УДК: 303.483:004.738.5

Степанюк Дарина Василівна
(наук. керівник – д-р філол. наук, професор Шкіцька І. Ю.)
Західноукраїнський національний університет, м. Тернопіль

ОЗНАКИ ШАХРАЙСЬКОЇ ПОВЕДІНКИ В СОЦІАЛЬНИХ МЕРЕЖАХ ТА СПОСОБИ ЇЇ НЕЙТРАЛІЗАЦІЇ

В епоху цифрових технологій соціальні мережі стали невід'ємною частиною нашого життя. Однак разом із перевагами вони мають недоліки, один із яких – поширеність шахрайств. Розпізнавання ознак шахрайської поведінки та знання способів її нейтралізації допоможуть захистити себе та підтримати цілісність онлайн-спільнот.

Перші соціальні мережі, як-от SixDegrees.com (заснована в 1997 році) та Friendster (заснована у 2002 році), були спрямовані на побудову онлайн-спільнот. Але з поширенням соціальних мереж у 2000-х роках почали з'являтися перші випадки шахрайства у вигляді спаму, фішингових атак, крадіжок особистої інформації тощо. Поступово збільшуючи свою популярність, соціальні мережі стали об'єктом вивчення з позиції кібербезпеки, соціології та інших дисциплін. Такі дослідження спрямовані на виявлення схем шахрайської поведінки, пошук методів її виявлення та пошук протистоянь кіберзлочинцям. Наразі фахівці з різних галузей знань, зокрема Д. Будін [1], В. Воронцовський [2], І. Кабачинський [3], В. Сабадаш [4], продовжують вивчати шахрайську поведінку в соціальних мережах, а також здійснюють пошук методів її виявлення та нейтралізації.

Тема шахрайства є дуже популярною в сучасному цифровому світі, оскільки соціальні мережі стали не тільки місцем спілкування, але й важливим каналом для розвитку бізнесу, маркетингу, реклами тощо. Інструментарій шахрайства стрімко розвивається, і кіберзлочинці постійно вдосконалюють свої методи, використовуючи соціальні мережі для фішингу, обману, поширення вірусів тощо. Користувачі соціальних мереж, особливо ті, які не дуже обізнані із цифровою безпекою, стають дуже вразливими перед шахраями. Це може призвести до крадіжок особистої інформації, фінансових втрат і навіть завдати шкоди їхньому психічному здоров'ю. Саме тому ця тема залишається актуальною і вимагає подальшого вивчення.

Мета нашої розвідки – описати ознаки шахрайської поведінки в соцмережах і визначити способи її нейтралізації.

Більшість онлайнових шахрайств здійснюються у популярних сьогодні соціальних мережах, як-от Instagram, Telegram, Facebook, Viber тощо.

Сфери шахрайства в інтернеті:

- працевлаштування;
- благодійність;
- купівля та продаж товарів;
- лотереї та розіграші;
- обман у сфері особистих стосунків [2].

Типовими ознаками шахрайської поведінки в соціальних мережах постають:

1) атипові моделі взаємодії. Ідеться про раптове збільшення кількості підписників, уподобань або коментарів. Така активність часто свідчить про використання ботів або платних сервісів для штучного завищення соціальних показників;

2) відсутність персоналізації (особистих даних користувача). Справжня взаємодія в соціальних мережах передбачає автентичність. Шахрайські облікові записи часто не мають цих характеристик. Вони можуть використовувати загальні привітання або коментарі, що здаються автоматизованими. Це вказує на участь ботів або зловмисників;

3) поширення підозрілих повідомлень. Це можуть бути фішингові відомості, призначені для викрадення особистої інформації під виглядом пропозицій неіснуючих послуг для довірливих користувачів;

4) раптові зміни в поведінці або ідентифікації облікового запису, наприклад, часта зміна фотографій профілю, імен користувачів або біографії. Такі зміни можуть свідчити про спроби уникнення викриття або імітування інших персонажів із метою обману;

5) надсилання великої кількості запитів на дружбу або приватних повідомлень для збільшення охоплення. Такі повідомлення часто містять привабливі пропозиції або запити на конфіденційну інформацію, закликають одержувачів діяти швидко і без сумнівів [3].

Для гарантування безпеки користувачам і збереження довіри до платформ необхідно вживати заходів із попередження та нейтралізації шахрайської поведінки. Розробники соціальних мереж можуть підвищити рівень захисту даних, використовуючи шифрування та двофакторну автентифікацію. Це допоможе захистити особисту інформацію і унеможливити доступ до облікових записів користувачів. Вдосконалення алгоритмів виявлення девіантної поведінки дасть змогу вчасно блокувати шахрайські облікові записи. Важливо мати ефективну систему звітності, щоб користувачі могли швидко повідомляти про підозрілу активність у профілях. Платформи повинні вчасно реагувати на такі скарги і вживати заходів для нейтралізації загроз. Також доцільно проводити інформаційні кампанії та навчальні заходи, щоб підвищити обізнаність пересічних громадян з питань безпеки в соцмережах.

Щоб захистити себе від кіберзлочинців, потрібно дотримуватися кількох правил: створювати надійні паролі, вмикати двофакторну автентифікацію, перевіряти налаштування конфіденційності, остерігатися підозрілих посилань і фейкових акаунтів, не ділитися особистою інформацією.

Отже, в сучасному суспільстві шахрайство стало поширеним, і кількість постраждалих від обманів у віртуальному просторі стрімко зростає. Ознаками шахрайства в соціальних мережах постають атипові моделі взаємодії, відсутність персоналізації, поширення спаму, раптові зміни в поведінці або ідентифікації облікового запису, надсилання великої кількості запитів на дружбу та прямих повідомлень від незнайомих контактів. Обачність і критичне мислення під час комунікації в соціальних мережах допоможуть виявляти та нейтралізовувати шахрайства і дадуть змогу створити безпечніше онлайнове середовище.

Список використаних джерел

1. Будін Д. Особиста безпека в соціальних мережах. *Математичні методи, моделі та інформаційні технології у науці, освіті, економіці, виробництві:* збірник тез ІІ Всеукраїнської науково-практичної Інтернет-конференції з проблем вищої освіти і науки, м. Маріуполь, 29 квітня 2020 р. / Маріупольський державний університет; уклад. Т. В. Шабельник, О. Ф. Дяченко, А. О. Морозова, Ю. А. Лазаревська. Маріуполь: МДУ, 2020. С. 207. URL: https://repository.mu.edu.ua/jspui/bitstream/123456789/1558/1/mat_metody_2020.pdf#page=207 (дата звернення: 26.03.2024).
2. Воронцовський В. Шахрайство в інтернеті. *Фінансовий журнал ITstatti.in.ua.* 01.02.2024. URL: https://itstatti.in.ua/zarobitok-v-interneti/377-shakhrajstvo-v-interneti.html (дата звернення: 25.03.2024).
3. Кабачинський І. П. Інтернет-шахрайство – методи, ознаки та як розпізнати по телефону і в мережі. *New Voice.* 27.11.2023. URL: https://nv.ua/ukr/ukraine/events/internet-shahraystvo-metodi-oznaki-ta-yak-rozpiznati-po-telefonu-ta-v-merezhi-50362848.html (дата звернення: 20.03.2024).
4. Сабадаш В. П. Шахрайство в електронній комерції: реалії сьогодення. *Вісник Запорізького національного університету. Юридичні науки.* 2011. № 1. С. 216–220. URL: https://web.znu.edu.ua/herald/issues/2011/ur_2011_1/216-220.pdf (дата звернення: 20.03.2024).

Анотація. У роботі досліджується шахрайство у віртуальному світі. Ознаками шахрайства в соціальних мережах постають атипові моделі взаємодії, відсутність персоналізації, поширення спаму, раптові зміни в поведінці або ідентифікації облікового запису, надсилання великої кількості запитів на дружбу та прямих повідомлень від незнайомих контактів. Обачність і критичне мислення під час комунікації в соціальних мережах допоможуть виявляти та нейтралізовувати шахрайства і дадуть змогу створити безпечніше онлайнове середовище.

Ключові слова: соціальні мережі, шахрайство, девіантна поведінка, інтернет-середовище, фішинг, спам.

УДК: 004.738

Чорняк Роман Андрійович
(наук. керівник – д-р філол. наук, професор Шкіцька І. Ю.)
Західноукраїнський національний університет, м. Тернопіль

ГІБРИДНІ ВІЙНИ ЯК РІЗНОВИД ІНФОРМАЦІЙНИХ ВІЙН XXI СТ.

Гібридна війна – це форма ведення війни, що передбачає застосування політичних, воєнних, економічних, інформаційних та інших засобів для досягнення цілей. Ідеться про використання методів, стратегій і тактик, що охоплюють різні сфери впливу. Інструментами гібридних війн постають дезінформація і пропаганда, що застосовуються в медіапросторі для поширення неправдивої інформації і зміни громадської думки. Кібератаки є важливою частиною гібридної війни й мають на меті дестабілізування мережі або викрадення інформації [8].

Хоча термін «гібридна війна» виник лише у XX ст., сьогодні він активно функціонує в науковому і публіцистичному дискурсі, адже такий від війни є невід'ємним елементом конфронтації у XXI ст. Проте прояви гібридної війни супроводжують конфлікти людей із давніх часів. Незважаючи на те, що тоді розпо-