|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ** | | | | | | | | | | | | | | | | | | | | |
| **НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ** | | | | | | | | | | | | | | | | | | | | |
|  | |  | | | | | |  | | | | |  | | | | |  | | |
| **КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ** | | | | | | | | | | | | | | | | | | | | |
|  | |  | | | | | |  | | | | |  | | | | |  | | |
|  | |  | | | | | |  | | | | |  | | | | |  | | |
|  | |  | | | | | |  | | | | |  | | | | |  | | |
|  | |  | | | | | |  | | | | |  | | | | |  | | |
|  | |  | | | | | |  | | | | |  | | | | |  | | |
|  | |  | | | | | |  | | | | |  | | | | |  | | |
|  | |  | | | | | |  | | | | |  | | | | |  | | |
|  | |  | | | | | |  | | | | |  | | | | |  | | |
|  | |  | | | | | |  | | | | |  | | | | |  | | |
|  | |  | | | | | |  | | | | |  | | | | |  | | |
|  | |  | | | | | |  | | | | |  | | | | |  | | |
| Пояснювальна записка | | | | | | | | | | | | | | | | | | | | |
| до бакалаврської роботи | | | | | | | | | | | | | | | | | | | | |
|  | | на тему: | | | | | | | | | | | | | | | |  | | |
| **«ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ЛОКАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ»** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | |  | | | | | |  | | | | |  | | | | |  | | |
|  | |  | | | | | | Виконав студент 4 курсу, групи БСД-42 | | | | | | | | | | | | |
|  | |  | | | | | | спеціальності 125 Кібербезпека | | | | | | | | | | | | |
|  | |  | | | | | | освітньо-професійної програми «Інформаційна та | | | | | | | | | | | | |
|  | |  | | | | | | кібернетична безпека» | | | | | | | | | | | | |
|  | |  | | | | | | (шифр і назва спеціальності) | | | | | | | | | | | | |
|  | |  | | | | | | Довгань Д.Ю. | | | | | | | | | | | | |
|  | |  | | | | | | (прізвище та ініціали) | | | | | | | | | | | | |
|  | |  | | | | | | Керівник | | Чумак Н.С. | | | | | | | | | | |
|  | |  | | | | | |  | | | | | (прізвище та ініціали) | | | | | | | |
|  | |  | | | | | | Рецензет | | |  | | | | | | | | | |
|  | |  | | | | | | (прізвище та ініціали) | | | | | | | | | | | | |
|  | |  | | | | | | Нормоконтролер | | | | | | | Чумак Н.С. | | | | | |
|  | |  | | | | | |  | | | | | (прізвище та ініціали) | | | | | | | |
|  | |  | | | | | |  | | | | |  | | | | |  | | |
|  | |  | | | | | |  | | | | |  | | | | |  | | |
|  | |  | | | | | |  | | | | |  | | | | |  | | |
|  | |  | | | | | |  | | | | |  | | | | |  | | |
|  | | КИЇВ – 2023 | | | | | | | | | | | | | | | |  | | |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ** | | | | | | | | | | | | | | | | | | | |  |
| Інститут | | ННІЗІ | | | | | | | | | | | | | | | | | |  |
| Кафедра | | Інформаційної та кібернетичної безпеки | | | | | | | | | | | | | | | | | |  |
| Ступінь вищої освіти | | | | Бакалавр | | | | | | | | | | | | | | | |  |
| Спеціальність | | | 125 Кібербезпека | | | | | | | | | | | | | | | | |  |
| Освітньо-професійна програма | | | | | | | Інформаційна та кібернетична безпека | | | | | | | | | | | | |  |
|  | |  | | | | |  | | | | |  | | | | |  | | |  |
|  | |  | | | | |  | | | | |  | | | | |  | | |  |
|  | |  | | | | |  | | | | | ЗАТВЕРДЖУЮ | | | | | | | |  |
|  | |  | | | | |  | | | | | Завідувач кафедри ІКБ | | | | | | | |  |
|  | |  | | | | |  | | | | | \_\_\_\_\_\_\_\_\_\_\_\_ | | | | | Гайдур Г.І. | | |  |
|  | |  | | | | |  | | | | | “\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 року | | | | | | | |  |
|  | |  | | | | |  | | | | |  | | | | |  | | |  |
|  | |  | | | | |  | | | | |  | | | | |  | | |  |
|  | | **З А В Д А Н Н Я** | | | | | | | | | | | | | | |  | | |  |
|  | | **НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ** | | | | | | | | | | | | | | |  | | |  |
|  | |  | | | | |  | | | | |  | | | | |  | | |  |
| Довганю Дмитру Юрійовичу | | | | | | | | | | | | | | | | | | | |  |
| (прізвище, ім’я, по батькові) | | | | | | | | | | | | | | | | | | | |  |
| 1. Тема бакалаврської роботи: | | | | | | «Дослідження методів захисту локальної | | | | | | | | | | | | | | |
| мережі підприємства від атак соціальної інженерії» | | | | | | | | | | | | | | | | | | | |  |
| керівник бакалаврської роботи | | | | | | | Чумак Надія Степанівна, ст. викладач | | | | | | | | | | | | |  |
|  | |  | | | | | (прізвище, ім’я, по батькові, науковий ступінь, вчене звання) | | | | | | | | | | | | |  |
| затверджені наказом закладу вищої освіти від « 24 » лютого 2023 року № 26 . | | | | | | | | | | | | | | | | | | | |  |
|  | |  | | | | |  | | | | |  | | | | |  | | |  |
| 2. Строк подання студентом бакалаврської роботи | | | | | | | | | | | | | | 29.05.2023 р. | | | | | |  |
|  | |  | | | | |  | | | | |  | | | | |  | | |  |
| 3. Вихідні дані до бакалаврської роботи | | | | | | | | |  | | | | | | | | | | |  |
| корпоративна інформаційна система | | | | | | | | | | | | | | | | | | | |  |
| наукова та технічна література, експлуатаційна документація. | | | | | | | | | | | | | | | | | | | |  |
| рішення GoPhish | | | | | | | | | | | | | | | | | | | |  |
|  | | | | | | | | | | | | | | | | | | | |  |
|  | | | | | | | | | | | |  | | | | |  | | |  |
| 4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) | | | | | | | | | | | | | | | | | | | |  |
| 1. Актуальність проблеми щодо атак СО на локальну мережу підприємства. | | | | | | | | | | | | | | | | | | | |  |
| 2. Медоти захисту локальної мережі підприємств. | | | | | | | | | | | | | | | | | | | |  |
| 3. Засоби захисту локальної мережі підприємств. | | | | | | | | | | | | | | | | | | | |  |
| 4. Рекомендації щодо використання засобів та методів захисту. | | | | | | | | | | | | | | | | | | | |  |
| 5. Перелік графічного матеріалу | | | | | | | | | | | |  | | | | |  | | |  |
| 1. Тема бакалаврської роботи. | | | | | | | | | | | | | | | | | | | |  |
| 2. Актуальність, об’єкт, предмет, мета та наукові завдання дослідження. | | | | | | | | | | | | | | | | | | | |  |
| 3. Результати аналізу існуючих інструментів та рішень з протидії атакам соціальної інженерії. | | | | | | | | | | | | | | | | | | | |  |
| 4. Встановлення та налаштування інструменту GoPhish | | | | | | | | | | | | | | | | | | | |  |
| 5. Особливості налаштування інструменту GoPhish | | | | | | | | | | | | | | | | | | | |  |
| 6. Рекомендації щодо застосування інструменту GoPhish | | | | | | | | | | | | | | | | | | | |  |
| 7. Висновки за результатами роботи. | | | | | | | | | | | | | | | | | | | |  |
|  | | | | | | | | | | | | | | | | | | | |  |
| 6. Дата видачі завдання | | | | | 24.02.2023 р. | | | | | | | | | | | | | | |  |
|  | |  | | | | |  | | | | |  | | | | |  | | |  |
|  | | **КАЛЕНДАРНИЙ ПЛАН** | | | | | | | | | | | | | | |  | | |  |
|  | |  | | | | |  | | | | |  | | | | |  | | |  |
| №  зп | Назва етапів  бакалаврської роботи | | | | | | | | | | | | | | | Строк виконання етапів бакалаврської роботи | | | Примітка |  |
| 1. | Аналіз наукової та технічної літератури з питань теми бакалаврської роботи. | | | | | | | | | | | | | | | 24.02.2023 р. | | |  |  |
| 2. | Дослідження існуючих методів атак соціальної інженерії. | | | | | | | | | | | | | | | 24.03.2023 р. | | |  |  |
| 3. | Аналіз існуючих засобів захисту від атак соціальної інженерії. | | | | | | | | | | | | | | | 24.04.2023 р. | | |  |  |
| 4. | Розроблення рекомендацій щодо застосування фреймворку GoPhish на основі проведених досліджень. | | | | | | | | | | | | | | | 24.05.2023 р. | | |  |  |
| 5. | Оформлення результатів дослідження. | | | | | | | | | | | | | | | 27.05.2023 р. | | |  |  |
| 6. | Підготовка доповіді до захисту. | | | | | | | | | | | | | | | 28.05.2023 р. | | |  |  |
|  | | | | | | | | | | | | | | | |  | | |  |  |
|  | |  | | | | | Студент | | | | | Довгань Д.Ю. | | | | | | | |  |
|  | |  | | | | |  | | | | | (підпис) | | | | | прізвище та ініціали | | |  |
| Керівник бакалаврської роботи | | | | | | | | | | | | Чумак Н.С. | | | | | | | |  |
|  | |  | | | | |  | | | | | (підпис) | | | | | прізвище та ініціали | | |  |
|  | |  | | | | |  | | | | |  | | | | |  | | |  |

**ВІДГУК РЕЦЕНЗЕНТА**

на бакалаврську роботу

студентаДовганя Дмитра Юрійовича

на тему: «Дослідження методів захисту локальної мережі підприємства від атак соціальної інженерії»

**Актуальність:** Кібербезпека є однією з найбільш актуальних тем сучасності, оскільки віртуальний простір став не менш важливим для людства, ніж фізичний. Розмір і складність мережевих структур, що використовуються в сучасному світі, створюють потребу у засобах, які можуть забезпечувати безпеку та захист цих структур від атак.

Дослідження шляхів та розробка рекомендацій щодо дослідження методів захисту локальної мережі підприємства від атак соціальної інженерії можуть допомогти організаціям підвищити рівень кібербезпеки своїх мереж та зменшити ризики виникнення кібератак. Особлива актуальність цього полягає в зростанні кількості віддаленої роботи, коли значна кількість працівників працює з дому, використовуючи власні пристрої та підключаючись до мережі організації.

**Позитивні сторони:**

1. У роботі становлено суть проблеми атак соціальної інженерії та захисту на основі проведеного аналізу.

2. Було досліджено методи та засоби захисту локальних мереж підприємств від атак соціальної інженерії.

3. Розроблення рекомендацій щодо застосування фреймворку GoPhish.

4. Текст має чітку структуру, грамотно викладений. Висновки є зрозумілими та повними. Графічний матеріал якісно оформлений. Список літератури свідчить про вміння автора користуватися матеріалами, пов'язаними з темою роботи.

**Недоліки:**

1. У бакалаврській роботі бажано було б надати більше графічного матеріалу в розділі аналізу предметної області.

2. У роботі не завжди використовуються посилання на використані джерела інформації.

**Висновок:** Враховуючи недоліки, бакалаврська робота заслуговує оцінку **добре,** а студент

Довгань Д.Ю. – присвоєння кваліфікації *бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.*

|  |  |  |
| --- | --- | --- |
| Якість роботи | | Підпис рецензента (\_\_\_\_\_\_\_\_\_\_\_\_\_\_)  Підпис засвідчую  Підпис особи, що засвідчує (\_\_\_\_\_\_\_\_\_\_\_\_) |
| Виконано на замовлення підприємства |  |
| Виконано за тематикою НДР |  |
| Виконано з макетом |  |
| Виконано з застосуванням ЕОМ та МПТ | √ |
| Має практичну цінність | √ |
| Проект-частина комплексної теми |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ** | | | | | | | | |  |
| **ПОДАННЯ**  **ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ**  **ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ** | | | | | | | | |  |
| Направляється студент | | Довгань Д.Ю. | | | до захисту бакалаврської роботи | | | |  |
|  | | (прізвище та ініціали) | | |  | | | |  |
| спеціальності 125 Кібербезпека | | |  | | |  | |  |  |
| освітньо-професійної програми | | | Інформаційна та кібернетична безпека | | | | | |  |
|  |  | | (шифр і назва спеціальності) | | | | | |  |
| на тему: | «Дослідження методів захисту локальної мережі підприємства | | | | | | | |  |
| від атак соціальної інженерії». | | | | | | | | |  |
| Бакалаврська робота і рецензія додаються. | | | | | |  | |  |  |
| Директор інституту | | |  | | | Савченко В.А. | | |  |
| (підпис) (прізвище та ініціали) | | | | | | | | |  |
|  |  | |  | | |  | |  |  |
|  | **Довідка про успішність** | | | | | | |  |  |
| Довгань Д.Ю. | | | за період навчання в інституті | | | | | |  |
| (прізвище та ініціали студента) | | |  | | |  | |  |  |
| ННІЗІ з 2019 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:  національною шкалою: відмінно \_\_\_\_%, добре \_\_\_\_%, задовільно \_\_\_\_%;  шкалою ECTS: А \_\_\_\_%; В \_\_\_\_%; С \_\_\_\_%; D \_\_\_\_%; Е \_\_\_\_%. | | | | | | | | |  |
| Секретар інституту, факультету (відділення) | | | | | |  | | Берестяна Т.В. |  |
|  |  | |  | | | (підпис) | | (прізвище та ініціали) |  |
|  | **Висновок керівника бакалаврської роботи** | | | | | | |  |  |
| Студент Довгань Д.Ю.обрав тему роботи, метою якої було дослідження системи виявлення вторгнень Snort та розроблення рекомендацій щодо її застосування для забезпечення кібербезпеки. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання бакалаврської роботи Довгань Д.Ю, показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.  Все це дозволяє оцінити виконану бакалаврську роботу студента Довганя Дмитра Юрійовича на оцінку **«добре»** та присвоїти йому кваліфікацію: *бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.* | | | | | | | | |  |
| Керівник бакалаврської роботи | | | | | |  | | Чумак Н.С. |  |
|  |  | |  | | | (підпис) | | (прізвище та ініціали) |  |
|  |  | |  | | | “\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_ 2023 року | | |  |
|  | **Висновок кафедри про бакалаврську роботу** | | | | | | |  |  |
| Бакалаврська робота розглянута. Студент | | | | Довгань Д.Ю. | | | | |  |
|  |  | |  | (прізвище та ініціали) | | | | |  |
| допускається до захисту даної бакалаврської роботи в Державній екзаменаційній комісії. | | | | | | | | |  |
| Завідувач кафедри Інформаційної та кібернетичної безпеки | | | | | | |  |  |  |
| (назва) | | | | | | | | | |
|  |  | | . | | |  | | Гайдур Г.І. |  |
|  |  | | (підпис) | | | (прізвище та ініціали) | | |  |
| “\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_ 2023 року | | |  | | |  | |  |  |

# РЕФЕРАТ

Текстова частина бакалаврської роботи: 61 сторінок, 26 рисунків, 2 таблиці, 14 джерел.

*Об’єкт дослідження* – процес захисту локальної мережі підприємства від атак соціальної інженерії.

*Предмет дослідження* – методи та засоби захисту локальної мережі підприємства від атак соціальної інженерії.

*Мета роботи* – розробити рекомендації щодо застосування методів та засобів захисту локальної мережі підприємства від атак соціальної інженерії.

*Методи дослідження* – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, проведення експерименту.

В роботі приведено основні відомості про застосування систем виявлення вторгнень.

Проаналізовано існуючі методи захисту від атак соціальної інженерії.

Здійснено аналіз існуючих заходів та технічних рішень протидії атакам соціальної інженерії. Досліджено можливості інструменту GoPhish для підготовки та проведення навчання персоналу з протидії соціальній інженерії

На основі досліджень проведених в роботі розроблено рекомендації щодо застосування інструменту GoPhish для захисту локальної мережі підприємства від атак соціальної інженерії.

Галузь використання соціальної інженерії охоплює компанії та організації, що працюють з конфіденційною інформацією, а також провайдерів мережевих послуг.

ЛОКАЛЬНІ МЕРЕЖІ ПІДПРИЄМСТВА, ЗАГРОЗИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ,

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ЛОКАЛЬНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ ВІД АТАК

СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ, РЕКОМЕНДАЦІЇ ЩОДО ПІДВИЩЕННЯ ОБІЗНАНОСТІ ПЕРСОНАЛУ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ЗМІСТ** | | | | | |
|  |  | | |  | Стор. |
|  | **ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ** ……………………………….................................... | | | | 8 |
|  |  | | |  |  |
|  | **ВСТУП** ……………………………………..………………................. | | | | 9 |
|  |  | |  | |  |
| 1 | **АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ** …………................................................................. | | | | 12 |
|  |  |  | | |  |
|  | 1.1 | Корпоративна мережа та її функції ............................................................................. | | | 12 |
|  | 1.2 | Локальна та глобальна мережі ..................................................................................... | | | 13 |
|  | 1.3 | Аналіз загроз локальній мережі організації від атак соціальна інженерії .......................................................................................................................................... | | | 16 |
|  | 1.4 | Існуючі методи захисту локальної мережі підприємства від атак соціальної інженерії ......................................................................................................................... | | | 21 |
|  |  |  | | |  |
| 2 | ДОСЛІДЖЕННЯ ІСНУЮЧИХ ЗАСОБІВ ПРОТИДІЇ АТАКАМ ............................................ | | | | 24 |
|  |  |  | | |  |
|  | 2.1 | Система антиспаму Symantec Email Security ….………………............................. | | | 24 |
|  | 2.2 | Система антиспаму Microsoft Exchange Online Protector ….…………………….. | | | 27 |
|  | 2.3 | Система виявлення вторгнень Cisco Stealthwatch ……………………………….. | | | 29 |
|  | 2.4 | Фреймворл GoPhish ………………………………………………………………... | | | 31 |
|  | 2.5 | Порівняння розглянутих засобів .............................................................................. | | | 33 |
|  |  |  | | |  |
| 3 | ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДІВ ЗАХИСТУ МЕРЕЖІ ПІДПРИЄМСТВА ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ .............. | | | | 36 |
|  |  |  | | |  |
|  | 3.1 | Аспекти роботи з GoPhish …………………………………..……………………... | | | 36 |
|  | 3.2 | Розгортання кампанії та аналіз результатів............................................................. | | | 49 |
|  | 3.3 | Розробка рекомендацій щодо застосування фреймворку GoPhish та підвищення обізнаності персоналу ................................................................... | | | 52 |
|  |  |  | | |  |
|  | ВИСНОВКИ …………………………………………………………………………………...... | | | | 58 |
|  |  | | | |  |
|  | ПЕРЕЛІК ПОСИЛАНЬ ................................................................................................................ | | | | 60 |
|  |  | | | |  |
|  | ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) ................................................................... | | | | 61 |

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ – програмне забезпечення

IDS – intrusion detection system

СО – соціальна інженерія

WAN – wide area network

LAN – local area network

IPS – intrusion prevention system

DLP – date loss prevention

VPN – virtual private nеtwork

ПК – персональний комп’ютер

ПЗ – програмне забезпечення

# ВСТУП

*Актуальність теми.* У сучасному світі, де технології широко використовувані й інформація найціннішим активом підприємств, захист мережі від різноманітних загроз є дуже актуальною проблемою. Зловмисними впроваджують різні методи атак, серед яких присутня соціальна інженерія. Атаки соціальної інженерії базуються на маніпуляціях та впливі на людей з метою отримання несанкціонованого доступу до інформації або завдання різної степені шкоди підприємству.

Дослідження шляхів захисту локальної мережі підприємства від атак соціальної інженерії може допомогти підприємствам підвищити рівень кібербезпеки своїх локальних мереж та зменшими ризики виникнення атак соціальної інженерії.

Дослідження шляхів захисту локальної мережі підприєства від атак соціальної інженерії має велике значення для різноманітних підприємств. Це дослідження дозволяє забезпечити більш ефективний захист мережі від атак соціальної інженерії та має важливе практичне значення для компаній, які займаються дослідженням, розробкою методів протидії атакам соціальної інженерії

*Мета роботи* – вивчення методів та інструментів захисту, які можуть бути використані для забезпечення безпеки локальної мережі підприємства від атак соціальної інженерії. Основними завданнями дослідження є:

Аналіз наявних методів та систем виявлення вторгнення, що використовуються для розпізнавання атак соціальної інженерії. Під час аналізу будуть оцінені їхні переваги, недоліки та ефективність в реальних сценаріях.

Вивчення цих методів з метою розробки рекомендацій щодо їх використання для попередження атак соціальної інженерії. Це включає вивчення правильного налаштування систем, належне використання функцій та інструментів, а також навчання персоналу щодо виявлення та запобігання таким атакам.

З результатами дослідження будуть розроблені рекомендації щодо використання цих методів та систем в конкретному контексті підприємства. Ці рекомендації будуть орієнтовані на досягнення оптимального рівня захисту від атак соціальної інженерії з урахуванням особливостей мережі та специфіки діяльності підприємства.

*Об’єкт дослідження* – процес захисту локальної мережі підприємства від атак соціальної інженерії.

*Предмет дослідження* – методи та засоби захисту локальної мережі підприємства від атак соціальної інженерії.

*Мета роботи* – розробити рекомендації щодо застосування методів та засобів захисту локальної мережі підприємства від атак соціальної інженерії.

*Методи дослідження* – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, проведення експерименту.

*Вивчення літератури* - ознайомлення з науковими публікаціями, документацією та іншими джерелами з метою отримання базових знань про методи захисту локальної мережі підприємства від атак соціальної інженерії.

*Експериментальний аналіз* - проведення тестувань методів захисту локальної мережі підприємства від атак соціальної інженерії на тестових наборах даних з метою визначення рівня їх ефективності та потужності.

Організація дослідження шляхів та розробка рекомендацій щодо методів захисту локальної мережі підприємства від атак соціальної інженерії може відіграти ключову роль у покращенні безпеки інформаційних ресурсів та захисту підприємства. Ось декілька способів, якими така організація може допомогти:

Виявлення вразливостей: Дослідження дозволить ідентифікувати потенційні вразливості в локальній мережі підприємства, які можуть бути використані зловмисниками для проведення атак соціальної інженерії. Це допоможе зрозуміти, які аспекти системи потребують підвищеної уваги та захисту.

Розробка стратегій захисту: На основі результатів дослідження можна розробити ефективні стратегії та методи захисту від атак соціальної інженерії. Це можуть бути технічні заходи, такі як впровадження антивірусного програмного

забезпечення, антиспам-фільтрів, систем виявлення вторгнень тощо, а також організаційні заходи, наприклад, навчання персоналу та встановлення політик безпеки.

Аудит та аналіз прогалин: Організація аудиту дозволить виявити поточні прогалини в системі захисту підприємства, які можуть бути використані

зловмисниками для атак соціальної інженерії. Це дасть змогу усунути існуючі проблеми та підвищити рівень захищеності.

Підвищення усвідомленості персоналу: Організація дослідження та розробка рекомендацій дозволять підвищити

У першому розділі роботи проводиться огляд теоретичних основ соціальної інженерії та її основних методів. Розглядаються характеристики атак, їхні види та наслідки для підприємств. Детально аналізуються механізми впливу на людей, використовані зловмисниками для отримання небажаного доступу до інформації.

У другому розділі роботи проводиться порівняльний аналіз різних методів захисту від атак соціальної інженерії. Розглядаються технічні засоби, такі як антивіруси, фаєрволи, системи виявлення вторгнень, що можуть бути використані для виявлення та запобігання атакам. Також досліджуються організаційні заходи, такі як навчання та підвищення освіченості персоналу, політики безпеки та процедури реагування на події.

Третій розділ роботи присвячений проведенню аудиту і підготовці на конкретному підприємстві – НСЗУ у м. Києві. Проводиться визначення рівня навченості персоналу компанії щодо ризиків соціальної інженерії та методів їх запобігання а також аналіз поточних прогалин у системі захисту та визначаються основні вразливості. На основі отриманих даних розробляються рекомендації щодо підвищення захищеності шляхом підвищення усвідомленості працівників про методи захисту від атак соціальної інженерії та підвищення кваліфікації персоналу.

У завершальному розділі роботи надаються висновки з проведеного дослідження, підводиться підсумок роботи та надаються рекомендації з покращення системи захисту від атак соціальної інженерії на підприємстві. Розглядаються перспективи подальших досліджень у цій області та значення

результатів для сфери інформаційної безпеки підприємств.

Дослідження шляхів та розробка рекомендацій щодо методів захисту локальної мережі підприємства від атак соціальної інженерії мають широкі можливості застосування в галузі кібербезпеки та захисту інформації. Ця робота може бути корисною для будь-якої організації або установи, що має власну мережу і прагне забезпечити ефективний захист своєї інформації. Результати дослідження можуть бути успішно використані в таких сферах, як фінансові установи, урядові організації, компанії, які займаються обробкою даних та інші.

Застосування розроблених методів та рекомендацій допоможе організаціям забезпечити надійний рівень захисту, ефективно виявляти й реагувати на потенційні загрози та підвищувати загальний рівень кібербезпеки.

# 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

# 1.1. Корпоративна мережа та її функції

Будь-яка організація може розглядатися як складова система, в якій взаємодіють різні елементи або підрозділи, кожен з яких може мати свою структуру. Ці елементи взаємодіють як функціонально, виконуючи різні завдання в рамках бізнес-процесів, так і інформаційно, обмінюючись різними видами документів, комунікацій та іншою інформацією. Крім того, вони також взаємодіють з зовнішніми системами як функціонально, так і інформаційно. Це є типовою ситуацією для різних організацій, незалежно від їхнього виду діяльності - це можуть бути урядові установи, банки, промислові підприємства, комерційні фірми та інші.

Такий загальний підхід до розуміння організацій дозволяє сформулювати загальні принципи розробки корпоративних інформаційних систем, або інформаційних систем, що охоплюють всю організацію.

Розуміння цих принципів має велике значення для побудови ефективних та добре інтегрованих інформаційних систем, які забезпечують оптимальну функціональність та обмін інформацією в організації.

Корпоративна мережа є інфраструктурою, яка забезпечує обмін інформацією між різними додатками та системами, використовуваними в рамках корпорації. Вона представляє собою мережу, створену в межах конкретної організації, і працює на основі протоколу TCP/IP та стандартів зв'язку, які використовуються в Інтернеті. Крім того, вона включає сервісні програми, що забезпечують передачу даних між користувачами, які використовують цю мережу.

Корпоративна мережа є ключовим елементом інформаційної інфраструктури корпорації, і вірно спроектована та ефективно функціонуюча мережа може покращити продуктивність, забезпечити безпеку даних та сприяти ефективній комунікації всередині організації.

Корпоративна мережа зазвичай охоплює розподілені по території офіси, підрозділи та інші структури, які знаходяться на великій відстані один від одного. Засади побудови корпоративної мережі суттєво відрізняються від тих, що використовуються при створенні локальної мережі. Це обмеження є принциповим, і при проектуванні корпоративної мережі необхідно вживати всіх заходів для зменшення обсягів передаваних даних. Проте, корпоративна мережа не повинна обмежувати, які програми використовуються та як саме передається інформація по цій мережі.

Ефективна корпоративна мережа дозволяє підприємствам забезпечувати швидкий та надійний обмін інформацією, сприяє спільній роботі та спілкуванню працівників, а також забезпечує гнучкість та масштабованість для майбутнього розвитку організації.

Крім того, функції корпоративної мережі також включають:

Надання можливості організації електронного документообігу та спільного зберігання документів, що дозволяє ефективно управляти документами в організації.

Впровадження корпоративної телефонної мережі з єдиною системою нумерації, що спрощує комунікацію та забезпечує зручність у внутрішньому зв'язку.

Організація систем конференц-зв'язку, включаючи відеоконференції, що дозволяє проводити зустрічі та спілкування на відстані між співробітниками, клієнтами та партнерами.

Побудова розподільних систем відеоспостереження з єдиним центром зберігання даних, що забезпечує збереження і контроль безпеки в різних локаціях організації.

Організація дистанційного доступу до файлів і серверів з базами даних, що дозволяє працювати з даними та програмним забезпеченням з будь-якого місця та пристрою. Підключення до мережі Інтернет з можливістю організації єдиної корпоративної політики інформаційної безпеки, що забезпечує захист даних та мережеву безпеку.

# 1.2 Локальна та глобальна мережі

Різниця між локальною комп'ютерною мережею (LAN) та глобальною мережею (Wide Area Network, WAN) полягає в їх розмірі та охопленні.

Локальна мережа (LAN) обмежена географічною областю, такою як будинок, офіс або кампус. Вона підключає комп'ютери та пристрої на невеликій території і зазвичай використовується в межах однієї організації. LAN забезпечує швидку передачу даних, високу пропускну здатність та низький рівень затримки.

Глобальна мережа (WAN), навпаки, охоплює велику територію, таку як країна, континент або навіть всесвіт. WAN об'єднує розташовані на великій відстані локальні мережі та дозволяє обмін даними між ними. WAN використовується для підключення віддалених місць, філій компаній та користувачів з різних регіонів. Вона може використовувати різні технології передачі даних, включаючи кабельні лінії, оптоволокно, супутникові зв'язок та безпроводні мережі.

# 1.2.1 Локальна мережа

Корпоративна мережа зазвичай побудована на основі стандартів локальної мережі (LAN) і включає в себе компоненти, такі як апаратні комутатори, маршрутизатори, Ethernet-кабелі, бездротові точки доступу Wi-Fi та програмне забезпечення брандмауера. Ці компоненти співпрацюють для забезпечення ефективної передачі даних і забезпечення безпеки мережі.

Однією з важливих функцій корпоративної мережі є підтримка розподіленого доступу до різноманітних ресурсів, таких як спільні файли, документи, електронна пошта та бази даних. Це дозволяє співробітникам обмінюватись інформацією та спільно працювати над проектами незалежно від їх географічного розташування.

У локальній обчислювальній мережі (LAN) кілька настільних комп'ютерів підключені один до одного з метою спільного використання різних ресурсів, таких як принтери, програмне забезпечення, файли, інтернет-з'єднання і багато іншого [9]. Для забезпечення безпечного доступу до мережі з настільних комп'ютерів або мобільних телефонів встановлюються облікові записи користувачів. Користувачам зазвичай необхідно авторизуватися, введенням пароля або за допомогою іншого методу перевірки особистості.

У корпоративних мережах часто використовується програмне забезпечення для роботи з віртуальною приватною мережею (VPN). VPN дозволяє користувачам забезпечити зашифрований доступ до веб-сайтів та серверів, які знаходяться поза межами локальної мережі LAN. Це забезпечує безпеку та приватність при обміні даними зовнішніх ресурсів і дозволяє користувачам працювати віддалено з будь-якого місця, забезпечуючи доступ до корпоративних ресурсів інформаційної системи. Використання VPN дозволяє забезпечити захищене тунельне з'єднання між віддаленими користувачами та внутрішньою мережею компанії, що забезпечує конфіденційність та цілісність переданих даних.

Для управління доступом до різних ресурсів у корпоративній мережі використовується програмне забезпечення брандмауера. Брандмауер дозволяє встановлювати правила, наприклад, для блокування доступу до певних веб-сайтів з офісу або авторизації підключень користувачів з конкретних IP-адрес для доступу до внутрішніх служб. Це дозволяє забезпечити безпеку мережі та контролювати доступ до різних ресурсів згідно з політикою компанії.

У корпоративній мережі використовуються високошвидкісні комутатори і маршрутизатори, які відповідають за передачу даних між настільними комп'ютерами, серверами і іншими пристроями. Ці мережеві пристрої фізично підключаються до оптоволоконних і широкосмугових з'єднань. Крім того, часто вони використовуються для виконання функцій брандмауера шляхом встановлення відповідного програмного забезпечення (мікропрограм) на пристроях.

Адміністратори та фахівці з обслуговування мережі підключають настільні комп'ютери до маршрутизаторів у офісах, освітніх установах або на виробництві за допомогою Ethernet-кабелів або бездротового з'єднання Wi-Fi. Кожному кінцевому пристрою присвоюється унікальний ідентифікаційний номер в мережі, що дозволяє його ідентифікувати.

Для забезпечення безпеки та контролю доступу, важливим кроком є налаштування правил брандмауера та обмежень доступу до Інтернету для мережі відповідно до організаційних вимог до управління. Це дозволяє системним адміністраторам встановлювати правила та обмеження, щоб забезпечити безпеку, конфіденційність та відповідність політикам організації. Крім того, для доступу до системи необхідно створити облікові записи користувачів, які перевіряються на коректність облікових даних.

Корпоративна локальна мережа (LAN) забезпечує можливість одночасного використання спеціалізованого програмного забезпечення відповідно до ліцензійних угод для множини користувачів і спільне використання принтерів. Додатково, в межах LAN може бути розміщений приватний центр обробки даних (ЦОД), який служить для обслуговування програм баз даних та іншого програмного забезпечення для співробітників. Веб-сервери, що працюють в мережі LAN, надають доступ до загальнодоступних ресурсів за допомогою стандартів передачі HTTP/HTTPS і TCP/IP для обміну файлами. Проте слід відзначити, що доступ до сервера LAN зазвичай обмежується лише уповноваженим співробітникам, що забезпечує безпеку і конфіденційність даних.

Сучасні корпорації все більше залучають постачальників і використовують платформи публічних хмар для отримання різноманітних ІТ-послуг, які необхідно інтегрувати в корпоративні політики безпеки. В цьому контексті важливо правильно налаштовувати брандмауери, щоб забезпечити підтримку додатків SaaS (Software-as-a-Service), які розміщуються у віддалених середовищах з використанням безпечних зашифрованих мережевих підключень через віртуальні приватні мережі (VPN). Усі електронні листи, завантажені матеріали, загальні файли та локальні додатки, що встановлюються, повинні пройти перевірку агентами брандмауера, щоб гарантувати безпеку мережі в корпоративному середовищі. Це забезпечує захист від потенційних загроз і зловмисного використання даних, збереження конфіденційності і дотримання внутрішніх політик безпеки.

# 1.2.1 Глобальна мережа

Глобальні мережі (Wide Area Network) відома також як територіальні комп'ютерні мережі, і вони призначені для надання своїх послуг великій кількості кінцевих користувачів, які розподілені на великій території - в межах області, регіону, країни, континенту або навіть усієї планети. Побудова глобальної мережі потребує значних витрат, оскільки вона включає в себе вартість кабелів і робіт з їх прокладання, витрати на комутаційне обладнання та проміжну підсилювальну апаратуру, яка забезпечує необхідну пропускну здатність каналу, а також експлуатаційні витрати для постійного підтримання працездатності розподіленого по великій території мережевого обладнання.

Ці глобальні мережі використовуються для передачі даних на великі відстані, що дозволяє підключати користувачів з різних географічних місць і забезпечувати обмін інформацією між ними. Вони забезпечують масштабні можливості комунікації і дозволяють компаніям, організаціям та іншим суб'єктам використовувати цілу низку ІТ-послуг та додатків на великій території. Оскільки глобальні мережі охоплюють значні відстані, їх збудовано з врахуванням надійності та стійкості, забезпечуючи резервування шляхів передачі даних, щоб уникнути перерв у зв'язку.

Глобальні мережі, як правило, будуються великими телекомунікаційними компаніями з метою надання платних послуг абонентам. Такі мережі відомі як публічні або громадські. У цьому контексті використовуються поняття оператора мережі та постачальника послуг мережі. Оператор мережі - компанія, яка забезпечує нормальну функціонування мережі. Постачальник послуг, також відомий як провайдер, надає платні послуги абонентам мережі. Власник, оператор і постачальник послуг можуть бути однією компанією або представляти різні організації. Вони співпрацюють для забезпечення ефективної роботи глобальної мережі та надання широкого спектру послуг абонентам.

# 1.3 Аналіз загроз локальній мережі організації від атак соціальна інженерії

Один з найбільш вразливих елементів у системі інформаційної безпеки є людина. Зловмисники використовують соціальну інженерію для отримання доступу до конфіденційної інформації користувачів. Вони використовують різні методи, такі як маніпулювання, використання психологічних трюків або зловживання довіри, щоб переконати людей розкрити свої паролі, доступ до систем або іншу цінну інформацію.

Соціальна інженерія є методом, який використовується для маніпулювання людьми з метою отримання конфіденційної інформації або здійснення певних дій. Вона не вимагає використання технічних засобів, а заснована на використанні людських слабкостей. Цей метод може мати серйозні наслідки і є широко використовуваним в різних сферах, зокрема в інтернеті[5].

Хоча соціальна інженерія часто сприймається як незаконний спосіб отримання інформації, варто зазначити, що вона може бути використана і в законних цілях. Наприклад, соціальні інженери можуть бути найманими організаціями для проведення тестування на проникнення, з метою виявлення слабкостей системи безпеки та запобігання потенційним атакам.

В сучасному цифровому світі соціальна інженерія набула особливої популярності в Інтернеті. Зловмисники можуть використовувати цей метод для отримання конфіденційної інформації, такої як паролі, особисті дані або фінансові реквізити, шляхом впливу на людський фактор. Вони можуть використовувати підступи, соціальні маніпуляції або імітувати довіру, щоб отримати доступ до цінної інформації. Запобігання соціальній інженерії вимагає підвищеної обережності та свідомого підходу до захисту своїх персональних даних

Зловмисник, щоб отримати інформацію, використовує різні методи соціальної інженерії. Наприклад, він може збирати дані про співробітників цільової організації шляхом звичайного телефонного дзвінка або навіть проникнення у саму організацію під виглядом її співробітника.

Отже, для ефективного захисту мережі організації необхідно звернути особливу увагу на навчання персоналу, свідомість щодо безпеки та впровадження необхідних заходів, таких як міцна політика паролів, перевірка безпеки мережі, регулярне оновлення програмного забезпечення та встановлення ефективних систем виявлення та реагування на інциденти безпеки[6].

Типовий сценарій полягає в тому, що зловмисник може зателефонувати до працівника компанії, видаючи себе за члена технічної служби, і попросити його розкрити пароль, посилаючись на потребу у вирішенні невеликої проблеми з комп'ютерною системою. Часто такі атаки успішні, оскільки багато співробітників компаній не мають достатньої експертизи в галузі комп'ютерної безпеки. Зловмисник також може дізнатися імена службовців під час дзвінків та дослідження імен керівників, які доступні на сайті компанії або в інших джерелах відкритої інформації. Це дає йому додаткову інформацію для подальших атак та маніпуляцій.

Ці методи соціальної інженерії демонструють, як зловмисники використовують підступи та маніпуляції, щоб отримати цінну інформацію зі службовців організації. Для запобігання таким атакам важливо, щоб співробітники були освіченими про ризики соціальної інженерії та вживали заходи безпеки при спілкуванні з незнайомими особами і розкритті конфіденційної інформації.

Соціальна інженерія є молодою наукою, яка входить у склад соціології. Вона спрямована на вивчення, організацію та оптимізацію процесу створення, модернізації та репродукції нових соціальних реальностей. Ця наука доповнює соціологію, завершуючи перехід наукових знань до моделей, проектів та конструкцій соціальних інститутів, цінностей, норм, алгоритмів діяльності, взаємин, поведінки і т.д. Основний акцент робиться на розвитку аналітично-синтетичного мислення і знань формалізованих процедур (технологій) конструкторсько-винахідницької діяльності. Заняття з соціальної інженерії спрямовані на зброювання слухачів методологією аналізу та синтезу із застосуванням формалізованих процедур (технологій) конструкторсько-винахідницької діяльності.

У рамках цієї науки велика увага приділяється формалізованим операціям, які складають її основу, зокрема операціям складної комбінаторики. Недооцінка системного підходу до комбінаторних операцій призводить до серйозних наслідків на всіх рівнях трансформаційних процесів у суспільстві.

# 1.3.1 Як проходить атака соціальної інженерії на мережу

На початковому етапі атак соціальної інженерії зловмисники збирають інформацію, зосереджуючись на широкій аудиторії. Інформацію, яку вони отримують, можна розділити на два типи. Перший тип - загальна контактна інформація про якомога більше потенційних жертв, яка використовується для початкового наближення до цільових осіб. Лише після аналізу цілей та їх оточення зловмисники переходять до наступного етапу. Крім того, злочинці можуть спотворювати цілі, щоб зібрати інформацію іншого типу. Сюди входять жаргон та інші терміни, які можуть бути пов'язані з цілями. Ця інформація часто допомагає зловмиснику на наступних кроках атаки соціальної інженерії. На цьому етапі багато людей, які не усвідомлюють наслідки розкриття інформації для безпеки, стають жертвами. Основні помилки полягають у тому, що вони не розуміють важливості своїх даних для соціального інженера, що веде до ненавмисного розкриття інформації. Це можуть бути такі випадки, коли люди розкривають інформацію, яка на перший погляд може здатися незначною з точки зору безпеки, але насправді може бути корисною зловмиснику[9].

Далі починається розвиток стосунків з ціллю, що є важливим етапом атаки соціальної інженерії. Особливо ефективним цей етап є у відношенні тих людей, які вже знають про соціальну інженерію. Зловмисники використовують зібрану на попередньому етапі інформацію, щоб вступити в контакт з потенційною жертвою. Вони намагаються створити сприятливу обстановку, використовуючи знану інформацію і створюючи образ, що може зацікавити ціль. Під час встановлення стосунків, зловмисники використовують спосіб спілкування, який виглядає довіреним. Вони стараються зробити жертву впевненою і встановлюють партнерство, яким в подальшому можуть маніпулювати. Люди мають природну потребу довіряти і дбати про інших, і саме цим користуються соціальні інженери, щоб створити автентичність та набути довіри. Контакт може бути здійснений через різні цифрові засоби комунікації, такі як телефон, електронна пошта або соціальні медіа.

Після збору інформації та розвитку стосунків з ціллю, зловмисники соціальної інженерії переходять до етапу експлуатації, використовуючи ціль та її створену впевненість. За допомогою вже встановлених стосунків та набутої довіри, зловмисники можуть змусити ціль виконати певні дії або надати конфіденційну інформацію, яку вона зазвичай не надала б під звичайними обставинами. Це може включати отримання паролів, доступу до систем або здійснення інших небажаних дій. На цьому етапі зловмисники можуть завершити атаку або перейти до наступного рівня, використовуючи отриману інформацію або отриманий доступ для досягнення своїх злочинних цілей.

Виконання атаки є остаточним етапом, на якому зловмисники соціальної інженерії використовують усю зібрану інформацію та встановлені стосунки, щоб досягти своєї основної мети - отримати гроші, конфіденційну інформацію або інші цінні ресурси від цілі. З врахуванням успішних попередніх етапів, зловмисники майже завжди досягають свого успіху, здійснюючи вирішальний крок, що призводить до досягнення своїх злочинних цілей. Цей етап може включати переказ грошей, отримання важливої інформації або виконання інших бажаних дій, які були спрямовані на шахрайство чи незаконне здійснення користувачем.

# 1.3.2 Варіанти атак соціальної інженерії на мережу

У рамках цієї науки велика увага приділяється формалізованим операціям, які складають її основу, зокрема операціям складної комбінаторики. Недооцінка системного підходу до комбінаторних операцій призводить до серйозних наслідків на всіх рівнях трансформаційних процесів у суспільстві.

Атаки соціальної інженерії є особливо успішними проти тих, хто ще не має досвіду з такими видами атак і не обізнаний щодо потенційних загроз і шахрайських намірів. У цьому контексті, важливо розуміти, що соціальна інженерія використовує психологічні методи та маніпуляцію, щоб отримати доступ до конфіденційної інформації. Зазвичай, атаки соціальної інженерії можуть бути розділені на чотири основні кроки[9]:

Претекстінг - це набір дій, відпрацьованих за певним, заздалегідь

складеним сценарієм, в результаті якого жертва може видати будь-яку інформацію або вчинити певну дію. Найчастіше даний вид атаки передбачає використання голосових засобів, таких як Skype, телефон і т.п. Для використання цієї техніки зловмисникові необхідно спочатку мати деякі дані про жертви (ім'я співробітника; посаду; назва проектів, з якими він працює; дату народження). Зловмисник спочатку використовує реальні запити з ім'ям співробітників компанії і, після того як увійде в довіру, отримує необхідну йому інформацію.

Фішинг – техніка інтернет - шахрайства, спрямована на отримання конфіденційної інформації користувачів – авторизаційних даних різних систем. Основним видом фітингових атак є підроблений лист, відправлений жертві по електронній пошті, який виглядає як офіційний лист від платіжної системи або банку. У листі міститься форма для введення персональних даних (пін-код, логін і пароль і т.п.) або посилання на web-сторінки, де розташовується така форма. Причини довіри жертви до подібних сторінок можуть бути різні: блокування облікового запису, поломка в системі, втрата даних та інше.

Троянський кінь - це техніка ґрунтується на цікавості, страху або інших емоціях користувачів. Зловмисник відправляє лист жертві за допомогою електронної пошти, як додаток до якого знаходиться «оновлення» антивірусу, ключ до грошового виграшу або компромат на співробітника. Насправді ж у вкладенні знаходиться шкідлива програма, яка після того, як користувач запустить її на своєму комп'ютері, буде використовуватися для збору або заміни інформації зловмисником.

Послуга за послугу - дана техніка передбачає звернення зловмисника до користувача по електронній пошті або корпоративному телефону. Зловмисник може представитися, наприклад, співробітником технічної підтримки та інформувати про виникнення технічних проблем на робочому місці. Далі він повідомляє про необхідність їх усунення. У процесі «рішення» такої проблеми, зловмисник підштовхує жертву на вчинення дій, що дозволяють атакуючому виконати певні команди або встановити необхідне програмне забезпечення на комп'ютері жертви.

Дорожнє яблуко - цей метод є адаптацію троянського коня і полягає у використанні фізичних носіїв (CD, флеш-накопичувачів). Зловмисник зазвичай підкидає такий носій в загальнодоступних місцях на території компанії (парковки, столові, робочі місця співробітників, туалети). Для того, щоб у співробітника виник інтерес до даного носія, зловмисник може нанести на носій логотип компанії і якусь підпис. Наприклад, «дані про продажі», «зарплата співробітників», «звіт в податкову» і інше.

Зворотня соціальна інженерія - даний вид атаки спрямований на створення такої ситуації, при якій жертва змушена буде сама звернеться до зловмисника за «допомогою». Наприклад, зловмисник може вислати лист з телефонами і контактами «служби підтримки» і через деякий час створити оборотні неполадки в комп'ютері жертви. Користувач в такому випадку подзвонить або зв'яжеться по електронній пошті із зловмисником сам, і в процесі «виправлення» проблеми зловмисник зможе отримати необхідні йому дані.

Плечовий серфінг - це метод, який застосовується у громадських місцях, що дозволяє зловмиснику спостерігати за комп'ютерами та телефонами потенційних жертв, стоячи позаду них. Іноді користувачі самі надають зловмиснику потрібну інформацію, вважаючи, що вони мають справу з порядною особою. У таких випадках можна говорити про зворотну соціальну інженерію.

Служби миттєвого обміну повідомленнями - сьогодні всі користувачі використовують служби миттєвого обміну повідомленнями, такі як Skype, Viber, WhatsApp, Telegram та інші, для спілкування у режимі реального часу. Ці служби є вразливими для різноманітних атак через їх широку доступність та швидкість. З метою безпеки рекомендується ігнорувати повідомлення від невідомих користувачів, утримуватися від надання особистої інформації та не переходити за посиланнями, надісланими ними.

# 1.4 Існуючі методи захисту локальної мережі підприємства від

**атак соціальної інженерії**

Отримання достатнього рівня захисту локальної мережі підприємства від атак соціальної інженерії вимагає комплексного підходу:

Навчання та освіта персоналу. Організація регулярних тренінгів та навчальних семінарів для своїх співробітників, щоб вони могли розпізнавати й уникати атак соціальної інженерії. Необхідно навчити персонал самостійно впізнавати підозрілі ситуації, які можуть включати небажаний електронний лист, підозрілі посилання або незаплановані відвідини невідомих осіб.

Системи виявлення вторгнень (IDS) та запобігання вторгнень (IPS): Встановлення IDS/IPS дозволяє виявляти та блокувати підозрілу активність в мережі, включаючи атаки соціальної інженерії. Ці системи можуть аналізувати мережевий трафік та спостерігати за незвичайними або підозрілими діями.

Системи антиспаму та антивірусного захисту для фільтрації та виявлення шкідливих електронних повідомлень. Це допоможе уникнути прийняття шкідливих вкладень або натискання на посилання, які можуть викликати атаку соціальної інженерії.

Зміцнення політик безпеки. Розробка і реалізація політик безпеки, що охоплють аспекти, пов'язані з соціальною інженерією. Вона може включати правила щодо розголошення конфіденційної інформації, обмеження доступу до даних і ресурсів, а також встановлення процедур перевірки та підтвердження запитів.

Збільшення свідомості про фішинг. Вчіть співробітників розпізнавати фішингові атаки. Попереджайте їх про загрозу, яку становлять підозрілі електронні повідомлення, вимагаючи негайних дій або надання конфіденційної інформації. Використовуйте симуляції фішингу для оцінки готовності персоналу та виявлення слабких місць.

Сильна аутентифікація: Використовуйте багатофакторну аутентифікацію для збільшення безпеки. Додатковий фактор, такий як одноразовий пароль, біометричні дані або фізичний токен, може ускладнити спроби несанкціонованого доступу до системи.

Моніторинг та виявлення загроз: Встановіть системи моніторингу та виявлення, які спроможні виявляти незвичайну або підозрілу активність у мережі. Вони можуть виявити намагання перехопити дані, виконати фішинг-атаку або отримати несанкціонований доступ до систем.

Фаєрвол (firewall) виконує важливу роль у захисті мережі від атак соціальної інженерії. Основна функція фаєрволу - контрольувати трафік, який входить і виходить з мережі, і застосовувати набір правил для фільтрації цього трафіку. Ось як фаєрвол сприяє захисту від атак соціальної інженерії.

Ці методи слід розглядати як частину комплексного підходу до безпеки мережі. Кожен підприємство має унікальні потреби, тому важливо пристосувати стратегії до своєї конкретної ситуації.

**Висновок до розділу 1**

У даному розділі описані основні теоретичні аспекти корпоративної локальної мережі, а також вивчено проблематику соціальної інженерії, різні типи кібератак і методи захисту від них. Під час дослідження було з'ясовано, що кібератаки стають все складнішими та багатогранними, що вимагає постійного оновлення та удосконалення методів захисту.

Були проаналізовані різні види атак, такі як фішинг, фармінг, соціальний інжиніринг та інші, а також їхні можливі наслідки для корпоративної мережі. Для запобігання таким атакам було розглянуто різні методи захисту, включаючи використання міцних паролів, шифрування даних, встановлення файрволу та систем виявлення вторгнень.

# 2 ДОСЛІДЖЕННЯ ІСНУЮЧИХ ЗАСОБІВ ПРОТИДІЇ АТАКАМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Соціальна інженерія є суттєвим аспектом в області кібербезпеки, і для захисту від неї також існують різноманітні технічні засоби.

Існує багато різноманітних методів для захисту мережі від атак соціальної інженерії. Кожен з цих методів використовується для певних цілей в певному секторі та має свої переваги та обмеженняє.

В даному розділі буде проведено аналіз таких систем як: системи антиспаму

Microsoft Exchange Online Protection та Symantec Email Security, система виявлення вторгненнь Cisco Stealthwatch та фреймворк для перевірки навченості на навчання персоналу GoPhish.

# 2.1 Symantec Email Security

Symantec Email Security, розроблений компанією Symantec (тепер - частина Broadcom Inc.), є комплексним рішенням для захисту електронної пошти від шкідливих атак, спаму, фішингу та інших загроз безпеці. Цей продукт надає широкий спектр функцій та технологій для забезпечення безпеки електронної комунікації в організаціях.

Symantec Email Security був створений для забезпечення захисту електронної пошти в організаціях. Основною метою цього рішення є запобігання шкідливим атакам, спаму, фішингу та іншим загрозам, які можуть впливати на безпеку та конфіденційність електронної комунікації.

Цей продукт допомагає організаціям зменшити ризик витоку конфіденційної інформації, зберегти продуктивність працівників шляхом зменшення кількості спаму та шкідливих повідомлень, а також запобігти вірусним атакам та фішинговим атакам, які можуть призвести до фінансових втрат або порушення репутації.

Функціональні можливості Symantec Email Security (Symantec.cloud) включають:

Фільтрація спаму: Система виявляє та блокує небажані електронні повідомлення, що включають спам, фішингові листи, небезпечні посилання та шкідливі вкладення.

Антивірусний захист: Вбудований антивірусний двигун сканує електронні повідомлення для виявлення та блокування вірусів, троянів, черв'яків та інших шкідливих програм.

Захист від атак пошти: Система виявляє та блокує атаки, спрямовані на електронну пошту, такі як атаки з використанням вразливостей, DDoS атаки та атаки з викраденням облікових даних.

Захист від витоку даних: Symantec Email Security надає можливості для виявлення та запобігання витоку конфіденційної інформації через електронну пошту, включаючи відстеження та блокування небезпечних даних.

Фільтрація контенту: Система дозволяє налаштовувати правила для фільтрації контенту в електронних повідомленнях, включаючи блокування небажаного вмісту, фільтрацію образливих слів, контроль використання конфіденційної інформації тощо.

Архівування пошти: Симантек Email Security може забезпечувати архівування електронної пошти для збереження та пошуку повідомлень згідно з внутрішніми та законодавчими вимогами.

Аналітика та звітність: Система надає засоби для моніторингу, аналізу та генерації звітів про активність електронної пошти, виявлення загроз[10].

Symantec Email Security має кілька ключових переваг:

Комплексний захист: Symantec Email Security надає широкий спектр захисних функцій, що охоплюють різні типи загроз, такі як спам, фішинг, віруси, шкідливі вкладення та соціальна інженерія. Це дозволяє організаціям мати повний контроль над безпекою електронної комунікації.

Ефективне виявлення загроз: Розвинуті аналітичні алгоритми та механізми машинного навчання Symantec Email Security дозволяють виявляти навіть найновіші та складні загрози. Вона використовує бази даних загроз, експертні правила та аналіз поведінки для раннього виявлення та блокування шкідливих повідомлень.

Автоматизація та інтелектуальність: Symantec Email Security використовує автоматизовані процеси для ефективного розпізнавання та обробки загроз. Вона здатна автоматично виконувати дії, такі як блокування спаму, карантинування шкідливих вкладень та сповіщення про підозрілі активності, що допомагає зменшити навантаження на адміністраторів та підвищує ефективність процесу захисту.

Розширені можливості аналізу та звітності: Symantec Email Security надає детальну аналітику трафіку електронної пошти, яка дозволяє організаціям розуміти загрози, виявляти тренди та здійснювати стратегічне планування для покращення безпеки. Також надаються розширені засоби звітності, які допомагають оцінювати ефективність захисту та виявляти потенційні проблеми.

Швидка інтеграція та підтримка: Symantec Email Security пропонує простий процес встановлення та налаштування, що дозволяє швидко запроваджувати захист електронної пошти в організації. Крім того, підтримка Symantec забезпечує постійну підтримку та оновлення продукту для забезпечення найвищого рівня безпеки.

Також запобігає витоку даних у масштабах підприємства за допомогою інтеграції із Symantec Data Loss Prevention і засобів контролю шифрування на основі політики.

Незважаючи на переваги, Symantec Email Security також має деякі недоліки, які варто врахувати:

Складність налаштування. Встановлення та налаштування Symantec Email Security може бути складним процесом для користувачів з обмеженим досвідом в області кібербезпеки. Вимагається налагодження правильних правил фільтрації та налаштування параметрів, щоб досягти оптимального рівня захисту.

Можливість фальшивих позитивів та негативів. Іноді Symantec Email Security може помилково визнавати легітимні повідомлення як загрози (фальшиві позитиви) або не виявляти деякі шкідливі повідомлення (фальшиві негативи). Це може призвести до втрати важливих повідомлень або небажаних перерв у роботі користувачів.

Потреба в постійних оновленнях. Швидко змінююча ситуація з кіберзагрозами вимагає постійних оновлень та патчів для Symantec Email Security, щоб забезпечити ефективну захист. Це може вимагати регулярного оновлення програмного забезпечення та контролю з боку адміністратора системи.

Вплив на продуктивність: Використання Symantec Email Security для обробки великого обсягу електронних повідомлень може впливати на продуктивність системи. Відсутність оптимальної конфігурації та масштабування може призвести до зниження швидкості доставки повідомлень та роботи поштових серверів.

Вартість: Symantec Email Security є комерційним продуктом, і його впровадження та підтримка можуть бути пов'язані з витратами. Вартість ліцензування та підтримки може варіюватися залежно від обсягу і потреб організації.

# 2.2 Microsoft Exchange Online Protection

Microsoft Exchange Online Protection – хмарна служба забезпечення безпеки електронної пошти, яку надає компанія Microsoft. Вона призначена для захисту організацій від різних загроз, пов'язаних з електронною поштою, зокрема спаму, шкідливих програм, фішингових атак та інших зловмисних дій. Є частиною Microsoft 365 і надає потужні функції безпеки для захисту електронної комунікації бізнесів [11].

З підвищенням популярності хмарних послуг у 2010-х роках, Microsoft розпочала перехід до хмарної моделі з випуском Microsoft Office 365. Як частина Office 365, Exchange Online став ключовим сервісом для керування електронною поштою в хмарі. У рамках Exchange Online впроваджено Exchange Online Protection як основний засіб забезпечення безпеки електронної пошти. Розвиток Exchange Online Protection: З часом Microsoft розширила функціональні можливості Exchange Online Protection, додавши продуктивність фільтрації спаму, виявлення та блокування фішингових атак, а також захист від вторгнень та адаптивні функції аналізу поведінки.

Сьогодні Exchange Online Protection є однією з провідних хмарних послуг забезпечення безпеки електронної пошти, яка надається корпорацією Microsoft.

Основні функції Microsoft Exchange Online Protection включають:

Фільтрацію спаму та шкідливих програм: EOP використовує передові алгоритми фільтрації для виявлення та блокування спаму та повідомлень, що містять шкідливі програми або віруси. Вона аналізує вміст електронних листів, вкладення та репутацію відправника для визначення законності вхідних повідомлень.

Фільтрацію контенту: EOP дозволяє адміністраторам визначати власні політики фільтрації контенту для керування потоком електронних листів на основі певних критеріїв, таких як ключові слова, вкладення та типи файлів. Це допомагає запобігати поширенню чутливого або неприпустимого контенту всередині організації.

Захист від фішингу та підробки: EOP застосовує різні техніки для виявлення та блокування фішингових атак та підробки електронних листів. Вона аналізує заголовки електронної пошти, відомості про відправника та зміст повідомлення для виявлення підозрілих патернів або характеристик, що часто пов'язані з фішинговими атаками.

Фільтрацію підключень: EOP використовує фільтрацію підключень для блокування або дозволу підключень електронної пошти на основі репутації IP-адрес, доменів та інших факторів. Це допомагає блокувати підключення з відомих зловмисних джерел або спамерів.

Шифрування повідомлень: EOP підтримує шифрування повідомлень для забезпечення безпеки та конфіденційності чутливої інформації. Вона використовує протокол Transport Layer Security (TLS) для шифрування комунікації електронної пошти між серверами і може інтегруватися з Microsoft Information Protection (MIP) для покращеного захисту даних.

Звітність та моніторинг: EOP надає детальні звіти та можливості моніторингу, які допомагають адміністраторам відстежувати потік електронної пошти, виявляти потенційні загрози та отримувати уявлення про тенденції в області безпеки електронної пошти. Вона надає видимість ефективності механізмів фільтрації та дозволяє активне управління безпекою електронної пошти.

Загалом, функціонал Microsoft Exchange Online Protection такий же що й у Symantec Email Security.

Основні плюси Microsoft Exchange Online Protection:

Висока ефективність фільтрації: EOP використовує потужні алгоритми та механізми фільтрації, що дозволяють ефективно виявляти і блокувати спам, шкідливі програми, віруси та інші загрози електронної пошти. Це допомагає знизити кількість небажаної пошти та зберегти час та ресурси користувачів.

Надійний захист від фішингу та підробки: EOP використовує розумні алгоритми для виявлення фішингових атак та підробки. Він аналізує електронну пошту, заголовки повідомлень та поведінку відправників, щоб ідентифікувати підозрілі патерни та запобігти небезпечним ситуаціям.

Легка інтеграція з Microsoft Exchange та Microsoft 365: EOP безперешкодно інтегрується зі службами Microsoft Exchange та Microsoft 365. Він надає надійний і додатковий рівень захисту для організацій, які використовують ці платформи для електронної пошти та спільної роботи.

Гнучкі настройки та настроювання: EOP дозволяє адміністраторам налаштовувати політики фільтрації, встановлювати правила доступу та керувати налаштуваннями безпеки електронної пошти. Це дозволяє підлаштувати захист під конкретні потреби та вимоги організації.

Постійні оновлення та підтримка: Microsoft постійно оновлює та покращує Exchange Online Protection, забезпечуючи захист від нових видів загроз та вразливостей. Користувачі отримують доступ до останніх оновлень та підтримки для забезпечення безпеки своїх електронних листів.

Управління спамом та захистом на рівні організації: EOP надає можливість налаштовувати політики фільтрації та керувати спамом та безпекою на рівні всієї організації. Це спрощує управління та забезпечує єдиночасний захист для всіх користувачів.

Недоліки Microsoft Exchange Online Protection:

Вимога до підключення до хмарної послуги: Оскільки EOP є хмарною послугою, вона вимагає наявності підключення до Інтернету для функціонування. Це може створити проблеми, якщо у вас виникають проблеми з підключенням або якщо у вас обмежена або нестабільна мережа.

Обмежені можливості настройки: Хоча EOP надає деякі можливості настройки політик фільтрації та захисту, інколи користувачам можуть бути потрібні більш гнучкі налаштування або спеціалізовані функції, які EOP не надає. В таких випадках може бути необхідно розглядати додаткові рішення або налаштовувати додаткові механізми захисту.

Затримки доставки: Іноді EOP може призвести до затримок у доставці електронних листів. Це може відбуватися через процес фільтрації та аналізу повідомлень, які призводять до додаткового часу, необхідного для доставки електронних листів. Хоча ці затримки зазвичай незначні, в окремих випадках вони можуть впливати на часові обмеження або нагальність комунікації.

Залежність від провайдера хмарної послуги: Використання EOP означає, що ви залежите від провайдера хмарної послуги, в даному випадку Microsoft. Це означає, що ви не маєте повного контролю над інфраструктурою та настройками захисту. Якщо виникають проблеми або недоліки з боку провайдера, це може вплинути на функціонування EOP.

Вартість: Використання Microsoft Exchange Online Protection вимагає плати за послуги, оскільки вона є комерційним продуктом. Це може створити фінансові обмеження для окремих організацій, особливо для менших підприємств або неприбуткових організацій.

# 2.3 Система виявлення вторгненнь Cisco Stealthwatch

Рішення для моніторингу та аналізу мережевої активності, яке призначене для виявлення та захисту від загроз кібербезпеки. Основною метою Cisco Stealthwatch є забезпечення безпеки мережі, виявлення аномальної поведінки, інцидентів та вторгнень, а також надання оперативної інформації для реагування на ці загрози.

Cisco Stealthwatch був інтегрований[12] з іншими рішеннями компанії Cisco, такими як мережеві комутатори та маршрутизатори, для отримання додаткової інформації про мережевий трафік та забезпечення більш повного моніторингу та захисту. Цей інструмент використовується для виявлення та захисту від різноманітних загроз кібербезпеки, включаючи атаки соціальної інженерії. Він надає функціональність для моніторингу та аналізу мережевої активності, що дозволяє виявляти незвичайні або підозрілі дії, включаючи такі, що пов'язані з соціальною інженерією.

Основні способи, якими Cisco Stealthwatch може допомогти в боротьбі з соціальною інженерією, включають:

Виявлення аномальної поведінки: Cisco Stealthwatch аналізує мережевий трафік та поведінку користувачів, пристроїв та додатків. Він може виявити незвичайні зміни у поведінці користувачів, такі як намагання отримати несанкціонований доступ до системи, пересилання конфіденційної інформації або спроби обхіду захисту. Це може допомогти виявити атаки соціальної інженерії, які базуються на маніпуляції поведінки користувачів.

Визначення аномальних комунікаційних зв'язків: Cisco Stealthwatch може виявити незвичайні або непривидні комунікаційні зв'язки між пристроями або мережевими сегментами, що може вказувати на соціальну інженерію. Наприклад, виявлення незвичайної взаємодії між пристроєм та екстернет-сервісом, або спроба підключення до важливих систем з неочікуваних джерел може свідчити про атаку, спрямовану на отримання несанкціонованого доступу або перехоплення даних.

Виявлення фішингу та шкідливих повідомлень: Cisco Stealthwatch може аналізувати мережевий трафік, що пов'язаний з електронною поштою та комунікаціями, для виявлення фішингових атак та розповсюдження шкідливих повідомлень. Він може виявити незвичайні шаблони поведінки або спроби використання соціальних інженерних технік для обману користувачів та отримання їхніх конфіденційних даних.

Аналіз поведінки користувачів: Cisco Stealthwatch може використовувати аналітику поведінки користувачів для виявлення незвичайних активностей, які можуть бути пов'язані з соціальною інженерією. Він може аналізувати звички, ролі та привілеї користувачів, щоб виявити зміни або підозрілі дії, які можуть свідчити про атаки або несанкціоновану діяльність.

Переваги Cisco Stealthwatch включають:

Виявлення загроз безпеки: Інструмент дозволяє виявляти незвичайну активність в мережі, таку як незвичайний трафік, аномальні поведінки користувачів або атаки на системи. Це дозволяє вчасно виявляти інциденти безпеки та вживати відповідні заходи.

Підвищення ефективності захисту: Інструмент допомагає виявляти загрози, які можуть пройти мимо інших методів захисту. Це зменшує кількість помилкових сповіщень про загрози та підвищує ефективність захисту мережі.

Візуалізація мережі: Інструмент надає візуальну карту мережі, яка дозволяє бачити всі з'єднання між комп'ютерами та пристроями в мережі. Це допомагає адміністраторам мережі краще розуміти мережеву топологію та виявляти проблеми з мережевим з'єднанням.

Інтеграція з іншими рішеннями Cisco: Cisco Stealthwatch може інтегруватися з іншими рішеннями безпеки Cisco, такими як Cisco Identity Services Engine, Cisco Firepower та Cisco Umbrella. Це дозволяє вирішувати проблеми безпеки в більш складних середовищах.

Широкі можливості аналізу: Інструмент пропонує широкі можливості аналізу мережевого трафіку, включаючи виявлення аномальних шаблонів та потенційно шкідливих дій. Це допомагає компаніям виявляти нові загрози та приймати проти них заходи.

Інтеграція з іншими системами безпеки: Інструмент може інтегруватися з іншими системами безпеки, такими як системи обліку подій та засоби контролю.

Незважаючи на свою ефективність, Cisco Stealthwatch також має деякі недоліки. Основні недоліки Cisco Stealthwatch включають:

Висока ціна: Cisco Stealthwatch є комерційним рішенням, і вартість його впровадження та підтримки може бути високою. Це може бути фінансовою перешкодою для менших компаній або організацій з обмеженими бюджетами.

Складність впровадження: Впровадження Cisco Stealthwatch може вимагати певних знань та експертизи в галузі мережевої безпеки. Це може бути складним завданням для компаній без достатнього персоналу або ресурсів для належної настройки та налагодження системи.

Обмежена сумісність: Cisco Stealthwatch оптимально працює з інфраструктурою Cisco, але може бути менш сумісним з продуктами інших виробників. Це може вимагати додаткових зусиль для інтеграції з існуючими системами та розширення функціональності.

Отже, Cisco Stealthwatch може бути корисним інструментом для аналізу мережевого трафіку, проте важливо враховувати деякі обмеження. Його встановлення та налаштування можуть виявитися складними завданнями. Крім того, важливо враховувати, що Cisco Stealthwatch може мати обмежену сумісність з продуктами інших виробників.

# 2.4 Фреймворк GoPhish

GoPhish - це відкритий фреймворк для проведення фішинг-кампаній та тестування безпеки електронної пошти в організаціях. Основною метою GoPhish є надання інструментів для створення та виконання фішинг-атак з метою підвищення рівня свідомості про безпеку серед співробітників.

Так як Gophish є проєктом з відкритим кодом, його репозиторій фреймворку знаходиться на Github[13]. Сам інструмент розроблений на мові програмування Go. Також існує графічний інтерфейс користувача, який дозволяє керувати фішинговими кампаніями та всім, що з ними пов'язано. За замовчуванням використовується база даних SqlLite.

Переваги Gophish включають:

Відкрите джерело: Gophish є програмним забезпеченням з відкритим кодом, що дозволяє користувачам переглядати, змінювати і вдосконалювати його функціональність за власним бажанням.

Безкоштовність: Gophish є повністю безкоштовним для використання всіма користувачами. Ви не маєте платити за ліцензію або витрачати кошти на придбання програми.

Створення фішингових кампаній: Gophish надає можливість легко створювати фішингові кампанії, включаючи створення шаблонів електронних листів, фішингових сторінок і керування списками адрес.

Моніторинг і аналітика: Інструмент надає детальну інформацію про результати фішингових кампаній, включаючи статистику переглядів, кліків і взаємодій користувачів з фішинговими матеріалами.

Тестування безпеки: Gophish дозволяє організаціям проводити тестування безпеки шляхом симуляції фішингових атак, щоб виявити слабкі місця в системі і покращити її безпеку.

Контроль над безпекою: Ви маєте повний контроль над всіма аспектами фішингових кампаній, включаючи відправлення листів, планування та моніторинг.

Налаштування і розширення: Gophish надає гнучкі налаштування і можливості розширення, що дозволяють вам відповідати вашим конкретним потребам і вимогам безпеки.

# 2.5 Порівняння розглянутих систем

Після дослідження різноманітних засобів протидії атакам фішингу вийшла таблиця для зіставлення їх можливостей(табл. 2.1):

Ці продукти відрізняються захистом, функціональністю та призначенням. Вибір конкретного рішення залежатиме від потреб вашої організації та вимог щодо захисту мережі та електронної пошти.

Таблиця 2.1

Порівняння інструментів для захисту локальної мережі від атак СО

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Symantec Email Security** | **Microsoft Exchange Online Protection** | **Cisco Stealthwatch** | **Gophish** |
| Функціональність | Висока | Висока | Висока | Середня |
| Захист від спаму | Так | Так | Так | Ні |
| Антивірусний захист | Так | Так | Так | Ні |
| Фільтрація контенту | Так | Так | Ні | Ні |
| Захист від фішингу | Так | Так | Ні | Так |
| Моніторинг мережі | Ні | Ні | Так | Ні |
| Виявлення загроз | Ні | Ні | Так | Ні |
| Керування політиками безпеки | Так | Так | Так | Ні |
| Система управління подіями та інцидентами | Ні | Ні | Так | Ні |
| Наявність UI | Так | Так | Так | Так |
| Вартість | Платна | Платна | Платна | Безкоштовна |
| Підтримка | Так | Так | Так | Обмежена |

Symantec Email Security:

Забезпечує ефективний захист від шкідливих електронних листів та спаму.Має інтуїтивний і легкий у використанні користувацький інтерфейс (UI). Пропонує аналітику та звітність щодо захисту електронної пошти. Підтримує міжнародні стандарти безпеки та регулятивні вимоги.

Microsoft Exchange Online Protection:

Забезпечує захист від спаму, вірусів та шкідливих посилань в електронній пошті. Інтегрований з Microsoft Exchange та іншими хмарними сервісами Microsoft. Надає зручний користувацький інтерфейс (UI) для керування настройками та перегляду звітів. Має розширені можливості по фільтрації та керуванню політиками безпеки.

Cisco Stealthwatch:

Призначений для виявлення та відповіді на загрози в мережі. Надає великий обсяг аналітичної інформації про мережевий трафік. Має потужні інструменти аналізу та візуалізації даних для виявлення незвичайної активності. Підтримує моніторинг в реальному часі та можливості розширеної аналітики.

Gophish:

Використовується для проведення фішингових кампаній з метою перевірки обізнаності персоналу. Має веб-інтерфейс (UI), що спрощує налаштування та управління кампаніями. Надає можливість створення персоналізованих шаблонів фішингових листів та відстеження взаємодії з ними. Підтримує аналіз результатів та звітність щодо успішності фішингових кампаній.

# Висновок до розділу 2

В результаті аналізу технічних методів захисту від соціальної інженерії

можна зробити наступний висновок:

Symantec Email Security - це комплексний рішення з електронної безпеки електронної пошти, яке призначене для захисту організацій від широкого спектру загроз, пов'язаних з електронною поштою. В цілому можна використовувати для блокуванн шкідливих посиланнь та вкладеннь, щоб переконатися, що вони не потрапляють у папку вхідних повідомлень ваших користувачів, для усунення атак за допомогою аналітики, яка забезпечує глибоке бачення цільових кампаній, для зменшення ризиків фішингу за допомогою вбудованих засобів оцінки безпеки та навчання. Також запобігає витоку даних у масштабах підприємства за допомогою інтеграції із Symantec Data Loss Prevention і засобів контролю шифрування на основі політики.

Microsoft Exchange Online Protection – хмарна служба забезпечення безпеки електронної пошти, яку надає компанія Microsoft. Вона призначена для захисту організацій від різних загроз, пов'язаних з електронною поштою, зокрема спаму, шкідливих програм, фішингових атак та інших зловмисних дій. Є частиною Microsoft 365 і надає потужні функції безпеки для захисту електронної комунікації бізнесів

Cisco Stealthwatch - це система моніторингу мережі, яка пропонує велику функціональність для аналізу великого обсягу мережевого трафіку і виявлення потенційних загроз у режимі реального часу. Stealthwatch має можливість інтеграції з іншими системами безпеки мережі, що робить його більш гнучким і забезпечує легкість розгортання та управління.

GoPhish - це відкритий фреймворк для проведення фішинг-кампаній та тестування безпеки електронної пошти в організаціях. Може сприяти збільшенню усвідомленості про кібербезпеку, підвищенню навичок розпізнавання фішингових атак та зменшенню ризиків, пов'язаних з несанкціонованим доступом до систем та інформації організації.

# 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДІВ ЗАХИСТУ МЕРЕЖІ ПІДПРИЄМСТВА ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

# 3.1 Аспекти роботи з GoPhish

Для розгортання GoPhish можна використовувати сервер з операційною системою Linux або Windows, доступний з Інтернету. Простий варіант - створити віртуальну машину на популярних хмарних платформах, таких як AWS, GCP, Azure або Digital Ocean. Ці платформи часто надають можливість отримати безкоштовні "кредити", яких достатньо для демонстрації GoPhish. Давайте розглянемо AWS як найпопулярніший варіант. Необхідно завантажити фреймфорк з офіційного сайту(рис. 3.1).

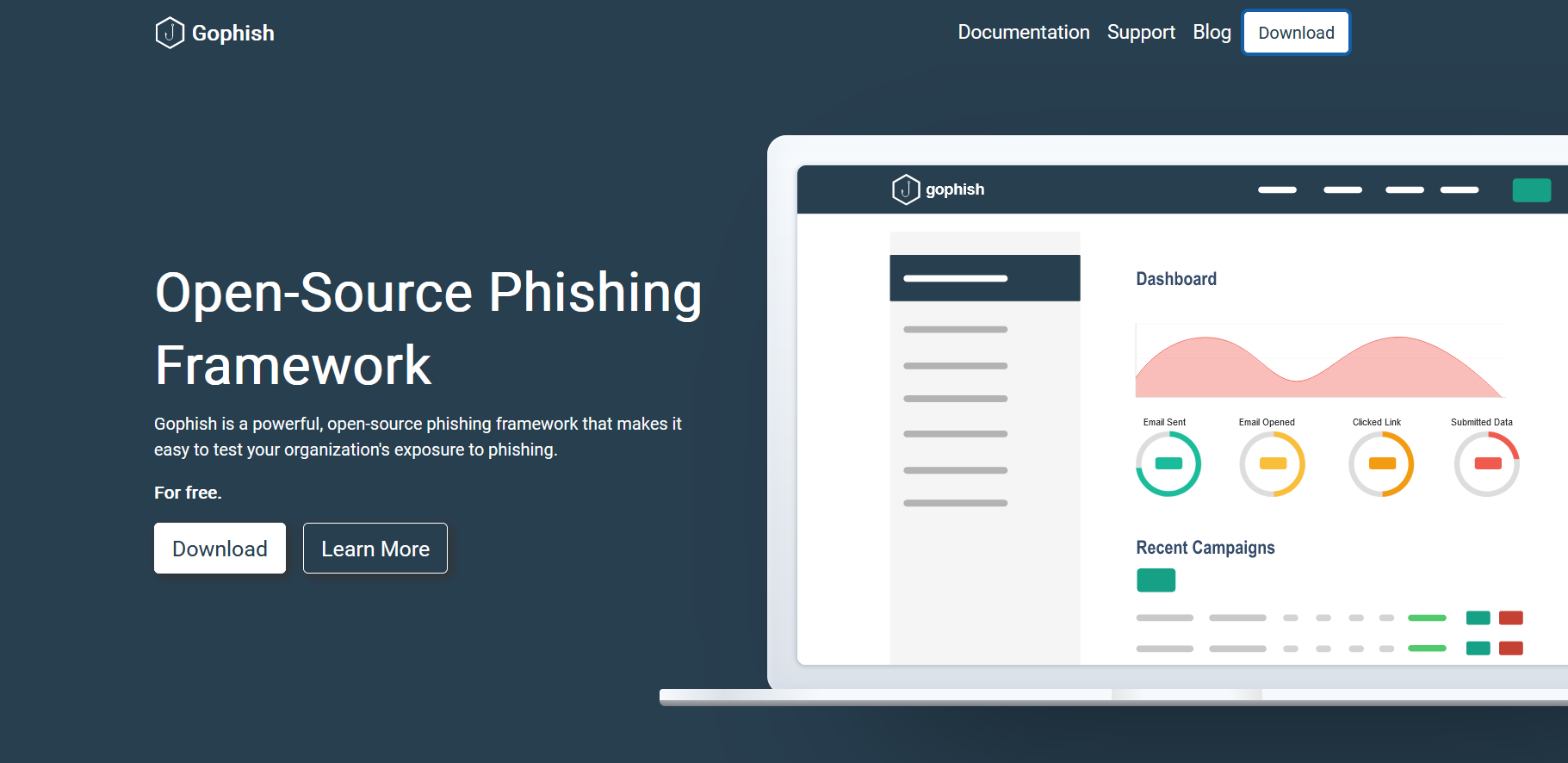


Рис. 3.1. Офіційний сайт GoPhish

# 3.1.1 Створення ВМ для розміщення GoPhish

Для створення нової віртуальної машини в AWS потрібно увійти до керуючої консолі EC2 і натиснути кнопку "Launch instances". Для демонстрації ми оберемо операційну систему Ubuntu(рис. 3.2).

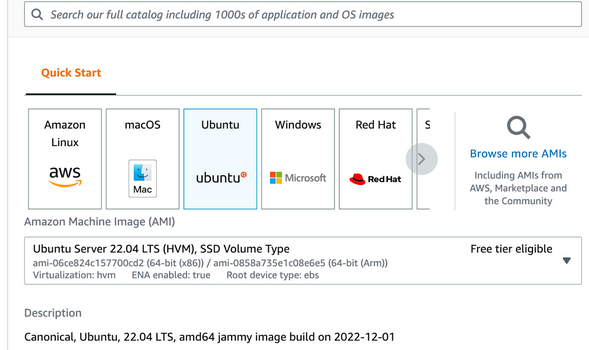


Рис. 3.2. Вибір створення ВМ за допомогою ЕС2

У розділі "Network Settings" треба вказати мережеві правила для доступу до нашої віртуальної машини. Для цього створимо нову групу безпеки і налаштуємо наступні правила:

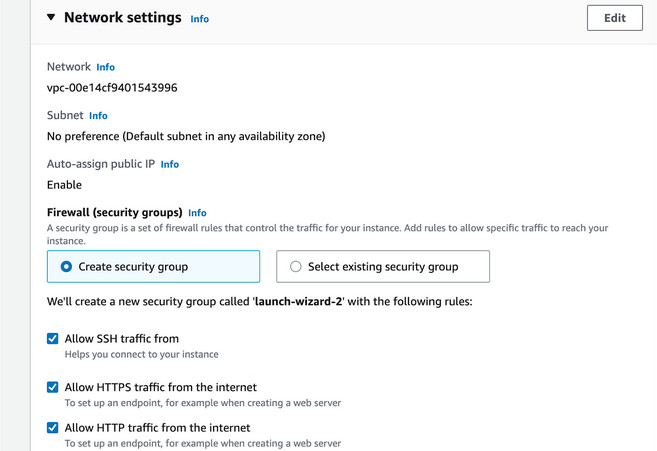
Надається дозвіл SSH трафік лише з вашої IP-адреси. Це забезпечить доступ до сервера лише з вказаної IP-адреси і зменшить ризик несанкціонованого доступу. Встановіть правило, яке дозволяє вхідні з'єднання SSH лише з вашої IP-адреси. Надається дозвіл HTTP і HTTPS трафік з будь-якої адреси Інтернету. Таким чином, фішингові сторінки, які будуть хоститися на сервері GoPhish, будуть доступні з будь-якої IP-адреси в Інтернеті. Встановіть правило, яке дозволяє вхідні з'єднання HTTP і HTTPS з будь-якої IP-адреси (рис. 3.3).

Рис. 3.3. Налаштування мережевих правил для ВМ

# 3.1.2 Встановлення та налаштування GoPhish

Створимо нову теку і перейдемо у неї(рис. 3.4):

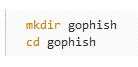


Рис. 3.4. Команди створення й переходу у теку

Зараз ми розпаковуємо вміст архівного файлу в поточну теку(рис. 3.5):



Рис. 3.5. Команда розпаковки вмісту

Необхідно отримати наступні файли й теки (рис. 3.6):



Рис. 3.6. Файли розпаковані з архіву необхідні для налаштування GoPhish

Тека "db" містить конфігураційні файли та міграції для баз даних. В теках "static" і "templates" знаходяться файли, що стосуються користувацького інтерфейсу. Файл "gophish" є бінарним файлом, який слід запускати. "config.json" - це файл, який містить налаштування інструменту[14]/

Файл конфігурації GoPhish визначає різні параметри та налаштування для фреймворку. Основні функції різних полів конфігурації включають:

admin\_server: Цей розділ визначає налаштування для сервера адміністрування GoPhish. listen\_url вказує IP-адресу та порт, на якому сервер прослуховує вхідні з'єднання. use\_tls вказує, чи використовувати шифроване з'єднання TLS.

phish\_server: Цей розділ визначає налаштування для сервера фішингу GoPhish. listen\_url вказує IP-адресу та порт, на якому сервер прослуховує вхідні з'єднання. use\_tls вказує, чи використовувати шифроване з'єднання TLS. landing\_page визначає, яку сторінку показувати "жертвам" після натискання на фішингове посилання.

db\_name та db\_path: Ці поля визначають ім'я бази даних GoPhish та шлях до бази даних на сервері(рис. 3.7).



Рис. 3.7. Файл конфігурації

Далі необхідно зробити файл "gophish" виконуваним на віртуальній машині, виконайте наступну команду(рис. 3.8):



Рис. 3.8. Команда надає файлу "gophish" право на виконання.

Далі запускаємо файл виключно з правами адміністратора (рис. 3.9):



Рис. 3.9. Команда запуску з правами адміністратора

В консолі ви бачите повідомлення з паролем для користувача "admin". Будь ласка, збережіть цей пароль в безпечному місці, оскільки він потрібний для першого входу в адміністративний інтерфейс Gophish Рис. 3.10.

Також, ви бачите повідомлення про старт фішингового сервера на порту 80 і старт адміністративного інтерфейсу на порту 3333. Це означає, що фішинговий сервер тепер активний і готовий до використання, а адміністративний інтерфейс доступний за адресою вашої віртуальної машини або локальної адреси з портом 3333.

Треба переконатись, що пароль збережено(Рис. 3.13) і звернути увагу на порти для доступу до фішингового сервера та адміністративного інтерфейсу (Рис. 3.10).

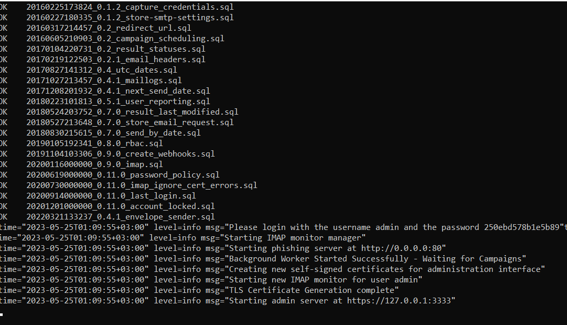


Рис. 3.10. Консоль запустила фреймворк та вивела данні для адміністратора

Далі необхідно на віртуальній машині відкрити браузер та ввести адресу що вказана у полі консолі “Starting admin server at” (Рис. 3.11.).

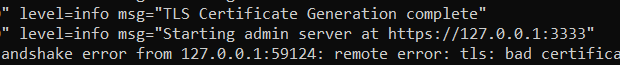


Рис. 3.11. Поле з потрібною адресою

Відкриття панелі адміністратора GoPhish було здійснено(Рис. 3.12).

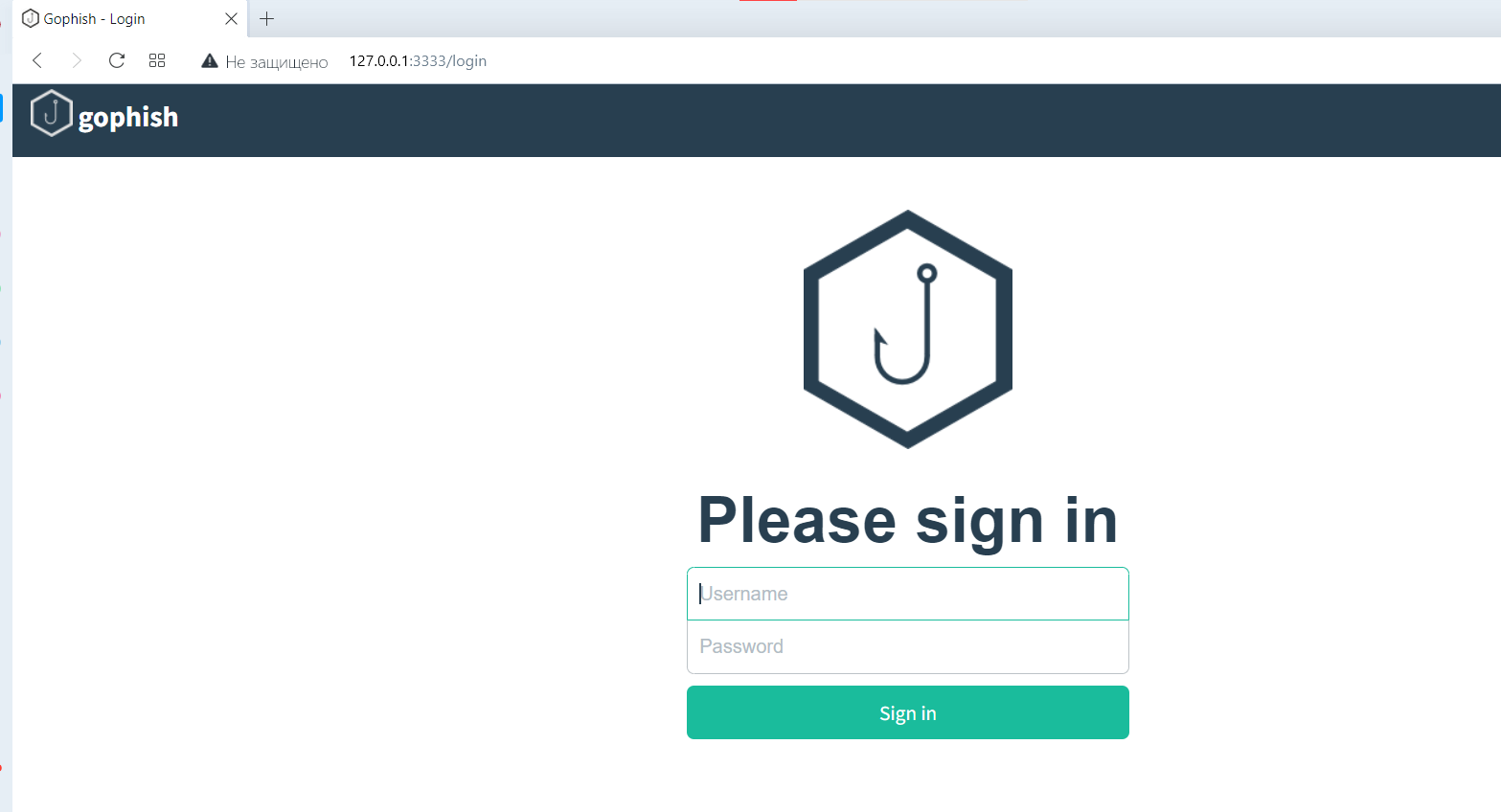


Рис. 3.12. Вікно входу до панелі адміністратора

Наступним кроком є використання тимчасового пароля з попереднього кроку для входу в "адмінку"(Рис. 3.13). Під час першого входу система попросить нас змінити цей тимчасовий пароль на власний.



Рис. 3.13. Повідомлення консолі про тимчасовий пароль

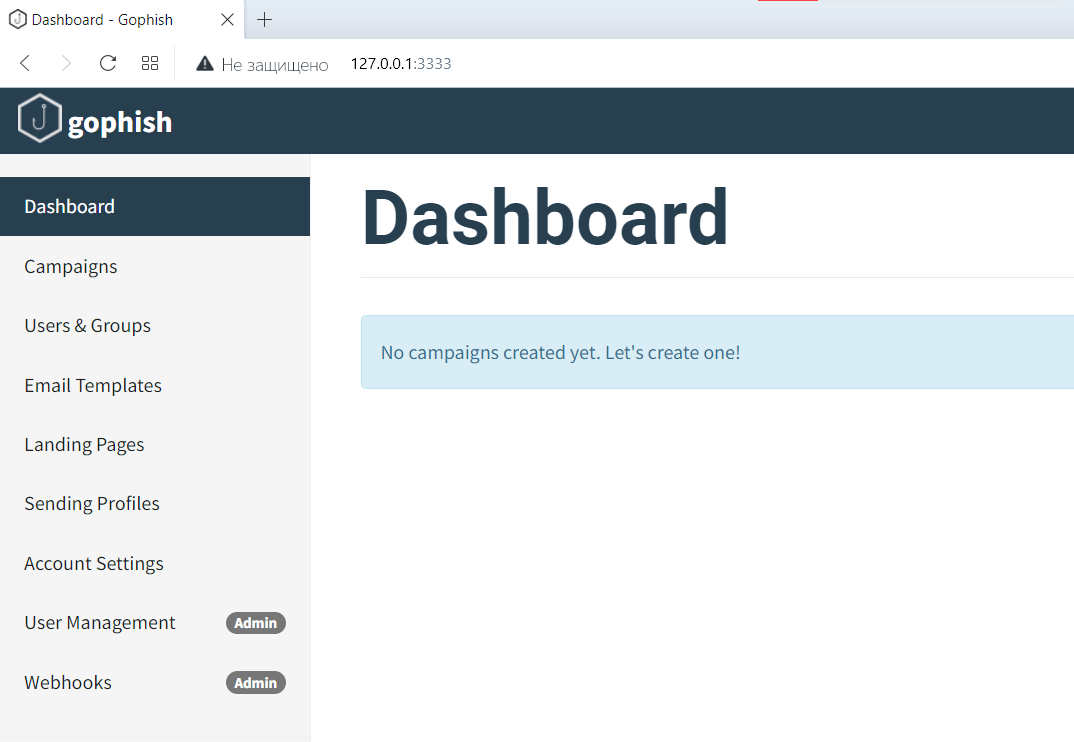
Після успішної авторизації ми будемо перенаправлені до інтерфейсу Gophish (Рис. 3.14).

Рис. 3.14. Інтерфейс адмінпанелі GoPhish

# 3.1.3 Налагодження фішингової кампанії GoPhish

HTML-сторінки, на які перенаправляють користувачі з фішингових посилань, є ключовою складовою відпрацювання заходів захисту від соціальної інженерії. Функціональність лендінгових сторінок дозволяє зберігати та отримувати дані, які надіслав користувач, що значно спрощує підготовку та аналіз отриманих відгуків.

У інтерфейсі створення Landing Page ви маєте можливість вручну додати HTML-сторінки або спробувати імпортувати сторінку безпосередньо з веб-сайту.

При цьому фреймворк автоматично переносить весь HTML-код у вигляд що зручний для редагування.

При створенні лендінгових сторінок для фішингових симуляцій важливо враховувати дизайн і контент, які будуть приваблювати та маніпулювати потенційну «цільову» аудиторію. Такі сторінки можуть імітувати авторитетні веб-ресурси, такі як банківські системи, соціальні мережі або електронна пошта провідних компаній. Вони можуть запропонувати введення особистої інформації, такої як логіни, паролі, фінансові дані або інші конфіденційні дані.

Додається нова сторінка, яка буде функціонувати як лендінгова сторінка, куди «цільовий» користувач потрапляє при переході з фішингового посилання. Ця сторінка написана на HTML і має можливість зберігати дані, які надіслав користувач, що значно спрощує процес підготовки(Рис. 3.15).

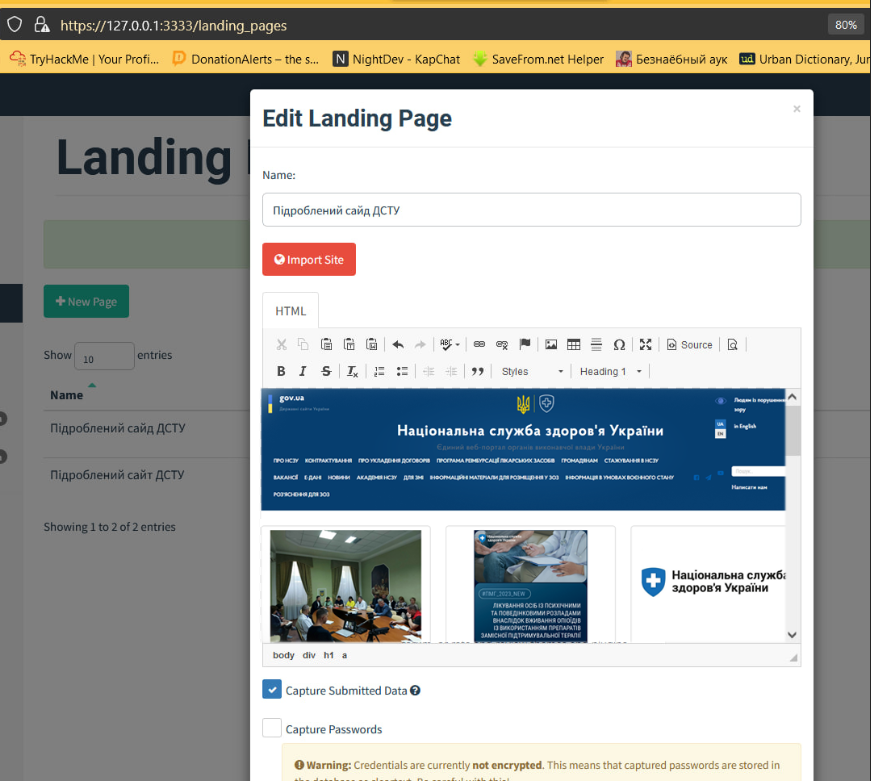


Рис. 3.15. – налаштована лендингова сторінка

У випадку зацікавленості в зборі логінів та паролів користувачів, ставляться галочки "Capture Submitted Data" і "Capture Passwords" у формі створення Landing Page. Додатково, вказується, щоб "ціль" перенаправлялась на сторінку профілю, щоб уникнути підозри, навіть після того, як користувач вже ввів свої дані. Також у полі переадресації вводиться адреса сторінки на яку буде переадресовано користувача після відправки данних (Рис. 3.16).

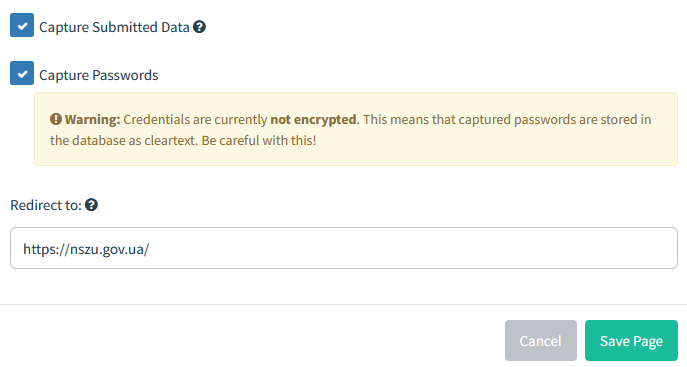


Рис. 3.16 – опції захоплення уведених данних та поле переадресації

Наступним кроком у плануванні атаки є підготовка фішингового листа, який має зацікавити та привести користувача на сторінку, яку ми вже створили.

Давайте спробуємо створити лист, який мотивує користувача перейти на фішингову сторінку та ввести свої облікові дані. Наприклад, можна повідомити користувача, що в результаті недавнього інциденту на платформі виникла необхідність перелогінитися для збереження доступу до особистого профілю. Для реалізації успішної кампанії потрібно проявити більшу креативність та прикласти більше зусиль.

Додатковою цікавою можливістю email-шаблонів є використання змінних, які дозволяють автоматично вставляти відповідні значення у конкретний лист, наприклад, ім'я чи адресу електронної пошти. Також існує можливість імпортувати вже наявний лист (Рис. 3.17).

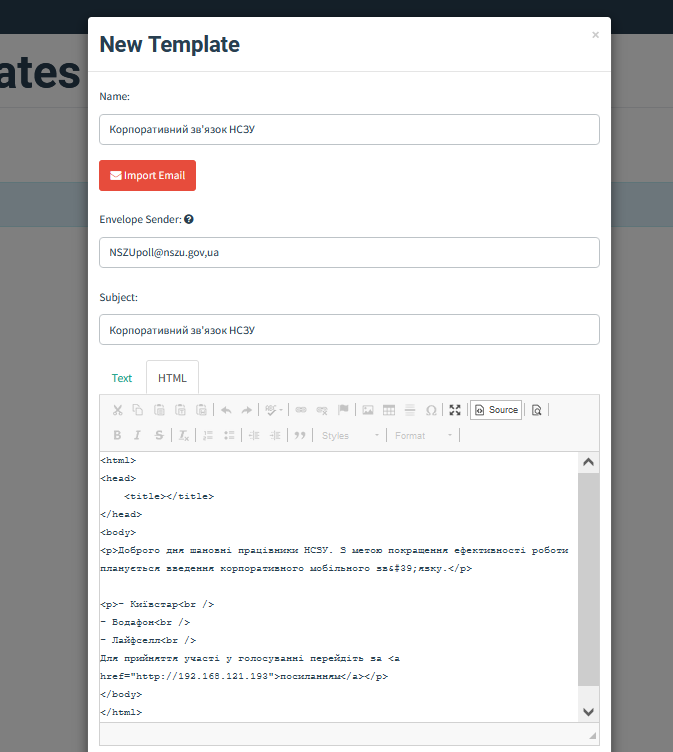


Рис. 3.17 Форма створення листа та HTML-код повідомлення

Для отримання статистики про відкриття електронного листа потенційними "жертвами", варто встановити прапорець "Add tracking image"(Рис. 3.18).

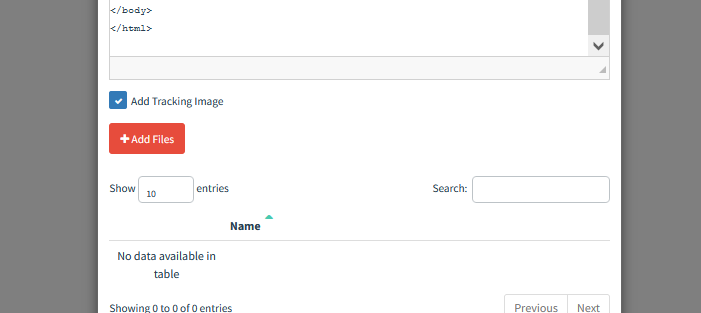


Рис. 3.18 – увімкнена опція статистики

Отриманий лист буде заблоковано з великою вірогідністю, тому необхідно в хмарній службі забезпечення безпеки електронної пошти та системі виявлення вторгнень до білого списку підмінену поштову адресу з якої відправляються повідомлення та IP-адресу віртуальної машини на якій хоститься GoPhish(Рис. 3.19).

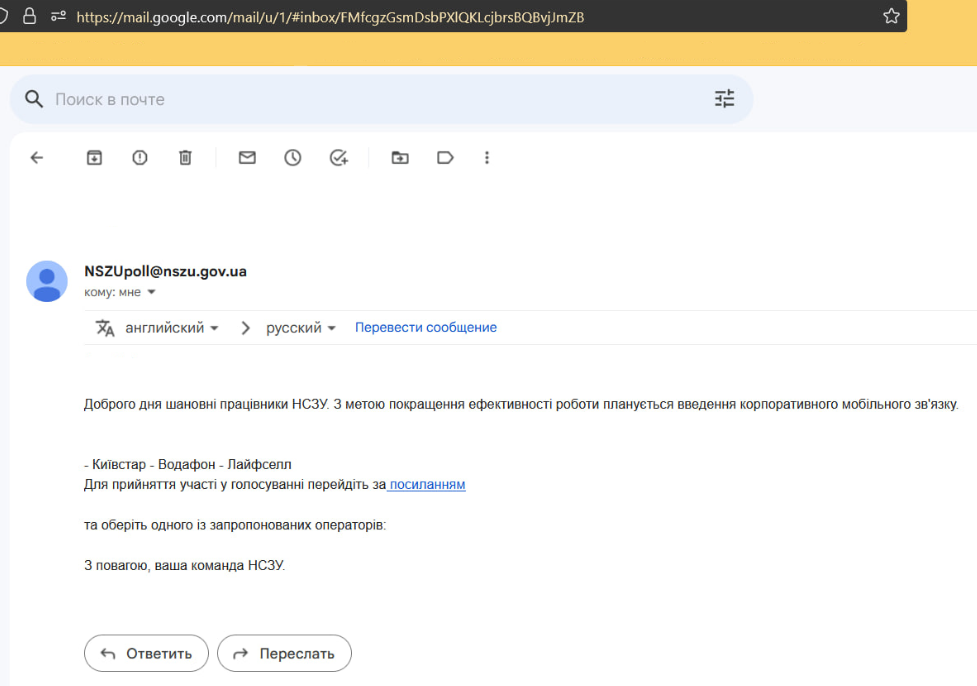


Рис. 3.19 – вигляд отриманого листа

# 3.1.4 Підключення до SMTP серверу

Далі, нам потрібен SMTP-сервер, який буде відправляти електронні листи. Gophish сам по собі не має такої функціональності. Для цього ми використали SMTP-сервіс email-розсилок Outlook (Рис. 3.20).

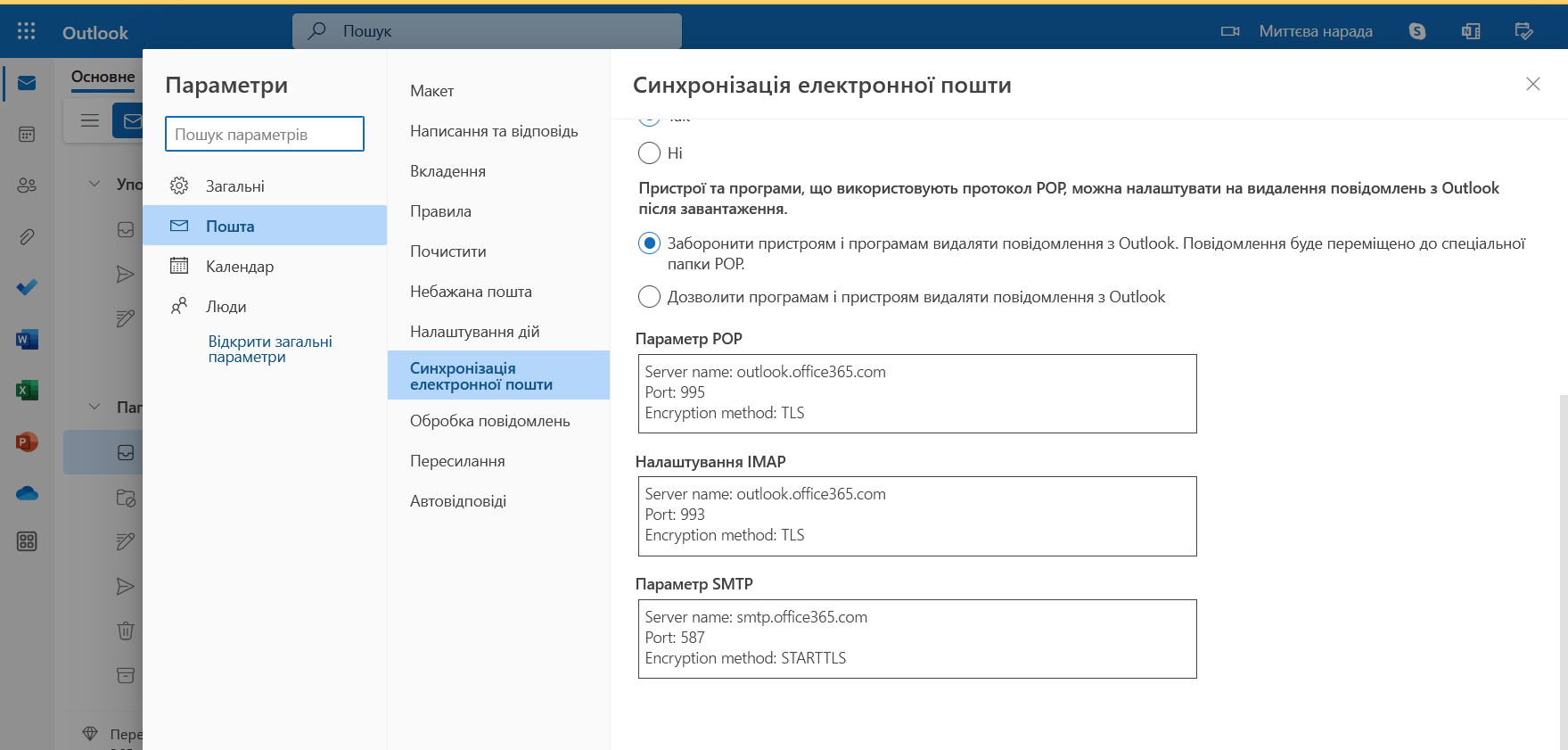


Рис. 3.20 – Параметр SMTP сервісу Outlook

Ця інформація знадобиться під час додавання профілю відправлення. Sending Profile (профіль відправлення) - це конфігураційний параметр в Gophish, який визначає налаштування для надсилання електронних листів під час фішингових кампаній. Використовуючи Sending Profile, ви можете визначити SMTP-сервер та облікові дані для автентифікації.

SMTP From – поштова адреса яку буде бачити отримувач.

Host – параметр адреси поштового хосту та порт що використовується. Username i Password – автентифікація на SMTP-сервері (Рис. 3.21).

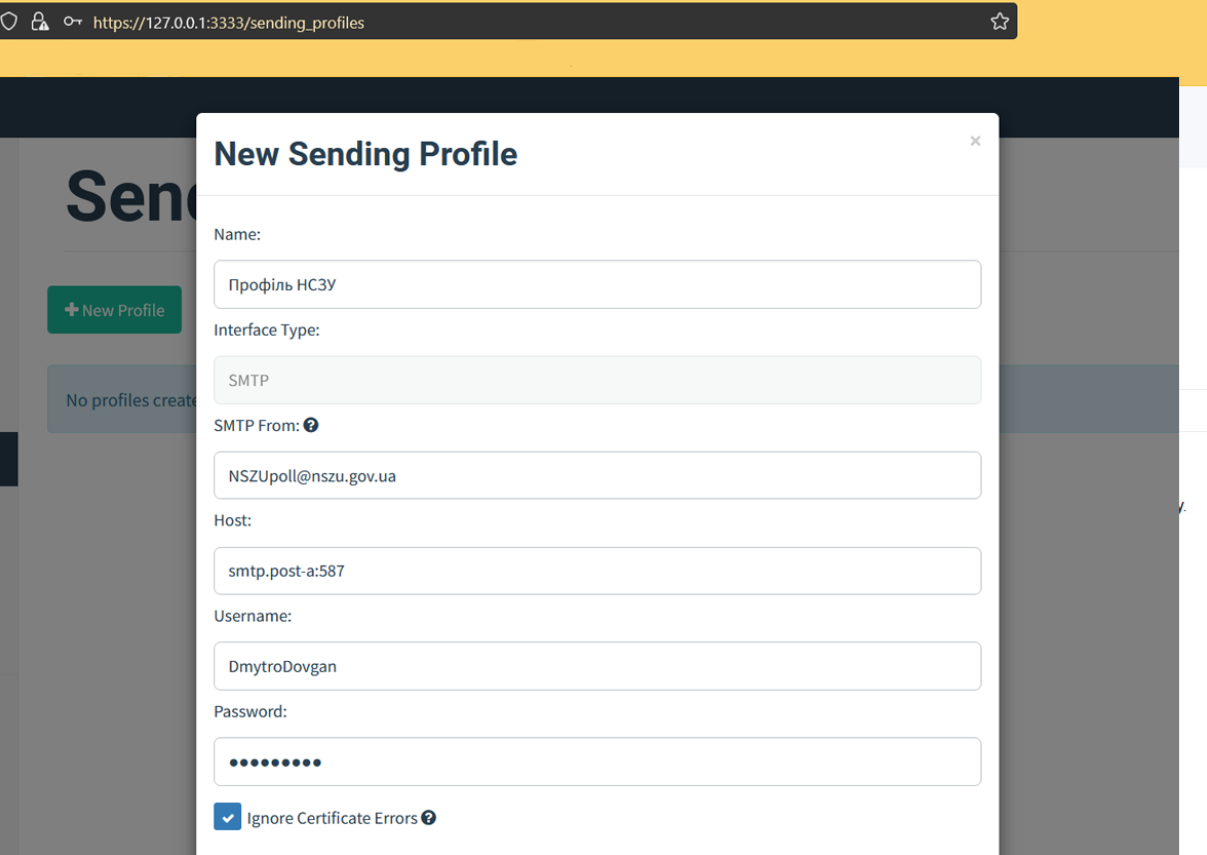


Рис. 3.21 – Профіль з параметрами відправлення

# 3.1.5 Створення списку цільових користувачів

Останнім кроком необхідно додати список електронних адрес, які стануть ціллю атаки. У формі створення нової групи можна додавати емейли по одному або імпортувати групу електронних пошт за допомогою csv-файлу (Рис. 3.22).

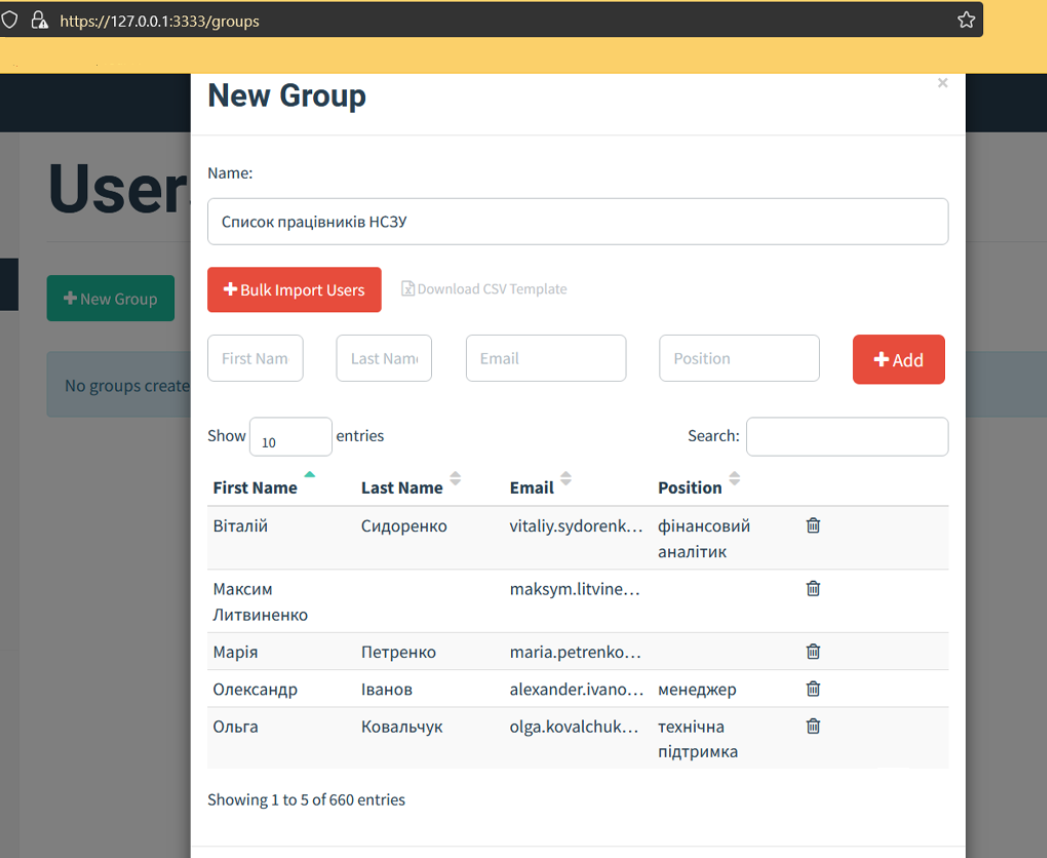


Рис. 3.22 – Список персоналу НСЗУ

# 3.2 Розгортання кампанії та аналіз результатів

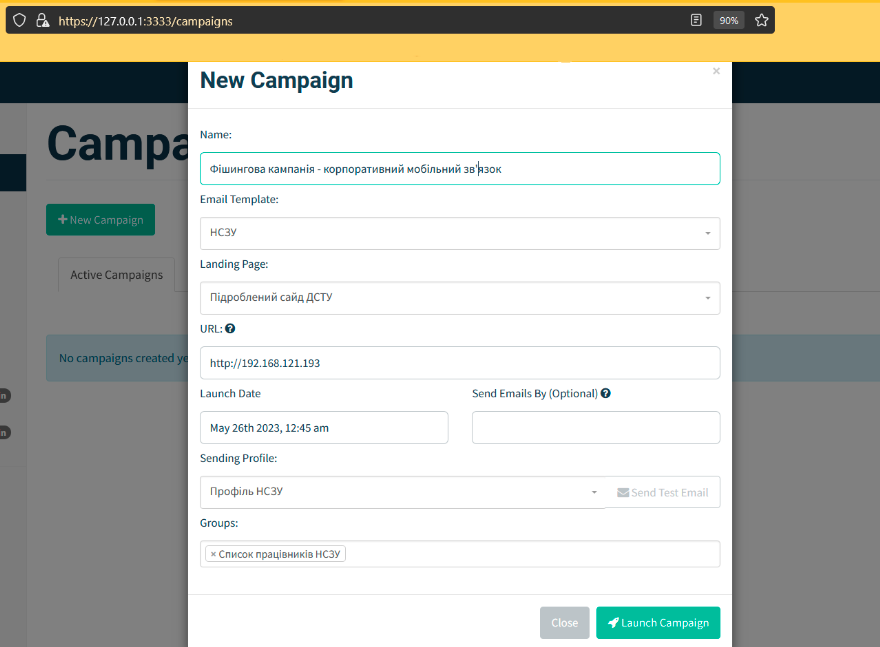
На формі створення вибираються попередньо додані електронні шаблони, сторінки-приманки, профіль відправлення та група електронних адрес для розсилки. Також потрібно вказати URL, де буде розміщена фішингова сторінка. У даному випадку використовується IP-адреса віртуальної машини, на якій розгорнутий Gophish(Рис. 3.23).

Рис. 3.23 – Фінальна конфігурація фішингової кампанії

Після запуску ми можемо переглядати докладну статистику та отримувати розширену інформацію про перебіг кампанії, включаючи дані про відкриття електронних листів, кліків на посилання, введення облікових данних, а також загальну ефективність кампанії(Рис. 3.24).

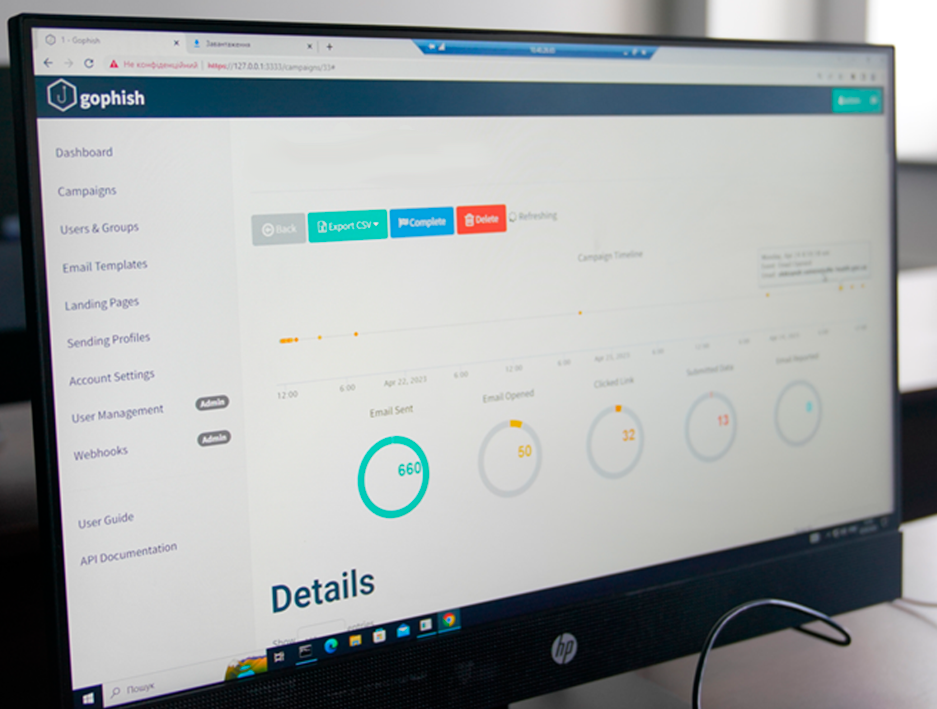


Рис. 3.24 – результати кампанії через два дні після запуску

Загальна кількість відправлених листів працівникам НСЗУ склала 660. З них 50 листів було відкрито, а 23 отримувачі натиснули на посилання в листі. В результаті цієї кампанії було скомпрометовано облікові дані 13 працівників(табл. 3.1).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Кількість відправлених листів** | **Працівники, що викрили фішинг** | **Кількість відкритих листів** | **Кількість натиснень на посилання** | **Кількість скомпрометованих облікових даних** |
| 660 | 574 | 50 | 23 | 13 |

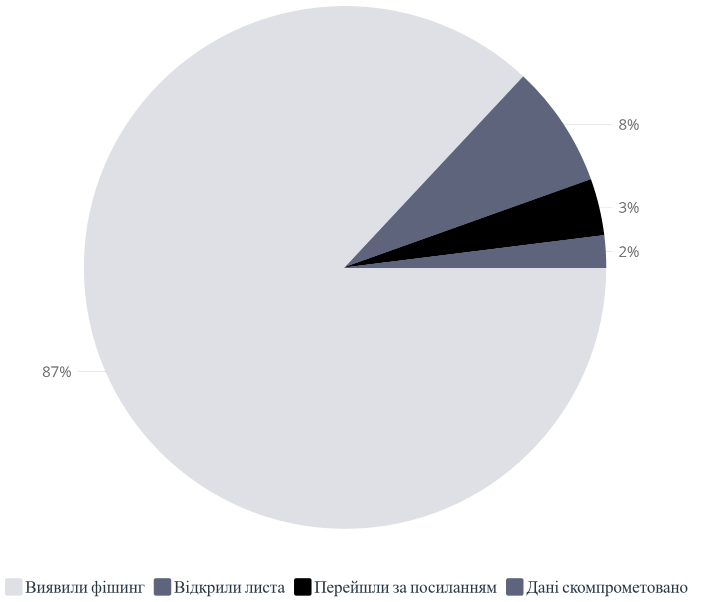


Рис. 3.25 – відсоткова діаграма реакції персоналу на фішингову кампанію

# 3.3 Розробка рекомендацій щодо використання GoPhish та підвищення обізнаності персоналу

# 3.3.1 Рекомендації щодо використання персоналом GoPhish

Персонал повинен бути ознайомлений з важливістю захисту конфіденційності та безпеки даних під час використання GoPhish. Важливо пояснити, що в симуляціях не повинні використовуватись реальні облікові дані, а всі дані повинні бути збережені в безпечному місці.

Працівникам необхідно пояснити, що ціллю використання Gophish є перевірка рівня їхньої обізнаності щодо фішингових атак та інших методів соціальної інженерії а також зазначити, що це робиться з метою забезпечення безпеки організації та її даних.

Забезпечення конфіденційності: Забезпечити працівників відомостями про те, що результати перевірки будуть триматися конфіденційними та використовуватися лише для внутрішньої оцінки та покращення безпеки. Пояснити, що жодні особисті дані не будуть використовуватися без їхньої згоди.

Інструктування щодо виявлення фішингових атак: Надати працівникам докладну інструкцію про ознаки та ідентифікацію фішингових атак. Пояснити, як розпізнати підозрілі листи, посилання та вкладення, а також як діяти, якщо вони стикаються з такими ситуаціями.

Персоналізовані навчальні матеріали: Розробити та надати працівникам навчальні матеріали, які відповідають їхнім конкретним обов'язкам та ризикам. Наприклад, для високопрофільних посад можуть бути важливі додаткові заходи безпеки.

3.3.2 Рекомендації щодо підвищення обізнаності персоналу

Компаніям потрібно, щоб співробітники отримували необхідні знання та могли застосовувати їх на практиці, ефективно працювали з інформаційною системою. Водночас, керівництво бажає мінімізувати перерви в роботі співробітників, пов'язані з навчанням, і щоб цей процес був оптимальним за часом і ресурсами.

У рамках підвищення безпеки та зменшення ризиків, пов'язаних з фішинговими атаками поштою, рекомендується розробити ефективну методику навчання та інструктажу персоналу. Ця методика повинна включати наступні аспекти:

Політика використання електронної пошти: Важливо встановити чіткі правила щодо використання електронної пошти, включаючи заходи безпеки проти віддалених атак, таких як віруси, хробаки і "трояни".

Фізичний захист: Персонал повинен бути навчений правильному використанню бейджиків та посвідчень як методу фізичного захисту. Це забезпечить контроль доступу до приміщень та обмежить несанкціонований доступ до інформації.

Протидія соціальній інженерії: Розробка методики для підвищення обізнаності персоналу щодо методів соціальної інженерії є ключовим аспектом. Працівники повинні бути навчені розпізнавати підступні техніки маніпулювання, що використовуються зловмисниками для отримання доступу до конфіденційної інформації. Регулярне навчання та періодичне тестування можуть допомогти зміцнити увагу та пильність співробітників.

Через це з’являється гостра необхідність розробки простої та ефективної методики підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії:

Розробка методичних вказівок: Створення детальних посібників та інструкцій, які містять основні принципи та практичні приклади протидії соціальній інженерії. Ці матеріали повинні бути доступними, легкими для розуміння та конкретно орієнтованими на ситуації, з якими співробітники можуть зіткнутися.

Розробка опитувального шаблону: Створення стандартизованого опитувальника, який використовується як метрика для оцінки ефективності методики підвищення обізнаності персоналу. Цей опитувальник дозволить виявити слабкі сторони у розумінні та вміннях співробітників щодо соціальної інженерії, а також визначити потреби в подальшому навчанні та покращенні (Рис.3.26.).

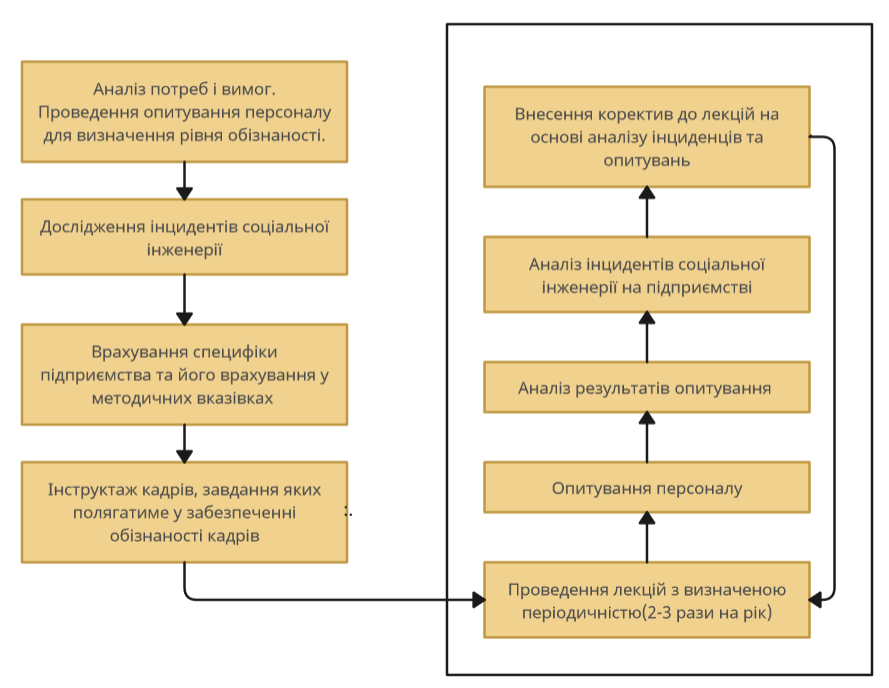


Рис.3.26 – Схема методики управління та покращення обізнаністі персоналу щодо протидії методам соціальної інженерії

Перший крок у розробці та впровадженні методики полягає в проведенні опитування на підприємстві, щоб визначити рівень обізнаності персоналу щодо протидії методам соціальної інженерії. Наступним кроком є аналіз інцидентів соціальної інженерії на підприємстві. З урахуванням результатів цього аналізу та специфіки підприємства (сфери діяльності, кількості співробітників, процесів зберігання та обробки конфіденційної інформації) вносяться виправлення до методичних вказівок та опитувальника.

Наступним етапом є проведення навчання з використання методики для співробітників підприємства, які будуть відповідальні за підвищення обізнаності персоналу щодо протидії методам соціальної інженерії на підприємстві. Цей ввідний навчальний процес включає:

Ознайомлення з метою та значенням методики управління обізнаністю персоналу щодо протидії методам соціальної інженерії.

Пояснення ключових термінів та понять, пов'язаних з соціальною інженерією.

Визначення загроз та ризиків, пов'язаних з методами соціальної інженерії.

Представлення методичних вказівок, які містять рекомендації та практичні поради щодо виявлення, запобігання та реагування на соціальну інженерію.

Навчання співробітників методам виявлення шахрайських схем, фішингових атак, підманювання та інших форм соціальної інженерії.

Практичні вправи та симуляції ситуацій, пов'язаних з соціальною інженерією, для покращення навичок виявлення та реагування на них.

Цей етап передбачає активну участь співробітників, їх взаємодію та можливість задавати питання для кращого розуміння та осмислення навчального матеріалу.

Наступним етапом є проведення ввідного інструктажу щодо користування методикою для співробітників, які будуть відповідальні за обізнаність персоналу у питаннях протидії методам соціальної інженерії на підприємстві. Ввідний інструктаж включає наступні компоненти:

Мета:

Забезпечити співробітникам необхідні знання та навички для виявлення, запобігання та реагування на методи соціальної інженерії.

Зменшити ризик використання соціальної інженерії для отримання несанкціонованого доступу до конфіденційної інформації підприємства.

Складові методики:

Ввідна лекція: Проведення першої лекції, яка служить прикладом для подальших лекцій на підприємстві. Ця лекція вводить співробітників у основні поняття та принципи протидії соціальній інженерії.

Правила користування опитувальником і метод аналізу результатів опитування: Розроблення інструкцій та правил для використання опитувальника та аналізу отриманих результатів. Це дозволяє оцінити рівень обізнаності персоналу та виявити слабкі місця, що потребують подальшого навчання.

Коригування лекцій: Аналіз результатів опитування для виявлення проблемних аспектів та корекції подальших лекцій. Цей процес дозволяє підвищити ефективність методики шляхом пристосування матеріалів до конкретних потреб та вимог підприємства.

Соціальна й економічна доцільність:

Методика сприяє зниженню ризику витоку конфіденційної інформації та потенційних фінансових втрат, що можуть бути спричинені методами соціальної інженерії.

Збільшує свідомість персоналу про потенційні загрози та покращує загальний рівень безпеки на підприємстві.

Методичний процес:

Опитування: Проведення опитування на початковому етапі для визначення рівня обізнаності персоналу.

Аналіз інцидентів соціальної інженерії: Вивчення інцидентів, які вже сталися на підприємстві, для врахування їх у методичних вказівках та опитувальнику.

Проведення ввідної лекції: Проведення першої лекції на підприємстві згідно з методичними вказівками.

Аналіз результатів опитування: Оцінка результатів опитування та ідентифікація слабких сторін обізнаності персоналу.

Корекція лекцій: Внесення змін у подальші лекції на основі аналізу результатів опитування для поліпшення ефективності методики.

Після цього процес впровадження методики продовжується на підприємстві співробітниками, які уповноважені управляти процесом обізнаності персоналу щодо протидії методам соціальної інженерії. Рекомендується проведення лекцій згідно з методичними вказівками двічі або тричі на рік, щоб забезпечити постійне оновлення знань та навичок персоналу.

Через 4-6 місяців після проведення лекції на підприємстві, проводиться аналіз інцидентів соціальної інженерії. Зважаючи на результати опитування персоналу та інформацію про інциденти, вносяться корективи до лекцій та опитувальника з метою більш детального врахування актуальних питань, пов'язаних з інцидентами соціальної інженерії на підприємстві.

Після внесення корекцій проводиться нова лекція на підприємстві, і процес повторюється. Таким чином, навчання персоналу відбувається кілька разів на рік. Аналіз результатів опитування та інцидентів соціальної інженерії надає можливість поетапного вдосконалення лекційного матеріалу з метою поступового підвищення рівня обізнаності персоналу та зниження кількості інцидентів соціальної інженерії на підприємстві до мінімуму.

# Висновок до розділу 3

В результаті практичної частини дипломної роботи було проведено фішингову кампанію на працівниках з метою оцінки їхньої обізнаності та вразливості перед методами соціальної інженерії. Ця кампанія дозволила отримати цінні дані про рівень усвідомленості загроз та вміння протидіяти їм у персоналу.

На основі отриманих результатів були сформульовані рекомендації щодо проведення інструктажу персоналу з метою підвищення обізнаності і захищеності від фішингу та інших методів соціальної інженерії. Рекомендації включають наступні аспекти:

Проведення регулярних навчань та інструктажів щодо методів соціальної інженерії, основних видів фішингу, ідентифікації шкідливих посилань та вкладень, а також процедур безпеки в роботі з електронною поштою та іншими комунікаційними каналами.

# ВИСНОВКИ

В сучасному світі це є особливо актуально, коли значна кількість працівників використовує комп'ютери та підключення до мережі для виконання своїх робочих обов'язків. Розробка та впровадження ефективних заходів захисту, таких як навчання персоналу, використання спеціалізованих програм та впровадження строгих політик безпеки, допоможуть забезпечити безпеку локальної мережі.

В даній дослідженні було зосереджено увагу на використанні засобів протидії атакам соціальної інженерії. Вивчено існуючі підходи до методів захисту від СО та їхньому використанні в різних сферах. Здійснено аналіз та порівняння чотирьох інструментів та систем: Symantec Email Security, Cisco Stealthwatch, Microsoft Exchange Online Protection та GoPhish.

Особливу увагу було приділено інструменту GoPhish. Було проведено встановлення та налаштування всіх необхідних компонентів а також фішингову кампанію, метою якої було визначити рівень обізнаності працівників.

У кінці дослідження були розроблені рекомендації, що стосуються ефективного використання інструменту GoPhish та проведення заходів з підвищення обізнаності персоналу. Ці рекомендації включають конкретні кроки щодо встановлення та налаштування GoPhish, а також оптимальні практики з організації фішингових кампаній. Крім того, надані поради щодо планування та проведення навчань з підвищення обізнаності персоналу, включаючи проведення регулярних навчань та інструктажів щодо методів соціальної інженерії, основних видів фішингу, ідентифікації шкідливих посилань та вкладень, а також процедур безпеки в роботі з електронною поштою.

Результати проведеної роботи свідчать про необхідність комплексного підходу до захисту мереж підприємств від соціально-інженерних загроз. Застосування інструменту GoPhish може виявитися ефективним у перевірці рівня обізнаності та навчанні персоналу. Однак, слід враховувати, що його ефективність залежить від правильної організації та проведення навчання. Організаційні заходи, спрямовані на підвищення обізнаності працівників, є важливою складовою для досягнення високого рівня захисту локальних мереж від соціально-інженерних загроз. Всі ці аспекти разом допоможуть забезпечити надійний захист мереж і знизити ризики виникнення кібератак.

Рекомендації щодо використання GoPhish можуть бути цінними для широкого спектру користувачів інформаційних систем та мереж, оскільки загрози соціальної інженерії є надзвичайно поширеними:

Компаній та організацій, які бажають перевіряти обізнаність свого персоналу щодо ідентифікації та уникнення соціально-інженерних атак.

ІТ-спеціалістів та кібербезпечних команд, які відповідають за захист мереж та інформаційних систем організації.

Користувачів, які бажають навчитися розпізнавати фішингові атаки та збільшити свою осведомленість щодо кібербезпеки.

Освітніх установ та тренерів, які прагнуть навчати своїх студентів або учнів принципам безпечного користування мережами та захисту від соціально-інженерних загроз.

Приватних осіб, які прагнуть забезпечити свою власну кібербезпеку та захистити свої особисті дані від атак соціальної інженерії.

# ПЕРЕЛІК ПОСИЛАНЬ

1. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).

2. NIST SP 800-53: NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

3. IEEE Computer Society. (2022). "802.3-2022 IEEE Standard for Ethernet". Стандарт IEEE 802.3-2022. https://standards.ieee.org/ieee/802.3cs/7449/

4. IEEE Computer Society. (2022). "802.11-2020/Cor 1-2022 IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems". Стандарт IEEE 802.11-2020/Cor 1-2022. https://standards.ieee.org/ieee/802.11/7028/

5. Махницький, О.В. Використання соціальної інженерії для крадіжки особистих даних. Стор. 55-60.

Режим доступу: http://er.dduvs.in.ua/bitstream/123456789/2459/1/6.pdf.

6. Гаврилов А. Соціальна інженерія в дії. Безпека. 2015. № 3. Стор. 118-122.

7. Курбанмурадов Д.М., Соколов В.В. Методика протидії соціальному

інжинірингу на об’єктах інформаційної діяльності. Кібербезпека: освіта та наука. 2018. – Стор. 6-17.

8. Гаврилов А. Соціальна інженерія в дії. Безпека. 2015. № 3. Стор. 118-122.

9. Зулкурнайн А., Чизарі Х., Хусайн А., Хаміді А. Пом'якшення нападів соціальної інженерії. - Стор. 188-199.

10. Broadcom. (23.05.2023). About Email Anti-Malware. [Електронний ресурс]. Режим доступу: https://techdocs.broadcom.com/us/en/symantec-security-software/email-security/email-security-cloud/1-0/about-email-anti-malware.html.

11. Microsoft. (02.24.2023). Microsoft 365 Security Documentation: Exchange Online Protection (EOP) Overview [Електронний ресурс]. Режим доступу: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/eop-about?view=o365-worldwide.

12**.** Cisco. (11.01.2021.). "Understanding the Basics of Network Security" [Електронний ресурс]. Cisco Press. Режим доступу: https://www.ciscopress.com/articles/article.asp?p=3100055&seqNum=2.

13. Gophish. (16.12.2022.). "gophish" [Електронний ресурс]. GitHub. Режим доступу: https://github.com/gophish/gophish.

14. Gophish. (12.01.2020). "User Guide" [Електронний ресурс]. Gophish. Режим доступу: <https://docs.getgophish.com/user-guide/>.

**ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ**

**(ПРЕЗЕНТАЦІЯ)**