УДК.658.3:316.6

В. С. Яковенко, к.е.н., доцент,
Н. К. Казеян,
Дніпропетровський національний університет ім. О. Гончара,
м. Дніпро

СОЦІАЛЬНА ІНЖЕНЕРІЯ В ІНТЕРНЕТ-ПРОСТОРІ

Анотація

У дослідженні актуалізовано питання здійснення впливу особою або групою осіб на користувачів Інтернет простору через інструменти соціальної інженерії. Здійснення прихованого впливу дозволяє отримувати негласно інформацію та впливати на свідомість Інтернет-користувачів. Проведено аналіз останніх досліджень у соціальній інженерії, що дало змогу довести те, що соціальна інженерія, як субнаука ще на етапі становлення та визначення ключових парадигм науки. Проаналізовано методи, які найчастіше застосовуються для здійснення управління учасниками Інтернет-спілок та окремих користувачів. Сформульовано якості та навички соціального хакера, якими він має володіти для здійснення ефективного впливу та маніпулюванням особою. Запропоновано методи протидії соціальній інженерії та висунуто пропозиції щодо подальшого вивчення цього наукового напрямку.

Ключові слова: соціальна інженерія, методи управління, соціальний хакер, Інтернет-середовище, користувачі, вплив.

В. С. Яковенко, к.э.н., доцент,
Н. К. Казеян,
Днепропетровский национальный университет им. О. Гончара,
г. Днепро

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

Аннотация

В исследовании актуализирован вопрос оказания влияния лица или группы лиц на пользователей Интернет пространства через инструменты социальной инженерии. Осуществление скрытого воздействия позволяет получать негласно информацию и влиять на сознание Итернет-лользователей. Проведен анализ последних исследований в социальной инженерии, что позволило доказать, что социальная инженерия, как субнаука еще на этапе становления и определения ключевых парадигм науки. Проанализированы методы, которые чаще всего применяются для осуществления управления участниками Итернет-сообществ и отдельных пользователей. Сформулированы свойства и навыки социального хакера, которыми он должен обладать для осуществления эффективного воздействия и манипулирования человеком. Предложены методы противодействия социальной инженерии и выдвинуты предложения по дальнейшему изучению научного направления.

Ключевые слова: социальная инженерия, методы управления, социальный хакер, Интернет-среда, пользователи, влияние.

Постановка проблеми. У сучасному житті той, хто не володіє інформаційними технологіями та не використовує Інтернет-простір,

обмежує себе у реалізації своїх амбіцій, професійних навичок, сучасному виді спілкування тощо. Зрозуміло, що поєднання життєвого простору людини з Інтернет-простором несе в собі не лише позитивні аспекти знаходження в ньому, а й загрози. Чим більше людина «занурюється» у цей простір, тим більше вона піддається впливу Інтернет-суспільства. Сила і якість такого впливу Інтернет-суспільства на людину досить різноманітна, усе залежить від мети створення цього суспільства та завдань, які ним сформовано. Отже, людина, як користувач Інтернету та учасник Інтернет суспільства повинен розуміти та відрізняти якість та силу впливу на нього, виділяти методи, якими намагаються маніпулювати ним та знати, як протидіяти цим впливам.

Аналіз останніх досліджень і публікацій. Метод маніпулювання як основа соціальної інженерії існує досить давно (перший відомий випадок соціального хакерства зафіксовано у VI ст. до н. е. у Китаї), проте із зростанням впливу технологій в цілому та Інтернету зокрема найбільш сильного значення вона набула в останні 15 років. Влучними прикладами дослідників цієї галузі можуть стати К. Ларрі [1], М. В. Кузнєцов [2], К. Мітник [3] – найвідоміший хакер у світі, Е. Кін [4] та А. Серіков [5]. Вченими та науковцями було досліджено основне підґрунтя управління поведінкою людини, наведено багато прикладів застосування основних атак хакерів, проаналізовано такі категорії, як «соціальна група» і «соціальна мережа» тощо. Серед невирішених проблем у соціальній інженерії наразі у наукових джерелах відсутня чітка структуризація методів впливу на користувача через Інтернет простір, а найголовніше – слабо розроблені методи протидії соціальному хакерству.

Формулювання цілей статті й аргументування актуальності поставленого завдання. Мета дослідження полягає у розробці дієвих механізмів протидії впливу на користувачів Інтернету соціальним хакерам, які переслідують не явні цілі своєю поведінкою.

Виклад основного матеріалу. Сучасне життя оповите технологіями. Наразі спектр їх використання настільки широкий, що вони вийшли вже за межі передбачуваності, якому додатково сприяли особливості поведінки людини. Стандартне використання комп'ютера або телефону, наприклад, є застарілим підходом, тому люди з їх допомогою, полегшуючи собі завдання, проникають у зовсім інші сфери та досягають успіху, стають лідерами у цих галузях [9].

Так, наприклад, колись набула популярності у соціальних мережах хвиля масового постування (розміщення) власних фотографій, яких немає на сайті, та подальшої передачі естафети іншим особам, яким у разі

невиконання умов гри присуджували образливі статуси. З одного боку, воно змушувало підкорятися тому, хто кинув тобі виклик, а з іншого – ця фотоманія тим самим безкоштовно розповсюджувала у публічному доступі великий обсяг інформації про своїх власників [7].

Виходить, що можна визначити певні методи, які дозволяють налаштувати особу в Інтернет-середовищі на виконання певних дій. Під час дослідження виявлено наступні варіанти програмування, що найчастіше застосовуються:

1. Інтернет-реклама. План дії соціального хакера виглядає наступним чином: вони долучаються до форумів та чатів, стають «своїм» у цьому осередку завдяки знанням та комунікабельності, а потім наголошують, що кращим є певний товар/робота/послуга, про який не було досить нічого відомо. Як наслідок, з мінімальними витратами інформація дуже швидко поширюється в Інтернеті. Прикладом може стати ситуація, коли покупцю необхідно придбати товар і він, щоб отримати «реальну життєву інформацію» про річ, переглядає відгуки на різних сайтах. Пастка криється у тому, що ці коментарі може залишати спеціальна група людей, метою якої є розхвалювання/критика конкретного товару.

2. «Вбивство» форуму. За цим сценарієм, по-перше, соціальний хакер на форумі створює образ антилідера, який свариться, нападає на адміністраторів, однак веде себе обачливо, не порушуючи правил сайту; по-друге, він створює фіктивну аудиторію, яка продовжує підтримувати точку зору антилідера; на останньому етапі підключаються справжні учасники і діють, як «усі попередні».

3. «Музичний танк». У цій ситуації група людей піддається впливу шляхом відтворення музики. Прикладом застосування цього методу в Інтернет-просторі був флешмоб Ice Bucket Challenge, учасники якого мали на меті допомогти нужденним. У цьому методі соціальним хакером виступав учасник, який змушував знайомих/друзів або облитись водою та передати естафету іншим, або зробити внесок у офіційну благодійну організацію.

4. Розповсюдження чуток. За цим методом діє закон Оллпорта-Постмана, який дає оцінку ступеню поширення чуток. Якщо предмет, про який «ходять чутки», є дуже важливим для особи, проте істина їй відома, то чутка у такому випадку зникає. Так, з початку 2016 року в Інтернеті поширилась інформація про відміну стипендій, яка за декілька місяців досягла такого великого масштабу, що МОН змушена була звернутись до керівників вишів в офіційному листі із роз'ясненням ситуації та скоригувати власну програму дій.

5. Метод «in wait» полягає у запрошенні інтернет-користувача отримати доступ для реєстрації на сайті або до закритого співтовариства. Розглядають 2 випадки: 1) використовується для власної користі – характерний для методу «взаємодопомога»; 2) в «in wait» міститься знайома/близька інформація для особи (наприклад, соціальна група в межах інтересів), а її рішення спирається на ступінь пов'язаності (кількість друзів, які вже є її учасниками) – характерно для соціального наслідування [10].

6. Шахрай із картами. Метод полягає у тому, що збирається інформація про жертву з метою подальшого управління стосунків із нею. Наприклад, цей метод може бути використаний для знайомства в Інтернеті. Так, хлопець, якій сподобалась дівчина на сайті знайомств, може розвідати інформацію про неї так, щоб вона не дізналася. Таким чином, він матиме більше даних для оперування (інтереси, місце навчання/роботи, хобі тощо), що допоможе краще налаштувати стосунки.

7. Взаємодопомога. Метод сформований на основі специфічності поведінки людини: вона бажає будь-яким способом, навіть у нерівній пропорції, віддячити особі, яка допомогла їй. Наприклад, в офісі робітник А попереджає робітника Б про можливі технічні проблеми та просить повідомити його, якщо виникне ця ситуація. Працівник «А» штучно призводить до настання негативних наслідків, далі самостійно «повертає усе на місця», а у результаті має повне право попросити робітника Б про «відповідну» допомогу.

8. Поклоніння авторитету. Індивідам властиве стереотипне мислення, створення ідеалів та авторитетів, яким хочеться наслідувати і довіряти. У відомій рекламі Colgate робився акцент на тому, що саме ця паста рекомендована всесвітньою асоціацією стоматологів. У цьому методі соціальним хакером виступає асоціація стоматологів, яка створена із посиланням на високий рівень розвитку хімічної промисловості та поширює ідею «якісного товару».

На рис. 1 наведено узагальнену схему функціонування соціальної інженерії за моделлю «хижак-жертва».

З рис. 1 випливає, що хакери мають велику кількість дієвих методів для здійснення впливу та отримання необхідних даних. Проте для досягнення таких результатів він повинен володіти специфічними навичками, які дадуть йому можливість встановити контакт із аудиторією чи конкретною особою. У процесі дослідження цієї галузі знань був виявлений тісний зв'язок соціальної інженерії із психологією, оскільки вона базується на використанні слабостей людського фактора, незмінності її принципів та стереотипів, за допомогою яких й відбувається управління.

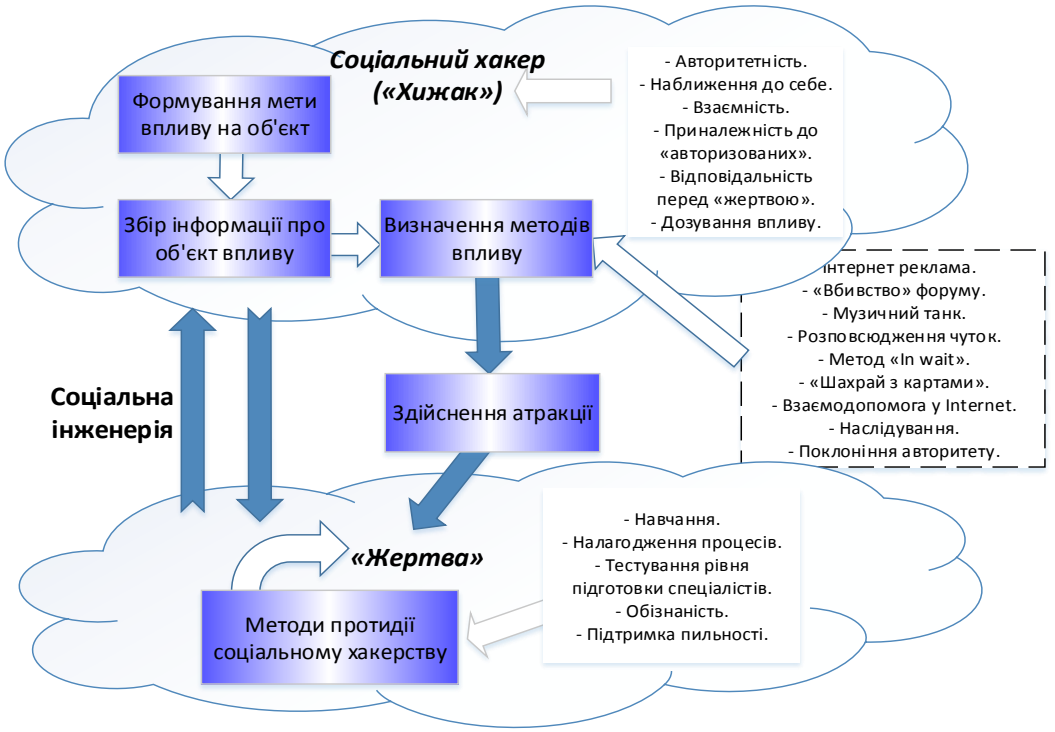

Рис. 1. Модель «Хижак-Жертва» у представлені соціальної інженерії*

*Джерело: Власна розробка.

Тому вирізняють наступні якості соціального хакера у процесі маніпулювання:

1. Авторитетність. Індивідам властиво задовольняти запит авторитету та бути впевненим у випадку, коли запитувач має владу або право ставити це питання. Так, хакер може видавати себе за авторитетну особу з IT-департаменту та довідуватися про необхідну інформацію.

2. Вміння правильно наближати до себе. Люди мають звичку задовольняти запит розташованої до себе людини або особи зі схожими інтересами, думками, поглядами, або бідами і проблемами. Так, соціальний хакер у процесі спілкування намагається виявити інтереси жертви, а потім вдало стверджує, що їх смаки збігаються.

3. Взаємність. Людина отримує річ/пораду/допомогу взамін зовсім несподівано, і це змушує її відплатити цій особі. Наприклад, соціальний хакер представляється співробітником IT-департаменту, повідомляє робітнику про особливі віруси та пропонує варіанти розв'язку проблем. Цей робітник запускає програму, проте нічого не відбувається (у той час як програма збирає усю інформацію про компанію) і вимикає її [8].

4. Відповідальність. Людям властиве дотримання слова і зазвичай виконання обіцяного здійснюється попри усі перепони.

5. Соціальна приналежність до авторизованих. Наприклад, співробітнику називаються імена знайомих йому працівників з перевірки, які начебто працюють разом із соціальним хакером, а потім вивідує інформацію.

Чим далі розвивається світ, тим більше ускладнюється проблема розпізнавання та протидії впливу на особистість. Розробляються нові методи, щороку технології здійснюють стрімкий прорив в інноваціях і значення такого суб'єкта, як людина, дуже знецінюється. Індивіда все легше можна обдурити, змусити відповідати запрограмованій схемі, тобто група таких осіб є зручним інструментом маніпулювання. Цим користуються соціальні хакери і, як наслідок, вони мають чітке підпорядкування та бажаний результат. Однак таким хакерам можна протидіяти, застосувавши наступні методи впливу:

1. Навчання.

2. Налагодження процесів.

3. Тестування рівня та система захисту. Остання виявляє недоліки захисту, які не були враховані при розробці політики безпеки. Тестування, як окремий компонент, включає в себе планові, раптові, неперервні перевірки та виявлення недоліків. За результатами роботи проводять коригування внутрішніх процесів та програм навчання.

4. Обізнаність. У протидії робиться акцент на залучення уваги людей до питань інформаційної безпеки, усвідомлення співробітниками серйозності проблеми, вивчення і впровадження необхідних методів і дій для підвищення захисту інформаційного забезпечення.

5. Підтримка пильності. Перелік можливих дій для реалізації методу:

- Інформаційні статті, розсилки, нагадування.
- Спеціальні плакати у приміщеннях.
- Дошки оголошень.
- Розсилки з нагадуваннями по електронній пошті.
- Хранителі екрану і заставки з нагадуваннями.
- Нагадування через голосову пошту.

Запропоновані методи захисту доцільно застосовувати виважено і методично, щоб результати їх використання мали дієвий практичний зміст.

Висновки з дослідження і перспективи подальшого розвитку. У повсякденному житті все частіше зустрічаються негативні наслідки впливу дії соціального хакера. Цей факт повинен налаштувати суспільство вдатися до певних протидій. Тому для цього під час роботи над проблемним питанням були визначені способи управління соціумом, які

застосовує соціальний хакер. Проаналізувавши численні приклади дії агентів впливу за допомогою методів соціальної інженерії, були виявлені якості людини, оволодівши якими вона зможе маніпулювати іншими. Під час дослідження було розроблено методи, які надають можливість користувачам контролювати своє оточення та правильно сприймати потік інформації в Інтернет-просторі.

Напрями подальших досліджень вбачаються у розробці нових, адаптованих до особливостей середовища методів протидії впливу, які будуть ще більш успішними та ефективними у застосуванні. Інновації ж у галузі науки стануть ключовими для подальшого існування суспільства.

Список використаних джерел:

1. Минина В. Н. Методы социального программирования: Учебное пособие / В. Н. Минина. – СПб.: Изд-во Санкт-Петербургского ун-та, 1999. – 60 с.
2. Кузнецов М. Социальная инженерия и социальные хакеры / М. Кузнецов. – Санкт-Петербург, 2007. – С. 73-215.
3. Митник К. Искусство обмана / К. Митник, Вильям Л. Саймон. – К.: Компания АйТи, 2004. – С. 114-204.
4. Кин Э. Ничего личного: как социальные сети, поисковые системы и спецслужбы используют наши персональные данные. – Москва, 2016. – С. 23-173.
5. Сериков А. Информационные технологии социального хакерства [Электронный ресурс] / А. Сериков. – Режим доступа: http://nefact.com/blog/metody-socialnoj-inzhenerii.
6. Яковенко В. С. Консолідація даних у бізнес-аналізі діяльності підприємств / В. С. Яковенко, Н. В. Зайцева // Глобальні та національні проблеми економіки. – 2015. – №8. – С. 1222-1227.
7. Тощенко Ж. Т. Тезаурус социологии: темат. слов.-справ. / Под ред. Ж. Т. Тощенко. – М.: ЮНИТИ-ДАНА, 2009. – С. 417-433.
8. Robert B. Cialdini (2001). Influence. Science and Practice, 4th ed.
9. Старостина Е. Мишень социальной сети – это вы сами / Е. Старостина, Е. Хрусталева // Инновационная безопасность. – 2015. – №9. – С. 64-67.
10. Резник Ю. М. Социальная инженерия: предметная область и границы применения / Ю. М. Резник // Социологические исследования. – 1994. – № 2. – С. 87–96.

Vladyslav Iakovenko, Ph.D.,
Naira Kazeian,
Dnipropetrovsk National University O. Gonchar
Dnipro

SOCIAL ENGINEERING IN THE INTERNET ENVIRONMENT

Abstract

The issue of personal or group of people influence on the users of Internet environment through the tools of social engineering is described in the article. Implementation of hidden influence allows to receive the information secretly, and to influence the minds of Internet users. An analysis of recent researches in social engineering has been conducted. It made possible to prove that social engineering as a sub-science is still at the stage of formation and identifying key

science paradigms. Methods, which are mostly used to manage members of Internet unions and individual users, have been analyzed. Qualities and skills of social character which should be possessed by the user to make an effective influence and to manipulate a person have been outlined. Methods of countering social engineering are offered, and proposals for further research in this sphere are highlighted.

Keywords: social engineering, management methods, social hacker, Internet environment, users, influence.

References:

1. Mynyna, V.N. (1999). Metody sotsyal'noho prohrammyrovanyia [Methods of social programming]. Saint-Petersburg University, Sankt-Peterburg, 60 p. (in Russ.).

2. Kuznetsov, M. (2007). Social'naja inzhenerija i social'nye hakery [Social engineering and social hackers]. Sankt-Peterburg, pp. 73-215 (in Russ.).

3. Mitnik, K., Sajmon, V. L. (2004). Iskusstvo obmana [The art of deception]. IT Company, Kyiv, pp. 114-204 (in Russ.).

4. Kin Je. (2016). Nichego lichnogo: kak social'nye seti, poiskovye sistemy i specsluzhby ispol'zujut nashi personal'nye dannye [Nothing personal: How social networks, search engines and special services are using our soft data]. Moscow, pp. 23-173 (in Russ.).

5. Serikov, A., Borovskyj, A. Information technology of social hacking. Available at: http://nefact.com/blog/metody-socialnoj-inzhenerii (in Russ.).

6. Iakovenko V.S., Zajtseva N.V. (2015). Consolidating of data in business analysis of the activity of enterprises. Hlobal'ni ta natsional'ni problemy ekonomiky [Global and national problems of economy], no. 8, pp. 1222-1227 (in Ukr.).

7. Toschenko, Zh. (2009). Tezaurus sotsyolohyy [Thesaurus sociology]. UNITY-DANA, Moscow, pp. 417-433 (in Russ.).

8. Robert B. Cialdini (2001). Influence. Science and Practice, 4th ed.

9. Starostyna, E., Khrustaleva, E. (2015). The target of social network is you yourself. Innovacionnaja bezopasnost' [Innovations of security], no. 9, pp. 64-67 (in Russ.).

10. Reznik, Ju. (1994). Social engineering: field of subject and limits in using. Sociologicheskie issledovanija [Social research], no. 2, pp. 87-96 (in Russ.).