
Л. М. Ткачук

ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ ВПЛИВІВ В КІБЕРПРОСТОРІ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Вінницький національний технічний університет

Анотація

В роботі досліджено інформаційні впливи на учасників спілкування у соціальних мережах, що визначають аспекти прояву загроз кібербезпеці держави. Виконано формалізацію проблеми забезпечення кібербезпеки. Запропоновано концептуальний базис виявлення й оцінювання загроз кібербезпеці, який полягає у з'ясуванні ознак інформаційних впливів, оцінювання рівня загроз та розроблення заходів протидії цим загрозам.

Ключові слова: кіберпростір, кібербезпека, інформаційні впливи, загрози кібербезпеці.

Abstract

The information influences on social networking participants, which determine the aspects of the threats manifestation to the cybersecurity of the state, is researched at the article. The formalization of the problem of cybersecurity are performed. The conceptual basis for detecting and assessing threats to cybersecurity, which consists in identifying signs of information influences, assessing the level of threats and developing measures to counteract these threats, is proposed.

Keywords: cyberspace, cybersecurity, information influences, cybersecurity threats.

Вступ

Сучасні інформаційні технології обумовлюють зростання соціальної активності індивідуумів. Особливо яскраво це проявляється при використанні технологій соціальних мереж, що зумовили істотні зміни у функціонуванні механізмів інформаційних обмінів у суспільстві. Постійне зростання потужності інформаційних потоків значно ускладнює процес їхнього контролю з точки зору кібербезпеки. Поки що системи державного контролю не можуть вчасно і повною мірою реагувати на змінні показники в кіберпросторі [1].

Метою роботи є розроблення концептуального базису виявлення і оцінювання загроз кібербезпеці держави для підвищення ефективності протидії цим загрозам.

Результати дослідження

Розглядаючи вплив кіберпростору на особистість, слід враховувати, що він поширюється на суспільство та державу і через них опосередковано на кожного індивідуума [2]. Серед багатьох способів інформаційних впливів, які реалізуються в кіберпросторі, можна виокремити поширення спеціально підібраної інформації – дезінформації. Цей спосіб впливу здійснюється у таких формах:

- розсилка листів електронною поштою;
- організація груп новин у соціальних мережах;
- створення сайтів з елементами інтерактивності (чати, голосування в режимі онлайн);
- розміщення інформації на приватних за змістом веб-ресурсах, тобто у блогах, соціальних мережах [3].

Поширення дезінформації у соціальних мережах із застосуванням технологій маніпулятивного впливу на індивідуальну і колективну свідомість може спричинити соціальну напруженість, незадоволення існуючою системою управління в державі, міжнаціональну ворожнечу тощо. Досвід збройної агресії Російської Федерації проти України чи не вперше яскраво продемонстрував, що соціальні мережі є одним з ефективних інструментів ведення нової форми протистояння – гібридної війни. Практика функціонування соціальних мереж в останні роки свідчить про те, що вони перетворилися на джерело загроз кібербезпеці держави [4, 5], актуалізувавши необхідність розробки методик та тех-

нологій, які були б ефективними для нейтралізації діяльності іноземних структур, спрямованої проти інтересів України.

Одним із найпоширеніших у соціальних мережах різновидів інформаційно-психологічної дії є тролінг (англ. trolling – «виспівувати»), застосовуваний для формування суспільної думки з актуальних питань та активного обговорення другорядних подій. Відповідно, тролями можуть бути люди або програми, які розміщують грубі і провокаційні за змістом повідомлення в мережі Інтернет. Результати аналізу текстового контенту, поширюваного тролями, свідчать, що він містить дезінформацію з елементами маніпулювання [6]. Такий контент, як правило, висвітлює актуальну тематику подій, яка загрожує кібербезпеці держави. Застосування маніпуляцій суспільною думкою викликає нав'язування і спонукання до виконання визначених дій не тільки у соціальних мережах, а й у реальному житті, що проявляється у проектуванні бажаних емоційних станів, обговоренні недостовірної інформації тощо [7].

Основним джерелом публікацій у соціальних мережах є користувачі, які використовують наявні засоби для публікації самостійно створеного контенту та поширення опублікованої інформації інших користувачів, спільнот чи ЗМІ. Оцінювання профілів користувачів соціальних мереж дає змогу виявити осіб, залучених до інформаційних-психологічних дій у соціальних мережах. Таким чином, загрози кібербезпеці держави характеризуються різними ознаками інформаційних впливів, що визначають аспекти їх прояву. Окремі інформаційно-психологічні операції можуть відрізнятися між собою не тільки змістом, а й використаними технологіями, що додатково ускладнює процедури виявлення ознак проведення та оцінювання рівня загроз.

Отже, проблема виявлення ознак інформаційних впливів у соціальних мережах, оцінювання рівня загроз кібербезпеці держави та розроблення заходів протидії цим загрозам першочергово зводиться до вироблення нових методів і технологій виявлення ознак інформаційних впливів (рис. 1).

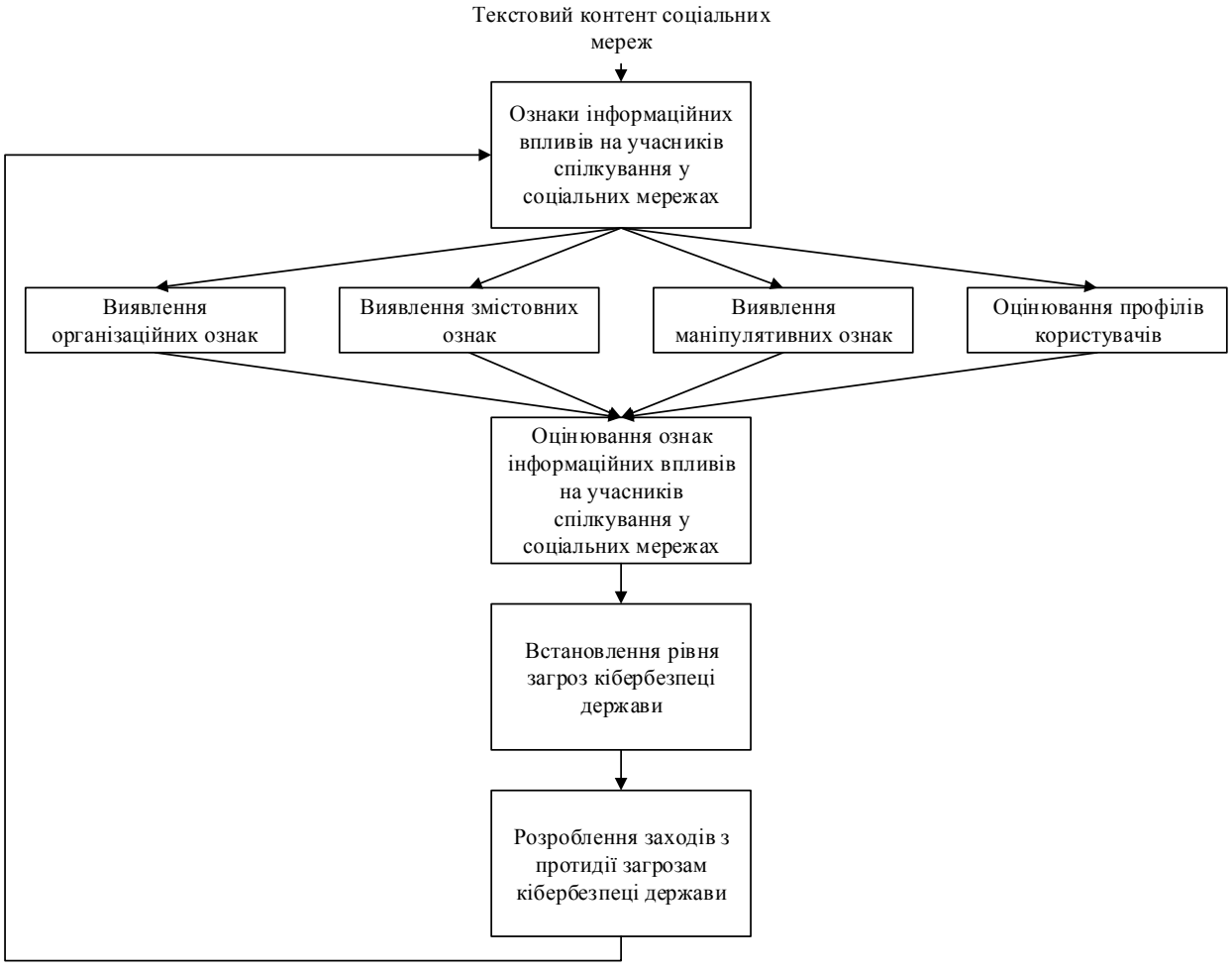

Рис. 1. Концептуальний базис виявлення й оцінювання загроз кібербезпеці держави

Виявлення ознак інформаційних впливів доцільно реалізувати за частинними ознаками їх прояву – організаційними, змістовними, маніпулятивними та на основі оцінювання профілів користувачів. Важливо врахувати, що загрози кібербезпеці держави не завжди проявляються одразу за усіма ознаками. На основі визначеного рівня ознак загроз у соціальних мережах проводяться заходи з їх нейтралізації та протидії відповідними уповноваженими структурами.

Висновки

Соціальні мережі є дієвим інструментом впливу на суспільні і політичні процеси у державі. Тому забезпечення кібербезпеки в умовах глобалізації інформаційного простору і гібридизації воєнних конфліктів є однією із нагальних проблем, які потребують нагального вирішення. Розроблений базис виявлення й оцінювання загроз кібербезпеці дає змогу підвищити ефективність протидії цим загрозам, оскільки, насамперед, полягає у виявленні інформаційних впливів, що визначають аспекти їх прояву.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Петрик В. Небезпеки інформаційного простору для особистості [Електронний ресурс] / В. Петрик // Українські підручники. – Режим доступу : http://westudents.com.ua/glavy/53529-rozdl-3-nebezpeki-nformatsynogo-prostoru-dlya-osobistost.html. – Назва з екрану.
2. Почепцов Г. Г. Інформаційна політика : навч. посіб. / Почепцов Г. Г., Чукут С. А. – [2-ге вид., стер.]. – Київ : Знання, 2008. – 663 с.
3. Шестаков В. І. Визначення характеристик інформаційного впливу на складові інформаційно-телекомунікаційних систем в умовах інформаційного протиборства / Шестаков В. І., Чернишук С. В. // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. – Житомир : ЖВІ НАУ, 2011. – Вип. 4. – С. 162–167.
4. Доктрина інформаційної безпеки України (затверджена Указом Президента України №47/2017 від 25 лютого 2017 року) : [Електронний ресурс] / Офіційне представництво Президента України. – Режим доступу : http://www.president.gov.ua/documents/472017-21374 (дата звернення 11.03.2018). – Назва з екрану.
5. Ознаковий принцип формування класифікацій кібератак / О. Г Корченко, С. В. Казмірчук, Є. В. Паціра та ін. // Вісник СНУ ім. В. Даля. – 2010. – №4, т. 1. – С. 184–193.
6. Чернишук С. В. Методика виявлення кібернетичних загроз у природномовних текстах / С. В. Чернишук // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. – 2013. – Вип. 8. – С. 112–121.
7. Сугестивні технології маніпулятивного впливу : навч. посіб. / [В. М. Петрик, М. М. Присяжнюк, Л. Ф. Компанцева та ін.] ; за заг. ред. Є. Д. Скулиша. – [2-ге вид.] – Київ : ЗАТ–ВІПОЛ, 2011. – 248 с.

Островська Вероніка Михайлівна – студентка групи БС–17м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: nika.ostrovska21@gmail.com

Науковий керівник: ***Ткачук Людмила Миколаївна*** — канд. екон. наук, доцент кафедри інтеграції навчання з виробництвом, Вінницький національний технічний університет, м. Вінниця

Ostrovska Veronika M. – Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, email: nika.ostrovska21@gmail.com

Supervisor: ***Tkachuk Lyudmila M.*** — Cand. Sc. (Eng), Assistant Professor of Integration education with production, Vinnytsia National Technical University, Vinnytsia