© Korchenko A., Gornitska D., Gololobov A. Extended classification of methods of social engineering // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 2, p. 197-205.

РОЗШИРЕНА КЛАСИФІКАЦІЯ МЕТОДІВ СОЦІАЛЬНОГО ІНЖИНІРИНГУ

Олександр Корченко, Дарина Горніцька, Андрій Гололобов

Національний авіаційний університет, Україна

КОРЧЕНКО Олександр Григорович, д.т.н., професор

Рік та місце народження: 1961 рік, м. Київ, Україна.
Освіта: Київський інститут інженерів цивільної авіації (з 2000 року – Національний авіаційний університет), 1983 рік.
Посада: завідувач кафедри безпеки інформаційних технологій з 2004 року.
Наукові інтереси: інформаційна та авіаційна безпека.
Публікації: більше 270 наукових публікацій, серед яких монографії, словники, підручники, навчальні посібники, наукові статті та патенти на винаходи.
E-mail: icaocentre@nau.edu.ua

ГОРНІЦЬКА Дарина Анатоліївна

Рік та місце народження: 1985 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2007 рік.
Посада: здобувач Національного авіаційного університету.
Наукові інтереси: інформаційна безпека, соціотехнічні атаки.
Публікації: більше 20 наукових публікацій, серед яких монографії, наукові статті та патенти на винаходи.
E-mail: darja85@ukr.net

ГОЛОЛОБОВ Андрій Юрійович

Рік та місце народження: 1983, м. Київ, Україна.
Освіта: Національний технічний університет України «КПІ», 2006 рік.
Посада: аспірант кафедри безпеки інформаційних технологій з 2012 року.
Наукові інтереси: інформаційна безпека, програмування.
E-mail: b2d@ukr.net

Анотація. *У зв'язку з інтенсивним розвитком сучасних інформаційних технологій соціотхенічні атаки набули широкого розповсюдження та удосконалення. Для розробки та впровадження ефективних засобів протидії соціотехнічним атакам (наприклад, таких як система управління інформаційною безпекою) необхідно сформувати найбільш повну множину їх характерних ознак та складових. Відома класифікація потребує доповнень та розширення для можливості побудови більш ефективних засобів протидії. На основі аналізу та узагальнення відомих публікацій відповідної предметної сфери була розширена відома класифікація методів соціального інжинірингу за рахунок введення нових ознак та їх складових. В загальному вигляді класифікація містить 12 базових ознак, що у сумі інтегрує більш ніж 50 відповідних характеристик. Результати роботи можуть бути використані, наприклад, для побудови систем оцінки ризиків, рівня підготовленості персоналу щодо протидії соціотехнічним атакам тощо.*

Ключові слова: *соціотехнічні атаки, методи соціального інжинірингу, класифікація соціотехнічних атак, ознакова 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. У роботі [7] здійснена найбільш повна класифікація МСІ, проте у зв'язку з інтенсивним розвитком сучасних інформаційних технологій соціотхенічні атаки набули широкого розповсюдження та удосконалення. Для розробки та впровадження ефективних засобів протидії соціотехнічним атакам (наприклад, таких як система управління інформаційною безпекою) необхідно сформувати найбільш повну множину їх характерних ознак та складових.

У цьому зв'язку метою роботи є розширення (на основі аналізу та узагальнення відомих публікацій відповідної предметної сфери) класифікації МСІ за рахунок введення нових ознак та їх складових.

Виходячи з базових підходів, описаних в [1, 7], класифікація МСІ здійснюється за ознаковим принципом, відповідно до якого вони поділяються за (рис. 1): взаємодією з політикою безпеки; дистанційністю; ініціалізацією; інструментарієм; маніпулюванням; порушенням характеристик безпеки; реляційними ознаками; степенем важкості; типом атакованого джерела; типом доступу; типом звернення; типом СТ.

За **взаємодією з політикою безпеки** МСІ є постполітизаційні та деполітизаційні [1].

Постполітизаційні засновані на використанні недоліків у вже існуючій політиці безпеки та можуть бути здійсненні як у *процесі* функціонування системи, так і у *періоді неактивованих* компонентів системи. [8]. Наприклад, такими недоліками можуть бути: неправильно побудовані правила розмежування доступу; використання програмних і апаратних засобів з недостатнім рівнем захищеності; прорахунки у блокуванні каналів витоку інформації з обмеженим доступом; заборона персоналу видавати імена та телефони джерелу (здійснюючого запит), яке достовірно не ідентифіковане тощо.

Деполітизаційні методи пов'язані з помилками і недбалістю [6, 9], які мають місце при реалізації заходів забезпечення 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 компанії отримати секретну інформацію.

Якщо атаки реалізуються за допомогою різних типів, то результуючим буде комбінований метод на основі вище згаданих, наприклад, постполі-тизаційно-деполітизаційого типу при використанні недоліків як у вже існуючій політиці, так і - користування нештатною ситуацією.

За **дистанційністю** МСІ поділяються на локальні та віддалені.

Локальні реалізуються шляхом безпосереднього індивідуального спілкування соціотехніка з атакованим. Наприклад, коли останній є службовцем компанії (включаючи користувачів системи, персонал, що обслуговує технічні засоби, керівників різних рівнів посадової ієрархії, співробітників підрозділу розробки і супроводу програмного забезпечення, технічний персонал, що обслуговує приміщення), а соціотехнік (класифікація СТ наведена нижче) шляхом прямого контакту представляється як співробітник, постачальник або працівник партнерської компанії, людиною зі служби підтримки тощо та просить про допомогу. За місцем дії локальні можуть бути: **КТ-локальні** (із контрольованої території без доступу в приміщення); **ПР-локальні** (усередині приміщення, але без доступу до технічних засобів системи); **РМ-локальні** (з робочих місць кінцевих користувачів системи); **ЗД-локальні** (з доступом у зону даних; та/або з доступом у зону керування засобами безпеки КСЗ). При будь-якому локальному методі для доступу до території (приміщень) можуть бути використані так звані *лок-засоби* – пристрої, які фізично обмежують доступ до приміщень та периметрів - замки, відмички, електронні ключі, магнітними картками, датчики руху, сигналізації тощо. Існує великий спектр класичних ключів.

Якщо атаки пов'язані з реалізацією різних типів локальних методів, то результуючим буде комбінований метод на основі вище згаданих, наприклад, КТ-ПР-локального типу при здійсненні атаки із контрольованої території без доступу в приміщення та з проникненням усередину приміщення без доступу до технічних засобів системи на різних кроках атаки.

Віддалені поділяються на Т- та МТ- та РП - віддалені. Дані МСІ реалізуються за допомогою засобів комунікації, такими, як телефон, факс, електронна пошта, віртуальна комп`ютерна мережа тощо і у більшості випадків здійснюються без доступу на контрольовану територію.

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 СТ і є таким об`єктом, якому можна довірити відповідну інформацію.

КЛАСИФІКАЦІЯ МЕТОДІВ СОЦІАЛЬНОГО ІНЖИНІРИНГУ										
	1.	За взаємодією з політикою безпеки	1.1. Постполітизаційні			1.2. Деполітизаційні				
	2.	За дистанційністю	2.1. Локальні			2.2. Віддалені				
	3.	За ініціалізацією	3.1. Умовні			3.2. Безумовні				
	4.	За інструментарієм	4.1. Програмні			4.2. Апаратні			4.3. Нетипові	
	5.	За маніпулюванням	5.1.Авторитет.			5.2. Взаємністні			5.3. Соціальністні	
			5.4.Прихильніс.			5.5.Відповідальн.			5.6.Обмеженістні	
	6.	За порушенням характеристик безпеки	6.1. К-дієві			6.2. Ц-дієві			6.3. Д-дієві	
	7.	За реляційними ознаками	7.1. Мономономні			7.2. Полімономні				
			7.3. Монополічні			7.4. Поліполічні				
	8.	За степенем важкості	8.1. Прості			8.2. Складні			8.3. Системні	
	9.	За типом атакованого джерела	9.1. ЕК-джерельні			9.2. КТ-джерельні				
			9.3. ЛІ-джерельні			9.4. ВД-джерельні				
	10.	За типом доступу	10.1. В-доступу			10.2. ВВ-доступ				
			10.3. К-доступу			10.4. С-доступу				
	11.	За типом звернення	11.1. Аверсні			11.2. Реверсні				
	12.	За типом СТ	12.1. ХК	12.2. ПС	12.3. ШГ	12.4. ЗІ	12.5. НС			
			12.6. ШХ	12.7. ВР	12.8. ПР	12.9. ВК				

Рис.1. Розширена класифікація МСІ

Для цього використовуються маскарадингові технології [1]. У наші дні, у час мобільних\стільникових телефонів, VoIP та телефонних серверів варіанти того, як соціальний інженер може використовувати телефон, виросли значно . Через те, що щоденно на підприємствах відбувається значна кількість дзвінків з приводу телемаркетингу, продажу та оголошень, соціальний інженер повинен мати досить суттєві навички, щоб успішно скористатися телефоном в ході атаки. В епоху, коли у кожного є мобільний телефон, люди ведуть персональні розмови в автобусах, метро або в будь-якому громадському місці, телефон може бути використаний у багатьох відношеннях. Прослуховування або дзвінки на мобільні телефони дозволяє отримати додаткові вектори, які не були доступні в минулому. Із збільшенням числа смартфонів, планшетів та інших мобільних пристроїв все більше і більше людей зберігають паролі, персональні дані та іншу приватну інформацію на своїх телефонах. Це відкриває можливість для соціальних інженерів мати можливість доступу до мети і необхідних даних в різних ситуаціях. Крім того, будучи на зв'язку 24 / 7 люди стають більш готовими видавати інформацію швидко, якщо телефонуючий надає певний набір « критерії », що робить його запит правдоподібним. Наприклад, якщо автоматичний визначник номеру на мобільному телефоні показує, що людина телефонує з корпоративної штаб-квартири, багато людей будуть надавати інформацією без перевірки. І iPhone (iOS) і Android- та інші смартфони мають додатки, які можуть бути використані для підробки ідентифікаційного номеру абоненту. Додатки типу SpoofApp (www.spoofapp.com) дозволяють соціальному інженеру здійснювати дзвінки, які виглядають так, як ніби вони надходять з будь-якого куточку землі при відносно низькій вартості за дзвінок. 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 методу 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 СТ 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.

РП-віддалені базуються на реєструючих та\або профілюючих інструментах, результатом чого є отримання профілю атакованого та виконання частини атаки або досягнення її кінцевої цілі. На даний час можливо знайти велику кількість реєструючих приладів, таких як камери різних форм; ручки; заховані в кінчики пір'я; всередині годинника тощо. СТ часто відстежують цілі до або після їх відходу офіс, наприклад з допомогою GPS Tracker. Разом з інструменти профілювання - які допомагають збирати профілі та паролі – та після того, як СТ зібрав всю інформацію про атакованого, яку можливо, наступним кроком є розробка анкети профілю. Анкета профілю представляє із себе один або декілька напрямків атаки, які атакуючий вважає будуть успішними, а також надає можливість розпочати будувати список потенційних паролів та спробувати їх у разі потреби. Підбор паролю інструментами профілювання може зайняти кілька годин або навіть днів. Щороку велике число людей стають жертвами простих атак, незважаючи на численні попередження та політик безпеки. Число людей, які перераховують відомості про себе, свої сім'ї і їх життя в Інтернеті на сторінках соціальних мереж є достатньо великим. Поєднавши дані, побудований з їхніх джерел з тим, що знаходиться в соціальних мережах за допомогою інструментів профілювання СТ може окреслити все життя людини. Одна з причин, чому це працює так добре, це те, як більшість людей обирають їх паролі. Багато людей використовують однакові паролі знову і знову і багато людей вибирають паролі, які легко вгадати. Наприклад, може бути використане таке ПЗ, як Common User Password Profiler (CUPP), CeWL та інші. І*нструменти для збіру інформації* є ключовою складовою соціальної інжинерії та успішної атаки СТ. Не приділяючи достатньої уваги збору інформації, СТ має високий шанс провалити атаку. В даний час багато інструментів є доступними, які можуть допомогти у зборі, консолідації та використанні зібраних даних. Ці інструменти можуть буквально змінити те, як соціальний інженер використовує дані та доступні в Інтернеті, наприклад, Maltego, SET: Social Engineer Toolkit, Whois, Search Engines.

Якщо атаки пов'язані з реалізацією різних типів віддалених методів, то результуючим буде комбінований метод на основі вище згаданих, наприклад, Т-РП-віддаленого типу при здійсненні атаки за допомогою телефонних дзвінків та реєструючих інструментів.

Якщо атаки пов'язані з реалізацією різних типів дистанційних методів (локальних і віддалених), то результуючим буде комбінований метод, наприклад, КТ-локально-МТ-віддаленого типу при здійсненні атаки із контрольованої території без доступу в приміщення та з використанням мережевих технологій.

За ініціалізацією [1]:

Умовні засновуються на виникненні певної події (механізм логічної бомби) і в свою чергу можуть поділятись на умовно-активні та умовно-пасивні. Умовно-активні МСІ здійснюють моніторинг стану окремих ресурсів і при його деякому зміненні формується сигнал початку атаки. Прикладом може бути переривання сесії з'єднання з сервером деякого користувача тощо. Прикладом умовно-пасивного методу може бути передача від потенційної цілі запиту деякого типу, який і буде умовою початку атаки.

Безумовні не супроводжуються певним зміненням стану ресурсу та визначається джерелом атаки (СТ).

За інструментарієм [1]:

Програмні засновуються виключно або частково за допомогою програмного забезпечення, технологій шпигування, кодів атак, фішингу тощо.

Апаратні засновані на різноманітних механічних, електричний, електромеханічних, електронних, електронно-механічних та інших пристроях, які використовуються автономно або сумісно з іншою апаратурою або засобами для виконання відповідних функцій.

Нетипові виконуються на основні таких засобів, які не входять до програмних та апаратних, наприклад, вибухівка, радіоактивні матеріали, кислоти, гризуни тощо.

Якщо атаки реалізуються за допомогою різних типів, то результуючим буде комбінований метод на основі вище згаданих, наприклад, програмно-нетипового типу при використанні програмних та нетипових інструментаріїв.

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 [10] 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 СТ 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, СТ 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 СТ 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 СТ 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, СТ 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, СТ 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, СТ 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, АВ-ВД-маніпулювання використовує авторитетнісну та відповідальнстну 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 СТ 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 К-Ц-Д-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 СТ (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, СТ 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 **степенем важкості** МСІ бувають прості, складні та системні.

Прості реалізуються невеликою кількістю кроків. Наприклад, при необхідності дізнатись імена службовців потрібного відділу на підприємстві, СТ 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 (розгалуженого, зі зворотними 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** [11] 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, ЕК-КН-джерельна пов'язана з експертом та контактером.

За **типом доступу** до інформації МСІ поділяються на ВК-, ВВ-, КН- та СК-доступу [1].

ВК-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.

ВВ-доступу пов'язані з доступом до інформації, яка відображена у відкритих джерелах, проте потребує захисту та обмеження доступу і є відносно відкритою. До такої слід відносити інформацію, важливу для особи, суспільства і держави (відповідно до Концепції технічного захисту інформації в Україні), важливі для організації відомості, порушення цілісності або доступності яких може призвести до моральних чи матеріальних збитків [12].

КН-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.

СК-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-КН-доступу орієнтований на відкриту та конфіденційну інформацію.

За **типом звернення** 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 ввічливості) 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 СТ 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 (СТ) 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), СТ 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.

Якщо атаки пов'язані з реалізацією різних типів звернень, то результуючим буде комбінований метод на основі вище згаданих, наприклад, аверсно-реверсного типу при використанні прямого та зворотнього зв’язку.

За **типом СТ** поділяються на [8]:

ХК-виконавчі здійснюються надзвичайно кваліфікованими ІТ-фахівцями (хакерами), які розуміють глибини роботи комп'ютерних систем. Постачальники програмного забезпечення (ПЗ) стають все більш кваліфікованими у створенні ПЗ, яке дедалі краще захищене від атак та зломів хакерів. Такі фахівці часто використовують як апаратні\програмні засоби, так і навички соціального інжинірингу для підвищення успішної атаки.

ПС-виконавчі методи реалізуються пенетрейшн-тестерами, що вчаться і використовують навички, які зловмисники використовують по-справжньому, з метою забезпечення безпеки клієнта. Дана категорія ніколи не використовує інформацію в особистих цілях або щоб завдати шкоди і у більшості випадків є внутрішніми тестами або зовнішніми консультантами.

ШГ-виконавчі використовують соціальну інженерію як науку життя, часто використовуючи кожен аспект соціальної інженерії і є експертами в цій науці. Шпигуни з усього світ вчать різні методи обману атакованих видаючи себе тими, ким вони не є. На додаток до вивчення мистецтва соціальної інженерії, шпигуни також спиратися на довіру жертви, знаючи дещо або навіть значно інформації про бізнес або уряд, який вони намагаються атакувати.

ЗІ-виконавчі найчастіше реалізуються так званими злодіями ідентичності, які займаються крадіжками даних та використанням інформації, такої як ім'я людини, номери банківських рахунків, адресів, дат народження або номер соціального страхування без відома власника. Цей злочин може варіюватися від одягнення уніформи з метою видати себе за когось іншого до набагато складнішого шахрайства. Злодії ідентичності використовують багато аспектів соціальної інженерії і з плином часу вони здаються більш сміливі та байдужі до переживань та проблем, які вони викликають своїми діями.

НС-виконавчі здійснюються незадоволеними співробітниками після розчарування або образи, коли вони часто змінюють (на ворожі) свої відносини з роботодавцем. Це часто може бути односторонньою ситуацією, тому що працівник зазвичай намагається приховати свій рівень незадоволення з метою зберегти робоче місце. Проте, чим більш незадоволені вони стають, тим легше вони наважуються на акти крадіжок, вандалізму або інших злочинів.

ШХ-виконавчі методи реалізуються шахраями, що звертаються до жадібності або інших принципів, які змінюють переконання людей бажаючи заробити чи отримати будь-які інші блага. Шахраї навчились читати людей і обирати маленькі прийоми, які здаються людині гарним "знаком". Вони також майстерно створюють ситуації, які представляють як неперевершені можливості для вигоди.

ВР-виконавчі здійснюються найчастіше виконавчими рекрутерами, які також повинні освоїти багато аспектів соціальної інженерії. Маючи навики майстерного виявлення та знання психологічних принципи соціальної інженерії, вони отримують великий досвід не тільки у розумінні людей, а й розуміння того, що мотивує людей.

ПР-виконавчі МСІ найчастіше здійснюються продавцями, які повинні опанувати багато вмінь працювати з людьми. Багато гуру продажів говорять, що хороший продавець заробляє не на маніпулюванні людьми, але використовує свої навички, щоб з'ясувати потреби, а потім оцінює, чи може ці потреби задовольнити. Мистецтво продажів потребує багато навичок, таких як збір інформації, виявлення, вплив, психологічні принципи та багато інших.

АВ-виконавчі є окремою категорією методів, яка потрібна для виявлення певних параметрів атак. Це можуть бути виконавчі частини коду або програми, використовуючи які СТ досягає успішної СА запускаючи їх через сервери, віддалено по інтернет тощо.

Можуть бути введені і інші групи СТ-методів залежно від специфіки діяльності. Наприклад на урядовців, лікарів, психологів, юристів, тоді вони будуть відповідно **УР-виконавчі** (методи засновані на діях урядовців та не часто розглядаються в якості соціальних інженерів. Урядовці використовують соціальну інженерію, щоб контролювати повідомлення які вони анонсують та людей, якими вони управляють. Цей тип соціальної інженерії не завжди негативний, тому що деякі повідомлення від уряду розраховані на благо народу і використання деяких елементів соціальної інженерії може зробити повідомлення більш привабливим і більш широко визнаним), **ЛР-виконавчі** (базуються на діях

лікарів), **ПС-виконавчі** (базуються на діях психологів)**, ЮР-виконавчі** методи (базуються на діях юристів) тощо: Хоча дані професії на перших погляд може не підпадає в дану класифікацію, ця група використовує ті ж самі методи, які використовуються СТ. Вони повинні використовувати навики соціальної інженерії щоб маніпулювати клієнтами з метою направити їх в потрібному напрямку.

Відповідно до узагальненого алгоритму [7] наведемо приклад здійснення СА з розширеною класифікацією. Метою атаки є отримання номеру кредитної картки та мобільного телефону начальника проекту нової продукції фірми А для конкурентної фірми В. Фактично дії можна розбити на три кроки.

Першим кроком є отримання інформації про підприємство С, де жертва є постійним клієнтом. Дану інформацію СТ дізнається на сторінці профілю однієї із соціальних мереж базуючись на вподобаннях та відкритій інформації. На сайті компанії С міститься телефон служби підтримки (довідкової служби). Цей етап заснований на такому класі MCI: Т-МТ-віддаленому, безумовному, апаратному, К-дієвому, ВВ-доступу, аверсному.

Наступним кроком, залетефонувавши у службу підтримки фірми С, СТ представляється клієнтом та дізнається номер телефону та імя потрібного службовця відділу клієнтів. Щоб запросити потрібну інформацію у відділі клієнтів, 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. На цьому етапі реалізовані наступні класи MCI: деполітизаційному, Т-віддаленому, безумовному, апаратному, АВ-маніпульованому, К-дієвому, складному, ЕК-джерельному, ВВ-доступу, аверсному, ШХ-виконавчому.

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 задовольнити запит серйозного клієнта. Після чого просить надати йому потрібну інформацію, даючи лише ім'я клієнта [7]. На цьому етапі реалізовані наступні класи MCI: деполітизаційному, Т-віддаленому, безумовному, апаратному, ВМ-маніпульованому, К-дієвому, ЕК-джерельному, КН-доступу, ШХ-виконавчому.

Відповідно до наведеного прикладу реалізація СА була заснована на такому класі MCI: деполітизаційному, Т-МТ-віддаленому, безумовному, апаратному, АВ-ВМ-маніпульованому, К-дієвому, монополічному, складному, ЕК-джерельному, ВК-ВВ-КН-доступу, аверсному, ШХ-виконавчому.

Запропонована в роботі ознакова класифікація MCI 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 соціотехнічним атакам.

Література

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

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

[3] Чириль Дж. Защита от хакеров. -СПб.: Питер, 2002. – 480 с.

[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. – 656 с.

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

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

[7] Класифікація методів соціального інжинірингу / О.Г. Корченко, Є.В. Паціра, Д.А. Горніцька // Захист інформації. – 2007. – №4 (36). – С.37-45.

[8] Cristoper Hadnagy. Social Engineering. The art of Human Hacking. Wiley Publishing, Inc.,2011 – 477 p.

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

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

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

[12] НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

УДК 004.056.5 (045)

Корченко А.Г., Горницкая Д.А., Гололобов А.Ю. Расширенная классификация методов социального инжиниринга

Аннотация. *В связи с интенсивным развитием современных информационных технологий социотехнические атаки получили широкое распространение и совершенствование. Для разработки и внедрения эффективных средств противодействия социотехнических атак (например, таких как система управления информационной безопасностью) необходимо сформировать наиболее полное множество их характерных признаков и составляющих. Известная классификация требует дополнений и расширения для возможности построения более эффективных средств противодействия. На основании анализа и обобщения известных публикаций соответствующей предметной области была расширена известная классификация методов социального инжиниринга за счет введения новых признаков и их составляющих. В общем виде классификация содержит 12 базовых признаков, в сумме интегрирует более 50 соответствующих характеристик. Результаты работы могут быть использованы, например, для построения систем оценки рисков, уровня подготовленности персонала по противодействию социотехнических атак и т.д.*

Ключевые слова: *социотехнические атаки, методы социального инжиниринга, классификация социотехнических атак, классификация методов социального инжиниринга по признакам.*

Korchenko O., Gornitska D., Gololobov A. Extended classification of methods of social engineering

Abstract. *Due to the rapid development of modern information technologies of social engineering attacks are widespread and improvement. To develop and implement effective means of combating social engineering attacks (eg, such as information security management system) is necessary to have the most complete set of characteristics and components. Known classification requires additions and extensions to make possible a more effective means of resistance. Based on the analysis and synthesis of well-known publications on the subject field has been expanded known classification techniques of social engineering by introducing new characters and their components. In general classification includes 12 basic characteristics, integrates more than 50 characteristics. The results can be used, for example, for the construction of a risk assessment, the level of preparedness of personnel to combat social engineering attacks, etc.*

Key words: *social engineering attacks, social engineering methods, the classification of social engineering attacks, attribute classification methods of social engineering.*

Отримано *11 червня 2014 року*, затверджено редколегією *02 липня 2014 року*