Бродський Ю. Б., к.т.н., доцент,
Сябрук М. О., магістрант
Державний університет «Житомирська політехніка»

РОЛЬ СОЦІАЛЬНИХ МЕРЕЖ В ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ

На початок 2023 року 4,76 мільярда людей на планеті є користувачами соціальних мереж (СМ), що є більшою частиною від загальної чисельності населення світу – зазначається у звіті Global Digital 2023. А оцінка веб-трафіку дає зрозуміти, що обсяг відвідувачів є ще більшим, оскільки включає людей, які не залогінені на цих платформах. Пік появи нових користувачів лишився в минулому, але цей показник і далі продовжує бути додатнім, отже, немає жодних підстав вважати, що СМ в найближчому майбутньому зазнають «неминучої смерті» [1].

Внаслідок вище сказаного, проблема кібербезпеки стає критичною. В переважній більшості, користувачі – це непідготовлені, необізнані учасники інформаційної діяльності, що не усвідомлюють змісту та структури інформаційного середовища, впливу, ризиків та його вразливих місць.

На жаль, історія показує, що передові технології в невмілих руках часто стають, швидше, шкодою, аніж допомогою. Кіберзагрози мають широку варіативність, починаючи від втрати конфіденційності, закінчуючи загрозою життю. Кіберзалякування, кіберпереслідування, викрадення, порушення чи фальсифікація даних, перебої, зломи та несанкціонований доступ - це наслідки брейнштормів зловмисників для задоволення власних потреб чи використання даних в комерційних цілях. Все частіше в мережі можна зустріти фішинг, ботів, DDoS-атаки, шкідливе програмне забезпечення.

Однак, кібератаки вже давно перестали бути інструментом окремих людей. Великі, могутні держави вдаються до соціальної інженерії загроз: кібершпигунства, кібертероризму, кібервійни, що включають в себе пропаганду, дезінформацію, залякування та маніпуляції.

Україна вже десятий рік добре відчуває на собі методи і наслідки гібридної війни з російською федерацією. Кіберзброя, що використовується в такій війні, це широкий спектр технічних і програмних інструментів. Завданням будь-якої кібервійни є досягнення певної мети в військовій, політичній, економічній та інших галузях. Крім того, таку війну можна назвати ще й психологічною, так як одним із її завдань є деморалізація, дезорганізація противника та створення хаосу всередині його держави. В першу чергу, внаслідок такої війни, страждають найбільш життєво важливі і функціональні системи. Можна відзначити, що: «Україна з 14 січня 2022 року залишається на першому місці у світі за кількістю кібератак проти неї», – заявив заступник голови Держспецзв'язку Віктор Жора [2].

Важливим моментом, про який не варто забувати, є те, що СМ містять велику кількість розвідувальної інформації, наприклад, маршрути пересування, місця знаходження, досьє військовослужбовців та докази причетності до злочинів.

Зменшенню негативних впливів СМ можуть посприяти такі фактори, як: культура кібербезпеки, невід'ємним елементом якої є відповідальність, та кіберобізнаність, які надаватимуть користувачам актуальну інформацію щодо вищезгаданих кіберзагроз, рекомендації щодо запобіжних заходів і чітко визначать правила поведінки та кібергігієни.

Іншим, не менш важливим, засобом для зменшення негативних наслідків від шкоди, завданої соціальними мережами, має головні завдання: виявлення та класифікація інформації певної тематики, оцінювання процесів поширення та пропаганди, виявлення ознак інформаційних операцій, моніторинг учасників заходів і розповсюдження контрповідомлень для протидії.

Таким чином, кібербезпека являє собою одну з основних складових національної безпеки, а СМ відіграють вагому роль в її забезпеченні. Тому, для розв'язування проблеми кібератак треба підходити комплексно: використовувати апаратно-програмні засоби, що стійкі до кібератак та забезпечують цифровий суверенітет; залучати компетентних фахівців; удосконалювати інтелектуальний потенціал; проводити заходи по забезпеченню користувачів СМ необхідною інформацією та правилами підвищення культури користування соціальними мережами.

Список використаних джерел

1. Digital 2023: global overview report. URL: https://datareportal.com/reports/digital-2023-global-overview-report.
2. Ексклюзивне інтерв'ю із заступником голови Держспецзв'язку України з питань цифрового розвитку, цифрових трансформацій і цифровізації Віктором Жорою агентству «Інтерфакс-Україна». URL: https://interfax.com.ua/news/interview/911979.html.