УДК 004.056.5 (045)

Корченко О.Г.,Паціра Є.В.,
Пуха Д.А.

КЛАСИФІКАЦІЯ МЕТОДІВ СОЦІАЛЬНОГО ІНЖИНІРИНГУ

Інтенсифікація розвитку інформаційного суспільства розширила можливості інформаційного обміну, що в свою чергу дало поштовх удосконаленню існуючих та розвитку нових методів атак на ресурси інформаційних систем. В останні роки набули розвитку методи соціального інжинірингу (МСІ), які за специфікою реалізації відповідної класифікації [1] відносяться до соціотехнічних атак.

В різних джерелах [1-6] соціальний інжиніринг має як достатньо звужене, так і широке трактування. Наприклад, його визначають і як дієвий метод [4] переконання користувачів у виконанні певних дій на користь соціотехніка (неавторизованої сторони, що використовує методи соціального інжинірингу), так і як набір заходів [5] для збирання відомостей про інформаційну систему (без технічних подробиць її реалізації), що заснований на людському чиннику. Найбільш узагальненим визначенням соціального інжинірингу з урахуванням [6] (соціотехніка, social engineering) є наступне: загроза безпеці інформації, заснована на отриманні певних даних (наприклад, імен користувачів, паролів, номерів телефонів віддаленого доступу тощо) від різних людей в процесі інформаційного обміну. В роботі [7] здійснені перші кроки класифікації методів соціотехніків, але викладений матеріал не є достатньо структурованим і не охоплює широкого спектру ознак, за якими можна виявити дії соціального інжинірингу.

У цьому зв'язку метою роботи є класифікація МСІ на основі аналізу та узагальнення відомих публікацій відповідної предметної сфери.

Виходячи з базових підходів, описаних в [1], класифікацію МСІ найбільш доцільно здійснити за ознаковим принципом, відповідно до якого вони поділяються за:

- взаємодією з політикою безпеки;
- дистанційністю;
- ініціалізацією;
- маніпулюванням;
- порушенням характеристик безпеки;
- реляційними ознаками;
- ступінню важкості;
- типом джерела;
- типом доступу.

За взаємодією з політикою безпеки МСІ є постполітизаційні та деполітизаційні.

Постполітизаційні засновані на використанні недоліків у вже існуючій політиці безпеки [6]. Наприклад, такими недоліками можуть бути: неправильно побудовані правила розмежування доступу; використання програмних і апаратних засобів з недостатнім рівнем захищенності; прорахунки у блокуванні каналів витоку інформації з обмеженим доступом; заборона видачі імен та телефонів персоналу джерелу (здійснюючого запит), яке достовірно не ідентифіковане тощо.

Деполітизаційні атаки пов'язані з помилками і недбалістю [6, 8], які мають місце при реалізації заходів із забезпеченням вже існуючої політики безпеки. Це, в першу чергу, пов'язано з людським чинником і залежить від недостатньої адміністративної підтримки, коректності виконання функцій захисту, своєчасності реагування на нештатні ситуації (тобто, коли створюються умови, які не описані в політиці безпеки і працівники не реагують на них з урахуванням відповідних заходів безпеки) тощо. Прикладом нештатної ситуації може бути неврахована поведінка персоналу при проханні найвищого керівництва компаії отримати секретну інформацію.

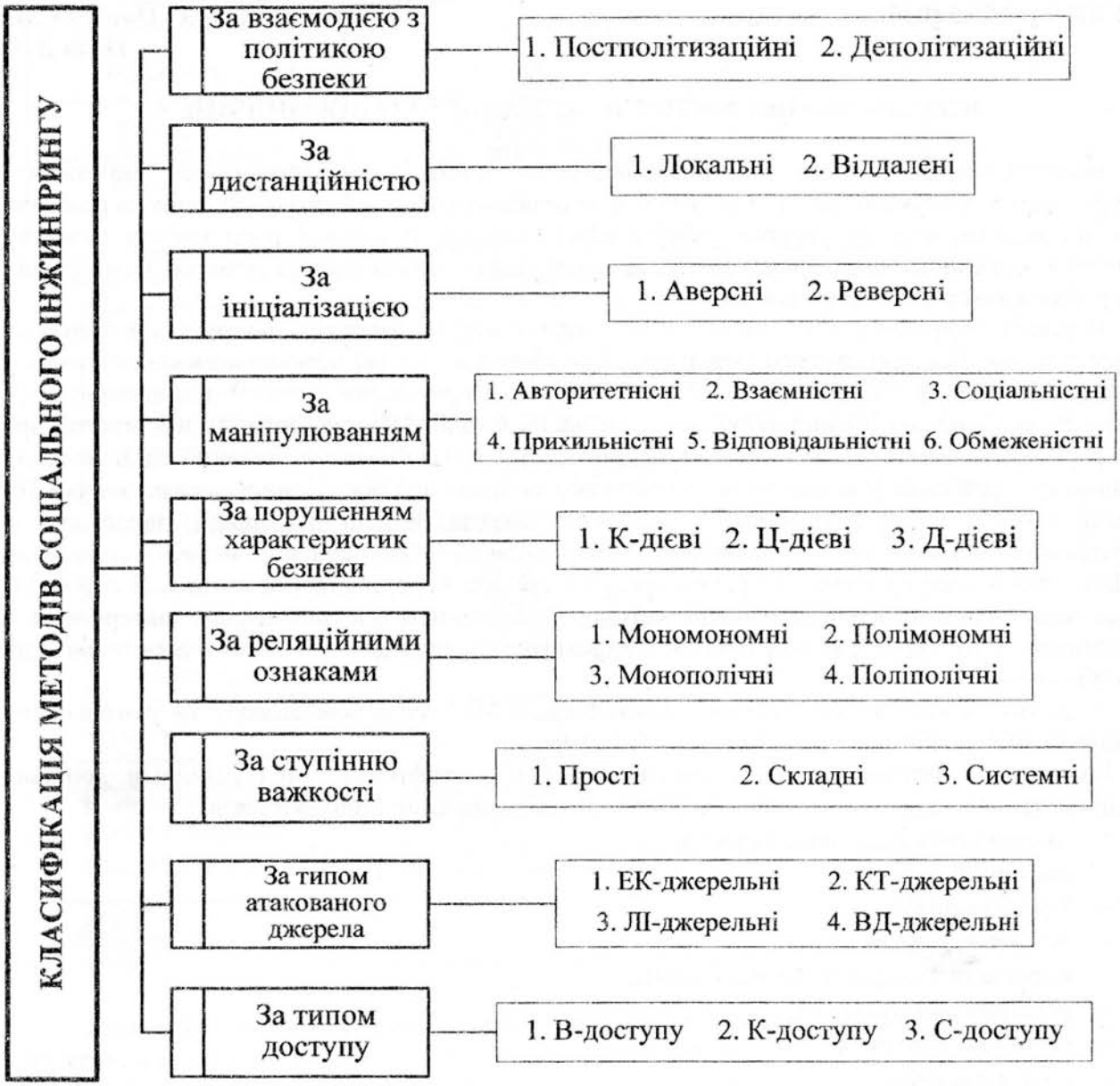

Рис.1. Узагальнена класифікація МСІ

За дистанційністю МСІ поділяються на локальні та віддалені.

Локальні реалізуються шляхом безпосереднього індивідуального спілкування соціотехніка з атакованим. Наприклад, коли останній є службовцем компанії, а соціотехнік шляхом прямого контакту представляється як співробітник, постачальник або працівник партнерської компанії, людиною зі служби підтримки тощо та просить про допомогу.

Віддалені поділяються на Т- та МТ-віддалені. Дані МСІ реалізуються за допомогою засобів комунікації, такими, як телефон, факс, електронна пошта, віртуальна комп`ютерна мережа тощо.

Т-віддалені базуються на використанні телефону, що є найпоширенішим підходом у проведенні соціотехнічних атак. Володіючи навичками маніпулювання основними рисами людської натури, атакуючий може добувати потрібну йому інформацію видавши себе за іншу особу та переконавши в цьому атакованого (це є особливо дієвим методом у великих корпораціях, оскільки знати всіх співробітників та слідкувати за прийомом нових достатньо складно). Соціотехніки звертають особливу увагу на те, як створити досконале психологічне

середовище для атаки. Незалежно від методу, що використовується, основна мета полягає в тому, щоб переконати людину (що розкриває інформацію) в тому, що соціотехнік і є таким об`єктом, якому можна довірити відповідну інформацію. Для цього використовуються маскарадингові технології [1]. Наприклад, соціотехнік може представитися співробітником віддаленого офісу і просити локального доступу до пошти, новим співробітником, що просить про допомогу, постачальником або виробником програмного забезпечення (ПЗ) та пропонувати його оновлення.

МТ-віддалені базуються на використанні мережевих технологій, наприклад, електронної почти, широкого спектру вірусного та іншого шкідливого ПЗ, Інтернет-ресурсів тощо. У разі використання електронної пошти жертві може бути відправлений запит або прохання на виконання певної дії від імені керівництва, співробітників, знайомих тощо. Прикладом такого типу може бути відправлення запиту відділу фінансів надання звіту за місяць керівництву, який потрібно відіслати на підставлену соціотехніком електронну поштову скриньку. Іншим випадком МТ-віддаленого МСІ може бути відправлення разом з листом або прикладним ПЗ вірусів чи шкідливого ПЗ, або адреси Інтернет-ресурсу на них. Це може бути здійснено шляхом відправлення вкладення до листа на електронну поштову скриньку, прикріплення шкідливого ПЗ до завантажувальної програми тощо. Також соціотехнік може надіслати атакованому лист з повідомленням, що винайдена нова корисна утиліта, яку можна отримати за певною адресою, де атакуючий розміщує шкідливу програму або вірус. Соціотехнік також може відправити тільки адреси Інтернет-ресурсу на відомі джерела з дуже схожою, але відмінної від справжньої, адресою. Оскільки атакуючим створено достатньо схожий графічний інтерфейс, то жертва не підозрюючи може зареєструватись, залишивши свій ідентифікатор, пароль чи адресу електронної поштової скриньки, або спробувати увійти як вже зареєстрований користувач. Соціотехнік може здійснити МТ-віддалену атаку шляхом використовування фальшивого pop-up вікна (небажане вікно, яке з`являється під час роботи з Інтернет-ресурсами), де можуть бути розміщені на перший погляд корисні, проте небезпечні, адреси Інтернет-ресурсів, форми для додаткової реєстрації, вікна завантаження шкідливого ПЗ під виглядом корисних додатків тощо.

За ініціалізацією МСІ поділяються на аверсні і реверсні.

Аверсні (прямі) є МСІ, при яких соціотехнік звертається до атакованого зі своєю проблемою, переконуючи його в своїй авторизованності та просить про допомогу. Аверсні соціотехнічні атаки також можуть бути реалізовані за допомогою шкідливого ПЗ та використання неуважності атакованого. Наприклад, соціотехнік може, представившись адміністратором комп`ютерного відділу і залетефонувавши на вихідних додому одному із службовців, який займається розробкою важливого проекту, з повідомленням (ніби в знак вічливості) про несправність локальної мережі та можливості її відновлення тільки через деякий час. А оскільки (і соціотехнік це знає) терміни закінчення проекту стислі, то атакований на відповідний запит погоджується видати свій ідентифікатор і пароль для швидкого відновлення потрібних файлів.

Реверсні (зворотні) пов`язані з тим, що соціотехнік створює ситуацію, в якій атакований стикається з певною проблемою і звертається до атакуючого для її розв`язання. Інша форма реверсної соціальної інженерії полягає в перенаправленні дій на атакуючого, тобто ціль (соціотехнік) розпізнає атаку і використовує різні методи (психологічні прийоми) для отримання максимально можливої інформації про атакуючого. Наприклад, представившись робітником технічної допомоги провайдера (компанії, які надають послуги доступу до мережі Інтернет), соціотехнік може повідомити жертві про можливі проблеми з доступом до глобальної мережі ближчим часом і дати свій номер телефону, за яким потрібно звернутися для швидкої ліквідації проблеми (в даному прикладі жертва є новим співробітником або знаходиться в філіалі компанії, де немає адміністратора). Після чого атакуючий телефонує провайдеру та представляючись начальником фірми просить відключити доступ вище згаданого філіалу у зв`язку із ремонтними роботами в офісі. Соціотехніку залишається тільки

чекати, коли жертва залетефонує в надії отримати допомогу, після чого атакуючий може сам приїхати на місце знаходження жертви та отримати доступ до робочої станції.

За маніпулюванням рисами людської натури МСІ поділяються на авторитетністні, прихильністні, взаємністні, відповідальністні, соціальністні та обмежувальністні, які відповідно назвемо АВ-, ПР-, ВМ-, ВД-, СЦ- та ОБ-маніпулюванням. Такі ознаки визначені шляхом узагальнення результатів соціальних досліджень [9] щодо впливів (маніпуляцій) на людей, де виділено шість рис людської натури, які можна використовувати для отримання потрібної інформації.

АВ-маніпулювання ґрунтуються на тому, що людям властиве бажання зробити (задовольнити запит) послугу особі з авторитетом (владою) і соціотехнік отримує необхідні дані, якщо атакований сприймає його як авторитетне чи компетентне джерело. Наприклад, соціотехнік може використовувати маскарадні технології [1] у вигляді ствердження, що телефонує керівництво, представитись як правоохоронні органи тощо.

ПР-маніпулювання засновуються на вмінні викликати у атакованого схильність до себе. Це пов`язано з тим, що люди зазвичай задовольняють запит суб`єкта, який викликає прихильність до себе, має схожі інтереси, проблеми тощо, наприклад, перед з`ясуванням необхідних даних шляхом здійснення ключового запиту соціотехнік з`ясовує інтереси жертви і представляє їх як свої, або повідомляє, що вони з атакованим з однієї ж школи, міста тощо.

ВМ-маніпулювання пов`язані зі схильністю людини машинально надавати інформацію у відповідь на певну взаємність (бажання відплатити), наприклад, матеріальну річ, пораду, допомогу тощо і це особливо ефективно тоді, коли атакований не чекає цього. Найефективніший шлях до взаємності (тобто отримання інформації) – неявно піднести подарунок, який би зобов`язав жертву. Наприклад, представитись співробітником департаменту інформатизації і сказати, що деякі комп`ютери компанії, інфіковані новим особливо небезпечним вірусом [1], який не виявляється наявними засобами захисту і пропонує розв'язати зазначену проблему. Далі (на свою користь) соціотехнік просить атакованого протестувати нову утиліту, що дозволяє користувачу змінити паролі.

ВД-маніпулювання ґрунтуються на звичках виконувати обіцяне, щоб не здаватися людиною, яка не заслуговує довіри. Наприклад, соціотехнік радить новому відповідальному співробітнику (відповідно до підписаної ним угоди) ознайомитися з процедурами і правилами політики безпеки, виконання яких надають законних повноважень щодо коректності користування ресурсами інформаційних систем компанії. Після обговорення декількох положень безпеки соціотехнік запитує пароль співробітника (для підтвердження виконання ним угоди) з метою перевірки його протистояння вгадуванню і далі надає рекомендації формування пароля в наступному разі. Атакований погоджується слідувати порадам, оскільки це відповідає політиці компанії і соціотехнік підтверджує його згоду слідувати угоді.

СЦ-маніпулювання пов`язані з належністю атакованого до певної авторизованої (соціальної) групи, а дії в ній інших є гарантом істинності в питанні поведінки. Тобто, необхідно виконувати те, що виконують інші. Наприклад, соціотехнік видає себе за перевіряючого із служби безпеки і називає імена інших людей з відділу атакованого, які вже пройшли відповідну процедуру перевірки. Жертва вірить цьому, що дозволяє атакуючому задавати різні питання, аж до визначення ідентифікатора і пароля, які використовує жертва.

ОБ-маніпулювання ґрунтуються на ліміті так званого "безкоштовного сиру", тобто віри в те, що об`єкт ділиться частиною інформації, на яку претендують інші, або ця інформація доступна тільки у даний момент. Наприклад, соціотехнік розсилає електронні листи з повідомленням про те, що ті, хто зареєструються на новому розважальному сайті до кінця тижня, отримають безкоштовно електронний альбом будь-якого виконавця. В процесі реєстрації ніщо не підозрюючий співробітник зазначає свій ідентифікатор, пароль, електронну пошту тощо. А як відомо люди часто, щоб не забувати паролів і ідентифікаторів,

використовують однакові у всіх системах. Скориставшись цим, соціотехнік може отримати доступ до службових або приватних інформаційних ресурсів атакованого.

Якщо в процесі атаки використовуються різні риси людської натури, то результуючим буде комбінований тип на основі вище згаданих, наприклад, АВВД-маніпулювання використовує авторитетнісну та відповідальнісну риси.

За порушенням характеристик безпеки МСІ поділяються на К-, Ц- та Д-дієві.

К-дієві спрямовані на порушення такої характеристики безпеки, як конфіденційність. Тобто, наприклад, внаслідок дій соціотехніка конфіденційна інформація стає відомою йому або будь-кому іншому при забороні доступу до неї.

Ц-дієві методи спрямовані на порушення цілісності інформації. Наприклад, якщо соціотехніку в результаті проведення атаки вдалось замінити блоки коду нового програмного продукту.

Д-дієві це такі МСІ, внаслідок яких порушується доступність інформації. Прикладом є відмова мережевого серверу в результаті отримання соціотехніком ідентифікатора та пароля адміністратора безпеки.

Якщо в процесі атаки порушуються різні характеристики безпеки, то результуючим буде комбінований тип на основі вище згаданих, наприклад, МСІ КЦД-дії порушують конфіденційність, цілісність та доступність інформації.

За реляційними ознаками МСІ поділяються на мономономні, полімономні, монополічні та поліполічні.

Мономономні спрямовані для здійснення атаки у напрямку від одного атакуючого до одного атакованого. Наприклад, здійснення дзвінка до співробітника з запитом на отримання потрібної інформації.

Полімономні це такі, при яких атака реалізується спрямованими діями від двох та більше атакуючих до одного атакованого. Прикладом може слугувати відправлення електронної пошти від декількох соціотехніків (які, наприклад, будуть видавати себе за знайомих жертви) до одного отримувача. При цьому атакованого спробують переконати відкрити надану адресу Інтернет-ресурсу, де, наприклад, його спіткає можливість завантажити шкідливе ПЗ.

Монополічні реалізуються направленими діями від одного атакуючого на два чи більше атакованих. Наприклад, якщо потрібно отримати інформацію, яка не може бути надана одним співробітником під загрозою викриття, соціотехнік може телефонувати в різні дні або різним людям для отримання потрібних даних.

Поліполічні це такі, що об`єднують в собі полімономні та монополічні технології, при яких атака реалізується спрямованими діями від двох та більше атакуючих до двох та більше атакованих. Група соціотехніків зможе більш ефективно отримати потрібну інформацію від групи людей, яку достатньо складно одержати вище перерахованими МСІ, що класифікуються за реляційними ознаками.

За ступінем важкості МСІ бувають прості, складні та системні.

Прості реалізуються невеликою кількістю кроків. Наприклад, при необхідності дізнатись імена службовців потрібного відділу на підприємстві, соціотехнік може використати наявні інформаційні ресурси компанії (наприклад, Web-сайт), дізнатись номер телефону служби підтримки і, зателефонувавши туди, дати запит на потрібну йому інформацію.

Складні здійснюються шляхом комбінування нескладних алгоритмів для виявлення потрібної інформації. Наприклад, якщо необхідно дізнатись паролі користувачів, то можна реалізувати таку послідовність: спочатку визначити, чиї паролі потрібні (тобто дізнатись імена), потім дізнатись, яке джерело може дати потрібну інформацію, після цього дія спрямовується на отримання пароля будь-яким із методів.

Системні реалізуються на основі використання складного алгоритму (розгалудженого, зі зворотніми зв`язками та циклічними процесами) для отримання інформації, яку не можливо дістати простими чи складними методами. Системні атаки можуть використовуватися для отримання кодів нових продуктів ПЗ, доступу до серверів систем безпеки тощо.

За типом атакованого джерела [10] МСІ поділяються на: ЕК-, ЛГ-, КН- та ВП-джерельні. Фактично тип джерела пов`язаний із рівнем інформованості атакованого.

ЕК-джерельні направлені на експерта, чиї професійні знання і контакти (як робота, так і хобі) забезпечують високу орієнтацію в питанні, що підлягає розробці соціотехніком. Експерт може видати як базові матеріали, так і вивести на невідомі джерела інформації. Загальна надійність отримуваних при цьому даних найчастіше є високою.

ЛГ-джерельні спрямовані на легковажну особу, що виказує потрібні факти в діловій, дружній, компанійській або інтимній бесіді. Така випадкова інформація може бути надзвичайно цінною, хоча загалом не виключена як звичайна брехня, так і навмисна дезінформація.

КН-джерельні атаки спрямовані на людей (контактерів), які будь-яким чином контактують або колись контактували з об'єктом, що вивчається соціотехніком (людиною, групою, організацією тощо). Це можуть бути випадкові ділові партнери, родичі або знайомі, працівники сервісу тощо. Разом з повідомленням певних фактів вони можуть сприяти в підході до об'єкту або ж брати участь у прямому вилученні у нього інформації.

ВП-джерельні атаки спрямовані на випадкового індивіда, який не розглядається як потенційний інформатор, проте є носієм важливої інформації. Зважаючи на випадковість і непередбачувальність на таку людину соціотехніки не покладаються, але намагаються отримати як найбільше потрібних даних.

Якщо в процесі атаки використовуються різні типи атакованих джерел, то результуючим буде комбінований тип на основі вище згаданих, наприклад, ЕККН-джерельна пов'язана з експертом та контактером.

За типом доступу до інформації МСІ поділяються на В-, К- та С-доступу.

В-доступу пов'язані з доступом до інформації, яка відображена у відкритих джерелах, наприклад, друковані періодичні видання, Інтернет-ресурси, засоби масової інформації, дзвінки в службу підтримки тощо.

К-доступу орієнтовані на отримання доступу до конфіденційної інформації, тобто до такої, яка є не секретною, проте доступ до неї контролюється особами, які несуть за неї відповідальність. Наприклад, імена, номери телефонів, поштові адреси, посади і т. ін.

С-доступу пов'язані з отриманням доступу до інформації, що має гриф секретності та привілеї на яку має обмежене коло довірених осіб. Такою інформацією можуть бути, наприклад, секретні коди доступу, новітні розробки, секретні матеріали тощо.

Якщо атаки пов'язані з реалізацією доступу до різних типів інформації, то результуючим буде комбінований метод на основі вище згаданих, наприклад, ВК-доступу орієнтований на відкриту та конфіденційну інформацію.

Узагальнений алгоритм реалізації соціотехнічної атаки (рис.2) включає:

Етап 1. Визначення мети.

Етап 2. Аналіз джерел, з яких є можливість добути інформацію, потрібну на початковому етапі. В першу чергу розглядаються відкриті джерела, оскільки немає режиму обмеження доступу до них.

Етап 3. Перевірка достатності добутої інформації для здійснення атаки. Якщо необхідні додаткові дані, то соціотехнік визначає кроки та реалізацію добування потрібної інформації, а якщо її кількість достатня для здійснення атакуючих дій, то соціотехнік переходить до наступного етапу.

Етап 4. Фінальні атакуючі дії.

На рис. 2 в наведеному алгоритмі дії соціотехніків представлені одновимірним масивом Д[i], який позначає необхідну додаткову інформацію, де $i=\overline{1,n}$, а n-кількість додаткової інформації.

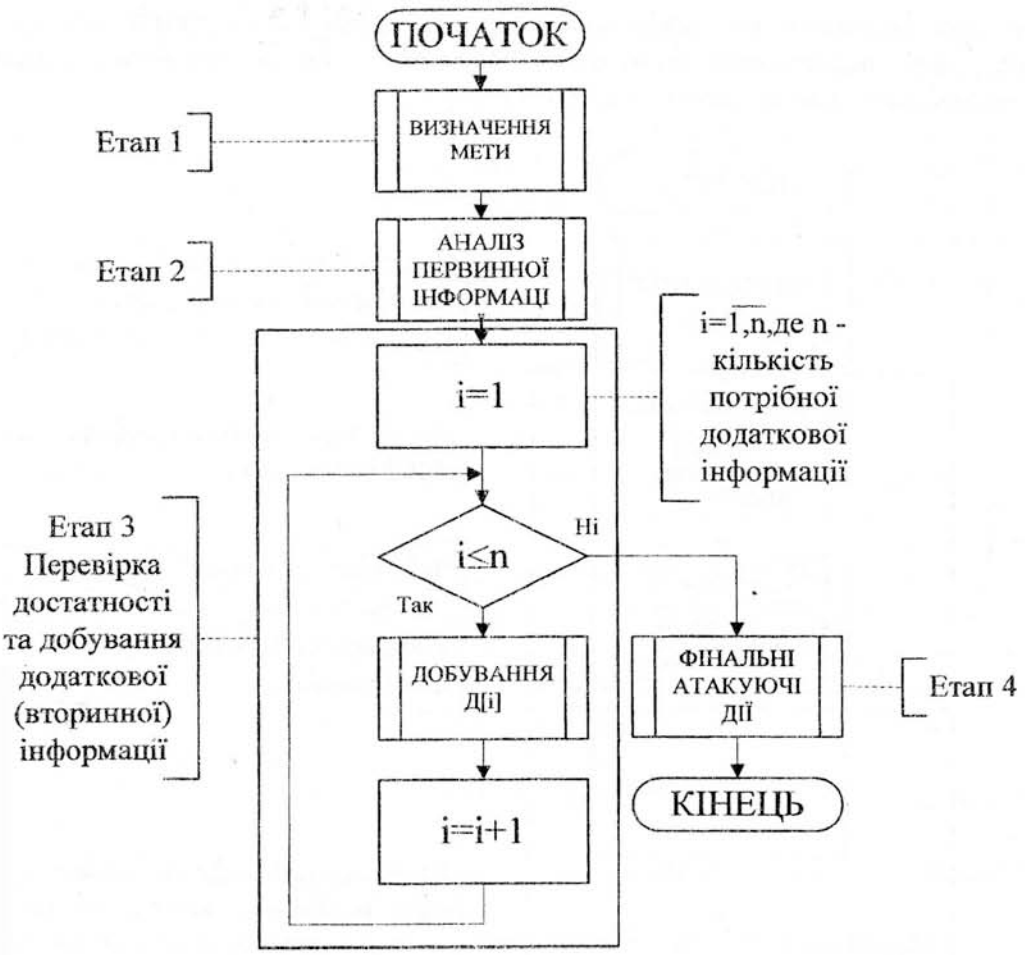

Рис.2. Узагальнений алгоритм здійснення соціотехнічної атаки

Відповідно до узагальненого алгоритму (див. рис. 2) наведемо приклад здійснення соціотехнічної атаки (див. рис. 3):

Етап 1. Дізнатися номер кредитної картки та мобільного телефону начальника проекту нової продукції фірми А для конкурентної фірми В.

Етап 2. Представники фірми В назвали підприємство С, де жертва є постійним клієнтом. На сайті компанії С міститься телефон служби підтримки (довідкової служби).

Етап 3. Залетефонувавши, соціотехнік представляється клінтом та дізнається номер телефону та імя потрібного службовця відділу клієнтів.

Щоб запросити потрібну інформацію, соціотехнік повинен знати процедуру видачі інформації про клієнтів. Під виглядом співробітника правоохоронних органів, він телефонує в службу підтримки компанії С та говорить про випадок крадіжки кредитної картки у людини, яка є клієнтом фірми С, та здійснює запит потрібної інформації (які дані надає клієнт і яким чином та чи надійно вони зберігаються). На що отримує відповідь, що кожен клієнт має свій порядковий номер, та в базі надійно зберігаються імена, номери контактних телефонів, кредитних карток, тощо. Отже тепер соціотехнік знає, куди потрібно зателефонувати та як зробити запит номеру кредитної картки та мобільного телефону начальника проекту нової продукції фірми С, щоб не викликати підозри. Але для здійснення атаки потрібно себе певним чином ідентифікувати. Знаючи структуру компанії С (інформація з сайту) атакуючий вибирає регіональне відділення в іншому місті. Телефонуючи у службу підтримки, соціотехнік дізнається ім'я та телефон працівника відділу рахунків.

Етап 4. Фінальним кроком є дзвінок у відділ клієнтів компанії С. Соціотехнік представляється службовцем відділу клієнтів регіонального відділення, називає ім'я і

повідомляє про зараження його комп`ютера вірусом та що він на даний момент не може відкрити базу, щоб задовільнити запит серйозного клієнта. Після чого просить надати йому потрібну інформацію, даючи лише ім'я клієнта [7].

Рис. 3. Приклад алгоритму здійснення соціотехнічної атаки

Відповідно до наведеного прикладу ця атака (що грунтується на МСІ) класифікується як: деполітизаційна, Т-віддалена, аверсна, АВВМ-маніпульована, К-дієва, монополічна, складна, ЕК-джерельна, ВК-доступу.

Запропонована в роботі ознакова класифікація МСІ розкриває багатогранність цього поняття та широту проявів соціотехнічних атак, а врахування цих чинників при розробці та виборі методів і засобів протидії дозволить підвищити ефективність відповідних впроваджуваних систем безпеки. Результати даної роботи можна також використати для побудови систем оцінки рівня підготовленості персоналу щодо протидії вторгненню, заснованому на певній множині визначених класів соціотехнічних атак.

Список літератури

1. *Корченко О.Г.* Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: «МК – Пресс», 2006. – 320с.

2. *Конеев И.Р., Беляев А.В.* Информационная безопасность предприятия. – СПб:БХВ-Петербург, 2003. – 752с.

3. *Чириль Дж.* Защита от хакеров (+CD).-СПб.: Питер, 2002. – 480с.

4. *Мак-Клар Стюард, Спенбреб Джоел, Курц Джордж.* Секреты хакеров. Безопасность сетей – готовые решения. – 4-е изд.: Пер. с англ. – М.: Изд. дом «Вильямс», 2004. – 656с.

5. *Коул Ерик.* Руководство по защите от хакеров: Пер. с англ. – М.: Изд. дом «Вильямс»., 2002. – 640с.

6. *Бабак В. П., Корченко О. Г.* Інформаційна безпека та сучасні мережеві технології. Англ.-укр.-рос. слов. термінів. – К.: НАУ, 2003. – 670 с.

7. *Kevin D. Mitnik, William L. Simon, Steve Wozniak,.* The Art Of Deception: Wiley, 2002. – 304с.

8. *Корченко А. Г.* Несанкционированный доступ к компьютерным системам и методы защиты: Учеб. пособие. – К.: КМУГА, 1998. – 116 с.

9. *Robert B. Cialdini.* The Science of Persuasion // Scientific American Magazine. – 2001, – №2. – P.76-81.

10. *И. Н. Кузнецов* Информация: сбор, защита, анализ. Учебник по информационно-аналитической работе. - М.: ООО Изд. Яуза, 2001. – 100с.

УДК 681.3.06 **Дóренський О.П.**

МЕТОД ВИЗНАЧЕННЯ ПОКАЗНИКА СТІЙКОСТІ ДО ЗАГРОЗ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ

Постановка проблеми

На сьогоднішній день більшість систем забезпечення безпеки інформації (СЗБІ) не повністю відповідають вимогам щодо організації надійної безпеки інформаційної системи (ІС), що пов'язано з рядом факторів, які не враховуються під час проектування і, відповідно, реалізації СЗБІ.

Аналіз

На основі проведеного дослідження [1, 2, 3] можна виділити основні напрямки вирішення комплексу задач, пов'язаних зі здійсненням оцінки та оптимального вибору варіантів побудови СЗБІ. При цьому аналіз впроваджених систем оцінювання СЗБІ [2, 4] показало, що більшість моделей СЗБІ окремо не виділяються та не розглядаються оцінювання показника стійкості самої СЗБІ до загроз, що є вірогідним. За умови відмови СЗБІ повністю унеможливлює організацію надійної безпеки інформації ІС.