DOI 10.18372/2310-5461.50.15684

УДК 004.056 : 32.019.51 : 007

О. К. Юдін, д-р техн. наук, проф.
Національна академія Служби безпеки України
orcid.org/0000-0002-6417-0768
e-mail: yak333@ukr.net;

О. В. Матвійчук-Юдіна**,** канд. пед. наук, доц.
Національний авіаційний університет
orcid.org/0000-0002-5906-5023
e-mail: metalen3@ukr.net;

О. М. Супрун**,** канд. фіз.-мат. наук, доц.
Київський національній університет імені Тараса Шевченка
orcid.org/ 0000-0002-1196-5655
e-mail: suprunso@ukr.net

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНА ВІЙНА ТА ТЕХНОЛОГІЇ СОЦІАЛЬНОГО ІНЖИНІРИНГУ

Вступ

Сучасне суспільство неможливо уявити без використання різних класів інформаційних потоків даних (або критичних даних), які потрібно зберігати, аналізувати, оцінювати, висвітлювати, та використовувати для подальшого прийняття рішень. Жодна держава та її територіальні громади, промисловість, організації різних форм власності не можуть існувати без інфокомунікацій та їх інфраструктури. В світі чітко встановились поняття «інформаційне суспільство», глобальна діджиталізація інформаційних ресурсів та система взаємовідносин.

Зрозуміло, що в умовах різкого поширення новітніх інформаційних технологій гостро постає питання правової адекватності або «порядності» використання інформаційних ресурсів з точки зору відповідності нормативно-правовому полю суспільства та встановлених морально-етичних правил.

Значну роль у протидії інформаційній війні слід приділяти захисту державних інформаційних ресурсів (ДІР) на основі сформованої інформаційної політики країни та впровадженню комплексного підходу до побудови систем захисту. Загрози інформаційній безпеці (ІБ) держави відіграють базову роль у формуванні політики та самої системи захисту ресурсів країни [1–3]. Виникає питання захисту ДІР від перекручувань та вільного трактування, особливо нормативно-правових актів, які впливають на людську свідомість або навіть більше — на національну безпеку держави.

Таким чином постає проблематика свідомого використання інформаційних потоків або ресурсів з метою впливу на свідомість особистості, груп людей або всього суспільства для отримання політичної, економічної, соціальної чи особистої вигоди.

Один з відомих учених, який займається питаннями теорії комунікацій, Георгій Почепцов у своїй праці «Психологічні війни» [4] надав таке тлумачення поняттю інформаційної війни: «Інформаційна війна має в якості своїх цілей два класи об’єктів: з одного боку, це комп’ютери і інформаційні системи, з іншої — індивідуальна і масова свідомість. Це як би її технічна і гуманітарна складові».

Поняття «інформаційно-психологічної війни» [*information psychological warfare*] має два основні визначення або спрямованості: класичне та суспільно-стихійне [5].

У класичному розумінні — це діяльність спеціальних органів однієї держави, що здійснюють психологічний вплив на цивільне населення і (або) на військовослужбовців іншої держави заради досягнення своїх політичних, економічних, а також чисто воєнних цілей. Офіційно психологічна війна проти іноземних держав може реалізовуватись тільки з санкції президента, уряду або ради національної безпеки. Проте в країнах зі слабкою виконавчою владою та загальним зневажливим ставленням до діючого законодавства інформаційно-психологічна війна здійснюється за допомогою засобів масової інформації з урахуванням інтересів чи керівництва політичних угруповань або

фінансово-промислових груп (у тому числі транснаціональних).

У повсякденному розумінні інформаційно-психологічна війна — це стихійне, некваліфіковане використання засобів поширення інформаційних потоків даних та механізмів соціально-психологічного впливу одними людьми проти інших людей. Зазначений вплив впроваджується з метою підкорення їхньої волі чи діяльності або створення сприятливих умов для свого існування й діяльності.

Такий підхід можна трактувати, як використання технологій і методів впливу на свідомість особистості або всього суспільства на основі маніпулювання інформаційними потоками даних і ресурсами (критичних даних або ресурсів).

Словосполучення «соціальна інженерія» чітко відображає суть поняття, що являє собою сукупність підходів і методів прикладних соціальних наук, які орієнтовані на цілеспрямовану зміну сталих соціальних процесів (бізнес процесів), організаційних структур, що визначають людську поведінку, використовуючи основані психологічні особливості людей: зацікавленість, довіра, звичка тощо і забезпечують контроль за ними. Соціальна інженерія є особливим родом «мистецтва» або «творчих думок», що різнобічно маніпулюють соціумом через виконання дій або розголошення конфіденційної інформації, зміни цілісності даних. Так звана інформаційна війна на сучасному етапі розглядається, як процес маніпулювання інформацією або інформаційними потоками даних, яким довіряє об’єкт впливу (без відома об’єкта) з метою прийняття рішення проти інтересів держави, установи або особистості [6].

Метою соціальної інженерії є спонукання людей виконувати певні дії, які вони за звичайних умов ніколи б не вчинили.

Наприклад, розголошувати власну конфіденційну інформацію, переходити на невідомі сайти, здійснювати дії за сумнівними інтернет-посиланнями, використовувати програмні продукти, що здійснюють крадіжку особистої інформації.

Уся система соціальної інженерії базується на тому факті, що саме людина є найслабкішою ланкою будь-якої системи інформаційної і кібербезпеки [7].

Саме тому за умови, що технічно отримати конфіденційну інформацію хакерам досить важко, вони впливають безпосередньо на користувача, який є найслабкішим місцем в системі інформаційної безпеки.

Аналіз останніх досліджень і публікацій

Сучасні підходи побудови системи соціального інжинірингу, які ґрунтуються на технічному отриманні конфіденційної інформації, інструменти тестування вразливості безпеки за межами ІТ-інфраструктури, в своїх наукових здобутках окреслюють Г. Г. Почепцов, В. В. Різун, О. Г. Корченко.

Проблематика в контексті побудови змісту невербальної комунікації в соціальній інженерії, уособлення знань та вмінь нейтралізувати зростаючу загрозу зловмисних соціальних інженерів, розкрити вразливі місця безпеки ІТ-інфраструктури висвітлені в працях таких провідних вітчизняних науковців, як Г. Г. Почепцов, А. В. Курбан, О. Г. Корченко, В. Л. Бурячок.

Дослідження тактики та методів соціального інжинірингу, класифікацію методів, яка враховує специфіку програмних продуктів з питань виконання етичних тестів соціальної інженерії та захисту від соціальних інженерів здійснено В. П. Шейновим, Е. Н. Волковим, С. А. Зелінським.

Мета статті

Метою статті є здійснення аналізу існуючих сучасних методів соціальної інженерії та визначення технологій використання різних класів методів в інформаційно-психологічній війні, а також застосування деструктивних засобів інформаційної безпеки, як складової психологічного впливу на особистість і суспільство.

Виклад основного матеріалу

Сутність соціальної інженерії і її місце в інформаційно-психологічній війні.

В сучасних умовах розвиненого інформаційного суспільства та поширення агресії з боку інших держав термін «інформаційно-психологічна війна» може характеризувати: політичну діяльність окремих осіб, угруповань, партій, рухів; виборчі компанії кандидатів на різноманітні виборні посади; рекламну діяльність комерційних структур чи економічних груп; боротьбу індивідів (і малих груп) у суперництві за лідерство у виробничих, наукових та інших колективах; політичне, економічне або культурне протистояння конфліктуючих між собою етносів; переговорний процес між конкуруючими фірмами або організаціями.

Основними цілями (метою) інформаційно-психологічної війни є зміна в бажаному напрямку психологічних характеристик людей (поглядів, думок, ціннісних орієнтацій, настроїв, мотивів, установок, стереотипів поведінки), а також групових норм, масових настроїв, суспільної свідомості в цілому.

В умовах протистояння комерційних структур чи економічних груп, індивідів — це формування інформаційного комплексу (або порушення цілісності існуючого), який одержується керівництвом, менеджерами, особовим кадровим складом або конкуруючими особами. Сформований таким чином інформаційний комплекс, повинен впроваджувати нав'язування негативної, не відповідної дійсності, деструктивної або беззмістовної інформації, яка позбавляє сторону, що атакована методами соціального інжинірингу, можливості вірно сприймати події або поточну обстановку та приймати адекватні і якісні рішення.

Загальна система соціальної інженерії базується на тому факті, що саме людина чи сукупність людей та їх свідомість (системний адміністратор, секретар керівника, оператори call-центра, менеджери по роботі із клієнтами, охоронці, адресати пошти або телефонного виклику, пересічний громадянин тощо), є найслабшою ланкою будь-якої інформаційної системи. Таким чином всі дії злочинців в цьому випадку спрямовані з метою інформаційно-психологічного впливу безпосередньо на користувача, як на най вразливе місце в системі інформаційної безпеки.

Сфери застосування соціальної інженерії, що запропоновані Кевіном Митником [6] та узагальнені в праці [9] такі: фінансові махінації в організації; загальна дестабілізація роботи організації з метою зниження її впливу, а згодом і повного її знищення; проникнення в мережу організації для дестабілізації з певною метою роботи її основних вузлів; фішинг та інші способи викрадення паролів із метою доступу до персональних даних, тощо; розвідка інформаційно-телекомунікаційних систем.

Сучасні методи соціальної інженерії в своїй основі найчастіше використовують стандартний алгоритм Шейнова, як покроковий інструмент впливу на соціально-психологічний об'єкт [10]. Однак, алгоритм має загальний характер. Згідно нормативно-правової бази будь-якої держави або суспільства, суб'єктами інформаційно-правових і соціальних відносин є особистість, суспільство та держава. Тому вся послідовність дій алгоритму соціальної інженерії буде стосуватись безпосередньо кожного інформаційного суб'єкту.

Нижче, автори пропонують власне розширене бачення цього алгоритму, створивши на його основі петлю:

1) формування мети і задач впливу на інформаційно-психологічний об'єкт;

2) пошук та отримання інформації про інформаційно-психологічний об'єкт інформаційного впливу;

3) вибір найуразливіших цілей та напрямів;

4) створення найсприятливіших умов для впливу на інформаційно-психологічний об'єкт (атракція);

5) примушення до виконання запланованих дій;

6) аналіз та використання результату впливу.

Таким чином можна сформувати систему чинників соціального інжинірингу (див. рисунок).

Соціальне програмування містить систему методів, що застосовуються для несанкціонованого доступу до інформації або системи її зберігання шляхом цілеспрямованого інформаційно-психологічного впливу на соціальні об'єкти, які забезпечують безпеку інформації та її зберігання. Реалізація цієї системи методів ґрунтується на здатності людини до конструювання нових і зміни існуючих елементів, структур соціального світу, що виражаються в застосуванні всіх видів реально підкріплених знань, досвіду і творчої уяви. І це все для того, щоб винайти, проектувати, створювати, змінювати, підтримувати і покращувати соціальні структури, системи і процеси.

Філософія психології соціального проєктування підкреслює невизначеність і мозаїчність життєвого простору і долається в області соціального проектування введенням параметрів типовості:

– потреби людей типові (що підходить для одного, то підходить для багатьох);

– життєві траєкторії типові (форми життєдіяльності одного є в більшості випадків формами життєдіяльності багатьох);

– поведінкові реакції людей типові (подібні стимули породжують подібні реакції);

– завжди знайдеться певний тип людей, що підтримають проєкт або потребують його здійснення.

Області застосування деструктивних впливів соціальної інженерії:

– фінансові махінації;

– проникнення в структуру організації для дестабілізації основних вузлів мережі;

– доступ до персональних даних;

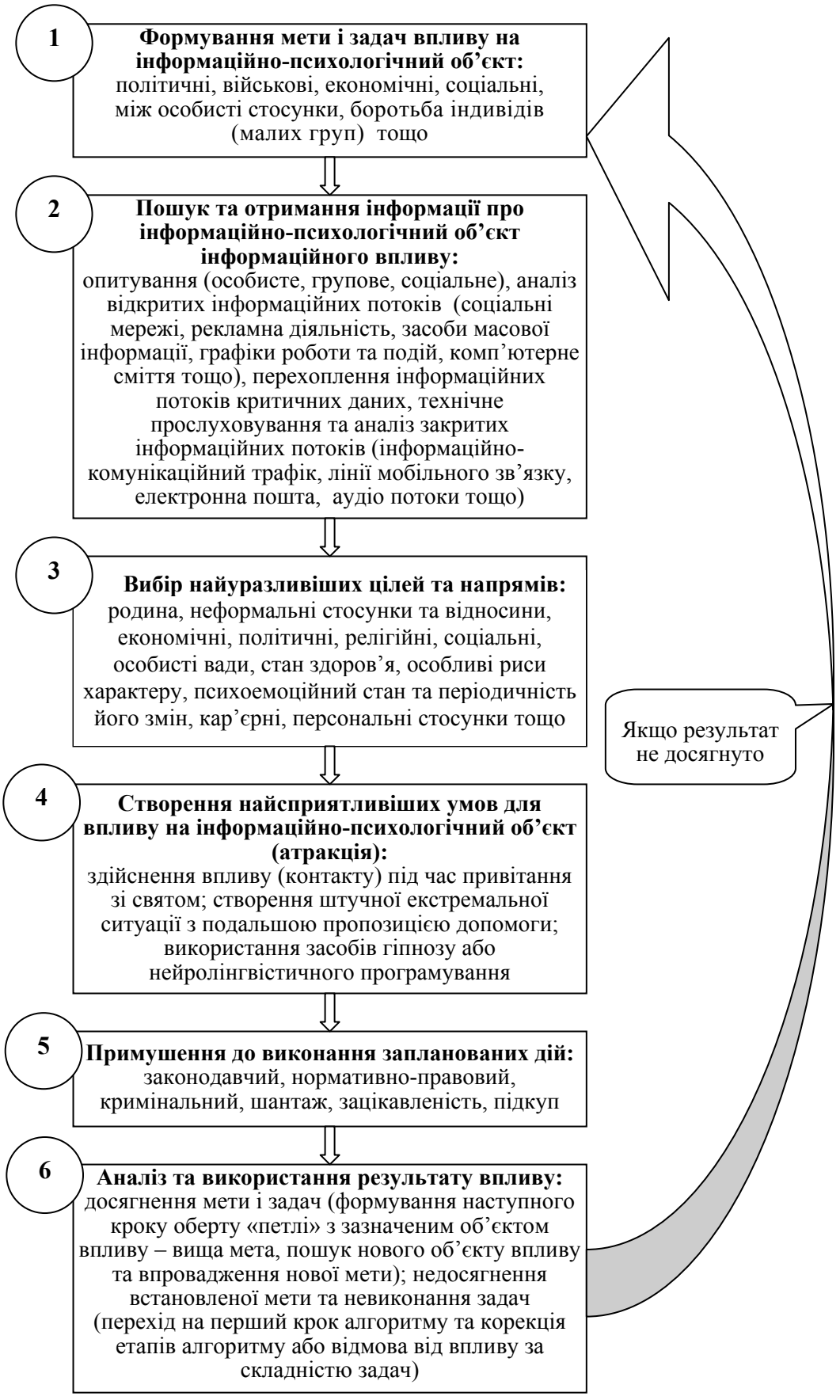
– загальна дестабілізація роботи організації з метою зниження її впливу і подальшого цілковитого руйнування;

– викрадення конфіденційної інформації;

– ведення конкурентної розвідки;

– отримання інформації про маркетингові та інші плани організації;

– отримання інформації про перспективних співробітників з метою їхнього виведення з організації.



Система чинників соціального інжинірнгу

Необхідно класифікувати область застосувань деструктивних впливів соціальної інженерії, а саме виділити основні напрями:

– несанкціонований доступ до персональних даних;

– проникнення до інфраструктури організації для дестабілізації основних вузлів інформаційної системи та її мережі;

– загальна дестабілізація роботи організації з метою зниження впливу на ринку послуг, а також подальше цілковите руйнування авторитету компанії та її структури;

– фінансово-економічне шахрайство;

– ведення конкурентної розвідки, а саме: вилучення конфіденційних відомостей та договорів;

– одержання комерційної конфіденційної інформації;

– отримання інформації про маркетингові плани та перспективні проекти організації;

– одержання інформації про перспективних співробітників, їх персональні дані для їх подальшої дискредитації в організації.

Таким чином, спираючись на класифікацію основних напрямів деструктивних впливів можемо визначити основні деструктивні аспекти застосування методів соціальної інженерії:

Обман співробітника — системного адміністратора, секретаря в приймальні, оператора call-центру, менеджера по роботі з клієнтами, охоронця на посту, адресата пошти або телефонного виклику.

Використання можливостей відкритих каналів телекомунікацій (телефон, електронна пошта, фальшиві інтернет-сайти, служба миттєвого обміну SMS, соціальні мережі): quid pro quo; IVR (телефонний фішинг); фішинг; pretexting; проникнення на територію; з'ясування і отримання телефонних номерів, паролів, відомостей; плечовий серфінг.

Кібершахраї, хакери використовують особливі методи соціальної інженерії, які розраховані на різні аспекти людської психології. Розглянемо детальніше основні методи соціальної інженерії.

Фішинг — особливий вид шахрайства побудований на надсиланні хибних (сфальшованих) листів від банку чи іншої установи з метою введення пароля чи іншої конфіденційної інформації (прохання, пропозиція, вимога тощо), яка необхідна кіберзлочинцю для реалізації встановленої мети. Слід звернути увагу на цільовий фітинг: масове або індивідуальне відправлення повідомлень електронною поштою користувачу з метою переконання його виконати будь-яку дію (зокрема перевірку даних) і записати послідовність, а також встановити шкідливе програмне забезпечення (ПЗ) для подальшого проникнення і отримання корпоративної інтелектуальної власності або конфіденційної інформації (логінів, паролів та ін.). Зловмисник здійснює цілу низку маніпуляцій.

Підготовка повідомлення зловмисником: підбір конкретної, інформації про людину або компанію; персоналізація — модифікація електронного повідомлення для конкретного користувача так, щоб складалось враження, що отримане з надійного джерела; забезпечення високої якості орфографії і граматики повідомлення; зміст повідомлення; отримання і читання повідомлення особою, на яку спрямовані дії шахрая; дотримання цією особою рекомендацій, сформульованих в тексті повідомлення.

Ознаки фішинг-атак: отримання відомостей — телефоном (IRV), електронною поштою, в он-лайн оголошеннях, в соціальних мережах, як результат дії пошукових систем, в спливаючих системних повідомленнях операторів, що містять: попередження, які викликають занепокоєння; загрози; обіцянки; запити про пожертвування; граматичні або пунктуаційні помилки; вітання з успіхом, перемогою, виграшем; нагадування про необхідність зміни облікових даних; повідомлення про потенційне зараження ПЗ і пропозиції установки антивірусних програм («scareware»).

Вішинг — вид інтернет-шахрайства, який полягає у імітуванні хибних (сфальсифікованих) дзвінків на мобільний телефон користувача від банківської установи та отримання запиту про комунікаційну інформацію з банком для підтвердження персональних даних.

Ознаки телефонного фішингу (вишинг — англ. vishing — voice fishing): підбір конкретної інформації про людину або компанію; попередній запис голосових повідомлень з метою відтворення «офіційних дзвінків» банківських та інші IVR систем; отримання жертвою запиту зв'язатися з банком для підтвердження або оновлення будь-якої інформації; отримання вимоги системи про аутентифікацію користувача введенням PIN-коду або пароля; для створення враження працюючої в даний момент системи попередньо записаних повідомлень вимога виконати типову команду: «Натисніть одиницю, щоб змінити пароль. Натисніть двійку, щоб отримати відповідь оператора».

Фармінг — особливий метод кібершахрайства, що полягає у перенаправленні шляхів запиту користувача-жертви на хибну IP-адресу сфальси-

фікованого за змістом і контентом сайту (спеціалізоване шкідливе ПЗ).

«Дорожнє яблуко» — метод здійснення шахрайства, що ґрунтується на використанні фізичних носіїв інформації (флеш-накопичувач, CD-диск) із зображенням або інформацією, які можуть зацікавити жертву та примусити її запустити ПЗ на своєму робочому місці. Цей метод шахрайства реалізовується шляхом підкидання «інфікованих» носіїв інформації, на яких записана програма, що ініціює атаку клієнтської робочої станції або мережі при її відкритті. Наприклад, в місця загального доступу (туалети, місця для паркування, їдальні, робоче місце співробітника тощо). Шкідливе ПЗ знаходиться всередині Excel, Word або PDF файлів. Використовувані носії позначаються написами, що привертають увагу («Фінансовий звіт», «Прайс-лист», «Суто конфіденційно» і т.п.), забезпечуються корпоративним логотипом і посиланням на офіційний сайт компанії. Співробітник через незнання може підібрати диск і помістити його в комп'ютер, щоб задовольнити свою цікавість.

Цілі такого роду шахрайств: завантаження і скачування файлів; копіювання помилкових посилань, що ведуть на підроблені веб-сайти, чати або інші сайти з реєстрацією; створення перешкод в роботі користувача; викрадення даних, що представляють цінність або таємницю (в тому числі інформації для аутентифікації), несанкціонованого доступу до ресурсів, які можуть бути використані в злочинних цілях; збір адрес електронної пошти і використання їх для розсилки спаму; знищення даних (стирання або переписування даних на диску, пошкодження файлів, які важко помітити), виведення з ладу або відмови обслуговування комп'ютерних систем, мереж; спостереження за користувачем і таємне повідомлення третім особам відомостей (наприклад, звичка відвідування сайтів); реєстрація натискань клавіш з метою крадіжки інформації про паролі і номери кредитних карток; дезактивація або створення перешкод роботі антивірусних програм і брандмауера.

Ознаки втручання: порушення роботи програм (зависання комп'ютера, яке можна усунути лише перезавантаженням, неможливістю запуску програм); імітація імені та інтерфейсу існуючої, неіснуючої або просто привабливої програми, компонента, або файлу даних, як для запуску користувачем, так і для маскування в системі присутності шкідливого ПЗ; наполеглива пропозиція в якості стартової сторінки спам-посилань, реклами або порносайтів; поширення в комп'ютері користувача порнографії; перетворення мови текстових документів в бінарний код; пропозиція виконати певну дію для запобігти наслідку, який важко виправити (безстрокового блокування користувача з боку сайту, втрати банківського рахунку, отримання доступу до управління комп'ютером, установки шкідливого ПЗ).

Претекстинг (*pretexting*) — здійснення атаки через маскування під іншу особу з використання голосових засобів зв'язку (телефон, Skype і т.ін.) для отримання інформації від імені третьої особи або з запевненням, що хтось потребує допомоги, застосовується найчастіше по відношенню до не технічних користувачів, які можуть володіти корисною інформацією.

Прояви і ознаки претекстінгу: використання невеликих запитів і згадування імен реальних людей в організаціях, зазвичай вищих ланок; пояснення, що хтось потребує допомоги, на підставі того, що більшість готова виконати невеликі прохання, які не сприймаються як підозрілі запити; після встановлення довірливого зв'язку, прохання виконати істотніше прохання, що здійснюється зазвичай з успіхом; прояв співрозмовником до жертви підвищеного інтересу, перебільшеної уваги і турботи; відмова того, хто звертається, повідомити свої координати; звернення до жертви з дивною або незвичайною пропозицією; спроби втертися до об'єкту шахрайства в довіру або застосування до нього лестощів; підкреслено начальницький тон.

Уявлення співробітників, на яких спрямований цей метод соціальної інженерії, можуть бути часто критично вразливими. Зокрема: співробітники вважають, що корпоративна система безпеки бездоганна; співробітники втрачають пильність; співробітники легко довіряють отриманій інформації, незалежно від її джерела; співробітники недооцінюють значущість інформації, якою володіють; співробітники щиро хочуть допомогти кожному, хто про це просить; співробітники не усвідомлюють згубних наслідків своїх дій; співробітники вважають дотримання корпоративної політики безпеки марною тратою часу і сил.

Плечовий серфінг (англ. *shoulder surfing*) — спостереження особистої інформації про жертву через її плече в громадських місцях (кафе, торгових центрах, аеропортах, вокзалах, в громадському транспорті тощо).

Quid pro quo (щось замість чогось/послуга за послугу) — звернення зловмисника в компанію з корпоративного телефону або електронної пошти.

Ознаки даного виду соціальної інженерії: зловмисник представляється співробітником

технічної підтримки, який повідомляє про виникнення технічних проблем на робочому місці співробітника і пропонує допомогу в їх усуненні; в процесі «вирішення» технічних проблем, зловмисник змушує вчиняти дії, що дозволяють запускати команди або встановлювати різне ПЗ на комп'ютері «жертви»; більшість офісних працівників готові розголосити конфіденційну інформацію (свої паролі), за послугу або винагороду; збір інформації з відкритих джерел соціальних мереж.

Загрози інформаційній безпеці, пов'язані з електронної поштою і з використанням служб миттєвого обміну повідомленнями спираються на фактори:

Електронні листи: обсяг кореспонденції, який унеможливлює приділення належної уваги кожному листу; жертва часто виконує запит, не замислюючись про свої дії; гіперпосилання, що дозволяють доступ неавторизованих користувачів до корпоративних ресурсів, або запитують дані.

SMS: неформальний характер спілкування в поєднанні з можливістю привласнювати собі будь-які імена дозволяє зловмисникові видавати себе за іншу людину; вірогідність вказівки посилання на шкідливу програму в тексті листа; ймовірність доставки шкідливої програми.

Не менш небезпечною для суспільства є зворотна соціальна інженерія: жертва сама пропонує потрібну інформацію зловмисникові, який, як правило, є особою, що має авторитет в технічній або соціальній сфері та часто отримує важливу особисту інформацію користуючись тим, що ніхто не сумнівається в порядності особи-отримувача. Співробітники служби підтримки ніколи не запитують у користувачів ідентифікатор або пароль (їм не потрібна ця інформація), але багато користувачів заради якнайшвидшого усунення проблем добровільно повідомляють ці відомості.

Зловмисник, який працює разом з жертвою, змінює на її комп'ютері ім'я файлу або переносить його в інший каталог. Жертва помічає зникнення файлу. Зловмисник заявляє, що може все виправити, але тільки увійшовши в систему з обліковими даними жертви. Жертва, бажаючи швидше завершити роботу або уникнути покарання за втрату інформації, погоджується. Також ознаками зворотної соціальної інженерії, наприклад, є: жертва просить зловмисника увійти в систему під її ім'ям, щоб спробувати відновити файл; зловмисник неохоче погоджується і відновлює файл, при цьому краде ідентифікатор і пароль жертви; успішно здійснивши атаку, зловмисник покращує свою репутацію, і цілком можливо, що після цього до нього будуть звертатися за допомогою і інші колеги. Такий підхід не перетинається зі звичайними процедурами надання послуг підтримки і ускладнює викриття зловмисника.

Ознаки несанкціонованого проникнення проявляються в наступних діях зловмисника: отримання фізичного доступу на об'єкт шляхом примусу або обману співробітників в обхід периметра безпеки; отримання конфіденційних даних і розташування прихованих пристроїв знімання інформації в дуже короткий проміжок часу; установка пристроїв, що забезпечують подальший Wi-Fi або 4G доступ до мережі.

На сьогодні все, чим займаються службовці, пов'язано з обробкою інформації. Тому не тільки керівники організації, які мають доступ до важливої інформації, а й працівники всіх рівнів можуть зацікавити зловмисників. Особливу увагу у мисливців за інформацією викликають новачки в групі обслуговування клієнтів. Люди повністю уразливі перед обманом, оскільки можуть змінити ставлення в бік довіри до співрозмовника, якщо зловмисник маніпулює ними певним чином. Соціальний інженер очікує підозру і недовіру до себе, тому він завжди готовий до перетворення недовіри до себе в довіру. Соціальний інженер створює проблему, потім дивним чином її вирішує, обманом примушуючи жертву надати доступ до найпотаємних секретів. Але цьому можна протистояти, попередивши злочини інформаційних шахраїв, завдяки здійсненню аналізу, запобіганню обману персоналу організації методами соціальної інженерії, спеціальними інструктажами.

Способи і прийоми вторгнення соціального інженера з метою здійснення інформаційних крадіжок:

- представлення себе відомою особою, колегою, знайомим, новим співробітником або виконання дій від їх імені;
- створення ситуації, коли визначений (протокольний) порядок реагування співробітником виявляється непридатним (про надання термінової допомоги, відсутності певної особи);
- використання детальної інформації (назва структури, відділів, посад, прізвищ керівників і співробітників, їх переміщень), яка отримана з відкритих джерел (довідників), та надає зверненню правдивий характер;
- безневинна фраза, вимовлена зловмисникові охоронцем (наприклад, бухгалтер у відпустці). За допомогою технічних засобів здійснюється доступ до локальної мережі, направляється повідомлення від імені бухгалтера

зі свого комп'ютера, набирається номер приймальні. Секретар знаючи, що бухгалтер у відпустці, переводить дзвінок на системного адміністратора. Той, почувши від секретаря, що на дроті бухгалтер, дає йому доступ до потрібного документу;

- звернення (наприклад, в кадрову службу) під іменем співробітника державної організації, (наприклад, воєнкома) з проханням надати персональні дані;
- спроби через адміністратора встановити віддалений доступ до документів з використанням обману (соціальний інженер видає себе за кадрового працівника), шантажем і навіть з використанням романтичних почуттів;
- звернення відвідувачів до охоронців під будь-яким безневинним приводом, що викликає співчуття (бабусі, жінки з дітьми, інвалідів з проханням «до медсестри»).

Заходи протидії діяльності зловмисника щодо несанкціонованого отримання інформації, яка не підлягає розголошенню:

– заборона виголошення зайвої інформації за жодних обставин будь-якій особі (в пункті посадової інструкції);

– перевірка у особи, що звертається з вимогою, знання кодового слова, яке щодня змінюється керівництвом;

– організація тестових спроб проникнення за участю людей, яких персонал не знає (безпекові навчання);

– видалення надлишкової інформації з сайту, рекламних буклетів, ЗМІ, візиток;

– заборона на розголошення телефонів та інших даних співробітників;

– проведення роз'яснювальних бесід про те, що персональні дані в жодному разі не можна розголошувати телефоном, навіть якщо співрозмовник є співробітником уповноваженої організації;

– співбесіда зі співробітниками про небезпеку вторгнень та реальних збитків;

– виховання і об'єднання колективу;

– своєчасні оновлення довідників з уточненням даних про вибулих і нових співробітників;

– навчання співробітників (особливо операторів, касирів, охоронців, секретарів) задавати уточнюючі питання, перевіряти відповіді у будь-який спосіб (перетелефоновуючи, забезпечуючи контроль над електронною поштою), не перемикати зовнішні дзвінки на внутрішню телефонну лінію, записувати дані всіх сторонніх, що звертаються;

– організація перевірок пропускного режиму і роботи охоронців з відвідувачами.

Способи захисту та протидії методам соціальної інженерії, що використовують електронну пошту, телефонію, служби миттєвого обміну повідомленнями:

- тверде усвідомлення того, що телефонуючий, відвідувач чи контактер не є особою, за яку себе видає тільки тому, що він знає імена деяких людей в компанії, корпоративну термінологію або процеси. Відповідач завжди повинен піддівати сумнівам всю інформацію, яку йому надає відвідувач, думати, що все є підозрілим;
- відмовитися від звички формувати свою думку про людину або компанію за якістю інтернет-сайту, зовнішністю, одягом, манерою розмовляти, зовнішніми даними. У сучасних умовах з точки зору безпеки зовнішні атрибути відвідувача можуть нічого не означати;
- позбутись звички передавати персональну або службову інформацію будь-кому, крім свого керівництва за його вимогою, а підлеглим — лише за крайньої необхідності. Виробничі завдання повинні визначатись за умови відсутності сторонніх щодо змісту завдань осіб;
- напрацювання навичок скептичного ставлення до несподіваних вхідних листів електронної пошти, телефонних дзвінків та миттєвих повідомлень;
- включення в політику безпеки принципів використання електронної пошти стосовно вкладених документів; гіперпосилань в документах; запитів особистої або корпоративної інформації, яка передається за межі підприємства; запитам особистої або корпоративної інформації, які здійснюються ззовні підприємства;
- під час передачі інформації за допомогою мобільного зв'язку (зокрема з використанням SMS) доцільно обрати одну платформу для миттєвого обміну повідомленнями; визначити параметри захисту, що задаються при розгортанні служби SMS; визначити принципи встановлення нових контактів; задати стандарти вибору паролів; скласти рекомендації по використанню служби SMS.

Інженерна графіка у соціальній інженерії

Мобільний додаток FaceApp, за допомогою якого можна «зістарити» будь-яку людину, розроблений російською компанією Wireless Lab [11], за десять днів заробив майже мільйон доларів. Сервіс обробки фотографії за допомогою нейромереж з'явився в 2017 році. Його творець Ярослав Гончаров працював в компаніях SPB Software, Microsoft до створення власної компанії Wireless Lab. Політика

приватності FaceApp містить збирання інформації про те, якими сервісами ще користується людина, з якого саме пристрою заходить, які сайти відвідує, і деяку іншу інформацію з браузера. Користувачі платять своїми особистими даними за те, щоб користуватися такими програмами. Сервіси використовують персональні дані, щоб краще вивчати користувачів і запонувати їм більше послуги та релевантну рекламу. Якщо особа маєте логін в FaceApp з використанням свого Facebook-профіля, FaceAp просить доступ до загальної відкритої інформації з профілю користувача, електронних адрес, всіх фотографій у Facebook (у тому числі, поширених тільки для друзів або тільки для себе). Якщо особа встановлює FaceApp як додаток на смартфон, FaceApp також буде мати доступ до всіх фотографій на смартфоні користувача, в тому числі до ніколи не поширюваних в Інтернеті. Програма може викрадати персональні дані і передавати ці відомості зацікавленим особам та організаціям.

Також набув популярності графічний редактор ADOBE PHOTOSHOP для соціальних мереж. Зокрема, успіх власного посту є серйозним фактором просування власного бізнесу в соціальних мережах. Використання інструментарію ADOBE PHOTOSHOP дає можливість додати текст на картинку, зробити кольори яскравіше, поміняти фон, захистити авторство водяними знаками, оформити спільноту в соціальних мережах, створити або редагувати посадкові сторінки на сайтах, створювати рекламні матеріали. На теперішній час розповсюджений метод комп'ютерної графіки за допомогою програми ADOBE PHOTOSHOP використовується різними шахраями в інформаційному просторі. Зокрема підробка банківських карток та розміщення їх у соціальних мережах для виманювання коштів, підробки різного роду документації, грошей. Комп'ютерна графіка та програма ADOBE PHOTOSHOP для соціальних мереж стала популярною серед інтернет-споживачів особливо в умовах карантину.

Висновки та перспективи подальших досліджень

Здійснено аналіз існуючих сучасних методів соціальної інженерії та визначено технології використання різних класів методів в інформаційно-психологічній війні, а також застосування деструктивних засобів інформаційної безпеки, як складової психологічного впливу на особистість і суспільство. Зокрема визначені основні області застосування деструктивних впливів соціальної інженерії, здійснено класифікацію областей застосувань деструктивних впливів соціальної інженерії, визначено основні деструктивні аспекти застосування методів соціальної інженерії, загрози інформаційній безпеці, пов'язані з електронної поштою і з використанням служб миттєвого обміну повідомленнями, а також розглянуто заходи протидії діяльності зловмисника щодо несанкціонованого отримання інформації, яка не підлягає розголошенню і способи захисту та протидії методам соціальної інженерії, що використовують електронні засоби спілкування.

Показано, що методи комп'ютерної графіки та обробки зображень засобами штучного інтелекту є інструментами соціального інжинірингу, які несуть загрозу для захисту персональних даних.

У подальших дослідженнях планується здійснення числової оцінки ризиків слабкоформалізованих класів загроз (інформаційно-психологічні операції, метою яких є здійснення деструктивного впливу на IT-інфраструктури держави та підприємств).

ЛІТЕРАТУРА

[1] Юдін О. К., Бучик С. С. Державні інформаційні ресурси. Методологія побудови та захисту українського сегмента дерева ідентифікаторів : монографія. Київ: Вид-во НАУ, 2018. 319 с.

[2] Юдін О. К., Бучик С. С. Принципи побудови комплексної системи захисту державних інформаційних ресурсів. *Наукоємні технології*. 2015. № 1 (25). С. 15–20.

[3] Юдін О. К., Бучик С. С. Класифікація загроз державним інформаційним ресурсам нормативноправового спрямування. Методологія побудови класифікатора. *Захист інформації*. 2015. Том 17 (2). С. 108–116.

[4] Почепцов Г. Г. Психологические войны. Москва: Изд-во «Рефл-бук», 2000. 529 с.

[5] Юдін О. К., Бучик С. С., Чунарьова А. В., Варченко О. І. Методологія побудови класифікатора загроз державним інформаційним ресурсам. *Наукоємні технології*. 2014. № 2(22). С. 200–210. https://doi.org/10.18372/2310-5461.22.6820

[6] Cristoper Hadnagy. Social Engineering: The Science of Human Hacking, Inc., 2018. 321 p. https://doi.org/10.1002/9781119433729

[7] Sharon Conheady: Social Engineering in IT Security: Tools, Tactics, and Techniques: Testing Tools, Tactics & Techniques Inc., 2014. 273 p.

[8] Kevin D. Mitnick, William L. Simon. The Art of Deception: Controlling the Human Element of Security Kindle Edition Inc., 2007. 355 p.

[9] Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ: Вид-во ДУТ, 2015. 288 с.
[10] Шейнов В. П. Скрытое управление человеком: Минск, АСТ, Харвест, 2006. 625 с. ISBN: 978-5-17-013673-5, 978-985-16-1349-2
[11] FaceApp: опасно ли популярное приложение, которое «старит» лица? URL: https://www.bbc.com/ukrainian/features-russian-49016214.
[12] Корченко О. Г., Горніцька Д. А., Гололюбов А. Ю. Розширена класифікація методів соціального інжинірингу. *Безпека інформації*. 2014. №2 (20). С. 197–205.

Юдін О. К., Матвійчук-Юдіна О. В., Супрун О. М.

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНА ВІЙНА ТА ТЕХНОЛОГІЇ СОЦІАЛЬНОГО ІНЖИНІРИНГУ

Сучасне суспільство неможливо уявити без використання різних класів інформаційних потоків даних (або критичних даних), таких як новини та інший медіа-контент, спілкування в соціальних мережах та багато інших, які потрібно зберігати, аналізувати, оцінювати, висвітлювати, та використовувати для подальшого прийняття рішень. Таким чином постає проблематика свідомого використання інформаційних потоків або ресурсів з метою впливу на свідомість особистості, груп людей або всього суспільства для отримання політичної, економічної, соціальної чи особистої вигоди. Інформаційна війна на сучасному етапі розглядається, як процес маніпулювання інформацією або інформаційними потоками даних, яким довіряє об'єкт впливу, з метою прийняття рішення проти інтересів держави, установи або особистості. Найчастіше ведення інформаційної війни здійснюється з використанням методів соціальної інженерії, які ґрунтуються на алгоритмі Шейнова. Авторами запропоновано розширене бачення цього алгоритму шляхом створення на його основі петлі. В статті окреслено методи соціального інжинірингу, зокрема використання методів комп'ютерної графіки як ключового аспекту психологічного впливу на людську свідомість і одного із можливих засобів ведення інформаційної війни, інструменту ведення гібридних війн на міждержавному рівні та в сфері бізнес послуг, фінансового шахрайства. Обґрунтовано основні підходи та принципи побудови соціального інжинірингу. Уточнено понятійно-термінологічний апарат. Проаналізовано міжнародний досвід технік і технологій соціального інжинірингу в інформаційних технологіях. Визначено особливості реалізації інструментарію соціального інжинірингу на базі інформаційно-комунікаційних технологій. Наведено приклади використання основних технологій соціального інжинірингу. Як результат проведеного аналізу, запропоновано базові підходи для протидії вищезгаданим загрозам.

Ключові слова: інформаційно-психологічна війна; конфіденційна інформація; соціальний інжиніринг; суспільство; свідомість.

Yudin O., Matviichuk-Yudina O., Suprun O.

INFORMATION-PSYCHOLOGICAL WAR AND TECHNOLOGIES OF SOCIAL ENGINEERING

Modern society cannot be imagined without the use of different classes of data streams (or critical data), such as news and other media content, social networking and more that need to be stored, analyzed, evaluated, covered, and used for further decision-making. Thus, the problem of conscious use of information streams or resources in order to influence the consciousness of individuals, groups of people or society as a whole for political, economic, social or personal gain. Information war at the present stage is seen as a process of manipulating information itself, or data streams, which are trusted by the persons of public influence, in order to make decisions against the interests of the state, institution or individuals. Most often, information warfare is performed using social engineering methods, which are based on Sheinov's algorithm. In this article an extended version of this algorithm, modified by creating a loop based on it is presented.

In the article the methods of social engineering, including the use of computer graphics as a key aspect of the psychological impact on human consciousness and one of the possible means of information warfare, a tool for hybrid wars at the interstate level and in business services and financial fraud are discussed and compared. The basic approaches and principles of construction of social engineering are substantiated. The conceptual and terminological apparatus had been clarified. The international experience of social engineering techniques and technologies in information technologies are analyzed. Peculiarities of realization of social engineering tools on the basis of information and communication technologies are determined. Examples of the use of basic technologies of social engineering are given. According to analyzed threats, the conclusions are made and basic approaches to resist mentioned danger are presented.

Keywords: information and psychological warfare; confidential information; social engineering; society; consciousness.

Стаття надійшла до редакції 13.04.2021 р.
Прийнято до друку 09.06.2021 р.