

ВПЛИВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ОРГАНІЗАЦІЙ

М. О. Шатковський^{1, а}

¹Національний технічний університет України «Київський політехнічний інститут»

Анотація

В даній роботі розглянуто питання людського чинника і соціальної інженерії в галузі інформаційної безпеки. Проаналізовано модель соціального інженера як порушника інформаційної безпеки. Розроблено та проаналізовано модель розрахунку суб'єктивної ймовірності ризику атаки методами соціальної інженерії.

Ключові слова: соціальна інженерія, людський чинник, соціальний інженер, атака, інформація з обмеженим доступом, суб'єктивна ймовірність

Вступ

На даному етапі розвитку суспільство не можливо відокремлювати від інформаційних систем, які наявні практично у всіх сферах життя людини. Вони надають величезні можливості для роботи, навчання та дозвілля. Водночас інформаційні системи працюють з інформацією, яка в тому числі є і конфіденційною. Отже, одна із серйозних вимог до інформаційної системи – забезпечення інформаційної безпеки. Інформаційні технології мають можливість впливати на людську свідомість, а також надають великі можливості тим, хто вміє їх використовувати. Тому така ситуація призводить до зростання ролі людського чинника у питаннях інформаційного захисту.

Як зазначають у своїй книзі Вільям Л. Саймон та Кевін Митник [1], людина є найменш надійною ланкою в системі захисту інформації. З усіх відомих вдалих спроб злочинів у сфері комп'ютерної інформації переважна більшість була скоєна за допомогою співників в установі, яка піддавалася атаці, або через малокваліфікованих в галузі інформаційної безпеки працівників, які не змогли розпізнати загрозу і зловмисника. Наслідками таких злочинів зазвичай є порушення конфіденційності корпоративної інформації фірм, підприємств, установ і закладів.

Найчастіше соціальну інженерію надзвичайно недооцінюють в процесі створення організаційних заходів та комплексних систем захисту інформації, а також і у процесі діяльності організації. На людський чинник через стрімкий прогрес ІТ звертають дедалі менше уваги. При розробці систем захисту акцентують саме захист від неавторизованого вторгнення в систему зловмисника власноруч. Не всі усвідомлюють, що зловмиснику не обов'язково потрібно знешкоджувати систему захисту, якщо можливий інший шлях – використання працівника персоналу через його людські якості, як позитивні, так і негативні.

В Україні на даний час не існує нормативного документу, який би регулював норми політик ін-

формаційної безпеки проти впливу на інформаційну систему зловмисника, який володіє навичками соціальної інженерії.

Метою даної роботи є дослідження людського чинника в інформаційній безпеці, визначення методології діяльності соціального інженера та областей його впливу на корпоративну безпеку, а також визначення та розробка способів удосконалення політик інформаційної безпеки на основі моделі розрахунку ймовірності ризиків атак соціальної інженерії з метою протидії діям зловмисника.

1. Методика досліджень

Соціальна інженерія у галузі інформаційної безпеки – це метод несанкціонованого доступу до захищених інформаційних ресурсів, який базується на способах впливу на людську психологію. Даний метод поєднує в собі як глибокі знання у сфері інформаційних технологій, так і неабиякі навички та знання з соціології та психології [2].

Людський чинник – термін, який описує можливість прийняття людиною помилкових і алогічних рішень в конкретних ситуаціях. Людський чинник базується на психологічних та психофізіологічних характеристиках людини, які не завжди є достатніми для вирішення проблем і задач певного рівня складності [3].

Соціальний інженер – фахівець широкого профілю, який зазвичай володіє нестандартним способом мислення, гнучким розумом, використовує обман, психологічний вплив, переконання, хороші манери в спілкуванні, позитивні та негативні якості людини для того, щоб змусити людину робити справи, які вони не робили б зазвичай для незнайомої людини [1].

Соціальний інженер в поняттях інформаційної безпеки [1] – це:

- порушник інформаційної безпеки;
- володіє навичками соціальної інженерії, обману та шахрайства;

^аm.shatkovskyi@gmail.com

- вміє психологічно впливати на людину, цим самим маніпулювати нею та спонукати її до певних дій;
- навчений збирати необхідну інформацію будь-якими способами;
- найбільш корисно використовувати всю інформацію, якою володіє;
- має глибокі знання з інформаційної безпеки, в області інформаційних технологій, комп'ютерних систем та мереж.

Визначимо більш конкретно інші пов'язані з соціальним інженером поняття. Область дії соціального інженера – організації різного типу, які володіють будь-якою ІЗОД.

Об'єкт впливу соціального інженера – ІЗОД, яка зберігається та оброблюється організацією.

Мета соціального інженера – викрадення, модифікація або знищення ІЗОД, іншими словами порушення конфіденційності, цілісності або доступності ІЗОД.

Суб'єкти впливу соціального інженера – особи, які є працівниками організації, або якимось чином з нею пов'язані, які володіють ІЗОД або будь-якою іншою інформацією, яка необхідна для атаки, мають доступ до певних ресурсів або мають права на виконання певних дій. Дані особи є основними знаряддями атак соціального інженера. Соціальний інженер проводить атаки руками даних осіб, маніпулюючи ними на основі прийомів психології, інформації, якою володіє, та людських якостей.

Загрози соціальної інженерії:

- витік конфіденційної інформації;
- обхід засобів захисту від витоку конфіденційної інформації;
- порушення авторських прав на інформацію;
- шахрайство з інформаційними активами;
- фінансове шахрайство;
- нецільове використання інформаційних ресурсів організації;
- пошкодження ІТ-інфраструктури організації;
- модифікація або знищення конфіденційної інформації.

Засоби і методи соціального інженера спрямовані на такі якості людської природи:

- відчуття авторитетності;
- відчуття спорідненості;
- взаємодопомога;
- відчуття відповідальності;
- соціальна приналежність до групи;
- відчуття терміновості.

Соціальний інженер зазвичай чітко розуміє, як можна скористатись людською природою. Вище зазначені 6 основних прийомів, які є водночас шістьма рисами людської натури, які найбільш часто і успішно застосовуються соціальними інженерами в спробах ким-небудь маніпулювати. Далі пояснимо їх більш детально.

Авторитетність. Людям властиве бажання прислухатись людині з більшим авторитетом. Спосіб полягає у запевненні людини в тому, що той, хто запитує,

– має владу або право задавати дане питання чи щось просити.

Відчуття спорідненості. Люди мають звичку довіряти людині, яка має схожі інтереси, погляди, думки, або біди та проблеми. Спосіб має на меті переконати людину в тому, що той, хто звертається, має схожість з нею в чому-небудь, щоб викликати до себе ще більшу довіру.

Взаємодопомога. Людина може машинально відповісти на питання, коли отримує щось натомість. Подарунком може бути і матеріальна річ, і порада, і допомога. Коли хтось робить щось для нас, ми відчуваємо бажання віддячити. Це дуже потужна риса людської натури і проявляється вона тоді, коли той, хто отримав подарунок, не очікував або не просив цього. Спосіб полягає у запевненні людини, що їй намагаються допомогти або зробити послугу.

Відповідальність. Люди мають звичку виконувати обіцянки і обов'язки. Пообіцявши, ми зробимо все, тому що не хочемо здаватися такими, що не заслуговують довіри. Людина буде намагатись подолати будь-які перепони для того, щоб здержати слово або втілити обов'язок. Соціальний інженер намагається запевнити жертву, що певне прохання є професійним обов'язком жертви.

Соціальна приналежність до групи. Людям властиво не виділятися в своїй соціальній групі. Дії інших являються гарантом істинності в питанні поведінки. Інакше кажучи, якщо так роблять інші, то людина вважає, що і їй потрібно так робити. Спосіб полягає в тому, що людину можна запевнити в приналежності до команди і викликати в неї відчуття «гри в команді».

Відчуття терміновості. Люди дуже часто губляться і стають неуважні, коли існує відчуття поспіху, коли часу на щось залишається дуже мало, і це вибиває людину з її звичної зони комфорту. Спосіб має на меті ввести людину в такий стан.

Найпоширеніші дії соціального інженера – це запити надання певної інформації:

- будь-які паролі, авторизаційні ключі, кодові слова, пін-коди, секретні відповіді тощо;
- дані про структуру організації, наявність та назви відділів і підрозділів, їх внутрішню організацію, склад персоналу інформацію про співробітників: посади, імена, обов'язки тощо;
- внутрішні телефонні номери співробітників, факси, номери керівників, номери внутрішніх офісів, відділів, службові та технічні номери тощо;
- інформацію про комп'ютерні системи, мережі, алгоритми обробки та передачі інформації, назви, версії, модифікації операційних систем, СУБД, ПЗ, назви служб, мережеві імена серверів та комп'ютерів, IP-адреси, способи і реквізити віддаленого доступу тощо;
- особисту інформацію: особисті телефонні номери (домашні або мобільні), номери соціального страхування, паспортні дані, адреси, минулі місця роботи, розмір заробітної плати тощо;
- конфіденційну або секретну інформацію про продукти компанії, стратегічні плани, вихідні коди

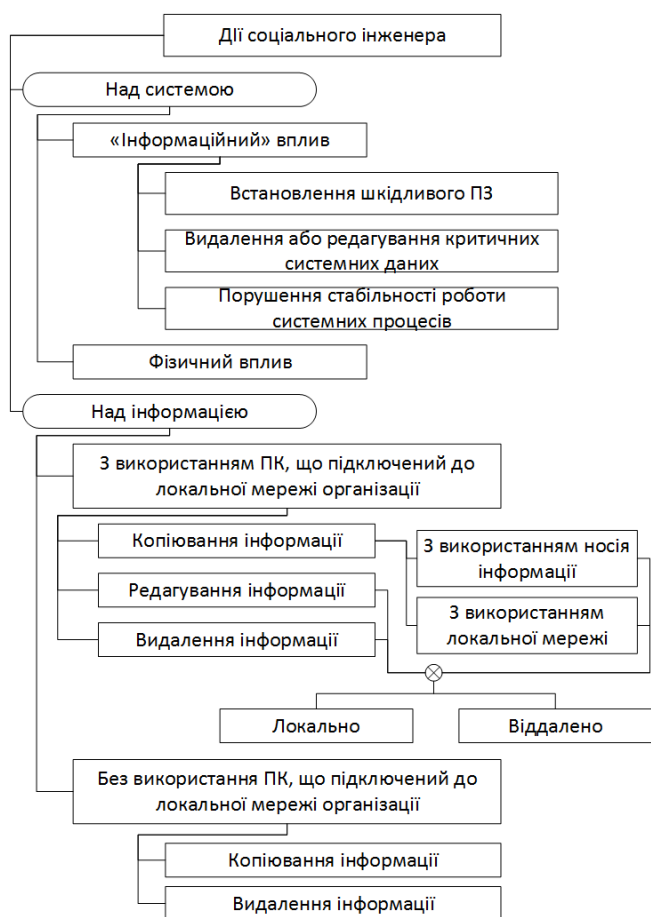


Рис. 1. Модель дій соціального інженера

програм, списки клієнтів, співробітників, партнерів, секрети бізнесу та торгівлі, інтелектуальну власність тощо,

Запити на виконання певних дій:

- відкрити додаток до листа;
- змінити пароль;
- передати інформацію будь-яким способом;
- ввести будь-які команди до діалогового вікна ОС;
- завантажити, встановити, видалити або відключити будь-яке ПЗ;
- змінити налаштування комп'ютера або мережі.

Варто відмітити, що за даною моделлю (рис. 1) описані дії можуть проводитись як соціальним інженером власноручно, так і особою, яка знаходиться під впливом соціального інженера.

Корпоративна інформація – це внутрішня інформація будь-якої компанії, фірми або підприємства, яка являє собою всю інформацію про організацію та її діяльність і не призначена для публічного користування, а також частково являється конфіденційною [5].

Корпоративну інформацію можна чітко поділити на захищену і мало захищену (Рис. 2).

Захищеною інформацією є конфіденційна, службова та таємна інформація, доступ до якої обмежений юридично положеннями про політику захисту внутрішньої інформації організації, грифами секретності та законодавством держави. До захищеної інформації відноситься інформація про економічну діяльність



Рис. 2. Корпоративна інформація

підприємства, комерційна таємниця, нематеріальні активи, договори, документи тощо.

Мало захищеною є інформація організації, яка може не бути визначена як інформація з обмеженим доступом, або навіть може не класифікуватись в інформаційній політиці організації взагалі. Це інформація про внутрішню структуру організації, назви її відділів, імена їх працівників і керівників, їх обов'язки, особисті контактні дані, інформація про обладнання, яке використовує організація, внутрішня термінологія організації, внутрішні номери телефонів і факсів. Дана інформація зазвичай визнається не зовсім важливою так як вважається такою, що не може нанести організації якоїсь шкоди або збитку.

Методологія атак соціального інженера. Соціальний інженер для своїх атак зазвичай використовує знання про організацію, які основані саме на мало захищеній інформації про неї.

За допомогою цих знань досить легко можна видати себе, наприклад, за працівника підприємства, для чого може бути достатньо знати його ім'я, номер телефону, відділ, в якому він працює, які обов'язки виконує, до чого має доступ, хто його керівник та достатню для атаки кількість внутрішньої термінології організації. За допомогою цієї інформації можна запевнити обрану жертву в особі іншого працівника організації, що атакуючий є тим, ким намагається себе видати.

2. Результати досліджень

В результаті роботи було розроблено практичну модель механізму оцінки суб'єктивної ймовірності ризику атак порушника[4], що володіє навичками соціальної інженерії Основним завданнями було визначення величин, від яких напряму залежить суб'єктивна ймовірність ризику атаки методами соціальної інженерії, визначення шкал розрахунку значень даних величин, а також розробка способу обрахун-

ку суб'єктивної ймовірності на основі визначених величин. Отож, було визначено три величини:

- 1) **CPIP** - **Condition of Protected Information Property** – Стан інформаційних ресурсів в організації, який показує, що інформаційний ресурс зберігається, обробляється або передається за межі контрольованої зони організації.
- 2) **PSA** - **Part of Staff with Access** – Відношення кількості осіб, що мають доступ до інформаційного ресурсу, до загальної кількості персоналу.
- 3) **IEP** - **Indicator of Education of Personnel** – Рівень знань персоналу в галузі інформаційної безпеки та навичок протидії атакам соціального інженера.

В ході дослідження були також розроблені способи розрахунку значень даних величин та розрахунку значення суб'єктивної ймовірності (далі **SP** – subjective probability) на їх основі. Інтервали на яких визначені ці величини:

$$CPIP \in [0, 3]$$

$$PSA \in [0, 1]$$

$$IEP \in [0, 1]$$

Тоді **SP** можемо розрахувати за формулою:

$$SP = \frac{CPIP + PSA + IEP}{\max(CPIP) + \max(PSA) + \max(IEP)}$$

Легко визначити, що

$$SP \in [0, 1],$$

тому величину **SP** дійсно можемо вважати ймовірністю.

Висновки

Запропоновано підхід до розрахунку суб'єктивної ймовірності ризиків атак соціального інженера, який відрізняється від існуючих методів тим, що дозволяє експерту отримати більш точні результати експертної оцінки систем захисту і визначити необхідність додаткових організаційних заходів, направлених на мінімізацію людського чинника і захист від соціальної інженерії.

Перелік використаних джерел

1. Кевін Д. Мітнік, Вільям Л. Саймон, Мистецтво обману. – М.: Компанія АйТі, 2004. – 360 с.
2. Social Engineering Fundamentals [Електронний ресурс] // scribd.com. – 2009. – Режим доступу до ресурсу: <http://ru.scribd.com/doc/19676093/Social-Engineering-Fundamentals>.
3. Человеческий фактор [Електронний ресурс] // Вікіпедія. – 2015. – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Человеческий_фактор.
4. Петренко С.А., Симонов С.В. Управління інформаційними ризиками. Економічно оправдана безпека. – М.: Компанія АйТі; ДМК Пресс, 2004. – ст. 76–77.
5. Еремичев И. А. Корпоративное Право / 3-е изд., перераб. и доп. / И. А. Еремичев, Е. А. Павлов. – Москва, 2010. – 438 с.