ефект, який згодом може викликати і зміни особистості. Наприклад, комунікативні, антистресові, мотиваційні тренінги; формування здорового способу життя; підготовки працівників поліції до дій в умовах підвищеного ризику; тренінгові програми корекції та терапії посттравматичних стресових станів тощо. До другого типу належать тренінги особистісного зростання (у їх основі лежить створення умов для саморозвитку поліцейських, розвитку здібностей рефлексії, підвищення відкритості до нового досвіду). Тут основний ефект спостерігається у внутрішньому плані – спочатку відбуваються внутрішні особистісні зміни (самооцінка, мотивація, ціннісні орієнтації і тощо), а потім, як наслідок, може змінитися і поведінка. В тренінгах особистісного зростання за допомогою відповідних технік учасники намагаються усвідомити та подолати власні психологічні проблеми, які перешкоджають вирішенню їх життєвих і професійних завдань. Кожен учасник тренінгу за допомогою інших учасників і тренера може позбутися внутрішніх бар'єрів, краще дізнатися, як його сприймають оточуючі люди тощо. Це дозволяє виявити та в подальшому більш ефективно використовувати свої соціально важливі якості, сформувати більш реальну оцінку здібностей, побачити власні помилки і недоліки.

УДК 004.056

Андрій Олегович СЕМЧУК,
курсант групи Ф4-102
Харківського національного університету внутрішніх справ
Науковий керівник: доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 ХНУВС кандидат наук з державного управління, доцент Ю. М. Онищенко

ОСНОВНІ МЕТОДИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Соціальна інженерія – це маніпулювання людьми через виконання дій або розголошення конфіденційної інформації іншим способом, ніж як через засоби технічного руйнування баз даних. Вказане явище є значно розвиненим як в Україні, так і в інший країнах. Майже кожному з користувачів Інтернету хоча б одного разу приходив так званий «лист щастя», в якому повідомлялося, що саме він став щасливчиком та виграв автомобіль або іншу цінну річ. Саме за допомогою таких простих дій, які впливають на психологічні характеристики людської особистості шахраї намагаються заволодіти нашими персональними даними (іншою конфіденційною інформацією) із явно більш негативною метою, ніж заповнити анкету для отримання бонусної карти в популярному магазині.

Соціальна інженерія базується на досить простих психологічних особливостях людини, таки як: принцип зворотності («ти мені – я тобі»), принцип соціальної перевірки (ви оцінюєте свою поведінку в контексті поведінки більшості), повага до авторитетів (ви будете більше довіряти лікарю та поліцейському, аніж пересічній людині). Всі ці принципи застосовуються і при здійсненні «офлайнового» шахрайства, однак мають свою специфіку під час вчинення у мережі Інтернет.

Найбільш популярною схемою впливу на особу, яка використовується в соціальній інженерії є схема Шейнова, яка полягає у таких кроках: формування цілі впливу на об'єкт, пошук інформації про об'єкт, виявлення найбільш зручних цілей впливу, створення найбільш сприятливих умов для впливу на об'єкт, примус до потрібної дії, результат.

Найбільш популярними видами інтернет-шахрайства є наступні способи застосування соціальної інженерії:

- фішинг;
- вішинг;
- фармінг;
- попередження про вірус на комп'ютері;
- Quid pro quo;
- «Дорожнє яблуко»;
- зворотна соціальна інженерія;
- претекстинг.

Слід зазначити, що основним недоліком у сфері запобігання негативним проявам соціальної інженерії є відсутність системної роботи щодо її виявлення та подолання, наявність лише декларативних положень у стратегіях (іншими вони і не можуть бути, що зрозуміло) та відсутність прийнятих законодавчих та підзаконних актів, що містять дієві механізми протидії кіберзлочинам, зокрема тим, що вчиняються із застосуванням методів соціальної інженерії.

Серед проблемних питань слід зазначити низький рівень поінформованості населення щодо можливих загроз соціальної інженерії (варто відзначити позитивну роботу деяких банків у цій сфері), а також високу латентність подібного роду злочинів, що унеможливлює виявлення та притягнення до відповідальності усіх винних осіб.

Перспективним напрямом роботи для запобігання кіберзлочинам, що вчиняються із застосуванням методів соціальної інженерії є проведення усіма зацікавленими суб'єктами (державними інституціями, приватним сектором, правоохоронними органами, банківськими установами тощо) комплексу превентивних заходів, спрямованих на підвищення обізнаності пересічних громадян про загрози, пов'язані з реалізацією вище зазначених способів соціальної інженерії.