МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

УДК 316.776:004.58
DOI: https://doi.org/10.37320/2415-3583/10.28

Половенко Л.П.
кандидат педагогічних наук, доцент,
Вінницький торговельно-економічний інститут
Київського національного торговельно-економічного університету
ORCID: https://orcid.org/0000-0002-9909-825X

Мерінова С.В.
кандидат економічних наук, доцент,
Вінницький торговельно-економічний інститут
Київського національного торговельно-економічного університету
ORCID: https://orcid.org/0000-0001-6563-5320

ВИЯВЛЕННЯ ОЗНАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ТА ТЕХНОЛОГІЯ ПРОТИДІЇ СОЦІАЛЬНИМ ХАКЕРАМ НА ПІДПРИЄМСТВІ

У статті висвітлено основні методи та техніки соціальної інженерії на підприємстві. Явище маніпулятивного впливу досліджено в розрізі економічної безпеки підприємства. Серед найбільш поширених методів соціальної інженерії виокремлено методи, побудовані на людських слабкостях, зокрема на використанні інстинктів «цікавості» та «довіри». Вивчено основні шляхи та форми нападу. Проаналізовано інструментарій соціального хакера, який він застосовує для досягнення конкурентних переваг. Обґрунтовано ефективність використання інструментарію економіко-математичного моделювання та інтелектуального аналізу для побудови системи захисту. Запропоновано дієві механізми, що дають змогу оперативно відслідковувати та виявляти ознаки соціальної інженерії на ранніх стадіях, попереджати кіберзагрози на підприємстві та протидіяти соціальному хакерству.

Ключові слова: *соціальна інженерія, кіберзагроза, несанкціонований доступ, когнітивні упередження, методи впливу, соціальний хакер.*

Постановка проблеми. Новітні технології та інновації глибоко змінюють процес організації виробництва, створюють підґрунтя для стійкого зростання бізнес-можливостей. Водночас сучасні смарт-технології, Інтернет речей, інтелектуальний аналіз, хмарні технології обробки та зберігання великих даних породжують нові загрози. Захист інформації набуває критичної важливості. Витонченість і складність атак у кіберпросторі постійно вдосконалюються.

Одним із найбільш уразливих моментів у розвитку сучасного бізнесу виступає соціальна інженерія. Методи отримання конкурентних переваг базуються на експлуатації людського фактору шляхом використання елементів психологічної маніпуляції. ІТ-службам підприємств складно протистояти хакерам соціальної інженерії, адже пастки для бізнесу будуються на основі інстинктів цікавості та довіри, а не на вразливості цифрових систем.

Соціальний інжиніринг займає одне з перших місць за кількістю атак та зламів інформаційних систем компаній. Ексклюзивні конкурентні переваги досягаються шляхом здійснення розвідки, виявлення слабких сторін та вразливих ділянок організації, переманювання та підкупу співробітників, дискримінації конкурента, розкрадання інтелектуальної власності, конфіскації банківських рахунків та втрати споживачів унаслідок бізнес-збоїв, розкриття конфіденційної інформації, продажу особистої інформації на чорному ринку, порушення основних даних, викрадання даних клієнтів та їх продажу тощо.

Тому підприємства потребують нових методів боротьби, які б давали змогу оперативно відслідковувати та виявляти ознаки соціальної інженерії, попереджати кіберзагрози та протидіяти соціальному хакерству. Одним з ефективних методів є використання інструментарію економіко-математичного моделювання та інтелектуального аналізу.

Аналіз останніх досліджень і публікацій. Основні принципи, ознаки і методи соціальної інженерії широко висвітлюються науковцями. В.М. Нам'ясенко [3], В.С. Яковенко, Н.К. Казеян [6]. В.Ю. Соколов, Д.М. Курбанмурадов [5] підкреслюють роль антропогенного чинника як реально існуючої вразливості в інформаційній безпеці підприємства. Саме низький рівень

обізнаності персоналу щодо соціотехнічних атак призводить до інцидентів соціального інжинірингу. Технології оцінювання маніпулятивного впливу розкривають С.О. Гнатюк, В.М. Сидоренко, Ю.Я. Поліщук, К.О. Тараненко [1]. Методика виявлення ознак кіберзагроз представлена у працях Г.М. Яровенко, А.І. Сковронської, М.М. Бояджян [7]. І.І. Ніколіна досліджує проблему моделювання життєвого циклу ринкової поведінки підприємства як інструменту наукового передбачення етапів розвитку економіко-виробничої системи [4]. Моделювання комплексного управління інформаційною безпекою розглядають В.А. Лужецький, А.В. Дудатьєв, В.В. Миронюк [2]. Водночас більшість дослідників зазначає, що актуальними залишаються розроблення дієвих методів протидії соціальному хакерству, побудова ефективних бар'єрів та превентивних інструментів захисту.

Мета статті полягає у виявленні ознак соціальної інженерії на ранніх стадіях, розробленні методики оцінювання маніпулятивного впливу на співробітників компанії та запропонуванні дієвих механізмів протидії соціальним хакерам на підприємстві.

Виклад основного матеріалу. Однією з головних загроз економічній безпеці системи є напади з використанням методів соціальної інженерії [3, с. 90]. Соціальний інжиніринг – це сукупність підходів прикладних соціальних наук, які орієнтовані на цілеспрямовану зміну організаційних структур, що визначають людську поведінку і забезпечують контроль над нею, або комплексний підхід до вивчення і зміни соціальної реальності, заснований на використанні інженерного підходу і наукомістких технологій [5]. Психологічною передумовою застосування технологій соціальної інженерії виступають когнітивні упередження – тенденції думати певним чином, шаблонність, стереотипність мислення, що дає змогу навіювати відповідні «стандарти», диктувати відповідний тип поведінки. У сфері інформаційної безпеки термін використовується для опису науки і мистецтва психологічної маніпуляції з метою несанкціонованого доступу до інформаційних ресурсів. Тобто існують приховані методи, які дають змогу «запрограмувати» працівника або групу працівників на виконання певних дій, спрямованих на отримання суттєвої вигоди, причому інструменти соціальної інженерії практично не потребують фінансових затрат. Людський чинник спроможний нівелювати багаторівневі технічні та технологічні фактори.

За статистикою аналітичного центру компанії Infowatch, 55% збитків, пов'язаних із порушеннями інформаційної безпеки, виникають із вини співробітників, що підпали під вплив соціальних інженерів [5, с. 8]. Соціальний інжиніринг здебільшого застосовується з метою отримання прямого доступу до захищених систем для крадіжки інформації, паролів, даних про кредитні картки тощо. Небезпека даного інструменту полягає у тому, що напад може бути або взагалі не виявленим, або ж бути виявленим через тривалий час, що спричиняє більш катастрофічні наслідки, ніж прямий доступ до інформаційної системи чи промислові диверсії.

Щоб завчасно розставити ефективні бар'єри та проводити певні профілактичні дії, важливо дослідити найбільш поширені методи соціальної інженерії на підприємстві, вивчити основні шляхи та форми нападу.

Розглянемо основні техніки соціального інжинірингу в розрізі економічної безпеки підприємства:

1. Фішинг-атаки – це найпопулярніший вид шахрайства у соціальному інжинірингу, який заснований на незаконному отриманні конфіденційних даних користувачів обманним шляхом: використанням фальшивих e-mail та розсилки через соціальні мережі шахрайських повідомлень, різних типів вірусних програм, агресивної реклами. Хакери змушують користувачів передавати паролі, номери соціального страхування, отримують доступ до номерів платіжно-розрахункових карт і PIN-кодів, адресних книг, історій відвідувань і закладок у браузері тощо. За даними Data Insider, близько 91% витоків даних у мережі починається саме з фішингу. Особливо небезпечним є фішинг, адаптований під організацію. Навіть для компаній, де проводиться навчання персоналу, ефективність такого фішингу зазвичай становить 5-7%, що призводить до значних фінансових збитків.

Більш складним видом фішингу є цільовий фішинг, або «таргінг». Об'єктом атаки вибирають цілком конкретну людину, яка за службовими обов'язками, як правило, працює з листами від зовнішніх відправників. Комп'ютери таких людей завжди перебувають у зоні особливого ризику.

2. Бейтинг – застосовують злоякісні троянські програми, які запускаються, коли атакований користувач відповідає на запит зловмисника. Впровадження дає змогу соціальному агенту збирати, видаляти або модифікувати інформацію, порушувати працездатність комп'ютера або використовувати ресурси користувача у своїх цілях. Ця техніка будується на експлуатації емоцій потенційної жертви, наприклад природної цікавості або жадібності (бажання отримати певні вигоди задарма). Зловмисник відправляє так званого «гарячого листа», у вкладенні якого міститься, наприклад, «цікава» пропозиція від банку тощо.

3. Претекстинг – атака, проведена за заздалегідь підготовленим сценарієм, для здійснення якої шахрай видає себе за іншу особу та вивідує у жертви необхідну інформацію. Такі атаки спрямовані на те, щоб викликати почуття довіри до зловмисника,

наприклад згадуючи імена реальних людей або описуючи реальні події, знизити увагу та «приспати» пильність. Головна тактика спланованої схеми обману – «поводитися, немов ти свій», що дає змогу, наприклад шляхом правильно побудованого діалогу, отримати конфіденційну інформацію. У невеликих компаніях хакери діють адресно, використовуючи попередньо зібрану інформацію про особу, наприклад із соціальних мереж. Часто використовується сценарій «Ви отримали подарунок!».

4. Зворотна соціальна інженерія, коли шахрай попередньо знайомий із жертвою та заслуговує на її довіру. У такому разі жертва сама звертається до шахрая (наприклад, системного адміністратора) із проханням допомогти відновити втрачений файл (який заховав сам шахрай). При цьому їй повідомляється, що таку дію можна зробити якнайшвидше, лише зайшовши у її обліковий запис. Таким чином, жертва за власним бажанням повідомляє всю інформацію шахраю. Також під час використання цього виду атаки шахраї можуть пообіцяти жертві вигоду в обмін на факти. Наприклад, зловмисник представляється співробітником технічної підтримки і пропонує встановити «необхідне» програмне забезпечення. Після установки програми порушник отримує доступ до системи.

Одним із різновидів зворотної соціальної інженерії є поклоніння авторитету. Зловмисники можуть «маскуватися» під установи, яким довіряє людина чи компанія у цілому. У рекламі часто використовується поширення ідеї «достовірної інформації», яка нібито опирається на авторитетні видання. Наприклад, покупець, щоб отримати «реальну життєву інформацію» про товар, переглядає відгуки на сайті компанії. Пастка криється у тому, що коментарі може залишати спеціальна група людей, метою якої є розхвалювання/критика конкретного товару.

Принцип обопільності «ти мені – я тобі». Метод сформований на основі специфічності поведінки людини: вона бажає віддячити особі, яка допомогла їй. Наприклад, в офісі «колега»-шахрай попереджає про можливі технічні проблеми та пропонує звертатися за допомогою до нього, якщо виникне така ситуація. Після чого штучно призводить до настання негативних наслідків, далі «усуває» проблему, а в результаті робітник почуває себе боржником і може погодитися виконати зустрічне прохання шахрая, не підозрюючи підступних намірів.

5. «Дорожнє яблуко» – спосіб базується на тому, щоб підкинути фальшивий або заражений фізичний носій інформації. Шахрай спонукає жертву до перегляду на своєму комп'ютері інформації із зараженого флеш-носія, CD-диска тощо. Наприклад, у компаніях, де часто поновлюється штат, висока плинність кадрів, під час проходження співбесіди виявляється, що претендент на вакантну посаду «випадково» забув роздрукувати заздалегідь резюме і пропонує скопіювати його з флешки. Або ж пропонує переглянути додаткову інформацію про себе із власного носія і, таким чином, інфікує комп'ютер.

Разом із тим засоби соціальної інженерії передбачають використання різних вкладок (пристроїв підслуховування, відео- та аудіоспостереження, перехоплення електромагнітних сигналів та запис різнотипних випромінювань тощо), замаскованих під предмети побуту, аксесуари індивідуального користування, іграшки тощо.

6. Сайти-пастки – сайти, головною функцією яких є негласний доступ до особистої інформації їх відвідувачів. Автори таких сайтів-пасток, досліджуючи та вивчаючи когнітивні упередження, спонукають до конкретних дій, зокрема заманюють відвідувачів різноманітними «вигідними» пропозиціями, обіцяють безумовні вигоди за неадекватно низьких затрат. При цьому зловмисник використовує низку різноманітних тактик: видає себе за іншу особу, відвертає увагу, нагнічує психологічну напругу тощо.

Отже, з погляду безпеки підприємства ми будемо розглядати соціальну інженерію як комплекс заходів, спрямованих на отримання зловмисниками несанкціонованого доступу до конфіденційної інформації, провокування внутрішніх інцидентів шляхом маніпулятивного впливу на працівників компанії.

Побудова системи захисту від проявів соціальної інженерії на підприємстві потребує комплексу превентивних заходів: аналізу вразливостей; прогнозування можливих атак, виявлення та розпізнавання ознак соціальної інженерії на ранніх стадіях, оцінювання наслідків маніпулятивного впливу на працівників компанії та розроблення дієвих механізмів протидії соціальним хакерам.

Підприємство ми будемо розглядати як відкриту систему з високим ступенем ентропії, найбільш незахищеним елементом якої виступає людський чинник, який фактично немає визначених параметрів стійкості. Об'єктом ефективної атаки може стати навіть сам керівник, який активно бореться з даним явищем.

Тестування системи на предмет проникнення методами соціальної інженерії ми пропонуємо здійснювати на основі використання інтелектуального аналізу. Даний метод є досить ефективним у галузі виявлення шахрайств та кіберзагроз, знаходженні помилок, виявленні незаконних операцій, маніпуляцій з інформацією [7].

З урахуванням розглянутих технік соціальної інженерії виберемо вхідні та вихідні показники для моделювання. Вхідними даними є такі параметри: визначення цілей соціального хакера, завдань маніпулювання, визначення стратегій маніпулювання, місцеположення фокус-груп; ініційоване місцеположення пристрою, через який

планується здійснення атаки; оцінювання фінансових витрат, що дасть змогу отримати звіт щодо фінансових витрат; визначення критеріїв для оцінювання параметрів; стратегій проведення атак та методів маніпуляції; ранжування загроз за ступенем їх небезпеки. Вихідні параметри: перелік вибраних цілей, критеріїв, завдань, стратегій, методів, технологій соціальної інженерії; виявлення найбільш зручних мішеней впливу та вразливих місць; якою відкритою інформацією про об'єкт може заволодіти; визначення джерел загроз, аналіз інцидентів на підприємстві.

Побудову моделі зручно реалізувати засобами аналітичного пакету SAS Enterprise Miner, що дає змогу обчислювати кількісні параметри, котрі характеризують величину маніпулятивного впливу.

Тест на проникнення методами соціальної інженерії є індикатором на виявлення найбільш сприятливих умов для злочинців; виявлення методів, через які планується спонукання до потрібної дії, обчислення кількісних параметрів, що характеризують величину маніпулятивного впливу соціальних агентів на діяльність підприємства.

Для подолання наслідків когнітивного упередження та розроблення дієвих технологій протидії соціальним хакерам ми пропонуємо такі підходи:

1) диференціація важливої інформації між кількома співробітниками, чіткий розподіл повноважень як у доступі до агрегованої бази даних, так і в розголошенні інформації;

2) обізнаність та навчання персоналу; привертання уваги людей до питань інформаційної безпеки, усвідомлення співробітниками серйозності проблеми, вивчення і використання профілактичних методів і дій для підвищення рівня захисту; саме обізнаність грає провідну роль у компенсації таких боків людської натури, як необережність і безтурботність;

3) побудова системи «раціональної довіри», що передбачає побудову здорової атмосфери на підприємстві (відсутність страху перед керівництвом);

4) максимальна автоматизація важливих процесів; розроблення процедури для перевірки особистості та авторизації осіб, які звертаються за інформацією або вимагають якихось дій від співробітників компанії; здійснення ввічливого відхилення запиту працівниками компанії про надання важливої інформації, поки не буде встановлено особу, яка подавала запит на її право на доступ до цієї інформації;

5) побудова надійної структури метрик для відстеження прогресу та вимірювання впливу засобами аналітичного пакету; щоб по-справжньому мати зрілу модель протидії соціальному хакерству, підприємство повинне не тільки змінювати поведінку та культуру, а й мати структуру метрик для демонстрації цих змін;

6) підтримка пильності персоналу; проведення тренінгів, які формують розвиток критичного мислення, вміння співставляти факти, аналізувати та тверезо оцінювати ситуацію з позиції «здорового глузду»; не піддаватися на паніку чи шантаж, не приймати «на віру», а раціонально оцінювати будь-які штатні, а тим паче нестандартні ситуації, відхилення; перевіряти підозрілу інформацію; впровадження системи розсилки нагадувань.

Висновки. Безпека інформаційної системи підприємства значною мірою залежить від правильного добору кадрів, вивчення працівниками основ соціального інжинірингу та неухильного дотримання вимог політики безпеки, дотримання правил «цифрової гігієни».

Працівник повинен розуміти та оцінювати якість і силу прихованого впливу, розпізнавати методи, якими намагаються маніпулювати ним, та знати, як протидіяти цим впливам. Головний захист від соціальної інженерії – це знання і постійне їх оновлення, що може значно зменшити ризики. Причому йдеться про всі рівні ієрархії – від глав компаній до рядових співробітників. ІТ-відділи також повинні регулярно використовувати різноманітні методи розсилки нагадувань, освіжати знання колег про нинішні ризики і методи захисту.

Список використаних джерел:

1. Оцінювання маніпулятивного впливу масмедіа на суспільну думку / С.О. Гнатюк та ін. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук. доп. наук.-практ. конф., м. Київ, 4 квітня 2019 р. Київ : Нац. акад. СБУ, 2019. С. 21–23.

2. Лужецький В.А., Дудатьєв А.В., Миронюк В.В. Багаторівнева модель управління комплексною інформаційною безпекою держави. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук. доп. наук.-практ. конф., м. Київ, 4 квітня 2019 р. Київ : Нац. акад. СБУ, 2019. С. 86–88.

3. Нам'ясенко В.М. Соціальна інженерія як одна із загроз економічній безпеці, що спричиняє негативний вплив на ефективність діяльності підприємства. *Економіка та держава*. 2016. № 3. С. 90–92.

4. Ніколіна І.І. Моделювання життєвого циклу ринкової поведінки підприємства задля забезпечення сталого розвитку. *Вісник Хмельницького національного університету.* 2017. № 5. С. 41–46.

5. Соколов В.Ю., Курбанмурадов Д.М. Методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності. *Кібербезпека: освіта, наука, техніка.* 2018. № 1(1). С. 6–16.

6. Яковенко В.С., Казеян Н.К. Соціальна інженерія в Інтернет-просторі. *Інформаційні технології та моделювання економічних процесів*. 2016. Вип. III–IV(63–64). С. 119–126.

7. Яровенко Г.М., Сковронська А.І., Бояджян М.М. Моделювання виявлення ознак кіберзагроз у банках із використанням інтелектуального аналізу. *Ефективна економіка*. 2018. № 7.

References:

1. Hnatiuk S.O., Sydorenko V.M., Polishchuk Yu.Ia., Taranenko K.O. Otsiniuvannia manipuliatyvnoho vplyvu masmedia na suspilnu dumku. [Evaluation of the manipulative influence of mass media on public opinion]. *Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy*: zb. tez nauk. dop. nauk.-prakt. konf. (Kyiv, 4 kvitnia 2019 r.). Kyiv : Nats. akad. SBU, 2019. S. 21–23.
2. Luzhetskyi V.A., Dudatiev A.V., Myroniuk V.V. Bahatorivneva model upravlinnia kompleksnoiu informatsiinoiu bezpekoiu derzhavy. [A multilevel model for managing the state's comprehensive information security.]. *Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy*: zb. tez nauk. dop. nauk.-prakt. konf. (Kyiv, 4 kvitnia 2019 r.). Kyiv : Nats. akad. SBU, 2019. S. 86–88.
3. Namiasenko V.M. Sotsialna inzheneriia yak odna iz zahroz ekonomichnii bezpetsi, shcho sprychyniaie nehatyvnyi vplyv na efektyvnist diialnosti pidpryiemstva. [Social engineering as one of the threats to economic security, which has a negative impact on the efficiency of the enterprise]. *Ekonomika ta derzhava*. 2016. № 3. S. 90–92.
4. Nikolina I.I. Modeliuvannia zhyttievoho tsyklu rynkovoi povedinky pidpryiemstva zadlia zabezpechennia staloho rozvytku. [Modeling the life cycle of an enterprise's market behavior to ensure sustainable development]. *Visnyk Khmelnytskoho natsionalnoho universytetu*. 2017. № 5. S. 41–46.
5. Sokolov V.Iu., Kurbanmuradov D.M. Metodyka protydii sotsialnomu inzhynirynhu na obiektakh informatsiinoi diialnosti. [Methods of counteracting social engineering on objects of information activity]. *Kiberbezpeka: osvita, nauka, tekhnika*. № 1(1), 2018. S. 6–16.
6. Yakovenko V.S., Kazeian N.K. Sotsialna inzheneriia v Internet-prostori. [Social engineering in the Internet space]. *Informatsiini tekhnolohii ta modeliuvannia ekonomichnykh protsesiv*. Vypusk III-IV(63-64), 2016. S. 119–126.
7. Yarovenko H.M., Skovronska A.I., Boiadzhian M.M. Modeliuvannia vyiavlennia oznak kiberzahroz v bankakh iz vykorystanniam intelektualnoho analizu. [Simulation of detection of cyber threats in banks using intellectual analysis]. *Efektyvna ekonomika*. №7, 2018.

Polovenko Liudmyla, Merinova Svitlana
Vinnytsia Trade and Economic Institute
of the Kyiv National University of Trade and Economics

DETECTION OF SOCIAL ENGINEERING SIGNS AND TECHNOLOGY OF COUNTERACTION TO SOCIAL HACKERS AT ENTERPRISE

The article substantiates the need of modern enterprises for effective methods of preventing social hacking. Social engineering is one of the most vulnerable sections in the development of modern business, as the sophistication and complexity of manipulative technologies is constantly improving. The purpose of the study is to identify the signs of social engineering at early stages, to develop a methodology for evaluating the manipulative impact on employees of the company and the formation of effective mechanisms to counteract social hackers in the enterprise. The basic methods and techniques of social engineering, ways of managing society, the phenomenon of manipulative influence on employees are covered from the standpoint of financial and economic security of the enterprise. Among the most common methods of social engineering are methods based on human weaknesses and cognitive biases, in particular, the use of instincts of "curiosity" and "trust", special attention is paid to techniques of reverse social engineering. The basic ways and forms of attack are studied: phishing, beating, pretexting, creation of trap sites. The social hacker toolkit that is used to gain competitive advantage is analyzed. The efficiency of using the tools of economic-mathematical modeling and intellectual analysis for the construction of the defense system is substantiated. Effective mechanisms have been proposed to quickly track and detect the signs of social engineering, to prevent cyber threats at the enterprise and counteract social hacking. Among the primary methods of counteraction are the following: personnel training, adjustment of testing and forecasting features of social engineering at early stages, construction and maintenance of the protection system; supporting staff vigilance, developing critical thinking, developing the ability to recognize attempts at manipulative influence; promoting computer literacy and knowledge of the basic rules of digital hygiene. The security of the enterprise information system depends to a large extent on the correct selection of personnel, the study of the basics of social engineering and strict adherence to the requirements of the security policy.

Key words: *social engineering, cyber threat, unauthorized access, cognitive biases, exposure methods, social hacker.*

JEL classification: C51, D23, D71, Z13.