УДК 004.056

С. В. Хилько
О. П. Войтович

ЗБИРАННЯ ІНФОРМАЦІЇ ПРО МІШЕНЬ ПІД ЧАС ІНФОРМАЦІЙНОЇ ВІЙНИ

Вінницький національний технічний університет;

Анотація

Запропоновано модель, що дозволяє покращити збирання інформації про мішень під час інформаційної війни, за рахунок вибору інформації на кожному з етапів проведення інформаційної операції у кіберпросторі.

Ключові слова: кібербезпека, інформаційна війна, модель кібератаки, OSINT,

Abstract

A model is proposed that allows to improve the collection of information about the target during the information war, due to the selection of information for each stage of the information operation in cyberspace.

Keywords: cyber security, information warfare, cyber attack model, OSINT

Вступ

З початком повномасштабного вторгнення Росії, актуальною є проведення атак, зокрема і у кіберпросторі. Основна мета проведення таких операцій – вплив на настрої груп у суспільстві через конкретних її представників. Для успішного проведення такої кібератаки необхідно чітке формування інформаційного мема, який би змусив конкретного користувача (мішень) виконати необхідні дії, наприклад, відкрити файл у додатку до листа, або перейти на фішингове посилання, або повірити у фейкову новину.

Метою роботи є розроблення моделі проведення інформаційної операції, яка враховує етапи проведення інформаційної атаки та допомагає обрати джерела для збору інформації, що дозволяє підвищити ефективність роботи спеціалістів з кібербезпеки.

Результати дослідження

Аналіз джерел [1-7] показав, що створення ефективних повідомлень під час інформаційної війни необхідно мати інформацію про особу, на яку здійснюватиметься атака. Відомі засоби дозволяють збирати великі обсяги інформації про особу без прив’язки до конкретного завдання та/або етапу на якому відбувається атака, що значно сповільнює та утруднює її провадження.

Модель проведення інформаційної операції, що враховує необхідні на кожному етапі видами та джерелами інформації, що потрібні на кожному етапі атаки, наведено на рис. 1.

Так, на першому етапі необхідно визначити мішень. Для цього потрібні наступні дані: паспортні дані, електронна пошта, IP-адреса, номер телефону. Дану інформацію можна отримати з наступних баз даних або сервісів: SmartSearchBot, Intelligience X, Info Baza.

На другому етапі необхідно почати формувати лист. Оскільки лист або СМС-повідомлення доставляється або на електронну пошту або на номер телефону доцільно скористатися тими самими базами даних.

На третьому етапі необхідно сформувати вміст листа, який зачепить потенційну ціль. Так, можна проаналізувати хобі, тип зайнятості, місцезнаходження та паспортні дані. Використавши цю інформацію можна створити таргетований лист. Дану інформацію можна отримати у соціальних мережах, державних реєстрах або у локальній базі системи, оскільки дані з попереднього етапу зберігаються.

На четвертому етапі можна використати ті самі дані, адже файл чи посилання так само повинні бути дотичними до потенційної цілі.

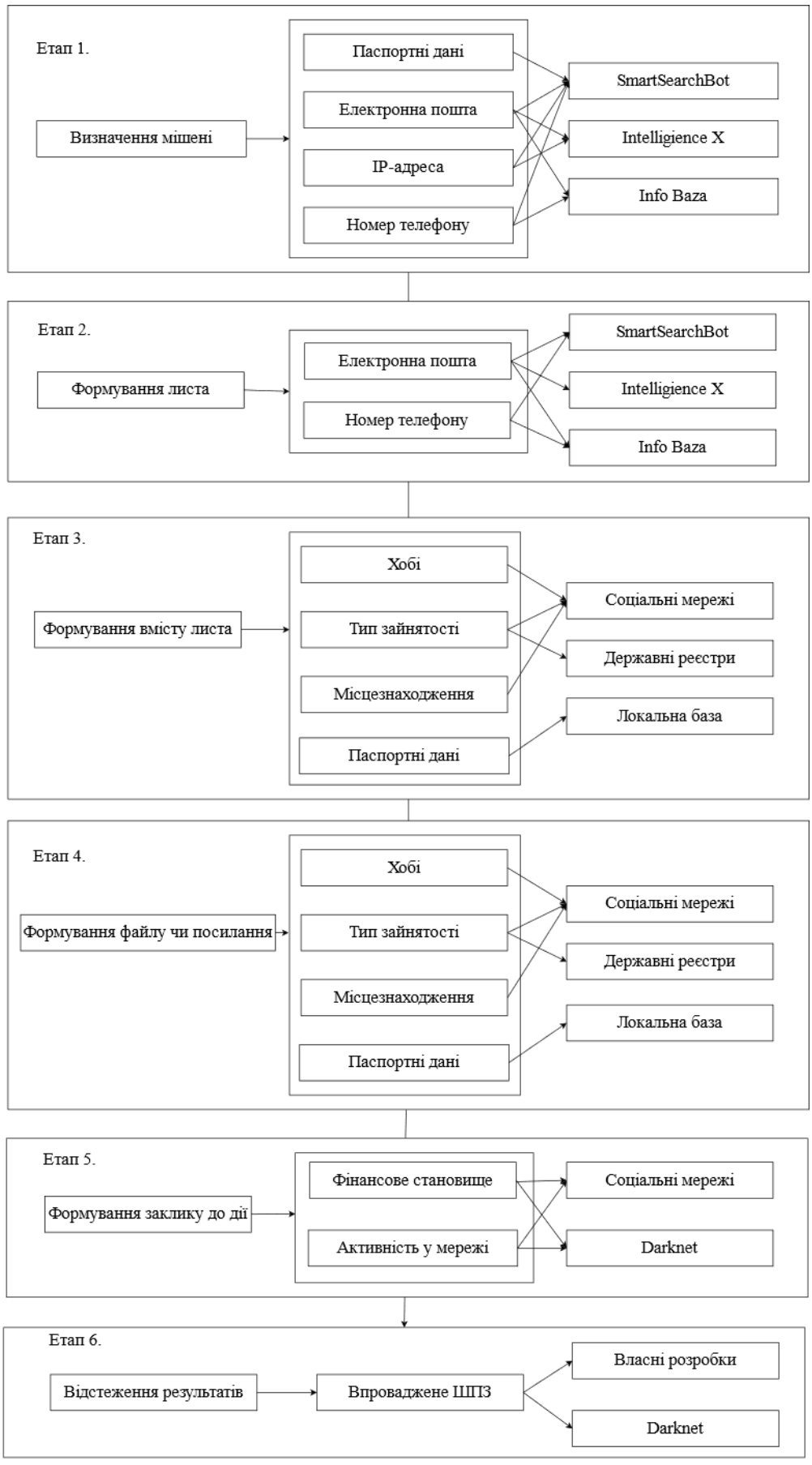

Рис. 1. Модель проведення інформаційної операції

На п’ятому етапі необхідно сформувати заклик до дії. Для цього можна скористатися таким тригером, як фінансове становище або відслідкувати активність цілі у мережі. Це можуть бути злиті історії покупок, дані банківських карток, пошукові запити тощо.

На останньому, шостому етапі, необхідно відслідковувати результати виконання атаки. Якщо за мету ставиться впровадження шкідливого програмного забезпечення, то його можна отримати у Darknet або створити власне.

На основі запропонованої моделі розроблено систему, що дозволяє збирати інформації про мішень під час інформаційної війни з різноманітних джерел.

Висновки

Встановлено, що запропонований підхід дозволяє підвищити швидкість та точність розгортання кібератаки проти супротивника під час інформаційної війни за рахунок підбору конкретного типу інформації та швидкого зчитування з потрібних баз даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Інформаційні війни в історії та сучасності: характерні ознаки новітніх протистоянь. URL: http://enpuir.npu.edu.ua/bitstream/handle/123456789/25591/Zhadko%2064-95.pdf?sequence=1 (дата звернення 10.09.2022).

2. Як працює OSINT-розвідка? Від бізнесу до оборони України. URL: https://www.issp.training/post/yak-pratsyuye-osint-rozvidka-vid-biznes-analizu-do-oborony-ukrayiny (дата звернення 16.09.2022).

3. Що таке OSINT і як він допоміг викрити вбивства у Бучі. URL: https://explainer.ua/shho-take-osint-i-yak-vin-dopomig-vikriti-vbivstva-u-buchi/ (дата звернення 10.10.2022).

4. Як OSINT впливає на війну в Україні? URL: https://blog.iteducenter.ua/articles/osint/ (дата звернення 15.10.2022).

5. Російські ІПСО – як Кремль психологічно тисне на українців? URL: https://24tv.ua/rosiyski-ipso-yak-kreml-psihologichno-tisne-ukrayintsiv-svit_n2210078 (дата звернення 16.10.2022).

6. Що таке ІПСО, чому важливо це знати і які операції зараз проводить Росія проти України. URL: https://tyzhden.ua/shcho-take-ipso-chomu-vazhlyvo-tse-znaty-i-iaki-operatsii-zaraz-provodyt-rosiia-proty-ukrainy/ (дата звернення 23.10.2022).

7. Соціальна інженерія – як один із проявів кіберзлочинності. URL: http://buk-visnyk.cv.ua/news/1581/ (дата звернення 27.10.2022).

Хилько Степан Вікторович — студент групи 1БС-21м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: stepankhylko@ukr.net

Войтович Олеся Петрівна — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет

Khylko Stepan Viktorovych — Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: stepankhylko@ukr.net

Voitovych Olesia P — Cand. Sc. (Eng), Docent of Departmen of Information Protection, Vinnytsia National Technical University, Vinnytsia