УДК 004.056

С.В. Лазаренко, д.т.н.,
Т.Л. Щербак, к.т.н.,
Національний авіаційний університет, Київ
О.М. Фурсенко, к.т.н.,
Інститут державного управління у сфері цивільного захисту
Б.В. Ткач
Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України

РЕАГУВАННЯ НА СОЦІОТЕХНІЧНІ АТАКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Об'єкти критичної інфраструктури – підприємства та установи (незалежно від форми власності), що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення [1]. На таких об'єктах здійснюється обробка, зберігання, передача інформації з обмеженим доступом, несанкціоноване розповсюдження якої завдасть значної шкоди. У подальшому найбільшу загрозу інформаційній безпеці будуть представляти методи соціальної інженерії, що застосовуються для злому існуючих засобів захисту.

Основною причиною цього є те, що застосування соціальної інженерії не вимагає значних фінансових витрат і досконалого знання інформаційних технологій. Тому, актуальним є своєчасне реагування на соціотехнічні атаки та знешкоджня наслідків таких атак.

Соціальна інженерія – метод несанкціонованого доступу до інформації або до систем зберігання інформації без використання технічних засобів. Метод заснований на використанні слабкостей людського фактору. Дослідження показують, що людям притаманні деякі поведінкові схильності, які можливо використати для маніпулювання. Більшість зломів систем безпеки відбуваються завдяки використанню соціальної інженерії, а не технічному (електронному) злому [2, 3].

Атаки, засновані на методах соціотехніки, можливо розділити на п'ять основних напрямків: мережеві атаки; телефонні атаки; пошук інформації в смітті; персональні підходи; зворотна соціотехніка.

Оцінка ефективності реагування служб захисту інформації (адміністраторів безпеки, менеджерів з кібербезпеки тощо) на соціотехнічні атаки, повинна здійснюватись за рахунок застосування процедури вибору заходів і засобів реагування на соціотехнічні атаки, які функціонують в нечіткому середовищі [3, 4].

Існують базові методи реагування на атаки за допомогою методів соціальної інженерії, до яких відноситься: тестування системи захисту; поінформованість; активний захист.

Такі заходи дозволяють оцінити критичність впливу соціотехнічних атак на об'єкти критичної інфраструктури, а також забезпечити своєчасне реагування на соціотехнічні атаки і як наслідок, застосовувати ефективні засоби, що дозволяють захистити інформаційний простір від таких атак зі сторони зловмисника [3].

Таким чином:

1. Впровадження систем реагування на соціотехнічні атаки надасть можливість службам захисту інформації швидко та оперативно виявляти і здійснювати оцінку такої атаки.

2. За результатами оцінки виявленої атаки будуть вжиті ефективні заходи з локалізації такої атаки та знешкодження її наслідків.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Постанова Кабінету Міністрів України від 23.08.2016 № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави».

2. Роуз М. Соціальна інженерія [Електронний ресурс] / Роуз Маргарет/ Режим доступу до ресурсу: http://searchsecurity.techtarget.com/definition/social-engineering

3. Рєзник Ю.М. Соціальна інженерія: В 2 ч. – Ч. 1. Теоретико-методологічні проблеми: Курс лекцій / Рєзник Ю.М., Щербина В.В. – М.: Союз, 1994. – 147 с.

4. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / Корченко А. Г. – К.: МК-Пресс, 2006. – 320 с.