МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій, обліку та фінансів
Кафедра комп'ютерних технологій
і моделювання систем

Кваліфікаційна робота
на правах рукопису

Коптяєв Максим Павлович
(прізвище, ім'я, по батькові здобувача освіти)

УДК 004.057:004.65

КВАЛІФІКАЦІЙНА РОБОТА

Оцінка методів соціальної інженерії щодо вразливостей інтернет ігор
(тема роботи)

125 «Кібербезпека та захист інформації»
(шифр і назва спеціальності)

Подається на здобуття освітнього ступеня магістр

кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи
Євсеєв Сергій Петрович
(прізвище, ім'я, по батькові)
Зав.кафедрою кібербезпеки д.т.н., професор
(науковий ступінь, вчене звання)

Житомир – 2024

Висновок кафедри _____
за результатами попереднього захисту: _____

Протокол засідання кафедри _____
№ ____ від «_____» _____ 20____ р.

Завідувач кафедри _____

_____ _____ _____
(науковий ступінь, вчене звання) (підпис) (прізвище, ім'я, по батькові)
«_____» _____ 20____ р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти _____ захистив (ла)
(прізвище ,ім'я, по батькові)
кваліфікаційну роботу з оцінкою:

сума балів за 100-бальною шкалою _____
за шкалою ECTS _____
за національною шкалою _____

Секретар ЕК

_____ _____ _____
(науковий ступінь, вчене звання) (підпис) (прізвище, ім'я, по батькові)

АНОТАЦІЯ

Коптяєв М.П. Оцінка методів соціальної інженерії щодо вразливостей інтернет ігор. – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття освітнього ступеня магістр за спеціальністю 125 «Кібербезпека та захист інформації» – Поліський національний університет, Житомир, 2024.

У кваліфікаційній роботі досліджено методи соціальної інженерії та їхню загрозу безпеці інтернет ігор. Метою було вивчення загроз соціальної інженерії та опис можливих методів захисту до, під час та після фішингової атаки, як на розробників так і на звичайних користувачів.

Ключові слова: Соціальна інженерія, Фішинг атака, Методи захисту.

SUMMARY

Koptyaev M.P. Evaluation of social engineering methods for vulnerabilities of Internet games.

Qualification work for the master's degree in specialty 125 “Cybersecurity and Information Protection” - Polissya National University, Zhytomyr, 2024.

The qualification work investigates the methods of social engineering and their threat to the security of online games. The aim was to study the threats of social engineering and describe possible methods of protection before, during and after a phishing attack, both on developers and ordinary users.

Keywords: Social engineering, Phishing attack, Protection methods.

ЗМІСТ

ВСТУП

В умовах стрімкого розвитку інформаційних технологій методи соціальної інженерії все частіше використовуються зловмисниками для збору особистих даних користувачів. Обізнаність населення також зростає, що дозволяє щорічно зменшувати відсоток атак, але загроза все ще доволі висока, бо зростає кількість нових можливостей для зловмисників дістати дані. Фішингові атаки стають більш незвичайними, за рахунок збільшення кількості соціальних мереж, а також місць де користувачі зберігають власні дані, від особистої інформації, до інформації банківських рахунків.

У зв’язку з цим питання захисту акаунтів що пов’язані з онлайн іграми набуває особливої актуальності. Дані користувачі онлайн ігор можуть зберігатися одразу кількома способами, починаючи від серверів розробників, завершуючи акаунтами у сервісах цифрової дистрибуції. У даній роботі основна увага приділена опису різних методів соціальної інженерії та їх практичне використання зловмисниками на прикладах.

Метою роботи є вивчення основних методів соціальної інженерії та їх вплив на дані користувачів онлайн ігор.

Предмет дослідження методи соціальної інженерії що використовуються зловмисниками.

Об'єкт дослідження – процесс оцінки методів соціальної інженерії що використовуються зловмисниками.

Наукова новизна роботи полягає у оцінці методів соціальної інженерії що використовуються зловмисниками та розробці рекомендацій для запобігання кібератакам у сфері соціальної інженерії.

Завдання роботи:

- Проаналізувати та дослідити сутність соціальної інженерії та її роль у кіберзлочинності в контексті інтернет-ігор.
- Дослідити принципи впливу та етичні аспекти соціальної інженерії.
- Охарактеризувати критерії оцінювання методів соціальної інженерії.

- Імплементувати методику оцінки методів соціальної інженерії в безпекові процеси розробки інтернет ігор.
- Розробити рекомендації щодо можливого захисту інтернет ігор.

Отже, зважаючи на актуальність питання безпеки в середовищі, де зловмисники можуть скористатись методами соціальної інженерії на свою користь, дана робота покликана систематизувати існуючі методи та підняти рівень обізнаності розробників та користувачів онлайн ігор. Описані способи протидії допоможуть як гравцям та розробникам, так і звичайним користувачам сучасних технологій вберегти себе від можливої атаки та витоку даних. Більша обізнаність користувачів в віртуозності використання зловмисниками методів соціальної інженерії, дозволить підвищити загальний рівень безпеки інформаційних систем, забезпечуючи ефективний захист даних від несанкціонованого доступу та атак зловмисників.

За результатами дослідження було прийнято участь у трьох наукових конференціях:

- Науковий простір : актуальні питання, досягнення та інновації (29 листопада 2024) – “ Аналіз сутності соціальної інженерії” [1]
- Інноваційна наука : пошук відповідей на виклики сучасності (6 грудня 2025) – “ Основні поняття в соціальній інженерії” [2]
- Період трансформаційних процесів в світовій науці: задачі та виклики (13 грудня 2024) - “ Загрози безпеці в сфері інтернет ігор” [3]

РОЗДІЛ 1. АНАЛІЗ ВРАЗЛИВОСТЕЙ ІНТЕРНЕТ ІГОР З ТОЧКИ ЗОРУ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

1.1 Визначення соціальної інженерії та її роль у кіберзлочинності

Соціальна інженерія описує ряд низько технологічних підходів, розроблених шахраями, щоб змусити вас розголошувати цінну приватну інформацію або займатися діяльністю, яка залишає комп'ютер вразливим до атак. Це може статися через Інтернет або особисто [4].

Соціальна інженерія полягає у використанні людської природи та вразливостей, щоб заманити людей у пастку та змусити їх виконувати небезпечні дії. Це досягається через маніпулятивні техніки, що базуються на довірливості, необачності або незнанні людей. Один із найпоширеніших прикладів соціальної інженерії - фішинг-атаки, де зловмисники намагаються отримати конфіденційні дані, такі як паролі або номери кредитних карток, змушуючи жертву натискати на посилання або розкрити інформацію по телефону [5].

Перш за все соціальна інженерія, як вид кіберзлочинності, працює способом людина-людина, тобто навіть якщо під час виманювання інформації, працює бот, цей бот був насамперед навчений людиною, щоб якнайкраще мати вміння маніпуляцій іншими людьми. Не зважаючи на те що соціальна інженерія може використовуватись на благо, в сучасному світі її техніки направлені на збір даних, без наслідків для того хто їх збирав.

Для кращого розуміння сфери використання соціальної інженерії, насамперед варто розглянути її завдання:

1. *Розуміння поведінки людей*: Одним з основних завдань соціальної інженерії є аналіз та розуміння того, як люди думають, відчувають та діють у різних ситуаціях. Це включає в себе вивчення психології, соціології та інших наук про людей.
2. *Розробка стратегій впливу*: Соціальні інженери розробляють стратегії та техніки, які допомагають впливати на людей та досягати певних цілей. Це може включати в себе створення ефективних комунікаційних кампаній, психологічний вплив або розвиток нових продуктів і послуг.

3. *Забезпечення етичності*: Етичні питання в соціальній інженерії дуже важливі. Завданням соціальних інженерів є забезпечення того, щоб їхні методи та техніки були етичними та не завдали шкоди іншим людям чи суспільству в цілому.
4. *Виявлення вразливостей*: Соціальні інженери також аналізують суспільні системи та виявляють їхні вразливості. Це може стосуватися вразливостей в системах кібербезпеки, а також в системах управління та прийняття рішень.
5. *Розвиток заходів безпеки*: У сфері кібербезпеки, соціальна інженерія може використовуватися для розвитку заходів безпеки, які мінімізують ризики впливу соціальних інженерів та забезпечують захист від атак [6].

Соціальна інженерія базується на досить простих психологічних особливостях людини, таки як: принцип зворотності («ти мені – я тобі»), принцип соціальної перевірки (особа оцінює свою поведінку в контексті поведінки більшості), повага до авторитетів (особа буде більше довіряти лікарю та поліцейському, аніж пересічній людині). Всі ці принципи застосовуються і при здійсненні «офлайнового» шахрайства, однак мають свою специфіку під час вчинення у мережі Інтернет [7].

Історія соціальної інженерії свідчить про те, як соціальні та політичні події впливали на її розвиток.

Зокрема, під час Другої світової війни, німецькі нацисти використовували соціальну інженерію для масової маніпуляції національними почуттями та переконаннями населення.

Сталінський режим у СРСР також використовував соціальну інженерію для зміцнення своєї влади та контролю над масами шляхом пропаганди та репресій.

Пізніше, під час холодної війни, соціальна інженерія стала інструментом боротьби між США та Радянським Союзом.

Обидва блоки використовували різноманітні методи впливу на суспільство та ідеологічні маніпуляції для залучення союзників та дезінформації ворогів [8].

У сучасному світі, історичний досвід соціальної інженерії нагадує нам про потенційні загрози та ризики, пов’язані з масовою маніпуляцією через соціальні мережі та засоби масової інформації.

Так вплив інформаційних кампаній з боку іноземних держав на виборчі процеси в різних країнах або використання соціальної інженерії для розпалювання конфліктів та дестабілізації суспільства [9].

Соціальний інженеринг це обширна тема, що містить в собі багато шарів роботи, як над собою та своїми можливостями для маніпуляцій іншими, так і над людьми на яких націлена атака. Для вдалого використання методів соціальної інженерії потрібно знати психологію людини, як виду, та мати достатньо ресурсів для збору інформації та подальшого її використання.

1.2 Важливі поняття соціальної інженерії

Соціальна інженерія – це спектр методів та технік, які використовуються для збору інформації шляхом маніпуляцій людьми. Вона включає кілька основних компонентів, за допомогою яких здійснюються основні види атак:

1. **Привід (pretexting):** Це акт видачі себе за іншу особу з метою взаємодії з жертвою. Наприклад, видаючи себе за працівника газової служби, можна отримати доступ до дому жертви.
2. **Пентестер:** Спеціаліст з інформаційної безпеки, найнятий для перевірки надійності захисту від вторгнень. Пентест (pentest) – скорочення від penetration test, тобто тест на проникнення в закриту область, наприклад, корпоративну мережу.
3. **Розвідка по відкритим джерелам (OSINT):** Збір інформації про ціль із загальнодоступних ресурсів, таких як газети, пошукові системи, документи регулюючих органів, соціальні мережі, реклами та оглядові сайти.
4. **Фішинг:** Найпоширеніша форма соціальної інженерії, яка полягає у розсилці шахрайських електронних листів з метою вплинути на жертву, змусивши її надати інформацію, відкрити файли або перейти за посиланнями.

5. **Приманки:** Об’єкти, що використовуються для примусу жертви виконати певну дію. Це можуть бути USB-накопичувачі або QR-коди, які змушують жертву завантажити шкідливий код.
6. **Сміттєві баки:** Метод фізичного збору даних шляхом копання у вмісті сміттєвих баків або пакетів зі сміттям, зібраних з офісу компанії-жертви для аналізу та збору інформації.
7. **Вплив:** Діяльність людини, яка мотивує інших до певного результату. Вплив може бути як позитивним, так і негативним. Наприклад, лікар може розмовляти з пацієнтом про стан його здоров’я, щоб надихнути на здоровий спосіб життя.

Ці поняття допоможуть відповісти на запитання «Що таке соціальна інженерія?», але більш детально вони будуть розкриті в другому розділі цього дослідження.

1.3 Фішинг та його підвиди

Фішинг – це вид кібератаки, де зловмисники намагаються отримати інформацію, таку як паролі, дані кредитних карток, соціальні номери або інші конфіденційні дані, шляхом обману та маніпуляцій [12]. Типові фішингові електронні листи зазвичай не адресовані конкретним отримувачам. Вони надсилаються на великі списки адрес електронної пошти, які шахраї та злочинці придбали. Це означає, що зловмисник може надіслати електронний лист великій кількості людей, не збираючи про них OSINT. Наприклад, без знання контексту жертви, можна надіслати універсальний електронний лист, що спробує обдурити користувача, змусивши його відвідати шахрайський веб-сайт або завантажити файл. При відкритті файлу на комп'ютері жертви може бути встановлений віддалений доступ до командного рядка або шкідливе програмне забезпечення. Після запуску віддаленої оболонки або встановлення шкідливого ПЗ, зловмисники можуть взаємодіяти з системою і проводити атаки за допомогою експлойтів та ескалації привілеїв, продовжуючи компрометацію системи та мережі.

Іноді комплекти експлойтів (ПЗ, яке використовується для здійснення інших атак і завантаження шкідливого ПЗ) використовують фішинг для поширення шкідливого ПЗ. За звітом Symantec Internet Security Report (ISTR) за 2018 рік, 0,5% всього трафіку URL є фішинговим, а 5,8% – шкідливим.

Існує кілька видів фішингу:

Спис-фішинг: Це тип фішингу, де зловмисник зосереджується на конкретній цілі. Як рибалка використовує спис, а не мережу, так і фахівець із соціальної інженерії збирає, агрегує та використовує OSINT про цільову компанію або особу. Пентестери, які зосереджені на соціальній інженерії, витрачають більшу частину свого часу на розробку фішингових атак. Це найпоширеніші атаки, які вимагають мінімальної прямої взаємодії, роблячи їх більш доступними для клієнтів. Починається все з OSINT-розслідування, наприклад, щодо постачальників послуг, якими користується жертва. Потім створюється фішинговий електронний лист від імені страхової компанії для збору облікових даних або завантаження файлу.

Вейлінг: Це фішинг, спрямований на «велику рибу» – топ-менеджерів компанії. Вони заслуговують більшої довіри і зазвичай мають більше прав доступу. Наприклад, це можуть бути локальні адміністратори в системі компанії. Підходити до атак на таких людей потрібно по-іншому. Наприклад, складання вейлінг листа від імені відділу кадрів з персоналізацією або використання професійного жаргону з OSINT.

Вішинг: Це вид фішингу, де зловмисник дзвонить жертві і спілкується по телефону. Вішинг складніший, оскільки вимагає імпровізації. Перевага в тому, що результати атаки видно відразу. Надсилаючи електронний лист, потрібно чекати на відкриття, але дзвінок дозволяє відразу змусити жертву виконати дію або надати інформацію. Записуйте дзвінки обережно, з мінімальним обсягом службової інформації, щоб не порушувати законодавство про розголошення персональних даних. Перед проведенням таких тестів варто проконсультуватися з юристом [5].

1.4 Розвідка з відкритих джерел

OSINT (розвідка на основі відкритих джерел) є формою процесу збору розвідувальних даних, що включає пошук, відбір, аналіз інформації з публічно доступних джерел та формування розвідувального документу для прийняття відповідних рішень.

OSINT охоплює збір та аналіз офіційних документів, проектів статутів, нових наукових розробок, баз даних, комерційних і державних сайтів, блогів та інших загальнодоступних джерел. Ця розвідувальна дисципліна доповнює наявні методи розвідки і залишається важливою. Використання **OSINT** дозволяє відповісти на безліч питань, які виникають у військово-політичного керівництва, та зосередити зусилля інших розвідувальних органів на складніших і специфічних завданнях, не відволікаючи ресурси на те, що можна отримати з відкритих джерел. Також **OSINT** допомагає заповнити інформаційні прогалини, коли інші види розвідки не можуть виконати поставлені завдання.

Згідно з різними експертними оцінками, американські розвідувальні служби отримують від 35 % до 95 % розвідданих з відкритих джерел, при цьому витрати на OSINT у розвідувальному бюджеті США складають лише 1 %.

У розвідці спецслужб США існують наступні основні методи збору розвідданих, відомі як «розвідувальні дисципліни»:

- Аеророзвідка (IMINT)
- Агентурна розвідка (HUMINT)
- Радіоелектронна розвідка (SIGINT)
- Розвідка на основі фізичних полів (MASINT)
- Геопросторова розвідка (GEOINT)
- Розвідка на основі відкритих джерел (OSINT) [13].

Для збору інформації використовуються такі джерела:

1. **Соціальні мережі**: Профілі користувачів на соціальних мережах, такі як Facebook, Twitter, LinkedIn, Instagram та інші, можуть містити значну

кількість особистої інформації, включаючи фотографії, відомості про сім'ю, інтереси та багато іншого.

2. **Оголошення та форуми:** Публічні форуми, дослідницькі ресурси та відгуки на сайтах можуть містити інформацію про діяльність та думки конкретної людини.
3. **Бізнес-профілі та резюме:** Ви можете шукати в інтернеті бізнес-профілі та резюме, які люди розміщують на робочих веб-сайтах або професійних мережах, як LinkedIn.
4. **Публічні записи та документи:** Публічні записи, такі як нерухомість, земельні права, судові рішення, публічні статті та інші офіційні документи можуть також містити інформацію про людину.
5. **Новинні джерела:** Медіа та новинні веб-сайти можуть містити інформацію про інциденти, події та інші аспекти життя особи.
6. **Бази даних та публічні архіви:** Деякі урядові та недержавні організації надають доступ до публічних баз даних та архівів, де можна знайти різноманітну інформацію, включаючи записи про народження, одруження, смерть і т. д [14].

З часів Другої світової війни і до сьогодні з'явилися різні терміни для характеристики OSINT:

- несекретна інформація (non-secret/unclassified information);
- відкрита інформація (open/overt information);
- відкрита розвідка (overt intelligence);
- загальнодоступна публічна інформація (public information);
- «біла» розвідка (white intelligence).

OSINT може як допомогти, так і нашкодити вашим зусиллям у соціальній інженерії, оскільки для успіху часто потрібні важливі деталі про компанію-жертву та її співробітників. Наприклад, яку віртуальну приватну мережу (VPN) вони використовують? Які технології вони застосовують у своїй роботі? Яке фізичне планування будівлі їхньої організації? Знання цієї інформації може значно

полегшити процес взаємодії. Декілька провідних пентестерів зазначили, що оптимальне співвідношення часу, витраченого на збір даних OSINT, до часу, витраченого на фактичне проникнення, варіюється від 30/70 до 70/30.

Розвиток інформаційних технологій, програмних та апаратних засобів, доступність Інтернету та збільшення потоку відкритої інформації сприяли виведенню розвідки на базі відкритих джерел на новий рівень, роблячи її ще більш актуальною та необхідною.

Висновок до першого розділу

У першому розділі було проведено аналіз соціальної інженерії як виду збору інформації, шляхом маніпуляції, її основні поняття та методи. Також було розглянуто ключові загрози безпеці, з якими стикаються розробники та користувачі інтернет іграми. Проведений аналіз підтвердив важливість проведення комплексної роботи з обізнаності методів соціальної інженерії, як для всіх верств населення, так і для користувачів відеоіграми окремо.

РОЗДІЛ 2. ОЦІНКА МЕТОДИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

2.1 Загрози безпеці в сфері інтернет ігор

В ігровій розробці безпека може бути порушена з декількох каналів: на етапі розробки, де загроза атаки висить над розробниками, а також на етапі експлуатації, де свої дані може втратити вже сам гравець.

З точки зору соціальної інженерії, етап розробки більш вразливий, бо втративши дані щодо розробки гри, можна втратити не тільки гроші, але й всю компанію, бо кожен учасник розробки так чи інакше пов’язаний між собою і втрата даних одного учасника може призвести до втрати даних всієї компанії. А якщо це багатомільйонні компанії з розробки, обізнаність співробітників в соціальній інженерії напряму впливає на безпеку всієї структури. Ресурси та активи, безпеці яких може загрожувати витік інформації через методи соціальної інженерії, включають:

- Вихідний код ігрових проектів: Весь програмний код, що розробляється в компанії, є інтелектуальною власністю та критичним активом. Він зберігається на серверах компанії та системах керування версіями.
- Ігрові ресурси: Це графічні файли, 3D-моделі, звукові ефекти, музика та інші мультимедійні елементи, які створюються або використовуються у розробці ігор.
- Персональні дані співробітників: Дані співробітників компанії, такі як імена, контактна інформація, дані про зарплату та інші особисті дані, зберігаються у базах даних компанії.
- Персональні дані користувачів: Інформація про користувачів ігор, включаючи акаунти, налаштування, ігрову статистику та інші дані, що можуть зберігатися на серверах компанії.
- Комерційна інформація: Фінансові звіти, маркетингові плани, стратегії розвитку та інші конфіденційні документи, які мають високу комерційну цінність.

В той же час, в самих іграх в більшості випадків є внутрішньоігрові покупки, на які гравець витрачає реальні гроші і якщо за використання ігрового додатку, користувач необережний в свої діях, це може вплинути не тільки на втрату прогресу, а й на втрату вже вкладених грошей.

Також не слід забувати про платформи для дистрибуції відеоігор (Steam, Epic Games Store). Це нефізичні платформи для розміщення ігор для розробників та покупки ігор для гравців. Зазвичай такі платформи містять дані користувачів та їх банківських карток, для покупок ігор та додатків. Менше з тим, користувачі не мають фізичні версії ігор, такі як диски, тому при втраті акаунту користувач втрачає також свої кошти, а з урахуванням цін на відеоігри втрачені суми можуть досягати десятків тисяч. Тому гравці, які користуються такими платформами, повинні бути достатньо обізнані в сфері соціальної інженерії, щоб не натрапити на зловмисників і не втратити свої покупки та дані банківських карток.

Як вже було сказано, з точки зору втрат, більш за все потерпають саме розробники, але гравцями можуть бути різні вікові категорії, в тому числі й діти, які можуть з необізнаності спричинити витік даних власних батьків, через підв’язані акаунти, банківські картки, особисту інформацію сім’ї, що може вплинути на більшу кількість людей ніж одна жертва на яку було здійснено атаку. Тому зважаючи на це, батьки також повинні слідкувати за тим де їхні діти використовують інформацію про них, бо у випадку з соціальною інженерією ніхто не несе відповідальність за втрату даних окрім них.

2.2 Принципи впливу та етичні міркування у соціальній інженерії

Прямий чи непрямий вплив на людей (індивідуумів, групи), це дія, що викликає зміну їхньої поведінки. При цьому суб’єкт, що впливає, повинен усвідомлювати цілі і наслідки свого впливу.

Поза світом психології люди зазвичай не бачать різниці між маніпуляцією і впливом. Але серед фахівців ці терміни мають абсолютно різне значення. Маніпуляція – це згубний вплив, зазвичай спрямоване на заподіяння шкоди. У соціальній інженерії і зловмисники, і пентестери з добрими намірами часто

використовують маніпуляцію замість впливу через недостатню підготовку або необдуманість.

Психолог Роберт Чалдіні виділяє шість основних принципів впливу: авторитет, привабливість, терміновість і дефіцит, сталість і послідовність, соціальний доказ, взаємність.

Застосування основних принципів:

- **Авторитет:** Люди зазвичай виконують дії, коли їм це радить авторитетна особа або вони вірять, що ця дія схвалена впливовою фігурою. Шахрай може зателефонувати та заявити, що дію від імені генерального директора, CISO або згідно з певним законом.
- **Привабливість:** Люди схильні допомагати тим, кого вважають милими та привабливими. Продавець може зробити комплімент вашій зовнішності або розуму, щоб завоювати вашу прихильність.
- **Терміновість і дефіцит:** Якщо людина боїться щось втратити, вона прагне цього більше. Шахраї часто стверджують, що продають щось рідкісне, спонукаючи жертву діяти швидко, щоб не втратити вигідну пропозицію.
- **Послідовність:** Люди цінують сталість і послідовність. Спеціалісти з соціальної інженерії використовують це, підтримуючи сталість або порушуючи її, щоб вплинути на жертву. Продавець може заявити, що завжди піклується про своїх клієнтів і розуміє їхні потреби з першого дня співпраці.
- **Соціальний доказ:** Ми часто робимо речі тому, що інші вважають це нормальним або статусним. Це називається соціальним доказом. Наприклад, продавець автомобілів може переконати вас купити розкішний автомобіль, заявивши, що його купують успішні люди вашого віку.
- **Взаємність:** Ми охочіше допомагаємо тим, хто допоміг нам. Соціальні пентестери часто допомагають людині, а потім просять про послугу у відповідь.

- **Співчуття:** Налагодження взаєморозуміння часто вимагає виявлення симпатії та емпатії. Важливо розуміти почуття іншої людини та вміти висловлювати свої. Спілкуючись з іншими, ви можете поділитися схожою історією зі свого життя або задати уточнюючі питання, щоб виразити співчуття до ситуації. Це важливо для створення взаєморозуміння в конкретних умовах. Вміння виражати свої почуття та розуміти почуття іншої людини, вміти впливати та знати, коли не перевищувати межу, також грає роль. Взаємодіючи з іншими, можна розповісти історію (будь-то реальна подія, вигадка або прикрашена комбінація) про схожу ситуацію, щоб проявити взаємне співпереживання та покращити ваше взаєморозуміння. Якщо ж розмова йде про ситуацію, до якої ви не маєте відношення, задайте уточнюючі питання і висловіть співчуття до цієї ситуації. Втім, будьте обережні: якщо ви завжди маєте готову відповідь або історію на будь-яку розповідь співрозмовника, він може почати підозрювати вас, тому використовуйте цей підхід з розумом. [5].

Етична відповідальність у соціальній інженерії виникає з усвідомлення необхідності дотримання високих моральних та етичних стандартів під час впровадження та застосування технік та методів соціальної інженерії.

Загальний принцип полягає в тому, що соціальна інженерія повинна сприяти позитивним суспільним змінам і споживати моральні та етичні цінності як орієнтир для дій. Важливо, щоб фахівці в цій галузі ретельно вивчали можливі етичні дилеми та завжди діяли в інтересах добробуту та безпеки індивідів та суспільства [16].

Займаючись соціальною інженерією, потрібно постійно враховувати, як ваші дії вплинуть на жертву. Це складне завдання, оскільки вам необхідно показати вразливість компанії (зазвичай через відсутність належної підготовки співробітників або погано організовані процеси), але зробити це, не наносячи прямої шкоди репутації та кар'єрі людей, через яких було виявлено вразливість.

У соціальній інженерії важливими є два основні правові аспекти: спуфінг (обман) та запис дзвінків. Один із найкращих способів уникнути юридичних проблем - це атакувати лише ресурси, що належать компанії-клієнту, уникаючи взаємодії з особистими ресурсами співробітників.

У більшості країн існують закони, що забороняють підробку телефонних номерів. Якщо ви дієте, імітуючи дії зловмисника згідно з угодою про перевірку безпеки і дзвоните лише на бізнес-номери клієнта, ви, швидше за все, залишитеся в рамках закону. Запис дзвінків, особливо без явної згоди чи навіть без повідомлення співрозмовника, є складнішим питанням. Чи може компанія виступати другою стороною, що надає згоду на запис розмов своїх співробітників через корпоративні засоби комунікації, є сірою правовою зоною. Це багато в чому залежить від положень стандартного трудового договору. Якщо вас попросили записати дзвінки, обов'язково проконсультуйтеся з юристом для отримання подальших пояснень у вашому конкретному випадку [17].

Недостатня етична увага при використанні соціальної інженерії може призвести до різних негативних суспільних наслідків, оскільки ця методологія впливає на взаємодію між людьми і може мати значний вплив на суспільство в цілому

- Порушення приватності: Недостатня увага до етики може призвести до незаконного збору та використання особистої інформації індивідів. Це може порушити їхню приватність та права на захист особистих даних.
- Маніпуляція та обман: Соціальна інженерія може використовувати техніки маніпуляції та обману, щоб отримати інформацію або домогтися певних цілей. Це може призвести до недоброчесних практик та впливу на рішення людей, які не відповідають їхнім істинним переконанням.
- Поширення дезінформації: Недобросовісні використання соціальної інженерії може призвести до поширення дезінформації і фейків. Це може підірвати довіру до інформації та інституцій в суспільстві.

  Найкращі практики:
- Порушення прав та рівність: Використання соціальної інженерії може порушити права і рівність людей, особливо якщо воно спрямоване проти конкретних груп або має дискримінаційні наслідки.

- Соціальні конфлікти: Недоброчесна соціальна інженерія може поглибити соціальні конфлікти та напруження, оскільки вона може сприяти поширенню ненависті, байдужості або психологічному тискові на індивідів і групи.
- Загроза кібербезпеці: Соціальна інженерія також може бути використана як засіб для кібератак і вторгнень в інформаційні системи та мережі, що може призвести до витоку чутливої інформації і завдати шкоди організаціям і суспільству.
- Загроза демократії: В недемократичних режимах соціальна інженерія може використовуватися для піддавання впливу на вибори і демократичні процеси, загрожуючи стабільності та легітимності влади.

2.3 Критерії оцінки методів соціальної інженерії

Для початку потрібно визначити ключові показники ефективності самих методів. Основними критеріями для оцінки методів соціальної інженерії були обрані:

Частота успішних атак:

- Як часто вдаються спроби соціальної інженерії. Кількість успішних атак за певний період часу.
- Час до виявлення атаки:
- Як швидко ігрова платформа виявляє атаки соціальної інженерії після їх початку. Середній час між початком атаки та її виявленням.
- Витрати на відновлення:
- Скільки ресурсів (часу, грошей, працівників) витрачається на відновлення після успішної атаки. Загальні витрати на відновлення в грошовому еквіваленті або в годинах праці.
- Рівень впливу на гравців:
- Наскільки значними були наслідки атаки для гравців. Кількість постраждалих гравців або оцінка рівня незадоволення гравців (через опитування, відгуки).

- Кількість вразливих точок:
- Кількість точок входу, де соціальна інженерія може бути ефективною. Кількість ідентифікованих вразливостей в ігровій системі.

Для порівняння будуть використані 3 види методів соціальної інженерії такі як фішинг, вейлінг як підвид фішингу та OSINT.

Таблиця 1. Порівння методів соціальної інженерії за поданими критеріями.

	Email фішинг	Спис-фішинг	Вейлінг
Частота успішних атак	500 тис. атак на місяць	200 тис. атак на місяць	10 тис. атак на місяць
Час до виявлення атаки	2-5 днів	2-5 днів	5-10 днів
Витрати на відновлення	В залежності від кількості уражених осіб. Чим більше уражень тим більше витрати.	Витрати залежать від статусу ураженої цілі	Найбільші витрати. Так як на високопосадовцях зав’язана вся важлива документація.
Рівень впливу на гравців	Високий	Високий	Мінімальний якщо ураження не стосується бази даних користувачів
Кількість вразливих точок	Весь штат звичайних співробітники/гравців	Весь штат звичайних співробітники/гравців	Голови відділів та директори

В таблиці зазначено що найзбитковішим є вейлінг, а найменш збитковим є OSINT але найчастіше використовують фішинг. Затрати зусилля/користь найоптимальніше показують себе у випадку фішингу, це й показує таблиця.

Отримавши дані з таблиці можна дізнатися які способи кібератак з використанням методів соціальної інженерії потрібно відслідковувати найбільше.

2.4 Комплексна оцінка методів соціальної інженерії

На основі проведеного аналізу наукових джерел можна здійснити комплексну оцінку методів соціальної інженерії за наступними ключовими критеріями та показниками. Частота успішних атак демонструє, що email-фішинг є найбільш поширеним методом з показником близько 500 тисяч атак на місяць, тоді як спис-фішинг характеризується меншою частотою - приблизно 200 тисяч атак, а вейлінг має найнижчий показник - близько 10 тисяч атак щомісячно.

Часовий інтервал до виявлення атаки варіюється від 2-5 днів для фішингу та спис-фішингу до 5-10 днів для вейлінгу, що свідчить про різний рівень складності виявлення цих методів.

Витрати на відновлення після атак корелюють з масштабом ураження та статусом цільової аудиторії - найбільші збитки характерні для вейлінгу через високопосадовий статус жертв та важливість скомпрометованої документації [24]. Рівень впливу на користувачів оцінюється як високий для фішингу та спис-фішингу, проте мінімальний для вейлінгу у випадках, коли атака не зачіпає базу даних користувачів [25].

Кількість вразливих точок також диференціюється - якщо фішинг та спис-фішинг охоплюють весь штат звичайних співробітників, то вейлінг концентрується виключно на керівниках відділів та директорах [26]. Ефективність методів соціальної інженерії значною мірою залежить від рівня підготовки персоналу та впровадження превентивних заходів захисту [27]. Комплексний аналіз цих показників дозволяє оцінити потенційні ризики та розробити відповідні стратегії протидії різним видам соціально-інженерних атак.

У ваще вказаній таблиці йдеться про порівняння методів соціальної інженерії (наприклад, фішинг, спіс-фішинг тощо) за кількома критеріями. Для аналізу, що охоплює Україну за останні 5 років, потрібні конкретні дані про ці методи атак, їх частоту, вплив та інші характеристики: Звіт за перший квартал 2023, Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки протягом 2022 року

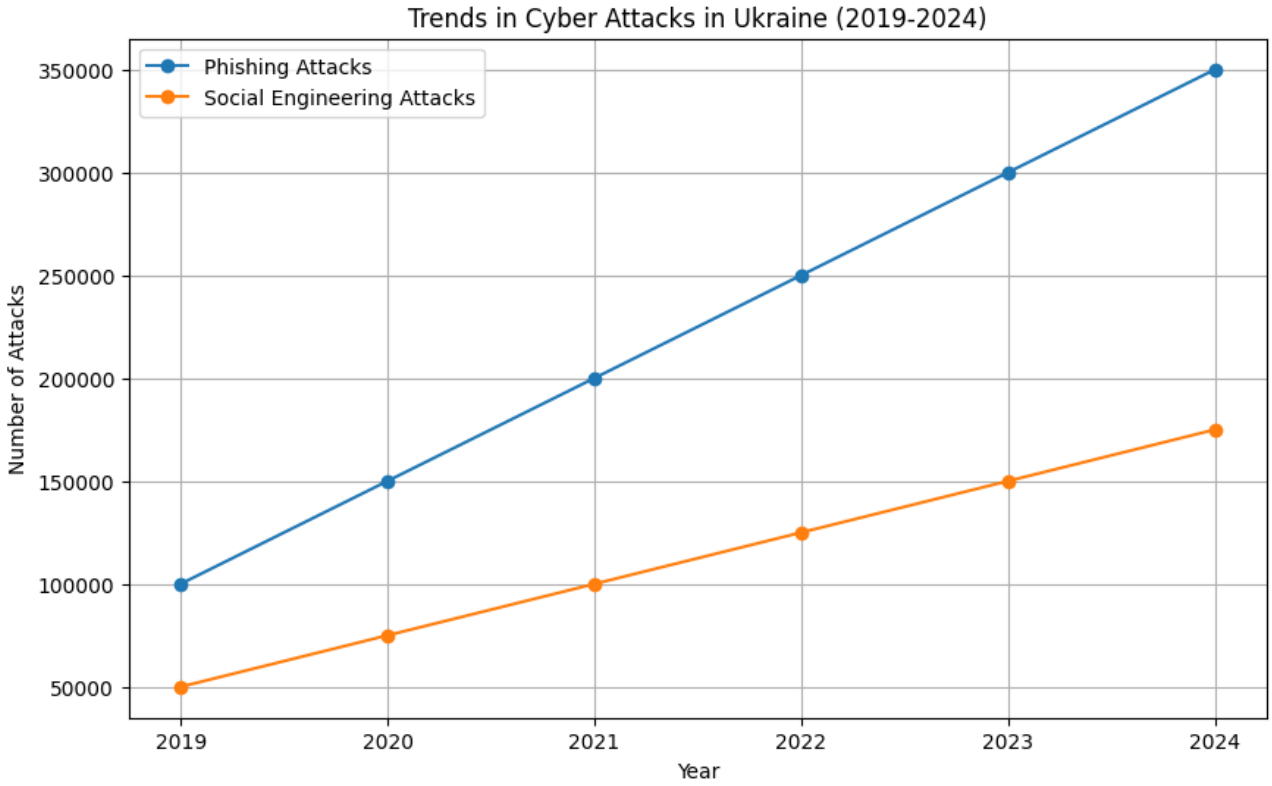

Рисунок 1 – Графік фішингових атак та атак за допомогою соціальної інженерії

За останні 5 років в Україні спостерігається значне зростання кількості кібератак та інцидентів соціальної інженерії.

Динаміка кібератак

У першому півріччі 2024 року зафіксовано 1739 кіберінцидентів, що на 19% більше порівняно з другим півріччям 2023 року [28].

Кількість критичних інцидентів зменшилася на 90%, проте зросла кількість атак на урядові організації та місцеві органи влади [29]. Фішингові атаки демонструють стрімке зростання - з 100 000 у 2019 році до 350 000 у 2024 році. Паралельно

збільшилась кількість атак соціальної інженерії - з 50 000 у 2019 році до 175 000 у 2024 році.

Таблиця 2. Кількість фішингових атак та атак за допомогою соціальної інженерії у відведеному періоді

Рік	**Фішингові атаки**	**Атаки соціальної інженерії**
2019	100 000	50 000
2020	150 000	75 000
2021	200 000	100 000
2022	250 000	125 000
2023	300 000	150 000
2024	350 000	175 000

Час виявлення атак становить від 2-5 днів для фішингових атак до 5-10 днів для вейлінгу.

Кількість кіберінцидентів у секторі безпеки та оборони, а також в енергетичному секторі зросла більш ніж удвічі . Особливу увагу зловмисники приділяють атакам на урядові організації, місцеві органи влади та об'єкти критичної інфраструктури .За даними платформи Опендатабот, лише за перші п'ять місяців 2024 року було відкрито понад 38 тисяч справ про шахрайство .

Висновок до другого розділу

У другому розділі було розглянуто основні методи соціальної інженерії, а також як вони можуть повпливати на ті чи інші процеси. Кожен з цих методів є тою чи іншою можливістю для зловмисників пробратись як в структуру компанії так і ошукати окремих людей. Також детально описано важливість етичного використання соціальної інженерії та наслідки які можуть бути за неналежного використання. Було описано критерії оцінки методів соціальної інженерії та проведена комплексна оцінка методів соціальної інженерії.

РОЗДІЛ 3. ВПРОВАДЖЕННЯ МЕТОДИКИ ОЦІНЮВАННЯ МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В БЕЗПЕКОВІ ПРОЦЕСИ РОЗРОБКИ ГРИ

3.1 Методика оцінювання методів соціальної інженерії

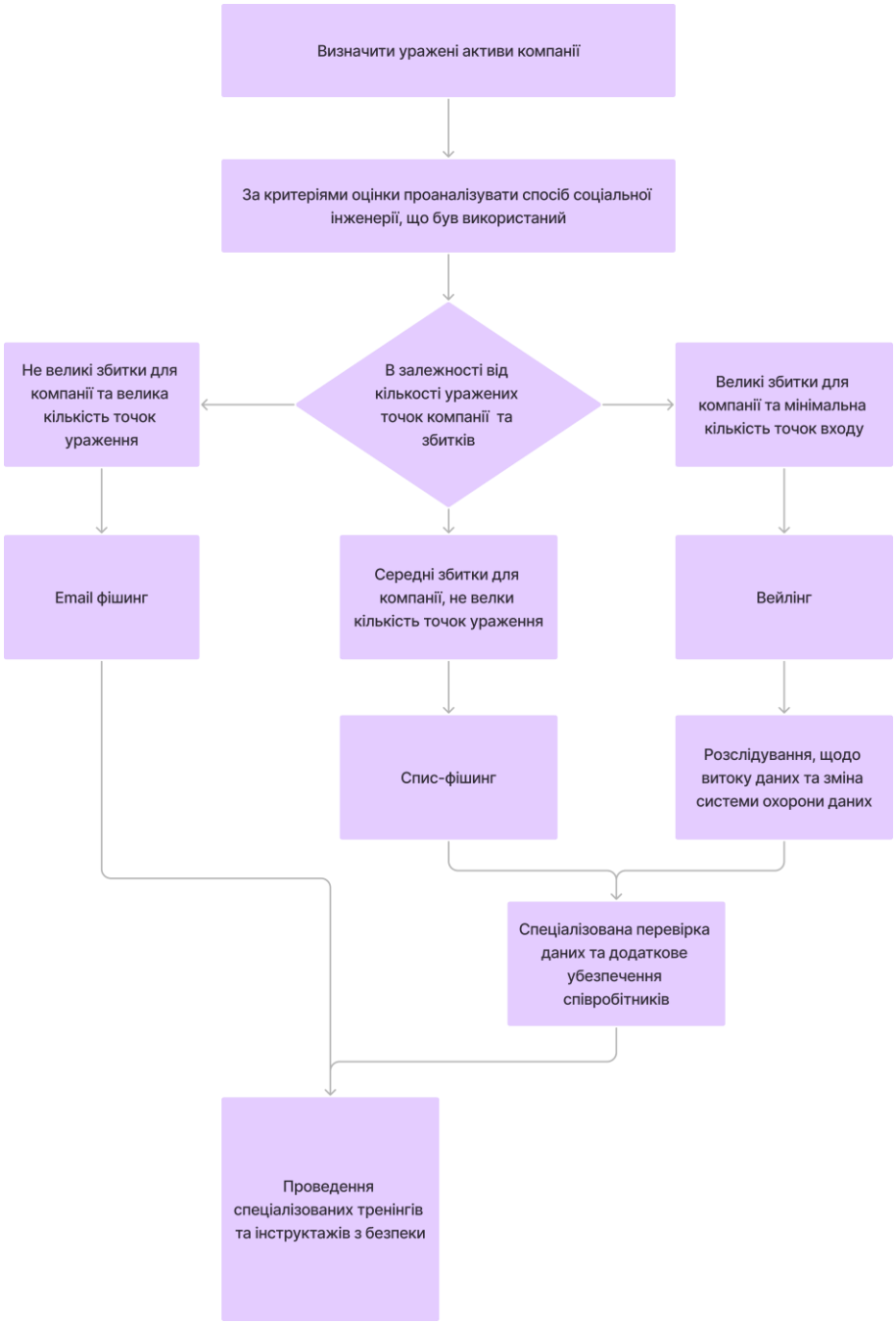

Рисунок 2 – Алгоритм методики оцінювання методів соціальної інженерії

- Етап 1 – Визначити уражені активи компанії.

  Дослідити уражені активи компанії та провести аналіз заданих збитків. У якої з категорій інформації під охороною відбувся витік та на яку з груп персоналу або гравців була націлена атака.

- Етап 2 – За критеріями оцінки проаналізувати спосіб соціальної інженерії, що був використаний

  За критеріями оцінки проаналізувати способи соціальної інженерії та визначити, що саме використовували зловмисники для кібератаки.

- Етап 3 – В залежності від кількості уражених точок та збитків визначити який саме метод соціальної інженерії було використано

  У випадку з не великими збитками та великою кількістю точок ураження це міг бути Email фішинг. У випадку з середніми збитками та не великою кількістю точок входу це міг бути спис-фішинг, що націлений на більш важливі посади. Якщо ж збиткі були досить вагомі а точок входу для такого ураження не багато то це вейлінг, що націлений на високопосадовців.

- Етап 4 – В залежності від кількості уражених точок та збитків використати запобіжні засоби.

  У випадку Email фішингу буде достатньо проведення спеціалізованих тренінгів та інструктажів з безпеки. Якщо ж це був спис-фішинг тоді до вищеописаного додається спеціалізована перевірка даних співробітника та аналіз сміжних до витоку даних, також додаткове убезпечення співробітників за допомогою контролювання робочої пошти задля безпеки співробітника від не бажаних листів. А у випадку вейлінгу до вищеописаного потрібно провести розслідування, щодо витоку даних та причетних до цього людей, також як додаткову міру безпеки слід змінити способи охорони інформації в компанії.

За допомогою даної методики оцінювання методів соціальної інженерії у сфері безпеки інтернет ігор можна передбачити кібератаки даного виду та зберегти активи компанії у безпеці. Так як безпека найголовнішого активу компанії, а саме гравців має знаходитися під надійним захистом потрібно проробити спеціалізовані кроки для досягнення повної безпеки.

Безпека гравців на пряму залежить від безпеки компанії тому, що база даних гравців знаходиться у серверних сховищах компанії, отже зловмисники при

великому зламі даних компанії з легкістю доберуться до бази даних гравців. Для того щоб такі атаки попередити та/або мінімізувати наслідки такої атаки і була розроблена ця методика яка допоможе оцінити методи соціальної інженерії які були використанні для кібератаки на компанії.
На жаль більшість аспектів безпеки буде все одно лежати на саміх співробітниках та гравцях тому, що соціальна інженерія направлена на людей і може бути передбачена лише при достатній обізнаності працівників, гравців та всіх причетних до гри.

3.2 Моделювання фішинг атаки на розробників

Розробка відеоігор напряму залежить від людського фактора і кількість людей які працюють над однією грою може бути як одна (незалежні розробники) так і тисячі. Зважаючи на те що створення ААА-проекту потребує великої кількості людського ресурсу, компанії поміж того що мають власних працівників, нерідко звертаються до послуг аутсорсингових компаній, задля тимчасового розширення штату. Таким чином, кількість людей яка задіяна на проекті збільшує також кількість можливостей витоку даних.

Також не варто забувати про те що відеоігри це перш за все продукт створений для людей. Тобто гравці можуть так само легко потрапити під атаку навіть не підозрюючи про це.

Якщо витік даних відбувся на стороні розробника, розробник, як фігура, що виступає посередником між гравцем та його даними, які він прив'язує до тієї чи іншої гри, несе повну відповідальність за злив цих даних. Звісно, не варто забувати про ще одну сторону, а саме серверних розробників, які ці дані й утримують. Але якщо мова йде саме про захищеність даних в ігровій розробці бути винними можуть бути двоє – розробник та гравець.

Одним із таких випадків можна розглянути випадок компанії з розробки ігор Insomniac Games.

Insomniac Games, відомий розробник відеоігор, став жертвою витоку даних у листопаді 2023 року. Інцидент був організований групою зловмисників Rhysida, яка

вимагала значний викуп за викрадені дані. У разі несплати викупу група виклала в мережу величезну кількість даних, включаючи конфіденційну інформацію про співробітників і матеріали, пов'язані з майбутньою грою Wolverine.

Серед даних, які були викриті в результаті витоку, були матеріали розробки гри, проектна документація, інформація про кастинги, проекти рівнів, внутрішні розслідування, дисциплінарні звіти, особисті дані співробітників, скани паспортів, відеозаписи зустрічей, інформація про контракти та ліцензійні угоди з компаніями Marvel та Nvidia.

Порушення вплинуло на дані, що стосуються понад 400 співробітників.
Група вірусів-вимагачів Rhysida проникла в системи Insomniac Games, ймовірно, за допомогою фішингових атак та інших методів, що призвело до масового витоку даних [18].

Зважаючи на характер ураження, а саме шляхом співробітників, можна припустити, що відбулась класична фішингова атака через електронну пошту.
З розповідей людей які потрапляли під фішингові атаки, навіть якщо це був звичайний тест від підприємства, можна побачити цікаву річ. Усім надіслали електронного листа з дуже схожим заголовком і форматом повідомлення, як зазвичай надходять листи від одного з постачальників програмного забезпечення (можливо, це був Adobe?). Лист виглядав абсолютно нормально і легально, і містив посилання для переходу до входу в обліковий запис.
Браузер відкривався, і користувач зустрічав нескінченну кількість спливаючих вікон, що відкривалися і закривалися. За долю секунди, поки будь-яке вікно залишалося відкритим, користувач міг бачити своє повне ім'я, IP-адресу, мітку часу і номер робочої станції. Електронні листи надсилалися в шаховому порядку, так що людина, яка сиділа поруч з вами, могла отримати його лише через годину або дві (це було зроблено для того, щоб ви не обговорювали/попереджували когось іншого). Пізніше того ж тижня IT-відділ проводив презентацію про безпеку та захист даних, і вони підготували велику довгу таблицю всіх, хто відкрив посилання, це було близько 70%+ переходів по посиланню [19].

Таким чином, можна відзначити, що особливих маніпуляцій в фішинговій атаці не потрібно, достатньо створити лист схожий на щось звичне для співробітників і надислати його не підряд. Це достатньо примітивно, але практика показує наскільки дієво.

Ото ж судячи з усього вище сказаного можна сказати що саме самоосвіта та обережність людей може вберегти від кібератак за допомогою соціальної інженерії. Розроблена методика дозволила б краще орієнтуватися в заходах безпеки проти таких атак та запобігти або ж хоча б знизити збитки отримані компанією від кібератаки.

3.3 Імплементація методів захисту

Провівши порівняння методів соціальної інженерії та визначення критеріїв оцінки заводної ними шкоди можна скласти схему для кращого розуміння безпекових процесів.

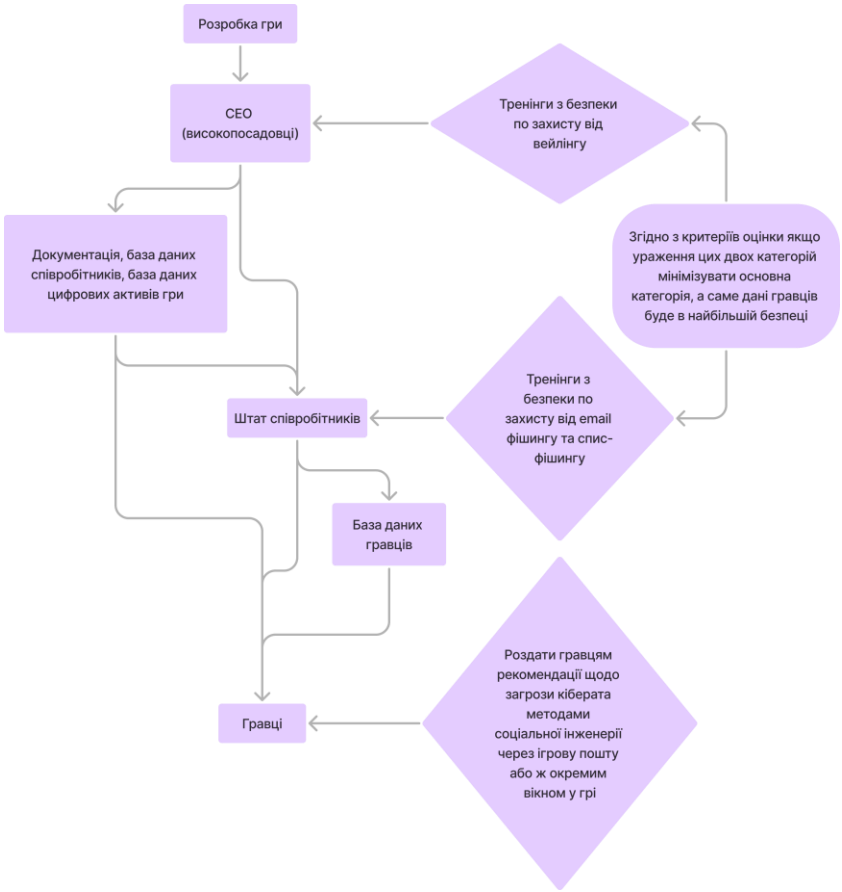

Рисунок 3 – Кроки імплементації методів оцінки соціальної інженерії у процес розробки гри задля мінімізації шкоди

Оцінивши метод за найбільш нанесеною шкодою можна мінімізувати цю шкоду за допомогою рекомендацій описаних нижче для кожної категорії, що задіяна в розробці гри та впливає на безпеку даних гравця.

3.4 Методи захисту власних даних в ігровій індустрії

І розробники і гравці, це перш за все звичайні люди, які для запобігання атак з використанням соціальної інженерії, можуть тільки виховати в собі уважність до власних даних та самих себе.

Якщо витік даних відбувся на стороні розробників постраждалі користувачі повинні:

- Змінити свої паролі: Негайно змінити паролі до всіх облікових записів, які могли бути скомпрометовані. Переконайтеся, що нові паролі надійні та унікальні, не використовувалися раніше на інших платформах.
- Відновіть паролі для інших акаунтів: Якщо ви використовували ті самі або схожі паролі для інших облікових записів в Інтернеті, скиньте їх також. Це дуже важливо, оскільки зловмисники часто намагаються використовувати викрадені паролі на кількох сайтах.
- Увімкніть двофакторну автентифікацію (2FA): Увімкніть 2FA для всіх уражених облікових записів. Подумайте про те, щоб увімкнути цю додаткову функцію безпеки для всіх інших важливих онлайн-акаунтів, щоб значно знизити ризик несанкціонованого доступу.
- Відстежуйте свої акаунти: Слідкуйте за своїми акаунтами на предмет будь-якої підозрілої активності та повідомляйте про будь-який несанкціонований доступ або транзакції відповідним особам [18].
- Коли користувач став жертвою фішингу і, можливо, впровадив шкідливе програмне забезпечення в середу, повідомлення електронною поштою може бути не найкращим рішенням. Це пов'язано з тим, що вся система електронної пошти може бути скомпрометована та зловмисники можуть прочитати, заблокувати або змінити повідомлення [23].

Фішинг-шахраї в ігровій спільноті експлуатують довіру та ентузіазм гравців. Однак, залишаючись поінформованими, пильними та на зв'язку, ви можете значно знизити ризик стати жертвою цих цифрових хижаків.

- Перевіряйте джерело: Вживайте заходів для перевірки електронної пошти відправника або походження повідомлення - кожного разу. Достовірна інформація буде надіслана від визнаного та уповноваженого суб'єкта.
- Звертайте увагу на тривожні сигнали: Фішингові атаки зазвичай демонструють неправильну граматику, орфографічні помилки та швидкий заклик до дії, наприклад, «дійте швидко, інакше ваш акаунт буде заблоковано».
- Ставте під сумнів пропозицію: Якщо вона схожа на кота, то, ймовірно, так воно і є. Справжні пропозиції від ігрових компаній не вимагатимуть ваших конфіденційних даних в електронних листах або текстах повідомлень.
- Використовуйте безпечні з'єднання: Переконайтеся, що веб-сторінка, яку ви відвідуєте, використовує захищений протокол (HTTPS), і шукайте значок замка в адресному рядку як індикатор безпеки.
- Використовуйте надійні, унікальні паролі: Для кожного свого ігрового акаунта створіть надійний, унікальний пароль, який ніхто не зможе вгадати. Використовуйте менеджер паролів, щоб упорядкувати їх.
- Увімкніть двофакторну автентифікацію (2FA): Багато ігрових платформ пропонують 2FA, що підвищує рівень захисту ваших акаунтів.
- Оновлюйте програмне забезпечення: Постійно оновлюйте своє ігрове програмне забезпечення та гаджети для захисту від загроз, що постійно змінюються.
- Самоосвіта: Будьте в курсі найновіших методів фішингу та діліться цією інформацією зі спільнотою.

Якщо ви зіткнулися з фішинговою атакою, негайно вживши заходів, ви допоможете не лише собі, але й усій спільноті, яка перебуває в зоні ризику. Ось що ви можете зробити:

- Не переходьте за посиланнями та не завантажуйте файли з джерел, які здаються вам підозрілими.
- Повідомте ігрову платформу або постачальника послуг про спробу фішингу. Багато компаній мають спеціальні канали для повідомлень про такі випадки.
- Поділіться своїм досвідом з друзями-гравцями та спільнотою, щоб підвищити обізнаність та запобігти жертвам.

Головним феноменом ігрової спільноти є не лише спільна пристрасть до ігор, але й здатність спільноти об'єднуватися та боротися проти спільного ворога. Онлайн-гравці можуть захистити себе від фішингу, створивши колективний щит, де вони обмінюються інформацією та ресурсами про кібербезпеку. Форуми спільнот, групи в соціальних мережах та ігрові конвенції є хорошими платформами для підвищення обізнаності та обміну порадами щодо найкращих практик кібербезпеки [22].

Висновок до третього розділу

У третьому розділі було більш детально розглянуто можливості зловмисників в атаках описаних у попередньому розділі. Зокрема, було наведено приклади вже відомих випадків в ігровій індустрії, від яких постраждали як компанії, так і гравці. Проводено аналіз розвитку фішингових атак та їхні зміни які відбулись в наслідок розвитку інтернету та різноманітних способів доступу до акаунтів. Була складена схема щодо оцінки загрози та імплементації методики оцінки методів соціальної інженерії у процес розробки. Також, були наведені рекомендації щодо захисту від фішингових атак, а також що робити якщо витік вже стався.

ВИСНОВОК

Під час виконання курсової роботи було здійснено глибоке дослідження методів соціальної інженерії, їх значення в умовах сучасного розвитку інформаційних технологій, а також розглянуті основні загрози безпеці, з якими можуть стикатися розробники та користувачі онлайн ігор. Соціальна інженерія є зручним інструментом для пошуку даних користувачів та її практичне значення для розвідки неоціненне. Але зловмисники користуються такими методами задля власної вигоди, що робить інтернет простір достатньо небезпечним, щоб не бути обізнаним в методах соціальної інженерії, для власного захисту. Тому належна обізнаність в методах соціальної інженерії є важливим аспектом в контексті забезпечення інформаційної безпеки.

У першому розділі роботи було здійснено визначення соціальної інженерії. Це дозволило отримати чітке уявлення про соціальну інженерію як про підхід до видобутку інформації. Також було розглянути основні поняття, що дозволило зрозуміти поверхнево яким чином можна використовувати соціальну інженерію. У результаті аналізу було розкрито можливі загрози безпеці під час розробки ігор та користування ними. Проведений аналіз підтвердив важливість проведення комплексної роботи з обізнаності методів соціальної інженерії, як для всіх верств населення, так і для користувачів відеоіграми окремо.

Другий розділ був присвячений основним методам соціальної інженерії, а також як вони можуть повпливати на ті чи інші процеси. Кожен з цих методів є тою чи іншою можливістю для зловмисників пробратись як в структуру компанії так і ошукати окремих людей. Також детально описано важливість етичного використання соціальної інженерії та наслідки які можуть бути за неналежного використання.

У третьому розділі було проаналізовано існуючі приклади використання методів соціального інженерингу на розробників та на звичайних користувачів. Ці приклади показують, що не залежно від розмірів структури (велика компанія з розробки чи окремі групи людей), методи соціальної інженерії перш за все направлені на людей і саме обізнаність людей може дозволити їм уникнути атаки,

або хоча б мінімізувати шкоду. Також було розглянуто можливі способи захисту до, під час або після фішингової атаки, які залежать від знання людей про методи соціальної інженерії.

Підсумовуючи, слід зазначити, що навігація в ігровому всесвіті вимагає обережності щодо фішингового шахрайства. Володіючи правильною інформацією та безпечними онлайн-звичками, гравці можуть захистити себе від прихованих небезпек. У результаті дослідження були виявлені основні методи соціальної інженерії та розглянуті можливості захисту від них. Описані методи є необхідними елементами для розуміння можливостей захисту себе не тільки в ігровому, а й в інтернет середовищі загалом.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Коптяєв М. Аналіз сутності соціальної інженерії : матеріали міжнар. наук. конф. Науковий простір : актуальні питання, досягнення та інновації (29 листопада 2024)
2. Коптяєв М. Основні поняття в соціальній інженерії науковий простір : матеріали міжнар. наук. конф. Інноваційна наука : пошук відповідей на виклики сучасності (6 грудня 2025)
3. Коптяєв м. Загрози безпеці в сфері інтернет ігор : матеріали міжнар. наук. конф. Період трансформаційних процесів в світовій науці: задачі та виклики (13 грудня 2024)
4. Що таке соціальна інженерія?/ Microsoft/ URL: https://support.microsoft.com/uk-ua/skype/%D1%89%D0%BE-%D1%82%D0%B0%D0%BA%D0%B5-%D1%81%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0-%D1%96%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D1%96%D1%8F-085cdf83-eade-4482-8eea-284b9ae97951 (accessed 18.11.2024)
5. Соціальна Інженерія: Методи та Захист в Цифровому Світі / Hackyourmom/ URL: https://hackyourmom.com/kibervijna/shho-take-soczialna-inzheneriya-chastyna-1/ (дата звернення 18.11.2024)
6. Лекція 1. Деструктивні методи соціальної інженерії як фактор загрози інформаційної безпеки. Сторінка 4. Зав. кафедрою кібербезпеки д.т.н., проф. Євсеєв Сергій Петрович
7. Соціальна інженерія: виклики та перспективи боротьби в українському контексті / Українське право/ URL: https://www.ukrainepravo.com/legal_publications/essay-on-it-law/it_law_demchuk_Social_engineering_perspectives_of_the_struggle_in_ukrain/ (дата звернення 18.11.2024)
8. Лекція 2. Історія та еволюція соціальної інженерії. Сторінка 8. Зав. кафедрою кібербезпеки д.т.н., проф. Євсеєв Сергій Петрович

9. Соціальна інженерія: в аспекті забезпечення кібербезпеки / Яготинський будинок дитячої та юнацької творчості Яготинської міської ради/ URL: https https://bdut.co.ua/pro-nas/socialna-inzheneriya/ (дата звернення 18.11.2024)
10. Лекція 2. Історія та еволюція соціальної інженерії. Сторінка 11. Зав. кафедрою кібербезпеки д.т.н., проф. Євсеєв Сергій Петрович
11. Соціальна інженерія та етичний хакінг на практиці. Джо Грей
12. Лекція 6. Історія та еволюція соціальної інженерії. Сторінка 2. Зав. кафедрою кібербезпеки д.т.н., проф. Євсеєв Сергій Петрович
13. Лекція 2. Історія та еволюція соціальної інженерії. Сторінка 13. Зав. кафедрою кібербезпеки д.т.н., проф. Євсеєв Сергій Петрович
14. Лекція 8. Історія та еволюція соціальної інженерії. Сторінка 2. Зав. кафедрою кібербезпеки д.т.н., проф. Євсеєв Сергій Петрович
15. Hamilton, B. The DNI's Open Source Center: An Organizational Communication Perspective / B. Hamilton //International Journal of Intelligence and CounterIntelligence URL: http://www.oss.net/dynamaster/file_archive/110802/98532478899216432d3d76e2f9d4534c/20110802%20Dr.%20Bean%20IJIC%20Open%20Source%20Center.pdf (accessed 18.11.2024)
16. Лекція 3. Історія та еволюція соціальної інженерії. Сторінка 2. Зав. кафедрою кібербезпеки д.т.н., проф. Євсеєв Сергій Петрович
17. Етичні засади соціальної інженерії: Захист, довіра та відповідальність/ Hackyourmom/ URL: https://hackyourmom.com/kibervijna/etychni-mirkuvannya-u-soczialnij-inzheneriyi-chastyna-2/ (дата звернення 18.11.2024)
18. Insomniac Games Data Breach: What & How It Happened? / Twingate/ URL: https://www.twingate.com/blog/tips/Insomniac%20Games-data-breach (accessed 25.11.2024)
19. Game Freak acknowledges massive Pokémon data breach, as employee info appears online/ Reddit / URL: https://www.reddit.com/r/Games/comments/1g2poef/game_freak_acknowledges_massive_pok%C3%A9mon_data/ (дата звернення 25.11.2024)

20. Police Advisory On Fake Online Platforms Selling Gaming Accounts / Singapoure police force/ URL: https://www.police.gov.sg/media-room/news/20221125_police_advisory_on_fake_online_platforms_selling_gaming_accounts (дата звернення 25.11.2024)
21. Watch out for fake game developers / Reddit/ URL: https://www.reddit.com/r/gamedev/comments/sshhc5/watch_out_for_fake_game_developers/ (дата звернення 25.11.2024)
22. Phishing Scams in the Gaming Community / Cyber management alliance/ URL: https://www.cm-alliance.com/cybersecurity-blog/phishing-scams-in-the-gaming-community (дата звернення 25.11.2024)
23. Лекція 9. Захист від соціальної інженерії. Сторінка 27. Зав. кафедрою кібербезпеки д.т.н., проф. Євсеєв Сергій Петрович
24. Види соціальної інженерії - CoreWin
25. 10.28925/2663-4023.2022.15.4562
26. Фішинг допомагає маніпулювати людьми заради даних. Як захиститися від кіберзагроз
27. https://www.bing.com/ck/a?!&&p=8c5fb057f74b184180e44ebb0a74754126498f3d57811c8b07a604791ebb509bJmltdHM9MTczNDA0ODAwMA&ptn=3&ver=2&hsh=4&fclid=038a8b68-832d-6883-01a9-9fb38246691f&psq=%d1%8e.+%d0%bc.+%d0%be%d0%bd%d0%b8%d1%89%d0%b5%d0%bd%d0%ba%d0%be%2c+%d0%bf%d0%b5%d1%82%d1%80%d0%be%d0%b2%2c+%d0%ba%d0%be%d0%b1%d0%b7%d0%b5%d0%b2&u=a1aHR0cHM6Ly9wc3ljaHBlZC5uYWlhdS5raWV2LnVhL2luZGV4LnBocC9wc3ljaHBlZC9hcnRpY2xlL2Rvd25sb2FkLzE0MDYvMTQwNS8&ntb=1
28. Кібербезпека № 5/2024
29. Російські кібератаки: зміна характеру атак та полювання на акаунти - MediaSapiens.