Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студентки ***Сєрак Тетяни Геннадіївни***

академічної групи ***125м-17-2***

спеціальності ***125 Кібербезпека***

спеціалізації[1]

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Розробка методики протидії методам соціального інжинірингу***

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.ф.-м.н., доц. Гусєв О.Ю.			
розділів:				
спеціальний	ас. Ковальова Ю.В.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2018

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту ***Сєрак Т.Г.*** (прізвище та ініціали) **академічної групи** ***125м-17-2*** (шифр)

спеціальності ***125 Кібербезпека***
спеціалізації[1]
за освітньо-професійною програмою ***Кібербезпека***

на тему ***Розробка методики протидії методам соціального інжинірингу***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора НТУ «Дніпровська політехніка» від 29.11.18 № 2025-л

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *процес передачі інформації в корпоративних мережах*

Предмет досліджень *методи протидії методам соціального інжинірингу*

Мета *підготовка методики протидії методам соціального інжинірингу на ТОВ «Азимут-Трейд» з метою захисту інформації персональних даних*

Вихідні дані для проведення роботи *законодавство України, міжнародні стандарти у сфері інформаційної безпеки та кібербезпеки, наукові публікації вітчизняних та іноземних авторів, статистичні дані*

3 ОЧІКУВАНІ РЕЗУЛЬТАТИ

Наукова новизна *полягає у розробці методики для ознайомлення та навчання співробітників організації протидії методам соціального інжинірингу та засобів протидії цим методам*

Практична цінність *полягає у розробці методичних вказівок для ознайомлення та навчання співробітників ТОВ «Азимут-Трейд» протидії методам соціального інжинірингу*

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Результати роботи мають відповідати вимогам чинного законодавства України і бути поданими у вигляді, що дозволяє безпосереднє використання для підвищення безпеки організації у питаннях протидії методам соціального інжинірингу

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт** (початок-кінець)
Огляд джерел за темою та напрям досліджень	03.09.18-06.10.18
Методи досліджень	07.10.18-31.10.18
Результати досліджень	01.11.18-24.11.18
Виконання економічного розділу	25.11.18-04.12.18
Оформлення пояснювальної записки	05.12.18-10.12.18

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *від реалізації результатів роботи очікується позитивним завдяки зниженню можливого збитку організації від реалізованих методами соціального інжинірингу загроз через застосування запропонованої методики*

Соціальний ефект *дипломної роботи полягає у підвищенні впевненості керівництва організації з точки зору протидії атакам методами соціального інжинірингу*

7 ДОДАТКОВІ ВИМОГИ

Завдання видано _____ Гусєв О.Ю.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 03.09.18р.

Дата подання до екзаменаційної комісії: 14.12.18р.

Прийнято до виконання _____ Сєрак Т.Г
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 113 с., 11 рис., 13 табл., 4 додатка, 38 джерел.

Об’єкт дослідження: процес передачі інформації в корпоративних мережах.

Предмет дослідження: методи протидії методам соціального інжинірингу.

Мета роботи: підготовка методики протидії методам соціального інжинірингу на ТОВ «Азимут-Трейд» з метою захисту інформації персональних даних.

В першому розділі проаналізовано теоретичні та методологічні основи соціального інжинірингу, розглянуто найпоширеніші техніки та види атак, якими користуються соціальні інженери, визначено вимоги нормативних документів з протидії методам соціальної інженерії.

В спеціальній частині розроблено методику протидії методам соціального інжинірингу, проаналізовано вразливості в організації до яких відносяться атаки соціального інжинірингу. Розглянуто теоретичні аспекти та проаналізовано технічні засоби від соціальної інженерії. Проведено аналіз соціальної інженерії в організації ТОВ «Азимут-Трейд», визначено необхідні заходи щодо виявлених вразливостей організації.

В економічному розділі проведено розрахунок вартості розробки та впровадження методики протидії методам соціального інжинірингу та оцінки можливого збитку від атаки на вузол або сегмент мережі.

Наукова новизна роботи полягає у розробці методики для ознайомлення та навчання співробітників організації протидії методам соціального інжинірингу та засобів протидії цим методам.

СОЦІАЛЬНИЙ ІНЖИНІРИНГ, ВИДИ АТАК, МЕТОДИКА ПРОТИДІЇ СОЦІАЛЬНОМУ ІНЖИНІРИНГУ, ТЕХНІЧНІ ЗАСОБИ

РЕФЕРАТ

Пояснительная записка: 113 с., 11 рис., 13 табл., 4 приложения, 38 источников.

Объект исследования: процесс передачи информации в корпоративных сетях.

Предмет исследования: методы противодействия методам социального инжиниринга.

Цель работы: подготовка методики противодействия методам социального инжиниринга на ООО «Азимут-Трейд» с целью защиты информации персональных данных.

В первом разделе проанализированы теоретические основы социального инжиниринга, рассмотрены техники и виды атак, определены требования нормативных документов по противодействию методам социальной инженерии.

В специальной части разработана методика противодействия методам социального инжиниринга, проанализировано уязвимости в организации к которым относятся атаки социального инжиниринга. Рассмотрены теоретические аспекты и проанализированы технические средства от социальной инженерии. Проведен анализ социальной инженерии в организации, определены меры по обнаруженным уязвимостям организации.

В экономическом разделе проведен расчет стоимости разработки и внедрения методики противодействия методам социального инжиниринга и оценки возможного ущерба от атаки на узел или сегмент сети.

Научная новизна работы заключается в разработке методики для ознакомления и обучения сотрудников организации противодействия методам социального инжиниринга и средств противодействия этим методам.

СОЦИАЛЬНЫЙ ИНЖИНИРИНГ, ВИДЫ АТАК, МЕТОДИКА ПРОТИВОДЕЙСТВИЯ СОЦИАЛЬНОМУ ИНЖИНИРИНГУ, ТЕХНИЧЕСКИЕ СРЕДСТВА

ABSTRACT

Explanatory note: 113 p., 11 fig., 13 tables, 4 supplement, 38 sources.

The object of the research is the process of transferring information in corporate networks.

The subject of research is methods of counteracting the methods of social engineering.

The purpose of the research is the preparation of methods of countering the methods of social engineering for Azimut-Trade LLC in order to protect personal information.

In the first section, the theoretical foundations of social engineering are analyzed, techniques and types of attacks are considered, the requirements of regulatory documents on counteracting social engineering methods are defined.

In a special part, a method of counteracting social engineering methods was developed, vulnerability in organizations was analyzed to which attacks of social engineering belong. Theoretical aspects are considered and technical means from social engineering are analyzed. The analysis of social engineering in the organization was carried out, the measures for the identified vulnerabilities of the organization were determined.

In the economic section, the cost calculation and the use of the method of counteracting social engineering methods and assessing the possible damage from an attack on a node or network segment are carried out.

The scientific novelty of the work lies in the development of methods for familiarizing and training employees of the organization in counteracting social engineering methods and means of counteracting these methods.

SOCIAL ENGINEERING, TYPES OF ATTACKS, METHODS OF COUNTERACTION TO SOCIAL ENGINEERING, TECHNICAL MEANS

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АТС – автоматична телефонна станція;

ДСТУ – державний стандарт України;

НСД – несанкціонований доступ;

ПБ – політика безпеки;

ПЕОМ – персональна електронно-обчислювальна машина;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

СІ – соціальний інжиніринг;

ІМ – служба миттєвого обміну повідомленнями;

ISO/IEC – International Organization for Standardization/International Electrotechnical Commission.

ЗМІСТ с.

ВСТУП

Використання комп'ютерних систем у всіх сферах сучасного життя, стрімкий розвиток мережевих технологій, крім переваг, спричинили за собою появу великої низки специфічних проблем. Однією з таких проблем є необхідність забезпечення ефективного захисту інформації, яка обумовлена зростанням правопорушень, пов'язаних з крадіжками і неправомірним доступом до даних, що зберігаються в пам'яті комп'ютерних систем і переданих по лініях зв'язку.

Сьогодні комп'ютерні злочини відбуваються у всьому світі, поширені в багатьох областях людської діяльності. Ці злочини характеризуються високою скритністю, складністю збору доказів за встановленими фактами їх здійснення і складністю доведення в суді подібних справ [1, с. 27].

За даними зарубіжних аналітиків, щотижня в світі реєструється більше 55 мільйонів різних комп'ютерних зломів. Розмір шкоди, заподіяної користувачам в результаті хакерських нападів, продовжує збільшуватися з кожним роком. На жаль, навіть настільки загрозлива статистика не заважає величезній кількості компаній і користувачам персональних комп'ютерів (ПК) ігнорувати будь-які правила комп'ютерної безпеки. За оцінками експертів, у світі лише 1% офісних співробітників слідує корпоративним правилам користування персональним комп'ютером. Дана обставина призводить до можливості здійснення деяких інформаційних загроз.

Перша загроза − це фізичні атаки. Найпростішою причиною просочування інформації є можливість фізичного доступу до комп’ютера, на якому ця інформація розташована [2, с. 14]. Фізична безпека має на увазі охорону комп’ютерного обладнання шляхом обмеження фізичного доступу до нього. Крадіжка або втрата комп’ютера або іншого пристрою стала причиною 57% випадків витоку інформації в другому півріччі 2011 року і 46% у першому півріччі [3, с. 109].

Друга загроза – це соціальні атаки. Одним із найбільш ефективних методів, комп'ютерними зловмисниками для проникнення в захищені паролем системи, є отримання конфіденціальних даних від користувачів під виглядом служби технічної підтримки, яка просить повідомити пароль.

Але найчастіше для отримання доступу до мережі застосовується метод, який називається соціальний інжиніринг. Соціальний інжиніринг заснований на управлінні особою людини для досягнення своєї мети.

В той час, коли служби безпеки установлюють антивіруси, розробляють складну систему допусків і паролів, зловмисники проникають в мережу за допомогою користувачів, які навіть нічого не підозрюють.

Насправді, 70% зломів і проникнень в комп'ютерні системи не можливі без соціального інжинірингу. Тому цей напрям дуже важливий, і люди повинні приділяти на його вивчення не менше часу, ніж на вивчення комп'ютерних систем.

Найслабкішою ланкою у будь-якій структурі інформаційної безпеки є людина. Можна створити надійну систему захисту і написати детальні інструкції з безпеки, проте недбале поводження співробітників з важливими відомостями, їх довірливість і безтурботна поведінка здатні звести нанівець усі зусилля.

Сьогодні для суспільства термін «соціальний інжиніринг» є синонімом набору прикладних психологічних і аналітичних прийомів, які у свою чергу, зловмисники застосовують для прихованої мотивації користувачів публічної або ж корпоративної мережі до порушень правил і політик в області інформаційної безпеки.

В основі цього підходу лежить системність, яка підкріплена методологією і аналізом, що дозволяє поєднувати технологічну інноваційність, інженерну точність розрахунків з використанням соціально-психологічного моделювання. Майстерне володіння цими інструментами є запорукою успішного вибудовування поведінкової моделі людей, які

«добровільно» і «самостійно» діють в потрібному напрямку для соціальних інженерів [4, с.73].

Основною метою соціальних інженерів є отримання доступу до захищених систем з метою крадіжки яких-небудь даних. Основна відмінність від простого злому є те, що в ролі об’єкту атаки вибирається не машина, а її оператор. Саме тому усі методи і техніки соціальних інженерів ґрунтуються на використанні слабкостей людського фактору, що може вважатися вкрай руйнівним, оскільки зловмисник отримує інформацію, наприклад, за допомогою телефонної розмови або шляхом проникнення в організацію під виглядом її співробітника. Для захисту від атак цього виду слід знати про найбільш поширені шахрайства, необхідно розуміти, що насправді хочуть соціальні інженери і своєчасно організовувати відповідну політику безпеки. Вся інформація у цьому світі захищається людьми, і її основними носіями є також люди, які мають свій звичайний набір комплексів, слабкостей і забобонів, за допомогою яких і «грають» соціальні інженери.

Проаналізувавши причини і методи злому програмного забезпечення (ПЗ) або каналів витоку інформації з різних структур, можна зробити цікавий висновок про те, що приблизно в 80% випадків, причина цього −людський фактор, або вміле маніпулювання ним.

РОЗДІЛ 1. ОСНОВИ ТА МЕТОДИ СОЦІАЛЬНОГО ІНЖИНІРИНГУ

1.1 Теоретичні та методологічні основи соціального інжинірингу

Соціальний інжиніринг − це метод несанкціонованого доступу до інформації або систем зберігання інформації без використання технічних засобів. Основна мета соціальних інженерів - це отримання доступу до захищених систем з метою крадіжки інформації, паролів, даних про кредитні картки і т.п. Основною відмінністю від простого злому - це те, що в ролі об'єкта атаки вибирається не машина, а людина [5]. Тому всі методи і техніки соціальних інженерів засновані на використанні слабкостей людського фактора, що вважається вкрай небезпечним, так як зловмисник отримує інформацію, наприклад, за допомогою звичайного телефону або шляхом проникнення в організацію під виглядом співробітника або іншої особи.

Незважаючи на те, що поняття «соціальний інжиніринг» з'явилося відносно недавно, люди в тій чи іншій мірі користувалися цими техніками споконвіку, так як в основі лежить психологія спілкування між людьми. Соціальний інжиніринг з'явився в світі з першим суспільством, так як саме слово «соціальність» − це громадськість, або ж громадянськість. Суть соціального інжинірингу − це змусити людину вчинити будь-яку дію, яка не вигідна йому, але необхідна соціальному інженеру.

Соціальний інжиніринг − це цілковитий напрямок в хакінгу, зломи комп'ютерних систем можна здійснювати не тільки технічними методами, а й на рівні психології.

Соціальний інжиніринг утворився як окрема частина з прикладної психології. Йому навчають шпигунів, таємних агентів. Всі техніки соціального інжинірингу засновані на особливостях прийняття рішень людьми, які називаються когнітивним базисом [6, с. 53].

Соціальний інжиніринг заснований на початковому прагненні людей надати допомогу іншим. Соціальний інжиніринг − найменш технічний, але й найбільш ефективний засіб в арсеналі зловмисників.

Соціальний інжиніринг, як незаконний метод отримання інформації, зазвичай використовує обман, вплив і переконання, але його можна також використовувати і в законних цілях, наприклад, для вчинення дій конкретною людиною. Найчастіше соціальний інжиніринг використовують для отримання закритої інформації, або інформації, яка є великою цінністю.

Основні області застосування соціального інжинірингу [5, с. 28] показані на рисунку 1.1.

Переважна більшість соціальних інженерів діє за однаковими або близькими шаблонами, тому вивчення прийомів їх «роботи» дозволяє розпізнати обман [6, с. 13] і не видати закриту інформацію.

Рисунок 1.1 − Основні області застосування соціального інжинірингу

Організації набувають кращі технології з безпеки, тренують та навчають співробітників, наймають охорону, але вони все ще залишаються вразливими.

Чим більше технологічних рівнів організація нагромаджує, тим більше різноманіття цих рівнів, і, тим сильніший повинен бути захист мереж в організації. Однак організаціям не завжди вдається уникнути невдач, тому, що вони не беруть до виду внутрішні проблеми. Навіть дуже надійно захищену мережу може обійти дуже простий і разом з тим багатогранний елемент – людський фактор [8, с. 79].

Успішні зловмисники частіше за все використовують соціальний інжиніринг і проводять атаку, маніпулюючи користувачами. З цієї причини, для підприємства важливо вкладати час і гроші у підготовку, навчання і тестування цього життєво важливого компонента безпеки.

Пояснення суті соціального інжинірингу і, зокрема, таких його різновидів, як гіпноз і нейролінгвістичне програмування (НЛП), є взаємодія між свідомістю і підсвідомістю. Люди вірять у те, що приймають рішення свідомо, але НЛП і гіпноз давно продемонстрували силу підсвідомості, а дослідження останніх років підтвердили, що підсвідоме прийняття рішень випереджає свідоме часом на 10 секунд. [9, с. 119].

На цьому засновані технології, які дозволяють маніпулювати людьми, аби змусити їх виконати певні дії і тим самим розкрити конфіденційну інформацію.

Багато професіоналів інформаційних технологій дотримуються неправильного уявлення, вважаючи, що вони використовують стандартні продукти з безпеки: фаєрволи, системи для виявлення вторгнень або серйозні пристрої для аутентифікації, такі як біометричні смарт-карти. Крім того, безпека – це не технологічна проблема, це проблема людей та управління. [10, с. 95].

Крім технічних методів захисту інформації, необхідна серйозна робота з персоналом, навчання співробітників застосування політики безпеки і

техніки протистояння соціальним інженерам – тільки в цьому випадку система забезпечення інформаційної безпеки є комплексною.

Атака соціального інженера розподіляється на три стадії підготовки:

1 Визначення точної мети (відбувається конкретне визначення, за якого роду інформацією йде полювання і де вона знаходиться, причому, у зв'язку зі знанням точного місце розташування інформації на диску або на іншому носії, «операція» проводиться дуже швидко, і в підсумку, ніхто не визначає такий доступ як НСД).

2 Збір інформації про об'єкт підготовки (здійснюється вивчення жертви – це дозволяє зрозуміти характер людини, його слабкі місця, звички та ін., джерелом інформації про об'єкт може служити практично все: аналіз трафіку, пошти, навіть касових чеків).

3 Розробка плану дій, моральна підготовка/тренування (відбувається опрацювання сценарію, кожне слово зіставляється з психологічною моделлю вивченої жертви) [11, с. 46].

Загальна схема роботи соціальних інженерів представлена [5, с. 22] на рисунку 1.2.

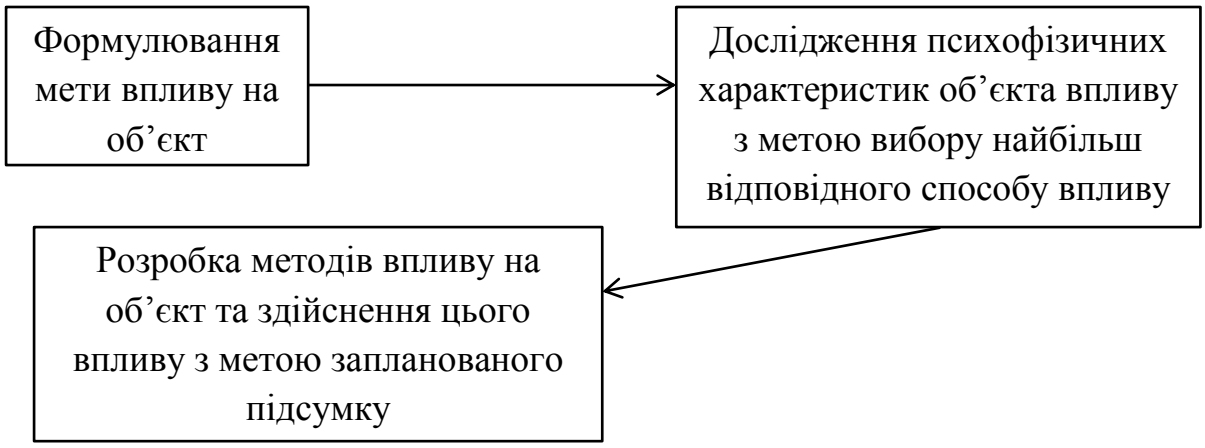

Рисунок 1.2 − Загальна схема роботи соціальних інженерів

Соціальний інжиніринг, у сукупності з технічними знаннями систем інформаційної безпеки, використовують для досягнення наступних цілей:

1 Збір інформації про потенційну жертву.

2 Отримання конфіденційної інформації (для досягнення даної мети при тривалому спілкуванні з жертвою, соціальний інженер входить у довіру і під зручними приводами отримує необхідну інформацію).

3 Отримання інформації, необхідної для несанкціонованого доступу (НСД) [12, с. 99].

4 Змушення об’єкту здійснити необхідні соціальному інженеру дії (тобто вчинення таких дій, які змушують жертву зробити те, що спричинить за собою потенційну можливість НСД).

Атаки соціальних інженерів представлені [5, с. 13] у вигляді рисунка 1.3.

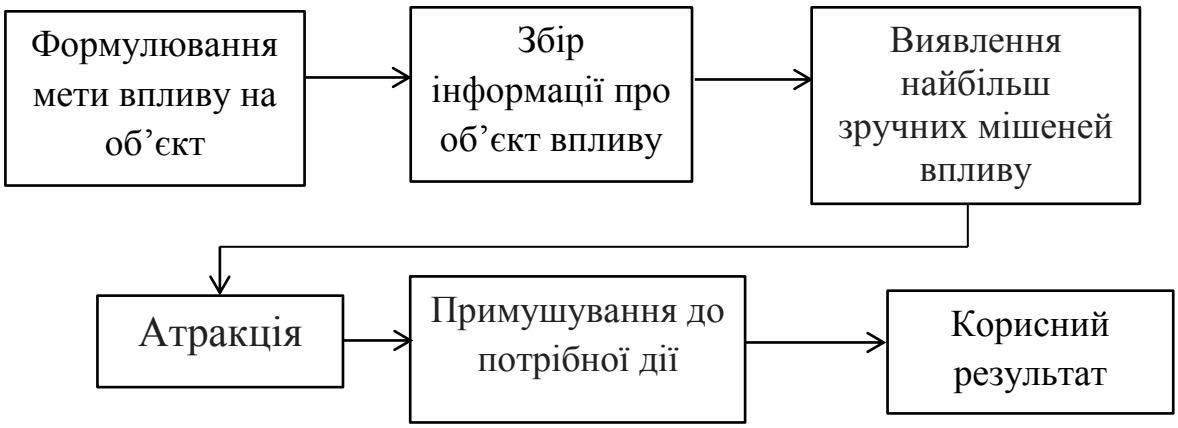

Рисунок 1.3 − Основна схема впливу в соціальному інжинірингу

Ця схема називається «схема Шейнова». У загальному вигляді вона приведена в книзі білоруського психолога і соціолога В.П.Шейнова, який довгий час займався психологією шахрайства [13, с. 89].

Спочатку завжди формулюється мета впливу на той чи інший об'єкт (під «об'єктом» розуміється жертва, на яку націлена атака соціального інженера). Далі збираємо інформацію про об'єкт, з метою виявлення найбільш зручних мішеней впливу, після чого настає етап, званий атракцією. Атракція (від лат. Attrahere - залучати, притягати) - це створення необхідних умов для впливу соціальних інженером на об'єкт. Примус до потрібного для соціального інженера дії найчастіше досягається виконанням попередніх етапів, тобто після того, як досягається атракція, жертва сама створює необхідні соціальному інженеру дії (наприклад: підкуп співробітника.

Мішенню є потреба співробітника в грошах. Про потребу в грошах впізнається на етапі збору інформації. Атракцією є створення умов, при яких співробітник буде дуже потребувати грошей).

Для того щоб обійти засоби безпеки, соціальний інженер знаходить спосіб обману співробітника, для розкриття інформації або отримання доступу до інформації.

У більшості випадків, успішні соціальні інженери володіють сильними людськими якостями. Вони чарівні, ввічливі і прості.

Велика частина корпоративної інформації може здаватися загальнодоступною або не таємною, але вона може бути дуже цінна для соціального інженера, тому що може зіграти істотну роль для більшої правдоподібності.

Багато атак соціальної інженерії є складними, включаючи в себе ретельно планований ряд кроків, поєднуючи маніпуляцію і технологічні знання [14, с. 14].

Щоб здійснити атаку, соціальний інженер покладається на міжособистісну взаємодію (соціальні навички), за допомогою якої компрометує відомості про організацію або її комп'ютерних системах. Якщо соціальний інженер не може зібрати достатньо відомостей з одного джерела, то він звертається до іншого джерела в тій же організації і, використовуючи інформацію, отриману від першого, підвищує свою переконливість.

Одна з основних технік соціального інжинірингу включає в себе створення почуття довіри з боку жертви. Чим природніше соціальний інженер спілкується з жертвою, тим більше він послаблює підозру.

Через високий темп життя, людині не вистачає часу, щоб задуматися над прийняттям якогось рішення, навіть дуже важливого. Заплутані ситуації, нестача часу, емоційне напруження – ось одні з передумов. Таким чином, рішення приймається в поспіху, отримана інформація не аналізується, такий процес називається автоматичною відповіддю.

Більшість співробітників організацій навіть не підозрюють про наявність загроз, пов'язаних з соціальним інжинірингом. Вони мають доступ до інформації, не розбираючись в деталях роботи, і не усвідомлюючи важливості оброблюваної інформації. Соціальний інженер, найчастіше, вибирає собі за мету співробітника з низьким рівнем володіння комп'ютером [15, с. 13].

Соціальні інженери використовують людські почуття. Одне з таких почуттів - це виклик співчуття у співрозмовника. При розповіді про причини, що викликають співчуття у співрозмовника, він пом'якшує своє прохання.

Так само, соціальні інженери використовують професійний жаргон, в зв'язку з тим, що співробітники довіряють тим, хто знає професійний жаргон, якусь внутрішню форму спілкування їх організації, яка прихована від сторонніх очей.

Соціальний інжиніринг ділиться на два види:

1 Короткостроковий;

2 Довготривалий.

Короткостроковий проводиться за короткий термін часу. Його плюс в тому, що він не вимагає зайвих тимчасових ресурсів, а мінус полягає в тому, що соціальний інженер не може змусити зробити людину якісь значимі дії [16, с. 23].

Довготривалий означає, що необхідно витратити багато часу на те, щоб підпорядкувати собі людину. Мінус - тривалість підготовки, плюс в тому, що можна змусити людину зробити більш значущі дії.

Як же зупинити соціальний інжиніринг? «Ціна питання - 64 мільйони доларів,− каже Стюарт Макклюр, президент і технічний директор «Foundstone» − єдиним успішним методом протидії є навчання » [20].

Річ Могулл, директор з досліджень «Gartner» в сфері інформаційної безпеки та ризиків, каже, що «соціальний інжиніринг− більш серйозна проблема, ніж хакерство. Люди за своєю природою непередбачувані і схильні до маніпуляції і переконання. Дослідження показують, що у людини існують

певні поведінкові тенденції, які можна експлуатувати за допомогою тонкої маніпуляції. Багато найбільш руйнівних проникнень в захищені системи відбуваються, і будуть відбуватися методами соціального інжинірингу, а не електронного злому або хакерства [20].

За словами Могулла, найбільш небезпечна крадіжка ідентифікаційних даних, так як більшість злочинців «заново винаходять старі афери» із застосуванням нової технології. Шахраї використовують соціальний інжиніринг для крадіжки ідентифікаційних даних або з корисливих мотивів, або для подальшого збору інформації про організацію. Це не тільки втручання в бізнес, а й порушення таємниці особистого життя. Так само ми переконані, що в найближче десятиліття головну загрозу для безпеки представлятиме соціальний інжиніринг [20].

Соціальний інжиніринг так само успішно застосовується для досягнення таких цілей, як:

1 Витяг прибутку;

2 Спосіб ведення статистики;

3 З метою підвищення рівня довіри відвідувача;

4 Формування цін;

5 Боротьба з конкурентами (наприклад, боротьба за клієнта в таксі. Мета − отримання грошей обманним шляхом).

При проведенні атаки з використанням соціального інжинірингу так само, як і в звичайних атаках, присутні класифікація ступеня доступу при успішно проведеній атаці. Цей ступінь залежить від рівня підготовленості соціального інженера і того, ким є жертва. Всього рівнів чотири, нижче вони перераховані в порядку убування повноважень:

1 Адміністратор;

2 Начальник;

3 Користувач;

4 Знайомий.

У таблиці 1.1 показана ймовірність отримання доступу різних рівнів і засоби застосування (1 - низька; 2 - середня, 3 - висока) [6, с. 14].

Таблиця 1.1 − Ймовірність отримання доступу різних рівнів

Клас атаки / підготовленість зловмисника	Новачок	Любитель	Професіонал
1	2	3	4
Засоби застосування			
Телефон	3	3	3
Електронна пошта	2	3	3
Звичайна пошта	1	3	3
Розмова по Internet	3	3	3
Особиста зустріч	1	2	3
Рівень спілкування (відносини)			
Офіційний	2	3	3
Товариський	3	3	3
Дружній	1	2	3
Рівень доступу			
Адміністратор	1	2	3
Начальник	1	2	3
Користувач	3	3	3
Знайомий	2	3	3

Тепер розглянемо найпоширеніші техніки і види атак, якими користуються соціальні інженери. Всі вони засновані на особливостях прийняття людьми рішень, відомих як когнітивні упередження. Ці забобони використовуються в різних комбінаціях, з метою створення найбільш відповідної стратегії обману в кожному конкретному випадку. Але спільною рисою всіх цих методів є введення в оману, метою яких є змусити людину

вчинити будь-яку дію, необхідне соціальному інженеру. Для досягнення поставленого результату використовується цілий ряд різноманітних тактик:

• видача себе за іншу особу;

• відволікання уваги;

• нагнітання психологічної напруги і т.д.

1 Претекстінг − це набір дій, які здійснюються за певним сценарієм (претексту). Дана техніка передбачає використання голосових засобів, таких як телефон, «Skype» і т.п. для отримання потрібної інформації. Як правило, представляючись третьою особою або вдаючи, що хтось потребує допомоги, соціальний інженер просить жертву повідомити йому пароль або авторизуватися на фішинговій веб-сторінці, тим самим змушуючи зробити необхідну дію або надати певну інформацію. У більшості випадків дана техніка вимагає яких-небудь початкових даних про об'єкт атаки. Найпоширеніша стратегія при цій техніці− використання на початку невеликих запитів і згадувати імена реальних людей з організації, в подальшому, соціальний інженер пояснює, що потребує допомоги (більшість людей можуть виконати завдання, які не сприймаються ними як підозрілі). Як тільки довірчий зв'язок встановлено, соціальний інженер може попросити щось більш суттєве і важливе.

2 Фішинг (від англ. Phishing, від fishing - риболовля, видобування) - це вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів. Досягається шляхом проведення масових розсилок електронних листів від імені популярних брендів, а також особистих повідомлень всередині різних сервісів (наприклад: від імені банків сервісів або всередині соціальних мереж (Facebook) [19, с. 95]. У листі міститься пряме посилання на сайт, який зовні не відрізняється від справжнього, або на сайт, що містить редирект (автоматичне перенаправлення користувачів з одного сайту на інший). Після потрапляння на підроблену сторінку, відбуваються спроби різними психологічними прийомами спонукати користувача ввести свої логін і пароль, які він

використовує для доступу до певного сайту, що дозволяє шахраям отримати доступ до акаунтів, банківських рахунків і т.п. Техніка фішингу перший раз була докладно описана в 1987 році, а сам термін з'явився 2 січня 1996 року в новинній групі «alt.online-service.America-Online» мережі «Usenet» [5]. Мабуть, це найпопулярніша схема соціального інжинірингу на сьогоднішній день. Жодний великий витік персональних даних не обходиться без хвилі фішингових розсилок. Найчастіше метою фішерів є клієнти банків і електронних платіжних систем. Соціальні мережі також представляють великий інтерес для фішерів, дозволяючи збирати особисті дані користувачів. В даний момент безліч посилань на фішингові сайти, націлені на крадіжку реєстраційних даних. За оцінками фахівців, понад 70% фішингових атак в соціальних мережах успішні.

Фішинг стрімко набирає свої оберти, а оцінки збитку сильно різняться: за даними компанії «Gartner», «в 2008 році жертви фішерів втратили 2,4 мільярда доларів США, в 2009 році - збиток склав 2,8 мільярда доларів, у 2010 - 3, 2 мільярди [5].

З Вішинг – дана техніка заснована на використанні системи попередньо записаних голосових повідомлень, метою яких є відтворення «офіційних дзвінків» від банківських та інших IVR (англ. Interactive Voice Response) систем [20, с. 175]. Зазвичай, жертва отримує запит (найчастіше через фішинг електронної пошти) про необхідність зв'язку з банком для підтвердження або поновлення будь-якої інформації. Система вимагає аутентифікації користувача за допомогою введення PIN-коду або пароля. Основна відмінність фішингу в тому, що, так чи інакше, задіюється телефон.

Згідно з інформацією від «Secure Computing» [23], шахраї конфігурують автонабір, який набирає номери в певному регіоні і при відповіді на дзвінок відбувається наступне:

• автовідповідач попереджає споживача, що з банківською картою виробляються шахрайські дії, і дає інструкції - передзвонити за певним номером негайно;

• при подальшому передзвонюванні, на іншому кінці дроту відповідає комп'ютерний голос, який повідомляє, що людина повинна пройти звірку даних і ввести 16-значний номер картки з клавіатури телефону;

• після введення номера, Вішер стає володарем всієї необхідної інформації (номер телефону, повне ім'я, адреса);

• потім, використовуючи цей дзвінок, можна зібрати і додаткову інформацію, таку, як PIN-код, термін дії карти, дата народження, номер банківського рахунку тощо.

Принцип дії IVR систем показаний на рисунку 1.4.

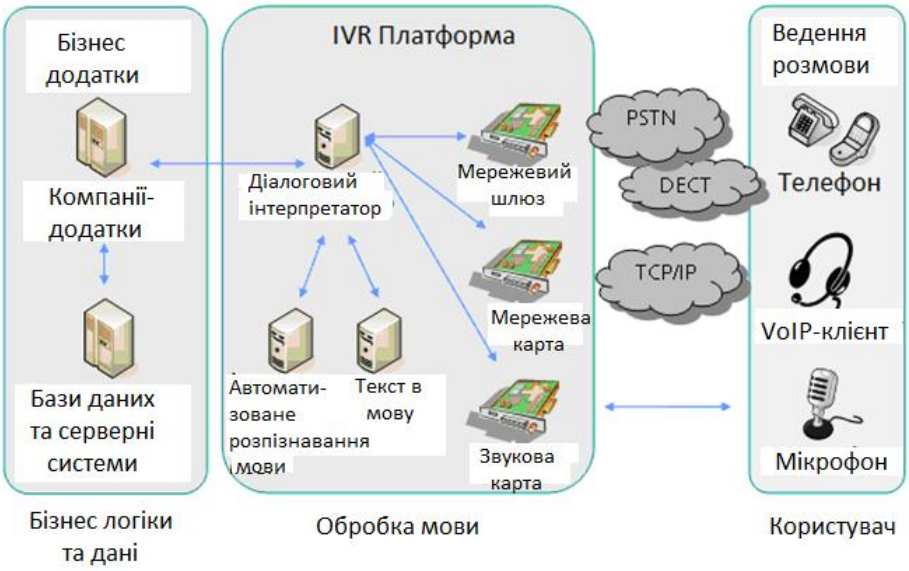

Рисунок 1.4 – Принцип дії IVR систем

4 Фармінг (англ. Pharming) – перенаправлення жертви за помилковою інтеренет-адресою. Для цього використовується якась навігаційна структура файл «hosts», система доменних імен - «domain name system») [21, с. 69]. Суть роботи фармінга має багато спільного зі стандартним вірусним зараженням. Жертва відкриває лист або відвідує будь-який веб-сервер, на якому виконується скрипт-вірус, при цьому відбувається спотворення файлу «hosts», в результаті жертва потрапляє на один з помилкових сайтів. Механізмів захисту від фармінга на сьогодні просто не існує.

5 Послуга за послугу − цей вид атаки має на увазі дзвінок соціального інженера в організацію з корпоративного (внутрішньому) телефону. У більшості випадків соціальний інженер представляється співробітником технічної підтримки, який робить опитування на виникнення технічних проблем. Під час процесу «рішення» технічних проблем, соціальний інженер «змушує» об’єкта вводити команди, які дозволяють йому запустити або встановити шкідливе ПЗ на комп'ютер користувача [22, с. 433].

6 Троянський кінь (або троянська програма) − це шкідлива програма, яка використовується соціальним інженером для збору і використання інформаційних ресурсів в своїх цілях [23, с. 473]. Дана техніка використовує цікавість, або інші емоції людини.

Розробники троянських програм використовують ті ж прийоми, що і маркетологи. Для досягнення своєї мети ті, хто пишуть віруси, використовують людські слабкості:

• недостатня підготовка;

• бажання виділитися;

• жалість і милосердя;

• бажання перегляду «цікавого» контенту;

• інтерес до продукту, який потрібен населенню або який дуже складно дістати;

• інтерес до методик швидкого збагачення за допомогою фінансових пірамід, супер-ідей для успішного ведення бізнесу.

Відкриваючи прикріплений до листа файл, співробітник встановлює на комп'ютер шкідливе ПЗ, яке дозволяє соціальному інженеру отримати доступ до конфіденційної інформації.

Поширення троянських програм відбувається шляхом розміщення їх на відкритих ресурсах (файл-сервери, відкриті для запису накопичувачі самого комп'ютера), носіях інформації або надсилаються за допомогою служб обміну повідомленнями (наприклад: електронна пошта, ICQ) з розрахунку на їх запуск на якомусь конкретному або випадковому комп'ютері [24, с. 174].

Рідко використання «троянів» є лише частиною спланованої багатоступінчастої атаки на певні комп'ютери, мережі або ресурси. Троянські програми найчастіше розробляються для шкідливих цілей. Існує класифікація, де вони розбиваються на категорії, засновані на тому, як «трояни» впроваджуються в систему і завдають їй шкоди.

Існує 5 основних типів:

• віддалений доступ;

• знищення даних;

• завантажувач;

• сервер;

• дезактиватори програм безпеки.

Метою троянської програми може бути:

• закачування або скачування файлів;

• копіювання помилкових посилань, що ведуть на підроблені веб-сайти, чати або інші сайти з реєстрацією;

• створення перешкод роботі користувача;

• викрадення даних, що представляють цінність або таємницю, в тому числі інформацію для аутентифікації, для несанкціонованого доступу до ресурсів;

• поширення інших шкідливих програм, таких як віруси;

• знищення даних (стирання або переписування даних на диску, важко помічаються пошкодження файлів) і обладнання, виведення з ладу або відмови обслуговування комп'ютерних систем, мереж;

• збір адрес електронної пошти і використання їх для розсилки спаму;

• шпигунство за користувачем і таємне повідомлення третім особам будь-яких відомостей;

• реєстрація натискань клавіш з метою крадіжки інформації такого роду як паролі та номери кредитних карток;

• дезактивація або створення перешкод роботі антивірусних програм і брандмауера [25, с. 37].

7 Збір інформації з відкритих джерел. Застосування технік соціального інжинірингу вимагає не тільки знання психології, а й уміння збирати про людину необхідну інформацію. Відносно новим способом отримання такої інформації став її збір з відкритих джерел, головним чином з соціальних мереж [26, с. 210]. Наприклад, такі сайти, як «livejournal», «Facebook» містять величезну кількість даних, які люди не приховують (приклад: «в ході слідства про викрадення сина Євгена Касперського, було встановлено, що злочинці дізналися розклад дня і маршрути слідування підлітка з його записів на сторінці в соціальній мережі »).

8 «Дорожнє яблуко»– являє собою адаптацію троянського коня, і полягає у використанні фізичних носіїв. Соціальний інженер підкидає «інфікований» диск, або флеш-карту в місце, де носій може бути легко знайдений (туалет, ліфт, парковка). Носій підробляється під офіційний, і супроводжується підписом, покликаної викликати цікавість [27, с. 80] (наприклад, соціальний інженер може підкинути диск, забезпечений корпоративним логотипом і посиланням на офіційний сайт організації, забезпечивши його написом «Заробітна плата керівного складу». Диск залишається на підлозі ліфта, або у вестибюлі. Співробітник через незнання підбирає диск і вставляє його в комп'ютер, щоб задовольнити цікавість).

9 Зворотний соціальний інжиніринг. Про нього згадують в тому випадку, коли жертва сама пропонує зловмиснику потрібну йому інформацію (наприклад: співробітники служби підтримки, для вирішення проблеми, ніколи не питають у співробітників ідентифікатор або пароль. Проте багато користувачів заради якнайшвидшого усунення проблем добровільно повідомляють ці конфіденційні відомості). Зворотний соціальний інжиніринг будується на трьох факторах:

• створення ситуації, яка змушує людину звернутися за допомогою;

• реклама своїх послуг або випередження надання допомоги іншими людьми;

• надання допомоги і вплив.

10 Людська відмова в обслуговуванні − суть атаки полягає в тому, щоб змусити людину (непомітно для нього) не реагувати на будь-які ситуації. Тобто, робиться так, щоб кожне слово соціального інженера сприймається як правда беззастережно і без осмислення. До такого роду атак відноситься і відволікання уваги. Соціальний інженер здійснює хибне уявлення про виконання однієї операції, а насправді виконує зовсім іншу. Таким чином, поки жертва зайнята одним, іншого вона не помічає. Атаки такого роду виконуються досить складно, тому що необхідно добре прорахувати психологію жертви, її знання і реакції на такі дії [11, с. 50].

11 Технічний соціальний інжиніринг. До цього виду атак можна адресувати ті атаки, в яких немає ні «жертви» ні «впливу на неї». В атаках цього типу використовуються принципи і стереотипи соціуму, що і відносить їх до соціального інжинірингу. Як приклад можна навести такі міркування: «Якщо стоять камери, то, швидше за все, ніхто не полізе» або «Чим більше організація, тим твердіше у людей думка про її захищеність». Такий спосіб більш широко відомий як аналіз ситуації. Людина бачить, що пройти звичайним шляхом (стандартним) не вийде, і починає переглядати інші варіанти, тобто займається аналізуванням ситуації [11, с. 51].

12 Особистий візуальний контакт − є найскладнішою технікою. Здійснити цю техніку можуть тільки професійні психологи або спеціально підготовлені люди. Техніка здійснюється наступним чином: до жертви знаходиться підхід, знаходиться слабке місце, обчислюється це за допомогою аналізу відповідей на питання. Головне для соціального інженера в такому випадку - розмовляти з жертвою «в рамках слабкого місця», що згодом призведе до того, що він дуже сподобається жертві як людина, і та викладе все, що необхідно, вважаючи, що нічого особливо важливого не розповідає.

13 Системи обміну миттєвими повідомленнями (ІМ). В даний час в інтернеті існує безліч програм, які можуть тим чи іншим способом впливати на роботу ICQ [28, с 18]. У список їх можливостей входить відсилання повідомлення від імені іншого користувача. Також зловмисник може

проводити атаку в вигляді спеціально сформованого тексту, але основним шляхом поширення вірусів через ICQ є передача файлів, тому необхідно бути дуже обережним з пропозиціями завантажити файл від сторонньої людини, тому що операційна система не завжди здатна правильно видати інформацію про файл, який запускається. Microsoft Windows за замовчуванням не показує розширення імен (наприклад: ім'я файлу «foto.jpg.exe» буде показано як «foto.jpg»).

Для маскування реального розширення застосовується подвійне розширення на зразок «xxx.jpg.exe» (в даному випадку може допомогти те, що деякі поштові сервери відмовляються пропускати виконувані файли) або додається велика кількість прогалин, через що ім'я файлу відображається не повністю.

Користувачі розцінюють дану службу як телефон і не пов'язують її з потенційними загрозами ПЗ. Балакуча природа IM, разом з опцією надання прізвиська досить розширює можливості для атаки [29]. На рисунку 1.5 показано, як працює імітація при використанні електронної пошти і IM.

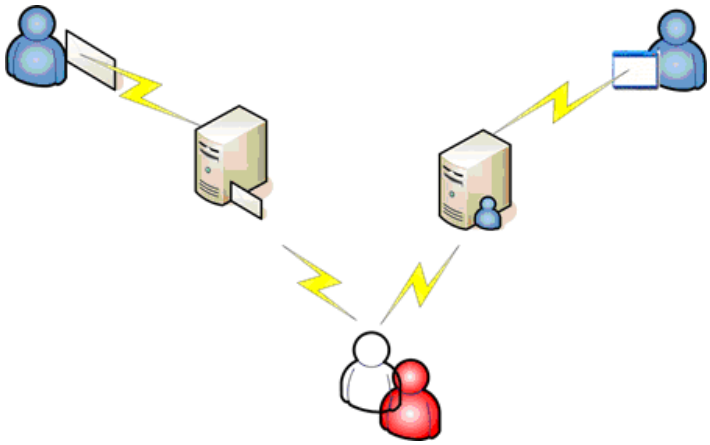

Рисунок 1.5 − Імітація при використанні IM і e-mail

Соціальний інженер (на рисунку виділено червоним кольором) виконує роль відомого користувача і посилає електронну пошту або IM-повідомлення, розраховуючи на те, що одержувачі візьмуть їх за повідомлення від того, кого вони знають.

14 Аналіз сміття − це цінна діяльність для соціальних інженерів. Ділові паперові відходи неоціненні [29, с. 85], тому що під час атаки, це може допомогти здаватися співробітником організації.

15 Особистісні підходи. Найпростіший шлях отримання інформації - це попросити про це безпосередньо. Існує чотири різновиди такого підходу:

•залякування (цей підхід може використовувати уособлення повноважень, щоб примусити жертву виконати запит);

• переконання (звичайнісінькі форми переконання включають лестощі);

• використання довірчих відносин (цей підхід вимагає більш тривалого терміну, протягом якого підлеглий або колега формують відносини, щоб отримати довіру і інформацію від жертви);

• допомога (в цьому підході пропонується допомогу жертві. Допомога буде вимагати, щоб жертва оприлюднила особисту інформацію).

Намагаючись піддати соціальній інженерії того, хто про неї знає, особливо кваліфікованих програмістів та інших хакерів, навряд чи можна багато чого досягти. Навіть якщо співрозмовник не знає про СІ як такої, він (або вона) може досить серйозно ставитися до попереджень "Зберігайте в таємниці свій пароль". Соціальна інженерія розрахована на наївних користувачів. Щоб спровокувати користувача на дії, які сприяють передачі інформації, що цікавить, використовують зворотну соціальну інженерію (ЗСІ).

Метою зворотної СІ є змусити жертву звернутися до зловмисника за «допомогою». Допомагаючи користувачеві вирішити проблеми, які виникли, хакер без особливих зусиль може дізнатися робочі імена і паролі. Атака за допомогою зворотного інжинірингу складається з трьох частин.

Диверсія. Це перший короткий контакт з певним комп'ютером, під час якого хакер створює якусь неполадку, що вимагає усунення, наприклад:

• зміна будь-якого параметра, невідомого новачкам або такого, про який вони не подумають, що встановлюється за замовчуванням: порти принтера, кольори екрану, макроси, приховані коди принтера, периферійні

технічні установки. Встановити файли в режимі «Тільки для читання», або перейменувати їх, або зробити невидимими в їх директоріях.

• втручання в апаратне забезпечення: переключити кольоровий монітор в монохромний режим, поміняти дисководи, відключити клавіатуру.

• інсталювати великі резидентні програми, що займають багато пам'яті. У цьому випадку користувач не зрозуміє, чому йому не вдається запустити програму.

• запустити модель програми, яка стане видавати повідомлення про помилки.

Реклама. Інформування користувача про те, що зловмисник розбирається в питаннях з області комп'ютерів. Наприклад, подзвонити за день, або навіть за кілька годин до вчинення диверсії, і повідомити того, хто підійде до телефону, новий номер виклику допомоги з комп'ютерного відділу (це буде номер зловмисника). При цьому, попросити користувача тримати цей номер під рукою на випадок виникнення проблем.

Допомога. Спілкування з користувачем, у процесі якого хакер вирішує проблеми користувача, а той, не підозрюючи, вирішує його проблеми.

Одним з найбільш знаменитих соціальних інженерів в історії є Кевін Митник. Будучи всесвітньо відомим комп'ютерним хакером і консультантом з безпеки, Митник є автором книг з комп'ютерної безпеки, присвяченим, в основному, соціальному інжинірингу та методів психологічного впливу на людину.

Незважаючи на те, зуміли реалізувати кілька великих схем шахрайства в Ізраїлі в 1990-х роках, використавши соціальний інжиніринг та підробку голосу. У телеінтерв'ю вони сказали: «Повністю від мережевих атак застрахований лише той, хто не користується телефоном, електрикою і ноутбуком».

Менш відомими соціальними інженерами є Френк Абігнейл, Девід Беннон, Пітер Фостер і Стівен Джей Рассел.

1.2 Вимоги нормативних документів з протидії методам соціальної інженерії

ДСТУ ISO/IEC 27033-3:2016. Інформаційні технології. Методи захисту. Безпечність мережі. Частина 3. Еталонні мережеві сценарії. Загрози, методи проектування та проблеми керування.

Керівництва, представлені в цьому стандарті для кожного з визначених типових мережевих сценаріїв, засновані на нижчеперелічених підходах:

• перевірка вступної інформації і рамок сценарію;

• опис загроз, відповідних до сценарію;

• проведення аналізу ризику щодо виявлених вразливостей;

• аналіз впливу на організацію розглянутих вразливостей;

• визначення рекомендацій щодо реалізації забезпечення безпеки мережі.

Послуги доступу до інтернету для співробітників

Організації, які повинні надавати послуги доступу до Інтернету для своїх співробітників, повинні продумати цей сценарій, щоб забезпечити впевненість у тому, що здійснюється доступ з чітко визначеними і санкціонованими цілями, а не загальний відкритий доступ. Організації повинні бути стурбовані питаннями управління доступом, щоб уникнути втрати пропускної здатності мережі і здатності до реагування, а також залучення до правової відповідальності співробітників.

Управління доступом співробітників до Інтернету викликає зростаюче занепокоєння, враховуючи кількість судових прецедентів, пов'язаних з Інтернетом. Таким чином, організація несе відповідальність за встановлення, моніторинг та втілення в життя точно вираженої політики використання Інтернету за допомогою забезпечення відповідних вимог в політиці:

• доступ до Інтернету надано в інтересах бізнесу;

•якщо доступ до Інтернету також дозволений (обмежений) в особистих цілях, то якими послугами дозволено користуватися;

•чи дозволено розширене застосування послуг для спільного використання;

• чи дозволено співробітникам брати участь в чаті, форумах і т.д.

Мобільний зв'язок

Цей сценарій повинні розглядати організації, що дозволяють співробітникам використання мобільних пристроїв.

Цей сценарій зосереджений на безпечних ділових відносинах підприємств, що використовують і розгортають мобільні пристрої і додатки. Хоча основним фактором для швидкого розвитку нових можливостей мобільних пристроїв, таких як смартфони або персональні інформаційні пристрої, є споживчий ринок, вони також використовуються в середовищі бізнесу. Часто такі пристрої є особистою власністю і використовуються як для цілей організації, так і в особистих цілях

Пристрої мобільного зв'язку дозволяють віддаленим користувачам координувати персональні бази даних, а також забезпечувати доступ до послуг мережі, таким як бездротова електронна пошта, перегляд веб-сторінок, а також доступ до Інтернету. Коли людина використовує одні й ті ж пристрої для приватних і для ділових цілей, виникає тенденція обходу політик або ігнорування їх використання, таким чином, на підприємство привносяться значні ризики інформаційної безпеки.

Безпека та службова інформація:

•зберігати паролі в секреті і не розділяти облікові записи. Авторизовані користувачі несуть відповідальність за збереження своїх паролів і облікових записів. Паролі системного рівня повинні змінюватися щокварталу, паролі рівня користувача слід змінювати кожні шість місяців;

• всі персональні комп'ютери, ноутбуки і робочі станції повинні бути забезпечені захищеної паролем заставкою з автоматичною активацією, встановленої на 10 хвилин або менше, або відключенням реєстрації (комбінація клавіш "control-alt-delete" для користувачів Win2), коли хост буде не обслуговатися;

•всі хости, які використовуються службовцями для підключення до Інтернету організації і належать співробітнику або організації, повинні безперервно сканувати антивірусною програмою з діючої (актуальною) базою даних вірусів, якщо не перевизначені відомчі або групові політики;

•співробітники повинні бути обережними при відкритті вкладення електронної пошти, отриманих від невідомих відправників, які можуть містити віруси, бомби електронної пошти, або код Троянського коня.

Системна і мережева діяльність

Наступні заходи, без винятків, є строго заборонені:

•впровадження шкідливих програм в мережу або на сервер (наприклад, вірусів, «черв'яків», «троянських коней", "бомб" електронної пошти, і т.д.);

•розкриття свого пароля облікового запису іншим особам або дозвіл використовувати свій обліковий запис іншими. Це стосується членів сім'ї та інших родичі;

•оформлення шахрайських пропозицій товарів, предметів або послуг, що виходять з будь-якого облікового запису компанії;

•надання інформації про співробітників або списків співробітників організації сторонам за межами організації.

Діяльність, пов'язана з комунікацією та електронною поштою:

•відправлення незатребуваних повідомлень електронної пошти, включаючи відправку "непотрібних повідомлень" або інших матеріалів рекламного характеру особам, які спеціально не запитують такі матеріали (спам електронної пошти);

•несанкціоноване використання або фальсифікація даних, що містяться в заголовку повідомлень електронної пошти;

•використання нав'язуваних поштою, що виходить із мереж компанії від інших постачальників послуг Інтернету від її імені або в рекламних цілях, будь-яких послуг, які виконуються хостом організації або підключеним через мережу організації;

•розсилка поштою однакових або аналогічних повідомлень, не пов'язаних з організацією, численним тематичним телеконференціям, що проводяться в призначених для користувача мережах (спам телеконференцій).

ДСТУ ISO/IEC 27004:2018. Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання

Цей стандарт містить рекомендації по розробці і використанню вимірювань і заходів вимірювання для проведення оцінки ефективності реалізованої системи менеджменту інформаційної безпеки (СМІБ), а також заходів і засобів контролю та управління або їх груп по ISO / IEC 27001.

Таблиця 1.2 − Навчання забезпечення інформаційної безпеки

Об'єкт вимірювання і атрибути	
Об'єкт вимірювання	База даних співробітників
Атрибути	Записи, що стосуються навчання
Специфікація основного заходу вимірювання	
Основна міра вимірювання	Число співробітників, які отримали щорічне навчання, спрямоване на підвищення обізнаності щодо інформаційної безпеки. Число співробітників, які повинні отримати щорічне навчання, спрямоване на підвищення обізнаності щодо інформаційної безпеки
Метод вимірювання	Підрахунок в журналах реєстрації / реєстрах відомостей, що відносяться до щорічного навчання співробітників, спрямованому на підвищення обізнаності щодо інформаційної безпеки, з поміткою "отримано"

Таблиця 1.3 – Якість паролів, що генеруються вручну

Визначення конструктивних елементів вимірювання	
Назва конструктивного елемента вимірювання	Якість паролів
Числовий ідентифікатор	Характерний для організації
Призначення конструктивного елементу вимірювання	Для оцінки якості паролів, що застосовуються користувачами для доступу до систем організації
Мета застосування заходів і засоби контролю і управління / процесу	Запобігти вибір користувачами небезпечних паролів
Міра і засіб контролю та управління / процес	Користувачі повинні дотримуватися правил безпеки при виборі і використанні паролів. Всі користувачі повинні вибирати надійні паролі для кожної системи: •довжиною більше восьми знаків; •не засновані на тому, що можна легко відгадати або отримати при використанні інформації, пов'язаної з особистістю, наприклад, на іменах, телефонних номерах, датах народження та ін.; •не перебувають з слів, включених в словники; •не містять наступних один за іншим ідентичних, повністю цифрових або повністю буквених знаків. Всі імена облікових записів і паролі користувачів для систем організації повинні контролюватися системою забезпечення/ контролю діяльності співробітників

Продовження таблиці 1.3

Об'єкт вимірювання і атрибути	
Об'єкт вимірювання	База даних паролей користувачів
Атрибути	Особисті паролі
Специфікація основної міри вимірювання	
Основна міра вимірювання	•Число зареєстрованих паролів •Число паролів, які відповідають політиці якості паролів організації для кожного користувача
Метод вимірювання	•Підрахунок числа паролей у базі даних паролей користувачів • Опитування кожного користувача про те, яке число паролів відповідає політиці паролів організації

ДСТУ ISO/IEC 27005:2015. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки

Цей стандарт являє керівництво з менеджменту ризику інформаційної безпеки (ІБ) в організації, підтримуючи, зокрема, вимоги до системи менеджменту інформаційної безпеки (СМІБ) відповідно до ISO / IEC 27001. Однак цей Стандарт не надає будь-якої конкретної методології по менеджменту ризику інформаційної безпеки. Вибір підходу до менеджменту ризику здійснюється організацією і залежить, наприклад, від області застосування СМІБ, контексту менеджменту ризику або сфери діяльності. Ряд існуючих методологій може використовуватися в рамках структури, описаної в цьому стандарті для реалізації вимог СМІБ.

Цей стандарт призначений для керівників і персоналу, що займається в організації питаннями менеджменту ризику інформаційної безпеки, а також,

при необхідності, для зовнішніх сторін, що мають відношення до цього виду діяльності.

Особливу увагу слід приділяти джерелам загроз, що походять від діяльності людини.

Таблиця 1.4 − Джерела загроз

Джерело загрози	Мотивація	Дія загрози
Хакер, зломщик	Виклик Зарозумілість Бунтарство Статус Гроші	Хакерство Соціальна інженерія Проникнення в систему, злом Несанкціонований доступ до системи
Особа, яка вчиняє комп'ютерний злочин	Руйнування інформації Незаконне розкриття інформації Грошова вигода Несанкціонована зміна даних	Комп'ютерний злочин Шахрайська діяльність (відтворення, видача себе за іншого, перехоплення) Інформаційний підкуп Отримання доступу обманним шляхом Проникнення в систему
Терорист	Шантаж Руйнування Використання в особистих інтересах Помста Політична вигода Охоплення середовища (передачі даних)	Вибух/Тероризм Інформаційна війна Системна атака (розподілена відмова в обслуговуванні) Проникнення в систему Псування системи

Продовження таблиці 1.4

Промислове шпигунство (відомості секретного характеру компанії, іноземні уряди, інші урядові об'єднання)	Конкурентна перевага Економічне шпигунство	Отримання інформаційної переваги Економічна експлуатація Розкрадання інформації Замах на недоторканність особистого життя Соціальна інженерія Проникнення в систему Несанкціонований доступ до системи
Інсайдери (погано навчені, незадоволені, зловмисні, безтурботні, нечесні або звільнені службовці)	Цікавість Зарозумілість Розвідка Грошова вигода Помста Ненавмисні помилки та упущення (наприклад, помилка введення даних, помилка в складанні програми)	Напад на службовця Шантаж Перегляд інформації, що є власністю фірми Неправильне використання комп'ютера Шахрайство і розкрадання Інформаційний підкуп Шкідливе ПЗ (наприклад вірус, логічна бомба, Троянський кінь) Продаж інформації особистого характеру "Жучки" в системі Проникнення в систему Несанкціонований доступ до системи

1.3.Висновки до першого розділу

У першому розділі було досліджено вимоги нормативних документів з протидії методам соціальної інженерії. А саме, було проаналізовано теоретичні та методологічні основи та розглянуто найпоширеніші техніки та види атак, якими користуються соціальні інженери. Особливу увагу слід приділяти джерелам загроз, що походять від діяльності людини.

Виходячи з результатів аналізу висновків до першого розділу, було поставлено задачі на подальше дослідження. Постає необхідним розробити методику протидії методам соціальної інженерії. Для цього необхідно розробити методичні вказівки у питаннях протидії методам соціальної інженерії. Задля обґрунтування доцільності розробленої методики необхідно проаналізувати практичну та економічну ефективності запропонованої методики.

РОЗДІЛ 2. РОЗРОБКА МЕТОДИКИ ПРОТИДІЇ СОЦІАЛЬНОМУ ІНЖИНІРИНГУ

У цьому розділі аналізується шаблон, який здатний убезпечити організацію від атак соціального інжинірингу. Якщо навчання персоналу, який займається обробкою інформації, не проводиться, то це буде тривати до того моменту, поки не відбудеться втрата інформації за допомогою соціального інжинірингу.

Ніякі технічні заходи захисту інформації практично не допоможуть захиститися від соціального інжинірингу. Пов'язано це з тим, що соціальні інженери використовують слабкості нетехнічних засобів, а як говорилося, людський фактор. У зв'язку з цим, єдиний спосіб протидіяти соціальним інженерам - це постійна і правильна робота з персоналом.

Для підвищення безпеки в організації, весь час повинні проводитися спеціальні навчання, постійно контролюватися рівень знань у співробітників, має проводитися тестування, а так само відбуватися внутрішні диверсії, які дозволять виявити рівень підготовленості співробітників в реальних умовах.

Найважливіший момент в підготовці користувачів, на яких слід звернути увагу – це те, що навчання – це циклічний процес, який повинен повторюватися з періодичністю в часі.

Форма навчання може складатися з таких видів, як:

1 Теоретичні заняття;

2 Практикум;

3 Онлайн-семінари;

4 Рольові ігри (тобто створення моделі атаки).

2.1 Теоретичні аспекти створення методики протидії соціальному інжинірингу

Для того, щоб створити методику навчання персоналу, яка буде працювати, необхідно зрозуміти, чому люди вразливі для атак. Для

виявлення цих тенденцій, необхідно звернути на них увагу завдяки дискусії - цим можна допомогти співробітникам зрозуміти, як соціальний інженер може маніпулювати людьми.

Маніпуляція, як метод впливу, почала вивчатися соціальними дослідниками в останні 50 років. Роберт Чалдіні (відомий американський експериментальний соціальний психолог, відомий по книзі «Психологія впливу»), написав статтю в «Американській науці» (лютий 2001 року), і об'єднав результати досліджень і виділив 6 «рис людської натури», які використовуються в спробі отримання потрібної відповіді.

Це 6 прийомів, які застосовуються соціальними інженерами найбільш часто і успішно в спробах маніпулювання [31, с. 124]:

1 Авторитетність – людям властиво бажання прислужитися людині з авторитетом (приклад атаки: соціальний інженер намагається видати себе за авторитетну особу з IT-відділу або посадову особу, яка виконує завдання організації).

2 Уміння розташувати до себе – люди мають звичку задовольнити запит людини, яку має в своєму розпорядженні, або людину зі схожими інтересами, думкою, поглядами, або бідами і проблемами (приклад атаки: в розмові атакуючий намагається з'ясувати захоплення та інтереси жертви, а потім з ентузіазмом повідомляє, що все це йому знайоме. Також він може повідомити, що він з тієї ж школи або місця. Соціальний інженер може навіть наслідувати цілі, щоб створити подібність, видиму спільність).

3 Взаємність. Людина здатна машинально відповісти на питання, коли отримує щось натомість. Це один з найбільш ефективних шляхів вплинути на людину, щоб отримати прихильність. Приклад атаки. Співробітник отримує дзвінок від людини, який називає себе співробітником Головного Офісу. Той, хто телефонує розповідає, що деякі комп'ютери компанії заражені новим вірусом, який не виявляється антивірусом. Цей вірус може знищити (пошкодити) всі файли на комп'ютері. Той, хто телефонує пропонує поділитися інформацією, як вирішити проблему. Потім він просить

співробітника протестувати недавно оновлену утиліту, що дозволяє користувачеві змінити паролі. Службовцю незручно відмовити, тому що той, хто телефонує лише пропонує допомогу, яка захистить користувачів від вірусу).

4 Відповідальність − люди мають звичку виконувати обіцяне (приклад атаки: атакуючий зв'язується з відповідним новим співробітником і радить ознайомитися з угодою про політику безпеки і процедури, тому що це - основний закон, завдяки якому можна користуватися інформаційними системами компанії. Після обговорення кількох положень про безпеку атакуючий просить пароль співробітника «для підтвердження згоди» з угодою. Він повинен бути складним для вгадування. Коли користувач видає свій пароль, той, хто телефонує дає рекомендації, як вибирати паролі в наступний раз, щоб хакерам було складно підібрати їх. Жертва погоджується слідувати порадам, тому що це відповідає політиці компанії. До того ж робочий передбачає, що той, що дзвонив тільки що підтвердив його згоду дотримуватися угоди).

5 Соціальна приналежність до авторизованих користувачів − людям властиво не виділятися у своїй соціальній групі. Дії інших є гарантом істинності в питанні поведінки (приклад атаки: той, хто телефонує говорить, що він перевіряє і називає імена інших людей з відділу, які займаються перевіркою разом з ним. Жертва вірить, тому що інші названі імена належать справжнім співробітникам названого відділу. Потім атакуючий може задавати будь-які питання, аж до того, які логін і пароль використовує жертва).

6 Обмежена кількість «безкоштовного сиру» − віра в те, що об'єкт ділиться частиною інформації, на яку претендують інші, або, що ця інформація доступна тільки в цей момент (приклад атаки: атакуючий розсилає електронні листи, що повідомляють, що перші 500 зареєстрованих на новому сайті компанії виграють 3 квитка на прем'єру відмінного фільму. Коли нічого не підозрюючи співробітник реєструється на сайті, його просять

ввести свою адресу електронної поштової скриньки на робочому місці і вибрати пароль.

Багато людей, щоб не забути безліч паролів, часто використовують один і той же у всіх системах. Скориставшись цим, атакуючий може спробувати отримати доступ до цільового робочого або домашнього комп'ютера зареєстрованого).

Організація відповідальна за те, щоб попередити співробітників наскільки серйозною може бути видача непублічної інформації. Добре продумана інформаційна політика безпеки разом з належним навчанням і тренуваннями поліпшать розуміння співробітників про належну роботу з корпоративною інформацією.

Навчання безпеки в рамках політики організації із захисту інформації повинно проводитися для всіх співробітників без винятку, а не лише для співробітників, у яких є електронний або фізичний доступ до інформаційних активів організації.

В сьогоднішніх умовах майже все, чим займаються співробітники, пов'язане з обробкою інформації. Ось чому політика безпеки організації повинна поширюватися по всьому підприємству, незалежно від положення співробітників [31].

Розробку протидій соціальному інжинірингу необхідно почати з створення групи людей, які будуть відповідати за безпеку. Вони повинні відповідати за розробку політик і процедур безпеки, які повинні бути спрямовані на захист окремих співробітників і мережі організації в цілому. Ця група повинна включати в себе співробітників з різних відділів.

До завдань цієї групи повинні входити такі речі як:

1 Забезпечення підтримки політик і процедур безпеки.

2 Допомога в розробці навчально-методичних матеріалів для співробітників.

Співробітник, відповідальний за розробку програми інформаційної безпеки повинен виробити специфічні вимоги для окремих груп

співробітників, що беруть участь в роботі з інформацією, яка обробляється організацією. Тренінги повинні проводитися для наступних груп персоналу:

1 Менеджери;

2 IT співробітники;

3 Користувачі ПК;

4 Обслуговуючий персонал;

5 Адміністратори і їх асистенти;

6 Техніки зв'язку;

7 Охоронці (потрібно короткий курс навчання).

Технічні засоби навчання повинні включати:

1 Демонстрацію соціального інжинірингу за допомогою гри за ролями;

2 Оглядові медіазвіти щодо останніх атак на інші організації;

3 Обговорення шляхів запобігання втрати інформації;

4 Перегляд спеціальних відеоматеріалів з безпеки.

Організація зобов'язана не тільки мати прописані правила політик безпеки, а й спонукати співробітників, що працюють з корпоративною інформацією або комп'ютерною системою, старанно вивчати і дотримуватися цих правил. Більш того, необхідно переконатися, що всі співробітники організації розуміють причину прийняття тих чи інших положень в правилах, тоді вони не будуть намагатися обходити ці правила заради отримання власної вигоди.

Правила безпеки повинні бути реалістичними, вони не повинні закликати співробітників виконувати занадто обтяжливі речі, які, швидше за все, будуть ними проігноровані. Також, програма навчання з безпеки повинна переконати співробітників, що необхідно виконувати доручення по роботі швидко, але найкоротший шлях, який нехтує системою безпеки, виявляється шкідливим для самої організації і співробітників.

Але, навіть ознайомившись з усіма документами і навчанням, багато співробітників навряд чи змінять свою щоденну поведінку. Для цього необхідно подбати про відповідне підкріплення.

Воно може бути двох типів:

•негативне;

• позитивне.

Негативне означає покарання за якусь провину щодо дотримання заходів безпеки (приклад: якщо під час перевірки виявилося, що співробітник приліпив лист з паролем на монітор, то йому повинна бути зроблена догана).

Інший метод − «прив'язати» турботу про безпеку до річного звіту про діяльність співробітника, що, в свою чергу, змушує зрозуміти її важливість і, врешті-решт, відповідальність за безпеку лягає на кожного. Негативне підкріплення може служити для запобігання серйозних порушень (наприклад: установка неавторизованої точки доступу або модему).

Позитивне підкріплення забезпечує натхненням співробітників з турботи про безпеку (приклад: замість пошуку порушників політики − встановлення, кого з користувачів слід заохотити за точне дотримання інструкцій).

Головною метою будь-якої навчальної програми є необхідність переосмислення співробітниками своєї поведінки і відносин, мотивування [32, с. 197], їх бажання захистити і зберегти інформацію організації. Хорошою мотивацією є демонстрація винагороди за участь не самої організації, а конкретних співробітників.

Основними цілями при розробці методики навчання персоналу та захисту інформації, є фокусування уваги на те, що:

• співробітники організації можуть бути піддані нападу в будь-який час;

• співробітники повинні вивчити і зрозуміти свою роль в захисті інформації організації;

• тренінг з навчання безпеки повинен бути важливішим, ніж просто правила, які надаються для ознайомлення.

Організація може вважати цілі досягнутими, якщо всі співробітники звикнуть до думки, що захист інформації - це частина їх обов'язків.

Співробітники повинні повністю зрозуміти, що атаки соціальних інженерів реальні, що втрата оброблюваної організацією інформації загрожує не тільки організації, але персонально кожному із співробітників, їх роботі та добробуту.

У своїй основі навчальний тренінг повинен бути побудований таким чином, щоб відвідувався усіма співробітниками. Знову прийняті на роботу співробітники повинні проходити тренінг як частина початкового ознайомлення і знайомства з новою роботою [33, с. 75]. Рекомендується взагалі не допускати співробітника до роботи з комп'ютером, поки він не ознайомиться з навчальним тренінгом і основами інформаційної безпеки.

Найпершим рекомендується заняття, яке присвячене позаштатним ситуаціям і системам оповіщення. Ознайомлення з набором коротких важливих повідомлень помітно полегшить сприйняття матеріалу співробітниками.

Особливе значення першого заняття слід висловити в особливій ролі гармонії, яка пануватиме в організації, після того як стануть керуватися цією програмою. Більш важливим, ніж навчальні тренування, буде мотивація, яка повинна спонукати співробітників прийняти персональну відповідальність за безпеку.

У ситуаціях, коли будь-які співробітники не можуть відвідувати загальні заняття, організація повинна вдатися до інших форм навчання, таким як відео, комп'ютерні програми, онлайн курси або друковані матеріали.

Після короткого вступного заняття інші довші заняття повинні бути сплановані так, щоб всі співробітники уважно ознайомилися зі слабкими місцями і техніками атак, які можуть застосовуватися конкретно на них.

Завершальним етапом програми слід проводити отримання підписів співробітників про угоду слідування встановлених політик безпеки і принципів поведінки. Відповідальність, яку повинні будуть брати на себе співробітники, підписавши угоду, допоможе уникати сумнівів (тобто

надходити як хто-небудь просить, або надходити як того вимагає політики безпеки).

Як мінімум один раз на рік необхідно проводити заняття для повторення всіх цих правил.

Начальники відділів повинні бути готові до того, що їм доведеться витрачати час на підлеглих для того, щоб допомогти їм зрозуміти і самим взяти участь у процесі навчання.

Тренінг слід робити в робочий час. Це варто пам'ятати і при ознайомленні з усіма положеннями організації, нових співробітників.

Співробітники організації, які отримали підвищення, повинні пройти тренінг ще раз відповідно до їх нових посадових обов'язків.

Практична інформація тренінгу з безпеки, що описує риси людського характеру і пов'язані з ними аспекти соціального інжинірингу, включає:

•опис того, як атакуючі використовують навички соціального інжинірингу;

•опис методів, використовуваних соціальними інженерами для досягнення своїх цілей;

•заходи щодо попередження можливих атак з використанням соціального інжинірингу;

•процедуру обробки підозрілих запитів;

•послідовність дій при повідомленні про спроби або вдалих атаках;

•важливість ідентифікації того, хто робить запит на отримання інформації;

•класифікацію інформації, процедури захисту, надання важливої інформації, включаючи будь-які дані про систему її зберігання;

•анотація ключових політик безпеки і їх призначення;

•обов'язки всіх співробітників слідувати політикам безпеки;

•політику використання електронної пошти, включаючи захист від віддалених атак за допомогою вірусів, червів і «троянів»;

•носіння бейджів і посвідчень як метод фізичного захисту.

2.2 Аналіз технічних засобів захисту від соціальної інженерії

До технічного захисту можна віднести засоби, що заважають отримати інформацію і засоби, що заважають скористатися отриманою інформацією. В цілому засоби забезпечення захисту інформації в частині запобігання навмисних дій в залежності від способу реалізації можна розділити на групи.

Технічні (апаратні) засоби. Це різні за типом пристрою (механічні, електромеханічні, електронні та ін.), які апаратними засобами вирішують завдання захисту інформації. Вони або перешкоджають фізичному проникненню, або, якщо проникнення все ж відбулося, доступу до інформації, в тому числі за допомогою її маскування. Першу частину завдання вирішують замки, решітки на вікнах, захисна сигналізація та ін. Другу − генератори шуму, мережеві фільтри, скануючі радіоприймачі і безліч інших пристроїв, які «перекривають» потенційні канали витоку інформації або дозволяють їх виявити. Переваги технічних засобів пов'язані з їх надійністю, незалежністю від суб'єктивних факторів, високу стійкість до модифікації. Слабкі сторони − недостатня гнучкість, відносно великі обсяг і маса, висока вартість.

Програмні засоби включають програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації типу тимчасових файлів, тестового контролю системи захисту та ін. Переваги програмних засобів - універсальність, гнучкість, надійність, простота установки, здатність до модифікації і розвитку. Недоліки − обмежена функціональність мережі, використання частини ресурсів файл-сервера і робочих станцій, висока чутливість до випадкових або навмисних змін, можлива залежність від типів комп'ютерів (їх апаратних засобів).

Змішані апаратно-програмні засоби реалізують ті ж функції, що апаратні і програмні засоби окремо, і мають проміжні властивості.

Організаційні засоби складаються з організаційно-технічних (підготовка приміщень з комп'ютерами, прокладка кабельної системи з

урахуванням вимог обмеження доступу до неї та ін.) і організаційно-правових (національні законодавства і правила роботи, що встановлюються керівництвом конкретного підприємства). Переваги організаційних засобів полягають у тому, що вони дозволяють вирішувати безліч різнорідних проблем, прості в реалізації, швидко реагують на небажані дії в мережі, мають необмежені можливості модифікації і розвитку. Недоліки - висока залежність від суб'єктивних чинників, в тому числі від загальної організації роботи в конкретному підрозділі.

Приклади технічних засобів захисту: міжмережеві екрани, шифрування, проксі-сервери, СКУД, системи охорони та сигналізації.

Panda Internet Security 2016 − комплексний антивірус з фаєрволом, хмарними технологіями і проактивним захистом. Включає інструменти для захисту від шкідливих і фішингових веб-сайтів, захисту персональних даних, онлайн резервного копіювання.

Містить:

•антивірус (захист від всіх типів вірусів, червів і троянів);

•технологія TruPrevent (блокування невідомих вірусів навіть при неоновленому антивірусу, аналіз невідомих вірусів на предмет їхньої поведінки);

•антишпіон / Анти-adware (захист ПК від шпигунів і рекламного ПЗ);

•захист від онлайн-шахрайства (антифішинг). Захист від шахраїв при роботі з онлайн-банками і магазинами;

•автоматичні оновлення;

•файервол (захист від проникнення хакерів на ПК);

•блокування підозрілих веб-сторінок (запобігає доступу до веб-сторінок з небезпечними скриптами);

•виявлення загроз в Wi-Fi мережах (безпека бездротових з'єднань);

•захист особистих даних і контроль приватності (безпека персональних даних та захист від спроб онлайн-крадіжки);

•антиспам (блокування небажаної пошти);

•віртуальна клавіатура (паролі в безпечному режимі завдяки віртуальній клавіатурі);

•режим гри / мультимедіа;

•менеджер домашньої мережі (перевіряє статус безпеки домашніх комп'ютерів за допомогою нового менеджера домашньої мережі);

•онлайн-резервування (отримайте доступ до даних з будь-якого місця завдяки функції онлайн-резервування з виділеним простором об'ємом 2 ГБ);

•віддалений доступ до ПК (отримаєте доступ до домашнього або офісного комп'ютера завдяки функції видаленого доступу до ПК);

•шифрування файлів (захист файлів від очей за допомогою функції шифрування файлів);

•знищення файлів (видалення необхідних файлів назавжди, щоб ніхто ніколи не зміг отримати доступ до даних).

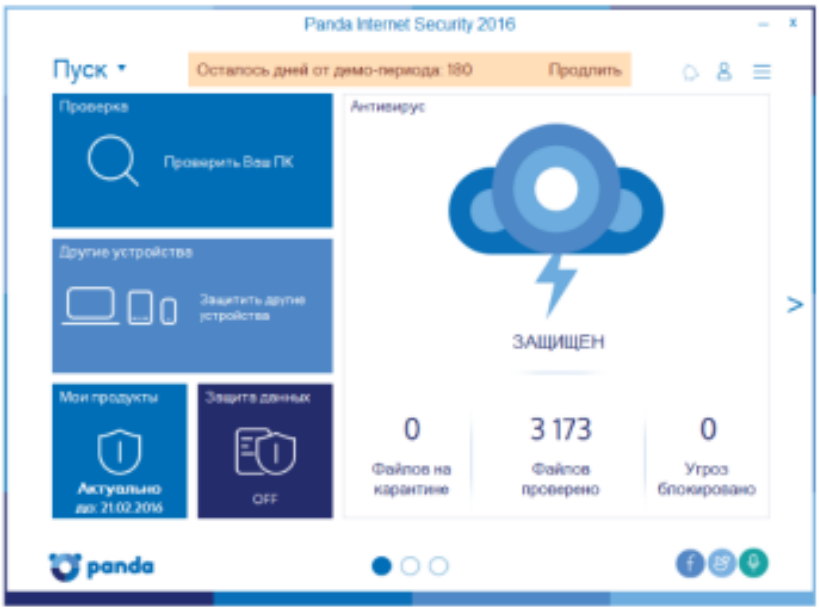

Рисунок 2.1 − Робота Panda Internet Security

Таким чином, Panda Internet Security є підходящим для організації, оскільки даний продукт максимально захищає робочі станції практично від усіх мережевих атак (фішинг, спам, реклама, банери). З точки зору ціни і функціональності це найоптимальніший варіант. Встановивши даний продукт на кожному робочому місці, можна значно скоротити кількість атак, які надходять через Інтернет.

2.3 Актуальні проблеми соціальної інженерії в організації ТОВ «Азимут -Трейд»

2.3.1 Характеристика організації

Дослідження даної проблеми розглядається на прикладі організації ТОВ «Азимут-Трейд», що має трирівневу ієрархію: головний центр − підлеглі управління – відділи.

Кількість працівників залежить від рівня ієрархії: на головний офіс припадає 100 осіб, підлеглі управління - 50 осіб, відділи - 8 осіб.

У даній організації відбувається обробка понад 100 тисяч персональних даних.

На кожен рівень ієрархії доводиться по одній базі даних і однієї локальної обчислювальної мережі (ЛОМ). Головний офіс і підлеглі управління мають 2 поштових сервера, відділи мають по одному. Загальна кількість ПЕОМ в головному офісі - 75, підлеглих управліннях - 35, відділах - 15.

2.3.2 Аналіз соціальної інженерії в організації ТОВ «Азимут-Трейд»

Оброблювана інформація може служити соціальним інженерам для вилучення будь-якої вигоди або для використання в певних цілях.

У зв'язку з тим, що обробляється велика кількість персональних даних, то до подібної бази даних має доступ велика кількість співробітників, які потенційно можуть бути схильні до соціальних атак, що може привести до розголошення інформації, в наслідок чого, організація понесе матеріальні збитки.

Для створення методики протидії загрозам, пов'язаних з використанням соціальної інженерії, необхідно виконати три дії. При цьому потрібно пам'ятати, що ефективність захисту багато в чому визначається під час її планування. Щоб не допустити можливих загроз, необхідно виконати три наступні дії:

1 Розробити стратегії управління забезпечення безпеки. Необхідно визначити завдання захисту від загроз, пов'язаних з соціальною інженерією і призначити співробітників, що відповідають за їх виконання.

2 Провести оцінку ризиків. Проаналізувати кожну загрозу і визначити, наскільки вона небезпечна для організації, яких збитків вона може завдати.

3 Провести інтеграцію принципів захисту від атак соціальних інженерів в політику безпеки організації. Розробити процедури, які регламентують дії співробітників в ситуаціях, які можуть виявитися атаками соціальних інженерів.

Стратегія управління забезпеченням безпеки дає загальне уявлення про загрози соціальної інженерії, яким піддається організація. Співробітники, відповідальні за розробку політик і процедур, які блокують ці загрози:

1 Куратор з безпеки. Повинен стежити за тим, щоб всі співробітники ставилися до забезпечення безпеки серйозно, і володіти необхідним для цього авторитетом.

2 Адміністратор з безпеки. Повинен відповідати за організацію розробки політик безпеки і їх оновлення відповідно до змін вимог.

3 Адміністратор по інформуванню співробітників про способи забезпечення безпеки - керівний співробітник, який повинен відповідати за розробку та проведення кампаній з інформування співробітників про загрози та способи захисту від них.

Співробітники, які виконують ці ролі, повинні формувати керівний комітет із забезпечення безпеки, який визначає головні цілі стратегії управління забезпеченням безпеки. Пов'язано це з тим, що без визначення цілей, буде складно залучати до участі в проектах із забезпечення безпеки інших співробітників і оцінювати результати таких проектів. Першою задачею, яка повинна бути виконана керівним комітетом щодо забезпечення безпеки, є виявлення в корпоративному середовищі вразливостей, що роблять можливими атаки соціальних інженерів. Для

швидкого отримання уявлення про можливі напрямки атак, була складена таблиця 2.1.

Таблиця 2.1 – Можливі вразливості, що допускають проведення атак, заснованих на методах соціальної інженерії

Напрямок атаки	Вразливість
Електронна пошта	Співробітники схильні до фішингових атак і атак, що стосуються «людського фактора»
Інтернет	Користування Інтернетом в особистих цілях погіршує становище неможливістю контролю за діями співробітників, можливі атаки типу «троянський кінь», «фармінг», «людська відмова в обслуговуванні»
Телефонні атаки	Вішинг-атаки
Служба підтримки	Атаки «послуга за послугу» і зворотна соціальна інженерія
Безпека офісу	Офіси знаходяться в незамкненому стані протягом всього дня. Це дозволяє зловмисникові потрапити в середину приміщення. Можливі атаки типу «дорожнє яблуко»
Атаки на зовнішнє і внутрішнє сміття	Від сміття кожен відділ позбавляється самостійно. Сміттєві контейнери розташовуються на території організації. Можливий витік інформації шляхом збору інформації з відкритих джерел

При розробці заходів щодо забезпечення безпеки завжди потрібно оцінити рівень ризику, якому піддається організація при різних атаках. Спираючись на інформацію про головні елементи стратегії управління забезпеченням безпеки, були згруповані фактори ризику. Нижче перераховані категорії ризику:

•витік інформації (ВІ);

•шкода репутації організації (ШРО);

•зниження працездатності організації (ЗПО);

•трата ресурсів (ТР);

•фінансові втрати (ФВ).

Використовуючи таблицю вразливостей, що допускають проведення атак соціальних інженерів, для організації визначені вимоги політик безпеки, типи і рівні ризику. Результат представлений у таблиці 2.2.

Таблиця 2.2 − Форма для визначення вимог щодо забезпечення безпеки і оцінки факторів ризику

Напрямок атаки	Вимоги політик безпеки	Тип ризику	Рівень ризику	Дія
Електронна пошта	Прийняти ПБ, яка регламентує дії співробітників при отриманні вкладень конкретних типів	ВІ ШРО ФВ	3	Розробити ПБ використання електронної пошти, створити єдиний поштовий клієнт-сервер
Інтернет	Прийняти ПБ, яка регламентує використання інтернету	ВІ ШРО ТР	4	Розробити ПБ використання інтернету
Спливаючі додатки	Включити в політику використання інтернету явні вказівки з приводу того, що слід робити при появі спливаючих вікон	ВІ ТР ФВ	3	Розробити політику використання комп'ютерів

Продовження таблиці 2.2

Служба миттєвого обміну повідомленнями	Прийняти політику, яка визначає підтримувані і допустимі клієнтські програми миттєвого обміну повідомленнями	ВІ ШРО	2	Розробити правила по роботі із службами миттєвими повідомленнями
Корпоративна телефонна станція	Прийняти політику управління обслуговуванням корпоративної телефонної станції	ВІ ФВ	2	Розробити політику роботи при телефонних переговорах
Служба підтримки	Прийняти політику, яка регламентує надання доступу до даних	ВІ ТР	2	Розробити політику управління доступом
Паперове сміття	Прийняти політику утилізації паперового сміття Визначити принципи використання сміттєвих контейнерів	ВІ ШРО ФВ	3	Розробити інформаційну ПБ
Електронне сміття	Прийняти політику утилізації електронного сміття	ВІ ШРО ФВ	3	Розробити інформаційну ПБ

Продовження таблиці 2.2

Фізична безпека	Прийняти політику роботи з відвідувачами	ВІ ФВ		Розробити ПБ роботи з відвідувачами
Безпека офісу	Прийняти політику управління ідентифікаторами і паролями користувачів	ВІ ШРО ФВ	З	Розробити ПБ ідентифікації і аутентифікації

Для полегшення реалізації цих заходів, необхідно розробити протоколи реагування на інциденти.

При отриманні інформації про атаку, співробітникам технічного відділу необхідно проводити додатковий аудит безпеки. Кожен інцидент надає нову інформацію для поточного аудиту безпеки відповідно до моделі реагування на інциденти.

При реєстрації інциденту потрібно з'ясувати, чи представляє він для організації нову або змінену загрозу, і, спираючись на зроблені висновки, створити або оновити політики і процедури.

Для управління інцидентами необхідно використання протоколу, реєструючи в ньому наступну інформацію:

1 Жертва атаки;

2 Дата;

3 Напрям атаки;

4 Опис атаки;

5 Результат атаки;

6 Наслідки атаки;

7 Подальші рекомендації.

Реєстрація інцидентів дозволить визначати шаблони атак і покращувати захист від майбутніх атак.

При повному аналізі організації, були виявлені наступні фактори, які роблять організацію уразливими до атак:

1 Більша кількість співробітників дозволяє соціальному інженеру провести атаку, представившись ким-небудь з органів управління або головного центру.

2 Інформація про місцезнаходження співробітників дозволяє соціальному інженеру використовувати таку інформацію в корисливих цілях, наприклад, посилаючись на співробітника, місцезнаходження якого йому відомо.

3 Інформація про внутрішні телефони і назви відділів допомагає соціальному інженеру досконально вивчити внутрішню структуру організацій, яка при проведенні атаки, дозволить оперувати йому точними назвами відділів і внутрішніми телефонами, які не повинні бути загальнодоступними.

4 Відсутність будь-яких документів, що регламентують політики та правила безпеки, так само відсутність повного навчання співробітників цих правил допомагає соціальному інженеру тим, що співробітники не навчені тому, як вести себе в тих чи інших ситуаціях, що в свою чергу дозволяє йому маніпулювати співробітниками без особливого зусилля.

5 Документи, які не повинні бути загальнодоступними, а за своєю суттю, є комерційною таємницею, можуть переплутати, загубитися або підібратися відвідувачами.

6 Відсутність будь-яких повідомлень від співробітників про те, що відбулися інциденти, що стосуються оброблюваної інформації. Соціальні інженери знають, що, навіть якщо їх виявлять, у співробітника немає можливості попередити інших співробітників про атаки. В результаті атака може бути продовжена з мінімальними змінами і після компрометації. По суті, компрометація тільки поліпшить атаку, так як атакуючі дізнаються, що

саме не спрацьовує. Це дозволяє соціальному інженеру практично на 100% бути впевненим в тому, що співробітник, на якого може бути проведена атака, не писатиме службових записок і доповідних, що тягне за собою некараність і не знання інших співробітників про проведену атаку, в зв'язку з чим, соціальний інженер може скористатися даним видом атаки знову і знову.

7 Використання особистих поштових скриньок на робочому місці створює уразливості комп'ютерних мереж організацій. Це дозволяє соціальному інженеру проникнути в мережу організації за допомогою поштової скриньки будь-якого співробітника через те, що не виробляється перевірка вхідних листів і по недбалості працівника.

Наступним етапом виявлення вразливостей необхідно виявити співробітників, які є головними об'єктами атак соціальних інженерів.

В першу чергу ними є:

1 Секретар в приймальні. При виникненні довіри, соціальний інженер здатний отримати телефони інших співробітників.

2 Співробітник по роботі з клієнтами. При поданні будь-яким клієнтом, можливо отримати інформацію щодо необхідної організації.

3 Телефонні довідники. Вони дозволяють знайти необхідні номери, а також отримати уявлення про структуру організації, тобто точні назви відділів, посад.

2.3.3 Проведення необхідних заходів щодо виявлених вразливостей організації

Після виявлених вразливостей, було прийнято рішення про їх усунення. Перелік вжитих заходів в організації включає:

1 Розробка політик безпеки і процедур. Були розроблені такі процедури і політики безпеки, як:

•інформаційна політика безпеки (метою є визначення секретної інформації організації і способи її захисту. Розроблена політика безпеки

передбачає захист для всіх форм інформації, як на паперових носіях, так і в електронному вигляді);

• політика використання комп'ютерів. Вона визначає собою:

а) хто може використовувати комп'ютерні системи, і яким чином вони можуть використовуватися;

б) всі комп'ютери належать організації, і що вони надаються співробітникам для роботи відповідно до їх посадових обов'язків;

в) забороняє використання комп'ютерів, для підключення до внутрішніх систем організації через систему віддаленого доступу, які не належать організації, для виконання роботи, пов'язаної з діловою діяльністю організації;

г) що вся інформація, що зберігається або використовується на комп'ютерах організації, належить організації;

д) що на комп'ютерних системах заборонене завантаження неавторизованого програмного забезпечення;

е) що працівник не повинен мати на увазі приватний статус будь-якої інформації, що зберігається, що відправляється або отримується на будь-яких комп'ютерах організації. Він повинен розуміти, що будь-яка інформація, включаючи електронну пошту, може проглядатися співробітниками технічного відділу. А співробітники відділу безпеки можуть відслідковувати всі дії, пов'язані з комп'ютерами, включаючи відвідування веб-сайтів.

• політика безпеки ідентифікації і аутентифікації (важливим моментом є встановлення основного механізму для аутентифікації співробітників і адміністраторів, в неї включені такі аспекти, як визначення мінімальної довжини пароля, і інших характеристик вибору пароля);

• політика управління доступом (при установці вимог до управління доступом до електронних файлів, механізм доступу і аутентифікаційний механізм працюють в парі, що забезпечує отримання доступу до файлів тільки авторизованим користувачам);

•політика використання інтернету (вона визначає відповідне призначення і нецільове використання інтернету);

•політики безпеки використання електронної пошти. Ця політика обумовлює як внутрішні проблеми, так і зовнішні;

•політики безпеки при проведенні телефонних переговорів (визначає правила ведення як внутрішніх, так і зовнішніх телефонних переговорів);

•політики безпеки роботи з відвідувачами (вона визначає правила для охоронців і співробітників, які працюють з відвідувачами).

а) внутрішні проблеми: політика роботи з електронною поштою не конфліктує з іншими політиками, пов'язаними з співробітниками організації, але визначає, що працівник не повинен вважати електронну пошту приватної;

б) зовнішні проблеми: політика пошти визначає, за яких умов в ній присутні посилання на інформаційну політику, яка визначає методи захисту секретних даних. Так само обумовлюються питання, пов'язані з вхідними повідомленнями електронної пошти. Вона посилається на політику безпеки організації, в якій йдеться про відповідні заходи, спрямовані на боротьбу з вірусами.

• процедура обробки інцидентів. Вона визначає способи реагування на виникнення інцидентів, пов'язаних з безпекою. Так само визначає, хто має право доступу і що необхідно робити, а так само визначає цілі організації, що досягаються при обробці інциденту. Цими цілями є:

а) захист систем організації;

б) захист даних організації;

в) відновлення операцій;

г) припинення діяльності зловмисника;

д) зниження рівня антиреклами або збитку.

2 Розробка переліків інформації, створення переліку відомостей, що становлять комерційну таємницю.

3 Надання методичного матеріалу, політик безпеки всім співробітникам. Всі співробітники організацій, під розпис були ознайомлені з

політиками безпеки, пройшли повні інструктажі та курс з протидії соціальним інжинірингом.

4 Розсилка інформаційних статей, нагадувань і т.п. за допомогою електронної пошти, локальної мережі і «особисто в руки». Співробітникам, за допомогою їх електронних пошт і локальної мережі організації, стали розсилатися постійно оновлювані інформаційні статті, що містять новини безпеки, а також постійні, але різноманітні нагадування з протидії соціальному інжинірингу.

5 Публікація найбільш надійного працівника місяця. Даний захід є своєрідним «пряником» в системі безпеки, тобто замість співробітника, який порушив політики безпеки, вибирається співробітник, який виконав всі обов'язки з безпеки на 100%, і заохочується.

6 Створення зберігачів екрану і екранних заставок з нагадуваннями. Технічним відділом були створені екранні хранителі для робочих комп'ютерів, які виглядають у вигляді постійно мінливих рад і нагадувань про можливих атак соціальних інженерів.

7 Створення системних повідомлень в локальній мережі. Технічним відділом була створена програма, яка використовує локальну мережу, і надалі працює за принципом спливаючих вікон. У всіх співробітників, в певний момент часу, в кутку екрану виникає спливаюче вікно з нагадуванням (вміст вікна постійно змінюється). Закрити вікно, можливо тільки натиснувши певну кнопку.

8 Створення єдиного поштового клієнт-сервера. Був створений єдиний поштовий клієнт-сервер, що дозволив технічному відділу контролювати вхідну і вихідну пошту. У зв'язку з цим, ймовірність загрози пов'язаної з електронною поштою, значно зменшилася.

9 Постійне обговорення питання безпеки на зборах, п'ятихвилинка і т.д.

Підсумком вжитих заходів стало те, що нагадування стали своєчасними і постійними.

2.4 Методика протидії соціальному інжинірингу

Необхідні дії і заходи дотримання правил. Для захисту організацій і їх співробітників слід застосовувати комплексні багаторівневі системи безпеки. Нижче перераховані особливості і обов'язки таких систем:

1 Фізична безпека− це бар'єри, які обмежують доступ в будівлі організації і до корпоративних ресурсів. Так само варто пам'ятати, що ресурси організації, наприклад, сміттєві контейнери, які розташовані поза територією організації, фізично не захищені [34, с. 70].

2 Дані−це ділова інформація (облікові записи, поштова кореспонденція і так далі). При аналізі загроз і плануванні заходів щодо захисту даних потрібно визначати принципи поводження з паперовими і електронними носіями даних.

3 Додатки − програми, що запускаються співробітниками.

4 Комп'ютери − це сервери і клієнтські системи, які використовуються в організації. Захист співробітників від прямих атак на їх комп'ютери, проводиться шляхом визначення принципів, які вказують які програми можна використовувати на корпоративних комп'ютерах.

5 Внутрішня мережа − це мережа, за допомогою якої взаємодіють корпоративні системи. Вона може бути локальною, глобальною або бездротовою. Співробітникам організації необхідно роз'яснювати, що вони повинні робити для організації безпечної роботи в будь-якому мережевому середовищі.

6 Периметр мережі − це межа між внутрішніми мережами організації і зовнішніми, такими як інтернет або мережі партнерських організацій.

Необхідно нагадувати співробітникам, що в разі розголошення комерційної таємниці кожного з них чекає звільнення за відповідними статтями Трудового і Цивільного кодексу України [35], що може негативно вплинути на можливість подальшого працевлаштування на відповідальну посаду.

Слід заохочувати співробітників, які виявляють спроби соціальних інженерів отримати доступ до конфіденційної інформації. Також необхідно заохочувати пильних співробітників за те, що вони відстояли честь організації і не піддалися на хитрощі соціального інженера. Таке стимулювання має привести до того, що всі співробітники будуть обережно ставитися до спілкування зі сторонніми особами.

Інша міра захисту − це об'єднання колективу, встановлення дружніх зв'язків всередині нього, проведення корпоративних вечорів. Коли співробітники знають один одного добре, в тому числі співробітників з філій, то ймовірність того, що стороння людина зможе представитися кимось із персоналу, буде значно менше, в зв'язку з тим, що співробітники будуть впізнавати один одного по голосу.

Телефонні переговори. Необхідно, щоб всі в організації, а особливо ті, що працюють з клієнтами, дотримувалися певних правил безпеки при розмовах з користувачами послуг і персоналом. При заочній розмові, необхідно повністю переконатися, що з того боку дійсно та людина. Необхідно навчити співробітників тому, щоб вони задавали уточнюючі питання для ідентифікації особи (наприклад: прохання підтвердити розмову по телефону повідомленням по електронній пошті).

Існує три основних типи атак, спрямованих на офісні АТС, під час яких:

•просять інформацію, зазвичай імітуючи законного користувача для звернення до телефонної системи безпосередньо або для одержання віддаленого доступу до комп'ютерних систем;

•отримують доступ до «вільного» використання телефону;

•отримують доступ до системи комунікацій.

Термін для атак такого роду називається фрікінг. Найпростіший підхід соціального інженера− це симулювання ролі телефонного інженера, як показано на рисунку 2.2.

Соціальний інженер не може досягти успіху у видобутку інформації від співробітника, який відповідає на всі виклики. Даний тип атаки, працює лише, коли соціальний інженер розмовляє із співробітників, чий номер телефону не доступний широкому загалу, в зв'язку, з чим створюється враження, що той, хто дзвонить, працює в організації.

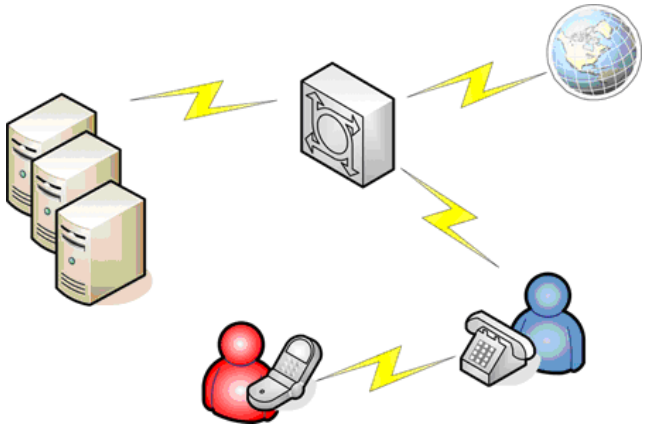

Рисунок 2.2 – Схема нападу на офісну АТС

Не дивлячись на переконливість уявлення запитуваного, незважаючи на статус або посаду в організації, ніяка інформація, яка не призначена для громадського доступу, не повинна бути надана, поки особистість того, хто телефонує не буде доведено (не можна використовувати візитні картки та іншу контактну інформацію, надану самою невідомою особою).

Співробітники повинні негайно зв'язуватися з співробітниками технічного відділу, якщо до них звертається хтось, який заявляє, що він співробітник технічної підтримки.

Навіть коли особистість того, хто дзвонить встановлена, не можна розголошувати конфіденційну інформацію по телефону та електронною поштою, якщо це не передбачено інструкцією. При чіткому регламентуванні правила передачі конфіденційних відомостей на паперових носіях з рук в руки, відходити від цього правила не можна, навіть якщо той, хто звернувся стверджує, що ці дані дуже необхідні.

Співробітники повинні записувати прізвище, ім'я та по батькові того, хто телефонував, телефон і назву організації, офісу або підрозділу, перш ніж покласти трубку. При необхідності передзвонити, співробітник повинен

переконатися, що у зазначеній організації дійсно є співробітник з таким прізвищем і що телефон, по якому треба передзвонити дійсно телефон цієї організації.

Якщо працівник не може перевірити номер телефону з незалежного джерела, його необхідно проінструктувати про інші способи зробити це, наприклад, звернувшись до безпосереднього начальника.

Технічний відділ повинен балансувати між безпекою та діловою ефективністю, а політика і процедури безпеки повинні допомагати в цьому.

Соціальні інженери намагаються створювати такі ситуації, коли звичайний порядок дій розмови по телефону виявляється непридатним.

Секретар, який здійснює прийом основного потоку дзвінків, повинен бути проінструктований щодо небезпеки перекладу підозрілих зовнішніх дзвінків на внутрішню лінію (пов'язано це з тим, що у співробітника, якому був переведений такий дзвінок, виникає відчуття, що йому подзвонили по внутрішньому номеру, і його пильність знижується) . Також потрібно, щоб секретар при проханнях дати номер будь-якого співробітника, директора або керівника уточнював особистість того, хто дзвонить, записував інформацію про нього в журнал, в тому числі вказував мету дзвінка (документувати такі ситуації необхідно якомога докладніше: хто дзвонив, з якого питання, корисно також передавати суть розмови).

Необхідно здійснювати захист аналітика технічного відділу. Процедури захисту повинні забезпечувати подвійну роль в цій ситуації:

• аналітик технічного відділу повинен мати гарантії аудиту всіх дій (необхідно вести журнал всіх дій так, щоб швидко виправити або обмежити будь-які збитки в разі атаки);

• аналітик технічного відділу повинен мати структуровану процедуру дій обробки запитів користувачів.

Аудит всіх процедур − найцінніший інструмент в запобіганні інциденту і подальшому його розслідуванні.

Слід мати окремий ідентифікатор для робіт, пов'язаних з підтримкою інформаційних систем. Наявність такого ідентифікатора дозволить відокремити функції технічного супроводу від інших і забезпечить додаткову безпеку як для робіт по супроводу, так і для взаємодії співробітників в організації.

Для контролю телефону, слід використовувати запис розмов, але необхідно пам'ятати про те, що співробітники пам'ятають інформацію і після закінчення робочого дня, в зв'язку з цим, соціальний інженер може зв'язатися з необхідним йому співробітником в неробочий час.

Також необхідно постійне оновлення телефонного довідника для того, щоб всі співробітники були в курсі про прийняття або звільнення співробітників.

Для того щоб класифікувати напади і визначити ризики в організації, необхідно використовувати матрицю векторів нападу, цілей нападу і описів, викладених в таблиці 2.3.

Таблиця 2.3 − Телефонні напади

Цілі нападу	Опис	Спрямованість
Запит інформації організації	Соціальний інженер виконує роль законного користувача для отримання конфіденційної інформації	Конфіденційна інформація Ділова довіра
Телефонний запит інформації	Соціальний інженер прикидається телефонним майстром для отримання доступу до офісної АТС	Ресурси Гроші
Використовуючи офісну АТС, звернутися до комп’ютерних систем	Соціальний інженер зламує комп'ютерні системи, використовуючи офісну АТС, захоплює або управляє інформацією	

Вішинг. Даний вид загрози названий за аналогією з фішингом, тільки в разі вішинг в повідомленні міститься прохання зателефонувати на певний міський номер. При цьому зачитується повідомлення, в якому потенційну жертву просять повідомити свої конфіденційні дані.

Перш за все, захиститися від такого виду атак можна за допомогою здорового глузду, а саме:

1 При дзвінку, організація, послугами якої ви користуєтеся, зазвичай звертається до клієнта по імені та прізвища, як по телефону, так і по електронній пошті. Якщо це не так, то швидше за все це шахрайство.

2 Не можна дзвонити з питань безпеки кредитної карти або банківського рахунку по запропонованому номеру телефону.

3 Якщо ж дзвонить хтось, хто представляється провайдером і задає питання, що стосуються конфіденційних даних - це шахраї, і слід перервати розмову.

Електронна пошта. Вхідні електронні листи можуть містити гіперпосилання, які змушують співробітників до порушення захисту корпоративного середовища. Такий вид шахрайства називається «фармінг».

Фармінг − це технологія інтернет-шахрайства, яка полягає в крадіжці особистих конфіденційних даних, таких як паролі доступу, дані банківських та ідентифікаційних карт і т.д. Приклад посилання, показаний на рисунках 2.3 і 2.4, не завжди веде на заявлені в листі сторінки. Якщо уважніше розглядати рисунок 2.3, то можна знайти дві відмінності: текст в пошті заявляє, що сайт безпечний, використовуючи «https», однак на екрані видно, що сайт фактично використовує «http», а так само назва організації в пошті - «Contoso», але посилання вказує на організацію під назвою «Comtoso».

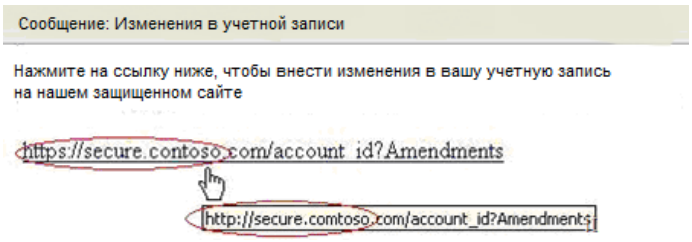

Рисунок 2.3 − Зразок гіперпосилання на фішинговий сайт

При активації надісланого гіперпосилання, співробітник може завантажити в корпоративну мережу троянську програму або вірус, що дозволяє легко обійти багато видів захисту. Гіперпосилання також може вказувати на вузли з спливаючими додатками, які запитують будь-які дані або пропонують допомогу. Найефективнішим способом захисту від подібного роду атак є скептичне ставлення до будь-яких несподіваних вхідних листів [36, с. 76]. Для поширення цього підходу в організації в політику безпеки включаються конкретні принципи використання електронної пошти, які охоплюють перераховані нижче елементи:

• вкладені файли;

• гіперпосилання;

• запити особистої або корпоративної інформації, які виходять із середини організації;

• запити особистої або корпоративної інформації, які виходять із-за меж організації.

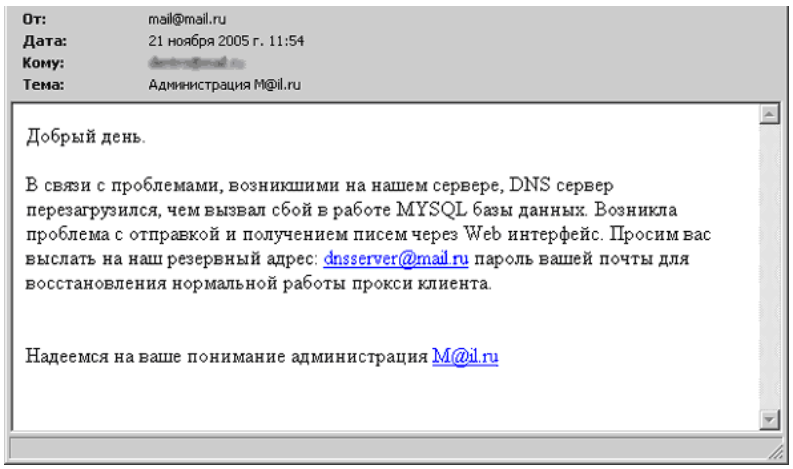

Рисунок 2.4 – Зразок фішингового листа

Прикладами можуть служити електронні листи, які містять пропозиції, що закликають діяти негайно, використовуючи такі ключові фрази як «дійте зараз», «залишилося тільки 20 місць» і т.д.

Так само необхідно вивчати листи, отримані від співробітників організації. Чи відповідає воно корпоративній політиці, чи присутній блок підпису, чи відповідають шрифти корпоративним стандартам.

Якщо легітимність листа із запитом викликає сумнів, то необхідно зв'язатися безпосередньо з організацією, від імені яких воно прийшло. Не можна покладатися на контактну інформацію, яка надана в листі або на веб-сайті, пов'язаним з даними запитом; замість цього слід використовувати координати, вже відомі з попередніх контактів з цією організацією.

Слід зберегти кілька подібних листів для наочного прикладу і нагадування співробітникам про існуючу проблему.

Слід остерігатися вкладених додатків у вхідній пошті і вільного програмного забезпечення.

Необхідно перевіряти доменні імена, в зв'язку з тим, що вкладений в електронний лист файл може містити подвійне розширення типу «creditcard.doc.exe» і значком, звичайно використовуваним для документів Microsoft Word, друге розширення найчастіше приховано, і співробітник не сумнівається, що прийшов саме текстовий документ. Для цього слід включити відображення розширення файлів, виконавши команду «Сервіс> Властивості папки» і зняти прапорець "Приховувати розширення для зареєстрованих типів файлів» на вкладці «Вид»). Це обумовлено тим, що більшість співробітників до сих пір вважають, що програму, яка запускається визначає значок (наприклад: клацнувши на значок із зображенням калькулятора, співробітник очікує, що запуститься калькулятор, а не якийсь там «W32.Bagle-A»).

Розпізнавання фішинг-атак. Найчастіше фішингові повідомлення містять:

• відомості, які викликають занепокоєння, або загрози, наприклад, закриття призначених для користувача банківських рахунків;

• обіцянки величезного грошового призу з мінімальними зусиллями або зовсім без них;

• запити про добровільні пожертвування від імені будь-яких благодійних організацій;

• граматичні, пунктуаційні або орфографічні помилки.

Популярні фішингові схеми:

• шахрайство з використанням відомих брендів будь-яких корпорацій (в таких фішингових схемах використовуються підроблені повідомлення електронної пошти або веб-сайти, які містять назви великих або відомих організацій, в повідомленнях може бути привітання про перемогу в будь-якому конкурсі, проведеному організацією, повідомлення про те, що терміново потрібно змінити облікові дані або пароль);

• підроблені лотереї (співробітник може отримати повідомлення, в якому буде говоритися про те, що він виграв у лотерею, яка проводилася будь-якою відомою організацією);

• помилкові антивіруси або програми для забезпечення безпеки (таке шахрайське ПЗ - це програми, які виглядають як антивіруси, хоча виконують зовсім інші функції, вони генерують неправдиві повідомлення про різні погрози, а також намагаються заманити співробітника в шахрайські транзакції. Співробітники можуть зіткнутися з ними в електронній пошті, в соціальних мережах, в результатах пошукових систем і навіть у спливаючих вікнах на комп'ютері, які імітують системні повідомлення).

Методи боротьби з фішингом, створені для захисту від фішингу:

1 Самостійне введення веб-адреси організації в адресний рядок браузера замість використання будь-яких посилань на підозрілому повідомленні (практично всі справжні повідомлення організацій, містять в собі інформацію, яка недоступна для соціальних інженерів.

2 Технічні методи:

•використання браузерів, які попереджають про загрозу фішингу;

•створення списку фішингових сайтів і подальша звірка з ним;

•використання спеціальних DNS-сервісів, які здійснюють фільтрацію відомих фішингових адрес;

•ускладнення процедури авторизації (наприклад: сайт «Bank of America» пропонує своїм користувачам вибирати особисте зображення і показує це вибране зображення з кожною формою введення пароля, в

результаті користувачам банківських послуг слід вводити пароль лише тоді, коли вони бачать вибране зображення, проте недавнє дослідження показало, що відсутність зображення не зупиняє більшість користувачів при введенні пароля);

•установка спеціалізованих спам-фільтрів, які можуть зменшити число фішингових електронних повідомлень (ця методика заснована на машинному навчанні та обробці природної мови при аналізі фішингових листів);

•послуги моніторингу (організації, що надають послуги цілодобового контролю, аналізу і допомоги в закритті фішингових сайтів).

Інформація, яка відправляється. Необхідно вибудувати систему, яка буде забезпечувати безпеку пересилання важливої інформації якомусь незнайомому особисто відправнику. Так само необхідно розробити спеціальні процедури для передачі файлів з важливою інформацією.

При запиті інформації від незнайомої людини, повинні бути зроблені кроки для підтвердження його особистості. Також повинні бути встановлені різні рівні доступу до інформації.

Засоби, які слід застосувати:

1 Необхідно зрозуміти, наскільки сильно необхідно знати запитувану інформацію запитувачу (даний крок може зажадати отримання схвалення з боку власника інформації).

2 Необхідно зберігати історію всіх транзакцій.

3 Необхідно затвердити список співробітників, які мають право відправляти важливу інформацію. Слід вимагати, щоб лише ці співробітники мали право надсилати інформацію за межі організації.

4 При запиті на інформацію в письмовому вигляді (e-mail, факс або пошта), необхідно вжити особливих заходів, щоб упевнитися в достовірності зазначених вище джерел.

Не можна розкривати особисті та фінансові відомості в електронному листі, не можна відповідати на повідомлення, які запитують подібні

відомості (в тому числі не можна переходити за посиланнями в таких повідомленнях).

Для контролю електронної пошти в організаціях слід зробити єдиний поштовий сервер, яким будуть користуватися всі співробітники організації або філій окремо.

Для того щоб класифікувати напади і визначити ризики в організації, необхідно використовувати матрицю векторів нападу, цілей нападу і описів, викладених в таблиці 2.4.

Таблиця 2.4 − Інтерактивні поштові напади

Цілі нападу	Опис	Спрямованість
Крадіжка інформації, яка належить організації	Соціальний інженер грає роль внутрішнього користувача, для отримання інформації організації	Конфіденційна інформація Ділова довіра
Крадіжка фінансової інформації	Соціальний інженер використовує фішинг, вішинг, фармінг для запиту конфіденційної інформації	Гроші Конфіденційна інформація
Завантаження шкідливого ПЗ	Соціальний інженер обманює користувача і, за допомогою відкриття гіперпосилання або відкриття вкладеного файлу, інфікує мережу організації	Доступність
Завантаження хакерського ПЗ	Соціальний інженер обманює користувача і, за допомогою відкриття гіперпосилання або відкриття вкладеного файлу, завантажує шкідливе ПЗ	Атака на ресурси Доступність Гроші

Спливаючі додатки і діалогові вікна. У зв'язку з переглядом інтернету співробітниками в особистих цілях, ці дії можуть принести небезпеку. Однією з найпопулярніших цілей соціальних інженерів є впровадження поштового сервера в межах комп'ютерної мережі, через яку в подальшому починається фішинг-атака чи інші поштові напади на інші організації або фізичні особи.

Для того щоб класифікувати напади і визначити ризики в організації, необхідно використовувати матрицю векторів нападу, цілей нападу і описів, викладених в таблиці 4.4.

Таблиця 2.5 – Онлайн атака за допомогою спливаючих додатків або діалогових вікон

Цілі нападу	Опис	Спрямованість
Крадіжка персональної інформації	Соціальний інженер запитує персональну інформацію співробітника	Конфіденційна інформація Гроші
Завантаження шкідливого ПЗ	Соціальний інженер обманює співробітника за допомогою гіперпосилання або вкладеного файлу, інфікує мережу організації	Доступність
Завантаження хакерского ПЗ	Соціальний інженер обманює користувача, за допомогою гіперпосилання чи вкладення, завантажує хакерське ПЗ	Атака на ресурси Доступність Гроші

Захист співробітників від спливаючих додатків полягає, перш за все, в розумінні. Необхідно на технічному рівні заблокувати спливаючі вікна і автоматичні завантаження.

Співробітники зобов'язані знати, що вони не повинні натискати посилання на спливаючих вікнах, не порадившись зі співробітниками

технічного відділу. Однак при цьому співробітник повинен бути впевнений, що співробітники технічного відділуне будуть поверхнево ставитися до прохань співробітників про допомогу, якщо він переглядає інтернет.

Служби миттєвого обміну повідомленнями (ІМ). Через швидкість і легкість використання цей спосіб комунікації відкриває широкі можливості для проведення різних атак. Двома основними видами атак, заснованими на використанні служби миттєвого обміну повідомленнями, є:

1 Вказівка в тексті повідомлення посилання на шкідливу програму.

2 Доставка шкідливої програми.

Однією з особливостей служб миттєвого обміну повідомленнями є неформальний характер спілкування. У поєднанні з можливістю привласнювати собі будь-які імена, цей фактор дозволяє соціальному інженеру набагато легше видавати себе за іншу людину і значно підвищує шанси на успішне проведення атаки. На рисунку 2.5 показано, як працює імітація при використанні ІМ.

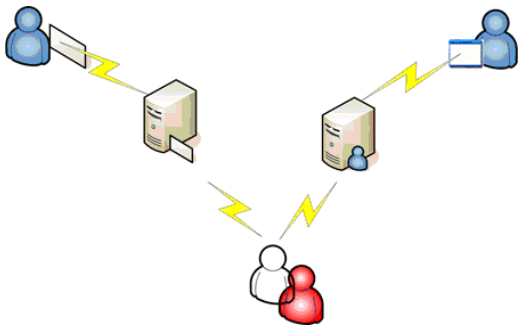

Рисунок 2.5 − Імітація при використанні ІМ

Соціальний інженер (на малюнку виділено червоним кольором) виконує роль відомого користувача і посилає ІМ-повідомлення, виходячи з міркувань, що одержувачі візьмуть їх за повідомлення від людини, яку знають. Знайомство послаблює призначену для користувача захищеність.

При використанні в організації програм, які забезпечують миттєвий обмін повідомленнями, необхідно передбачити в корпоративних політиках безпеки механізми захисту від відповідних загроз. Для отримання надійного

контролю над миттєвим обміном повідомленнями в корпоративному середовищі слід виконати кілька вимог:

• вибрати одну платформу для миттєвого обміну повідомленнями;

• визначити параметри захисту, які задаються при розгортанні служби миттєвого обміну повідомленнями;

• визначити принципи встановлення нових контактів;

• задати стандарти вибору паролів.

Для запобігання неприємностей, що виходять від співробітників, що використовують ІМ і відповідних програм, існує кілька рішень:

1 Блокування загальних портів брандмауерами.

2 Агенти аудиту, які налаштовані на таке ПЗ для відстеження недобросовісних користувачів і усунення додатків, які несуть ризик;

3 Рішення, на зразок, що випускаються «Akonix», які дозволяють застосовувати політику безпеки, включаючи шифрування і виявлення вірусів.

У таблиці 2.6 вказані цілі нападу, опис нападу і спрямованість нападу за допомогою ІМ.

Таблиця 2.6 − Напади ІМ передачі повідомлень

Цілі нападу	Опис	Спрямованість
Запит на конфіденційну інформацію організації	Соціальний інженер, виконуючи роль колеги, використовує ІМ імітацію, для запиту ділової інформації	Конфіденційна інформація Довіра
Завантаження шкідливого ПЗ	Соціальний інженер обманює співробітника за допомогою гіперпосилання або вкладеного файлу, інфікує мережу організації	Доступність
Завантаження хакерского ПЗ	Соціальний інженер обманює користувача, за допомогою гіперпосилання чи вкладення, завантажує хакерське ПЗ	Атака на ресурси Доступність

В цілому, методи захисту від соціального інжинірингу при використанні IM клієнтів, нічим не відрізняються від методів захисту при використанні електронної пошти [37, с. 20].

Паролі. Всі співробітники, що мають доступ до інформації, повинні чітко розуміти, що така проста процедура, як зміна пароля, може привести до серйозної проблеми в безпеці системи.

Співробітники повинні підозріло ставитися до будь-якого запиту з приводу їх облікових даних, тому що саме з паролями пов'язано більшість атак соціальних інженерів.

Ніколи не можна використовувати стандартні паролі, а також не рекомендується користуватися стандартними відповідями на секретні питання. Пароль повинен являти собою набір великих і малих літер, різних символів і цифр. А також розмір повинен бути ніяк не менше шести-семи символів.

Пароль повинен бути досить простим, щоб його не можна було забути, але не настільки, щоб його можна було зламати і скористатися ним.

Паролі, які часто зламують:

• електронна пошта, тому що так можна отримати доступ до всіх сервісів, на яких проводилася реєстрація;

• Skype;

• Facebook.

Паролі, які легко зламати:

• дата народження;

• 111, 333, 777 або щось начебто цього;

• 12345 або qwerty - літери клавіатури йдуть підряд;

• прості імена - sergey, vovan, lena;

• українське слово набране в англійському кодуванні, напр. Сергій вийде Cthutq.

Захищеним паролем є:

• довгий (8-15 символів);

• складно зламати пароль в якому присутні ВЕЛИКІ БУКВИ, малі літери і цифри (не дата народження!);

• не з словника, тобто не слово, і не ім'я;

• окремий пароль для кожного окремого сервісу;

• не пов'язаний зі співробітником (адреса, номер стільникового і т.д).

Рекомендується мати унікальний пароль: для електронної пошти та платіжних систем. Решта паролі можна групувати. наприклад:

• простий пароль і логін для реєстрації у всіх тимчасових і не важливих місць;

• надійний пароль для всіх форумів і соціальних мереж і т.д .;

Найскладніший пароль повинен бути для електронної пошти. Пов'язано це з тим, що якщо отримати доступ до електронної пошти, то можна отримати доступ до всіх місць, де проводилася реєстрація. Тому цей пароль повинен бути надійним.

Ні в якому разі не можна створювати в комп'ютері папку з паролями, краще запам'ятати або записати на папері. Якщо паролі збережені на папері, то необхідно зробити другу копію і зберігати оригінал і копію в недоступному місці, подалі від чужих очей.

Не можна вводити пароль на чужих і підозрілих сайтах, і надсилати поштою, навіть якщо цього вимагає адміністрація сайту, можливо, це шахраї. Так само небажано вводити пароль з чужого комп'ютера, і в громадських місцях, такі як: кафе з доступом в інтернет, термінали.

При зберіганні важливої інформації, слід міняти пароль раз на місяць. Такий спосіб рекомендує Microsoft, і так роблять великі структури, включаючи банки.

Зворотний соціальний інжиніринг будується на трьох факторах:

• створення ситуації, яка змушує людину звернутися за допомогою;

• реклама своїх послуг або випередження надання допомоги іншими людьми;

• надання допомоги і вплив.

Якщо незнайома людина надає послугу, а потім просить зробити що-небудь, ні в якому разі не можна це робити, не обдумавши те, що він просить.

Соціальний інженер найчастіше вибирає метою співробітників, у яких обмежені знання в галузі використання комп'ютерів.

Так само нові співробітники організації є цілями соціальних інженерів, в зв'язку з тим, що нові співробітники не знають всіх процедур надання та обробки інформації в організації. Це пов'язано зі спробою створення гарного враження про себе і бажання показати, як швидко і добре вони можуть працювати і відгукуватися на прохання.

Перш, ніж новим співробітникам буде дозволено отримати доступ до комп'ютерних систем, вони повинні бути навчені правилам безпеки, особливо правилам про паролі.

Одна основна частина рішення: необхідно призначити співробітників в кожному відділі, які будуть працювати з усіма проханнями про відправку інформації поза групою.

Особистісний підхід. Найпростішим способом отримання інформації для соціального інженера є прохання. Існує чотири різновиди такого підходу:

•залякування (цей підхід використовує уособлення повноважень для примусу виконання запиту);

•переконання (звичайнісінькі форми переконання включають лестощі);

•використання довірчих відносин (цей підхід вимагає більш тривалого терміну, протягом якого соціальний інженер формує відносини для отримання довіри і інформації від об'єкта);

•допомога (допомога буде вимагати, щоб співробітник оприлюднив будь-яку інформацію).

Схема з використанням залякування з посиланням на авторитет працює особливо добре в тому випадку, коли співробітник, проти якого використовують залякування, має досить низький статус в організації. При використанні важливого людського імені пропадають не тільки підозри, але і з'являються такі властивості, як уважність.

Захистом проти нападу залякування є розвиток культури «відсутності страху через помилку», якщо нормальною поведінкою є ввічливість, то успіх залякування зменшується.

Необхідно пам'ятати, що неприйнятно залежати від чийогось авторитету. Слід уникати впливу авторитету в дружніх або ділових відносинах, але без нанесення шкоди спілкуванню. Більш того, такі дії повинні вітатися вищим керівництвом.

Захистом від переконання є суворе дотримання інструкцій і політикам безпеки.

Напади «допомоги» можуть бути скорочені, якщо є ефективна технічна підтримка. Внутрішній помічник - часто результат втрати довіри до існуючих послуг технічного відділу організації. Для запобігання таких атак:

•необхідно закріпити в політиці безпеки, що технічний відділ − це єдине місце, куди потрібно повідомляти про проблеми;

•слід гарантувати, що технічний відділ має узгоджений процес відповіді в межах встановленого рівня обслуговування;

•необхідно перевіряти виконання сервісних робіт регулярно, щоб упевнитися, що співробітники отримують відповідний рівень відповідей і рішень.

Існує два правила, які дозволяють уникнути такі типи атак.

1 Жоден із співробітників організації не повинен знати більше, ніж йому належить знати за посадою. Це пов'язано з тим, що більшість людей не вміють зберігати секрети.

2 Дане правило застосовується у випадках, коли у когось із співробітників виникає бажання з кимось поділитися інформацією. У трудовому договорі з працівником обов'язково повинно бути чітко прописано, що є комерційною таємницею, а також повинен бути пункт про те, що за розголошення комерційної інформації співробітника чекає відповідальність аж до кримінальної, в тому числі і того співробітника, який звільнився після розголошення предмета комерційної таємниці.

Також співробітникам слід знати кілька правил, яких бажано дотримуватися і намагатися не відхилятися від даного списку. Це дасть можливість при спробі маніпулювання соціальним інженером, помітити і припинити ці дії.

1 Репутація. Чим більше репутація у співробітника в організації, тим менше шансів, що він буде підданий атаці з боку соціального інженера.

2 Суперечки. Будь-який спір необхідно уникати - це вчить бути врівноваженим і не приймати швидких, і часом, неправильних рішень, ця вимога залишає співробітника холоднокровним в будь-якій ситуації і допомагає тверезо оцінювати ситуацію.

3 Плітки. Бажано намагатися ні з ким не обговорювати іншу людину, навіть намагатися не ділитися новинами місцевого характеру (ті ж плітки). У розмовах, що містять плітки, необхідно виходити з них якимись історичними фактами. Необхідно плавно змінювати тему на котрусь із наукових для того, щоб співрозмовнику дана тема була не цікава, і він був би змушений сам змінити тему на більш відповідну.

4 Постійна зміна співрозмовників. У людини існує така властивість, як швидке звикання, як до хорошого, так і до поганого, як тільки співробітник звик до іншого, він починає помічати вади і ставити на рівень нижче, ніж при знайомстві або початку бесіди. Людина ніколи не зможе посваритися зі співрозмовником, з яким нещодавно познайомився, але як тільки вони починають звикати один до одного, вони починають собі дозволяти набагато більше, ніж в початковий момент спілкування. При зміні співрозмовника мається на увазі не буквальне розуміння «зміни партнера», тут мова йде про те, що бажано не вести тривалі бесіди, а бажано намагатися швидко обговорювати важливі речі і по можливості знаходити нового співрозмовника і проводити з ним стільки ж часу в дискусії. Ні в якому разі не можна замикатися в собі і не показуватися на очі іншим співробітникам. Якщо співробітника не бачитимуть, то першу вимогу в списку не зможе бути дотримано.

5 Не посвячення нікого в свої проблеми. Кожен буде намагатися надати допомогу у вирішенні будь-якої проблеми і тут співробітник автоматично стає жертвою соціального інженера, так як після надання допомоги буде йому зобов'язаний.

Інформація на паперових носіях. Необхідно провести призначення різних категорій інформації та визначення того, як персонал повинен з ними поводитися. Категорії повинні включати:

•конфіденційна інформація (необхідно знищувати всі папери, що мають даний шифр в спеціальних знищувачах паперу);

•приватна інформація (необхідно знищувати всі папери, що мають даний шифр в спеціальних знищувачах паперу);

•відомча інформація (необхідно знищувати всі папери, що мають даний шифр в спеціальних знищувачах паперу перед викиданням в загальнодоступні урни);

•загальнодоступна інформація (можна позбутися від загальнодоступних документів в будь-який урні або використовувати їх як чернетки).

Пропозиції щодо захисту від загроз включають в себе використання ящиків, які замикаються і шаф для зберігання папок, а також використання шредерів для знищення паперів.

Аналіз сміття. Цілеспрямовані пошуки в сміттєвому контейнері − загальний метод для зловмисників для отримання інформації, яка компрометує організацію. Цілі, спрямованість і опис подібних атак представлені в таблиці 2.7.

Політика безпеки організації повинна включати положення про управління життєвим циклом носіїв, включаючи процедури руйнування або стирання.

У зв'язку з тим, що атаки на сміття не можна вважати правопорушеннями, слід гарантувати, що персонал організації в повній мірі розуміє значення викинутих паперових або електронних носіїв.

Одна з найбільш ефективних заходів при роботі зі сміттям - це специфікація класифікації даних. Проводиться призначення різних категорій інформації та визначення того, як персонал повинен з ними поводитися і знищувати. Категорії повинні включати:

•конфіденційна інформація (необхідно знищувати всі папери, що мають даний шифр в спеціальних знищувачах паперу);

•приватна інформація (необхідно знищувати всі папери, що мають даний шифр в спеціальних знищувачах паперу);

•відомча інформація (необхідно знищувати всі папери, що мають даний шифр в спеціальних знищувачах паперу перед викиданням в загальнодоступні урни);

•загальнодоступна інформація (можна позбутися від загальнодоступних документів в будь-який урні).

Таблиця 2.7 − Аналіз сміття

Цілі нападу	Опис	Спрямованість
Паперові відходи в зовнішніх урнах	Соціальний інженер бере папір з зовні розміщеної урни зі сміттям для захоплення будь-якої доречної інформації про організацію	Конфіденційна інформація Атака на довіру
Паперові відходи у внутрішніх урнах	Соціальний інженер бере папір з внутрішніх офісних урн, здійснюючи обхід будь-яких рекомендацій захисту	
Електронні відходи цифрових носіїв	Соціальний інженер захоплює інформацію і додатки з викинутих електронних носіїв, а також краде самі носії	Конфіденційна інформація Атака на довіру Ресурси

«Дорожнє яблуко». Для боротьби з цим методом атак, слід перевіряти на окремій ізольованій машині все, що надходить в організацію, неперевірені джерела інформації. Так само всім співробітникам необхідно утриматися від самостійних експериментів і передавати носії в технічний відділ для перевірки.

В правила технічного відділу повинні бути включені:

• кожна дія технічної підтримки повинно бути заплановано;

•підрядники та внутрішні співробітники, які здійснюють локальне обслуговування або установку будь-якого обладнання або програм, повинні мати документи, що ідентифікують особу;

• при проведенні робіт працівник зобов'язаний передзвонювати в технічний відділ, щоб повідомити їм час прибуття співробітника технічного відділу і час його відходу;

• кожна вироблена робота повинна мати документи, які підписуються співробітниками;

• користувач ніколи не повинен звертатися до інформації або реєстрації на комп'ютері для забезпечення доступу співробітнику технічного відділу.

Пропускний режим. При безперешкодному пересуванні по будівлі організації, наражається на небезпеку приватна інформація організації. В наш час, коли загроза тероризму нависає над суспільством, це більше, ніж просто інформація, якою можна ризикувати. Єдиний вихід з цієї ситуації - це посилити процедури ідентифікації.

Менш поширеним, але більш ефективним методом соціального інжинірингу є особистий контакт зі співробітником.

Ситуація, в якій неправомочна людина слідує за співробітником, проходячи в організацію, є найпростішим прикладом нападу з використанням соціального інжинірингу.

Захищеність від таких загроз залежить від виконання співробітниками дій, які засновані на ефективну політику безпеки організації, що враховує три області:

• приміщення організації;

• дім;

• мобільна робота.

Необхідні дії, при яких буде неможливий фізичний напад з використанням соціального інжинірингу в межах організації:

• ідентифікація за допомогою фотографій на пропусках;

• книга відвідувачів, в якій розписується відвідувач і співробітник, якого він відвідує;

• картка відвідувача (бейдж відвідувача), яка повинні бути видна завжди, поки він знаходиться в будівлі і яка повертається при виході;

• книга підрядників, в якій розписується підрядник і співробітник, який уповноважив їх роботу;

• картка підрядника (бейдж підрядника), яка повинна бути видна завжди, поки він знаходиться в будівлі.

Охоронець, який здійснює пропускний режим в організації, повинен бути проінструктований щодо можливих дій соціальних інженерів. Охоронець зобов'язаний дотримуватися наступних правил:

•пропускати тільки співробітників з пропусками;

•відвідувачів реєструвати в журналі при наявності документа, що підтверджує особу;

•дозволяти проходити в приміщення тільки в супроводі інших співробітників організації (супровід має проводитися від самого входу до місця призначення і назад, не дозволяючи їм самостійно ходити по організації).

Відступати від цих правил не можна ні в якому разі.

Для того щоб упевнитися, що кожен відвідувач представляється охороні, вхід в організацію повинен бути організований так, щоб відвідувачі мали йти безпосередньо повз пост охорони так, щоб пред'явити свої пропуски або зареєструватися. При цьому неприпустимо скупчення народу перед охоронцем, яке може утруднити роботу охорони.

Необхідно, щоб співробітники охорони переглядали весь прохід і не заважали один одному, коли вони перевіряють кожну людину.

Для того щоб класифікувати напади і визначити ризики в організації, необхідно використовувати спрямованість нападу, цілей нападу і описів, викладених в таблиці 2.8.

Таблиця 2.8 – Фізичні напади

Цілі нападу	Опис	Спрямованість
Крадіжка мобільного ідентифікатора співробітника	Соціальний інженер спостерігає за законним користувачем, що набирає ім'я і пароль для входу в систему	Конфіденційна інформація
Крадіжка домашнього ідентифікатора співробітника	Соціальний інженер зображує сервіс-менеджера для отримання доступу до домашнього комп'ютера і запитує користувальницький ідентифікатор і пароль, для перевірки успішності оновлення	Конфіденційна інформація
Прямий мережевий контакт через домашню мережу співробітника	Соціальний інженер звертається до мережі організації через домашню мережу співробітника, зображуючи співробітника технічного відділу	Конфіденційна інформація Ділова довіра Ділова доступність Ресурси Гроші
Зовнішній доступ до домашньої мережі співробітника	Соціальний інженер отримує доступ до інтернету через незабезпечену домашню мережу	Ресурси

Продовження таблиці 2.8

Несупроводжуваний доступ до офісу організації	Соціальний інженер отримує доступ під виглядом авторизованого співробітника організації	Конфіденційна інформація Ділова довіра Ділова доступність Ресурси Гроші
Звернення до людини в офісі організації	Соціальний інженер звертається до співробітника для використання комп'ютерного обладнання або паперових ресурсів	Конфіденційна інформація Ділова довіра Ділова доступність Ресурси Гроші

Робота технічного відділу. Адміністратори баз даних і локальних мереж, які працюють з програмним забезпеченням,зобов'язані встановлювати особу людини, яка звернулася до них за порадою або інформацією.

Необхідно змінити облікові дані на всіх комутаторах організації, в зв'язку з використанням однакового сервісного облікового запису на всіх комутаторах.

Ті ж самі дії необхідно зробити і з телефонними комутаторами.

Необхідно використовувати утиліту «L0phtcrack4» для перевірки «слабких» паролів або аналогічні їй.

Для того щоб заходи щодо забезпечення безпеки мали сенс - як для адміністраторів мережі, так і для співробітників, що використовують мережеві ресурси - необхідно визначити мережеву політику безпеки, в якій потрібно чітко описати, що можна і чого не можна робити в мережі.

Для ознайомлення співробітників з політиками забезпечення безпеки комп'ютерів і мережі необхідно використовувати наступні документи:

1 Політику мережевих з'єднань.

2 Процедури щодо усунення наслідків вторгнення.

3 Правила користування комп'ютером.

Ознайомлення з цими документами має підтверджуватися підписом співробітників, подібно до того, як це відбувається при інструктажі з техніки безпеки.

1 Політика мережевих з'єднань. Документи цього типу повинні містити перелік пристроїв, які дозволяється підключати до мережі, а також звід вимог щодо забезпечення безпеки - які функції операційної системи використовуються, відповідальні особи за твердження підключення до мережі нових пристроїв. Так само повинні бути передбачені прямі інструкції на випадок настройки нового комп'ютера, комутатора і навіть маршрутизатора - що дозволено робити, а що заборонено. Окремо повинна складатися політика підключення до мережі для брандмауерів - з описом того, який тип мережевого трафіку пропускається через брандмауер в мережу і з мережі.

При роботі співробітниками через віртуальну приватну мережу (Virtual Private Network, VPN), необхідно розробити спеціальні документи з докладним описом налаштування портативних і настільних комп'ютерів. У документації необхідно описати всі процедури отримання облікового запису комп'ютера, а також права і привілеї всіх типів, які можуть бути надані обліковому запису, мережеві адреси, які можуть бути використані, і способи їх контролю. Необхідно ясно озвучити, що ніякі з'єднання, що йдуть врозріз з описаними процедурами і політиками безпеки і відбуваються без відома відповідальних осіб, не допускаються.

При наданні співробітникам права комутованого доступу, співробітники повинні чітко розуміти, що ні в якому разі не можна повідомляти інформацію, необхідну для такого доступу.

Слід заборонити співробітникам працювати вдома з робочого комп'ютера (ноутбука, нетбука і т.д.).

При бажанні співробітником отримання дозволу на будь-яке послаблення встановленої політики, від нього необхідно вимагати письмову заяву з обґрунтуванням свого прохання. При проханні установки програми, яку не підтримує технічний відділ, не можна давати дозвіл на її установку тільки через гостру виробничу необхідність. В останньому випадку програму необхідно внести в політику мережевих з'єднань і навчити персонал технічного відділу її використовувати. Ні в якому разі не можна дозволяти співробітникам завантажувати і встановлювати програми з інтернету.

2 Усунення наслідків вторгнення. В організації повинен бути спеціальний співробітник або співробітники, які повинні відповідати за дослідження питань, що мають відношення до забезпечення безпеки. Крім того, наявність документа, в якому розписані процедури на випадок тих чи інших порушень системи захисту, показує співробітникам, наскільки важлива безпека мережі і наскільки ретельно потрібно виконувати заходи щодо її дотримання.

У документі, який повинен містити опис процедур по усуненню наслідків вторгнення, слід дати визначення того, що вважається проломом в захисті. Це може бути наступне:

• крадіжка апаратних засобів або програмного забезпечення;

• підбір або розголошення пароля;

• неприпустима передача будь-кому носіїв інформації, в тому числі дисків, флеш-драйверів і паперових носіїв;

• спільне використання одного облікового запису або розголошення імені користувача і пароля;

• перегляд мережі без відповідних повноважень;

• підозріле проникнення в мережу ззовні;

• комп'ютерні віруси;

• порушення фізичного доступу.

Деякі з цих ситуацій здаються цілком очевидними. Однак наївно розраховувати впоратися з подібними проблемами без заздалегідь написаних інструкцій.

3 Інструкція з використання комп'ютера. В інструкції з використання комп'ютера має бути ясно прописано, що всі комп'ютерні програми повинні надаватися виключно організацією; використання на комп'ютері, що належить організації, або в корпоративній мережі сторонніх програм забороняється. Слід переконатися, що всі співробітники розуміють це і що організація таким чином захищена від можливих судових розглядів.

Так само, в документації необхідно відзначити про заборону копіювання користувачами програмного забезпечення і даних, які належать організації, забирати їх додому або використовувати іншим недозволеним чином.

Необхідно зобов'язати співробітників повідомляти про будь-які підозрілі дії або неправомірне використання комп'ютерних ресурсів. На співробітників також має покладатися відповідальність за прийняття необхідних заходів щодо захисту даних і програм в межах їх повноважень - зокрема, вони не повинні залишати робочу станцію, зареєстровану для роботи в мережі, без нагляду на тривалий час, (для цього слід користуватися захищеним паролем зберігачем екрану); не повинні залишати на видному місці звіти та інша конфіденційна інформація тощо.

Інструкції з використання комп'ютера можуть включати багато нюансів. При її складанні необхідно врахувати наступні моменти:

• невдоволення користувачів (в кращому випадку користувачі не стануть виконувати дуже сувору інструкцію, яка створює серйозні незручності, - особливо якщо їм незрозуміло, наскільки ці заходи виправдані, в гіршому - можливо наростання прихованої агресії і відкритий конфлікт);

• покарання (якщо правило має на увазі прийняття деяких болючих заходів, то воно завжди повинно виконуватися з максимальною значущістю і строгістю, в ідеалі такі заходи повинні прийматися один раз);

• співробітники (в будь-якому документі, який містить інструкції по використанню мережі, має бути підкреслено, що співробітники, перебуваючи в мережі, зобов'язані вести себе етично);

• зовнішні з'єднання (ще однією областю, якій часто приділяється недостатньо уваги, є співробітники, які приходять в організацію і отримують тимчасовий доступ до мережі. Для співробітника, який найнятий за контрактом для виконання певних робіт, обов'язково повинні бути розроблені правила використання комп'ютера - такі співробітники повинні прочитати ці правила і підписом підтвердити факт ознайомлення з ними).

В інструкціях так само має бути сказано, що співробітник не має права обговорювати з ким-небудь не тільки інформацію, до якої він має доступ, але навіть і тип цієї інформації.

Робота відділу кадрів. Дуже часто, коли мова заходить про безпеку організації, в тому числі, коли справа стосується соціального інжинірингу, не можна забувати про те, що небезпека може бути всередині організації. Пов'язано це з тим, що у співробітників можуть бути свої вади. Типами співробітників є:

1 Вперті співробітники (вони вперті й впевнені, що роблять щось правильно і це не може підлягати ніякому критичному обговоренню).

2 Недобросовісні співробітники (вони демонструють ділову активність поки за ними спостерігаєш, як тільки спостереження припиняється - вони перестають працювати).

3 Розкрадачі (за даними Національної Американської Асоціації від «50 до 70% збитків організації доводиться на крадіжки, які здійснюють співробітники»). До розкрадачів можна віднести і тих співробітників, які найняті конкурентами.

Згідно зі статистикою, представленою на рисунку 2.6, «відсоток чесних співробітників дорівнює 10, 65% готові порушити закон в тому випадку, якщо вони будуть впевнені у своїй безкарності. Решта 25% готові порушити закон при будь-яких обставинах».

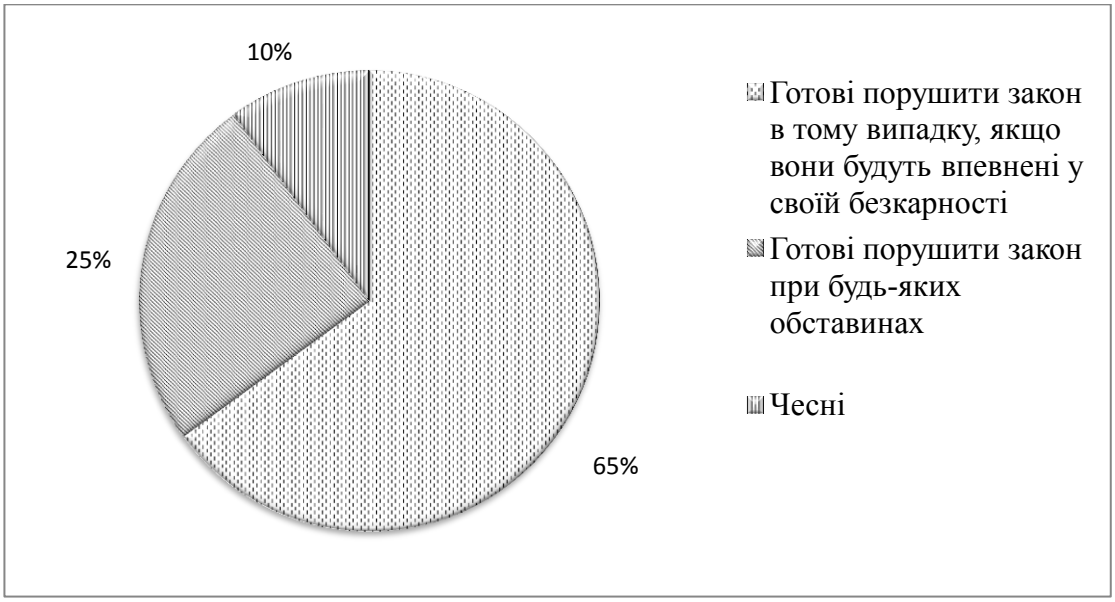

Рисунок 2.6 − Статистика чесності співробітників

Відділу кадрів рекомендується спостерігати за співробітниками на всіх стадіях їх розвитку в організації.

Будь-який співробітник в організації завжди проходить три стадії розвитку:

1 Влаштування на роботу;

2 Етап роботи;

3 Звільнення.

При прийомі співробітника на роботу необхідно зібрати про нього якомога більше відомостей, з метою прогнозу поведінки в будь-яких ситуаціях. Як правило, такі перевірки простіше проводити за допомогою стандартних психологічних тестів. Так само слід визначити, чи не належить кандидат на посаду до однієї з категорій «незручних співробітників», класифікацію і опис яких наведено нижче.

Не можна допускати в своїй організації існування алкогольно-сексуальних груп (мова йде про стиль поведінки людей, що входять в цю групу) [38, с. 186].

Лояльність співробітників - це означає, що співробітник задоволений роботою в організації, як в моральному, так і в матеріальному плані. Всіх співробітників можна розділити на чотири групи:

1 Співробітники, які задоволені роботою в організації, як в моральному, так і в матеріальному плані.

2 Співробітники, які задоволені роботою в організації в моральному плані, але в матеріальному плані вони не отримують гідної винагороди за свою працю, при цьому ставляться до цього поблажливо, тому що вважають, що іншої такої ж цікавої роботи вони не знайдуть, а на нецікавій роботі вони працювати не можуть.

3 Співробітники, які працюють тільки за зарплату, яка їх поки влаштовує, а до будь-якої роботи вони відносяться тільки як до обов'язку, яку потрібно виконати, щоб отримати гроші (ця група є небезпечною, тому що такого співробітника можна підкупити).

4 Співробітники, які незадоволені роботою в організації ні в моральному, ні в матеріальному плані (ця група співробітників є найнебезпечнішою, оскільки якщо в організації більшість співробітників належить саме до цієї групи, то така організація зруйнує сама себе.

Не можна створювати незамінних співробітників, пов'язане це з тим, що співробітник, який відчув свою значимість, починає шантажувати організацію [1, с. 117].

Повідомлення від співробітників, про спроби атак. Служба безпеки зобов'язана надати співробітника або групу, яка сформована, як орган, в яку повинні надходити всі звіти про підозрілу діяльність, спрямовану на атаку організації.

Якщо є думка, що співробітники розкрили інформацію про організацію, необхідно повідомити про це належним співробітникам організації: в службу безпеки і / або системним адміністраторам. Їх же можна попереджати про будь-яку підозрілу або незвичайну активність.

Якщо існує підозра, що були скомпрометовані відомості фінансового характеру, слід негайно довести до відома фінансову організацію і заблокувати відповідні рахунки. Слід звертати увагу на будь-які неясні видаткові операції по своїх рахунках.

Необхідно повідомляти про інцидент в правоохоронні органи.

Співробітник повинен скласти протокол, який описує спробу атаки, з вмістом наступної інформації:

• назва;

• відділ;

• мета нападу;

• ефект нападу;

• рекомендації;

• дата;

• підпис.

Всі співробітники повинні негайно повідомляти про всі запити , які були зроблені при незвичайних обставинах.

Також повинні повідомляти про всі невдалі спроби встановити особу запитувача.

Проводячи протоколювання спроб атаки, можна ідентифікувати їх в подальшому. Необхідно пам'ятати, що тільки ретельний аналіз і розбір інцидентів зможе допомогти знизити їх наслідки в подальшому.

Поради щодо поліпшення. Необхідно використовувати яскраві заставки, які будуть з'являтися при включенні комп'ютерів у співробітників, і кожен раз містити нову раду з безпеки. Повідомлення повинно бути побудовано таким чином, щоб воно не зникало автоматично, а вимагало від співробітника натискання на певну кнопку.

Слід виробляти постійні нагадування про безпеку. Для цього можна використовувати внутрішню щотижневу розсилку. Повідомлення повинні мати кожен раз різний зміст.

Так само слід використовувати короткі анотації. Необхідно робити кілька маленьких колонок, як маленький екран у власній газеті. У кожній анотації слід представляти чергове нагадування в короткому і у вигляді, який добре запам’ятовується.

Для розширення тренінгу рекомендується активна і яскрава програма винагород. Слід оголошувати співробітникам, хто відзначився, виявивши і запобігши атаку соціального інженера, або домігся великого успіху в освоєнні програми безпеки та обізнаності. Існування такої програми заохочення повинно бути підкреслено на кожному заході, який присвячено тренінгу, а зломи повинні бути широко висвітлені і розібрані всередині організації [14, с. 204].

Але так само співробітники повинні розуміти, що порушення політик безпеки і встановлених процедур і недбалість карані.

2.5 Висновки до другого розділу

У другому розділі розроблено методику у питаннях протидії методам соціального інжинірингу, аналізується шаблон, який здатний убезпечити організацію атак від соціального інжинірингу. Методика спрямована на розробку політик і процедур безпеки, які повинні бути спрямовані на захист окремих співробітників і організації в цілому.

Для розробки методики було розглянуто теоретичні аспекти створення методики протидії методам соціального інжинірингу, проаналізовано технічні засоби захисту від соціального інжинірингу.

Проведений аналіз проблем соціальної інженерії на прикладі організації ТОВ «Азимут-Трейд». Використовуючи таблицю вразливостей, що допускають проведення атак соціальних інженерів, для організації визначені вимоги політик безпеки, типи і рівні ризику. після виявлення вразливостей визначено перелік вжитих заходів в організації.

При розробці методики детально розкрито етапи процесу розробки та впровадження методики в організації, визначено методичні вказівки, необхідні дії та заходи дотримання правил у питаннях протидії методам соціального інжинірингу.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Метою даного розділу є обґрунтування економічної доцільності застосування у питаннях протидії методам соціального інжинірингу в організації.

Для визначення ефективності необхідно розрахувати:

1) витрати на розробку, впровадження та підтримку методики;

2) оцінку можливого збитку від атаки (злому) на вузол або сегмент мережі;

3) економічну доцільність застосування методики в організації.

3.1 Витрати на розробку, впровадження та підтримку методики

Витрати на розробку методики $К_м$складаються з загальної тривалості створення методики t, вартості одної години машинного часу ПК $З_{мч}$ та заробітної плати за годину виконавця методики $З_{зп}$:

$$К_м = t\,(З_{мч} + З_{зп}) \tag{3.1}$$

Вартість 1 години машинного часу ПК визначається за формулою:

$$З_{мч} = P \cdot C_e + \frac{Ф_{перв} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \frac{грн}{год}, \tag{3.2}$$

де Р – встановлена потужність ПК, кВт;

$С_е$– тариф на електричну енергію, грн/кВт·година;

$Ф_{перв}$– первісна вартість на ПК на початок року, грн;

$Н_а$– річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$– річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$– вартість ліцензійного програмного забезпечення, грн.;

$F_р$– річний фонд робочого часу (за 40-годинного робочого тижня Fp = 1920 год).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_е$), визначається за формулою:

$$С_{ел} = Р \cdot F_p \cdot Ц_е , \text{ грн,} \quad (3.3)$$

$$C_e = 0{,}25 \cdot 1920 \cdot 1{,}68 = 806{,}4 \text{ грн.}$$

У таблиці 3.1 наведено час t, який витрачається на розробку методики.

Таблиця 3.1 − Тривалість розробки методики

№	Задачі	t, год/рік
1	Ознайомлення із структурою організації	20
2	Розробка стратегії управління забезпечення безпеки	36
3	Оцінка ризиків. Аналіз загроз, вразливостей	30
4	Інтеграція принципів захисту від атак соціальних інженерів в політику безпеки організації	35
5	Визначення методів протидії	45
6	Розробка політик безпеки і процедур	50
7	Розробка навчально-методичних матеріалів для співробітників	50
8	Аналіз технічних засобів захисту від соціального інжинірингу	34
9	Всього	300

Отже, тривалість розробки методики t складає 300 годин.

Річна норма амортизації на ПК $Н_а$:

$$Н_а = \frac{1}{T} = \frac{1}{5} = 0{,}2$$

Річна норма амортизації на ліцензійне програмне забезпечення $Н_{апз}$:

$$Н_{апз} = \frac{1}{T} = \frac{1}{1} = 1$$

Дані для розрахунку вартості 1 години машинного часу $З_{мч}$:

Р=0, 25 кВт;

C_e=806,4 грн.;

$Ф_{перв}$= 6550 грн.;

$К_{лпз}$= 4912 грн.

$$З_{мч} = 0,25 \cdot 806,4 + \frac{6550 \cdot 0,2}{1920} + \frac{4912 \cdot 1}{1920} = 204,84 \text{ грн/год}$$

Заробітна плата виконавця за годину складає 37 грн/год.

Отже, витрати на розробку методики протидії складають:

$$К_м = 300 * (37 + 204,84) = 72552 \text{ грн.}$$

Витрати на впровадження методики є одноразовими та розраховуються за формулою:

$$К_в = К_м + К_{ппз} + К_{вл}, \quad (3.4)$$

де $К_м$ - одноразові витрати на розробку методики, грн.;

$К_{ппз}$ - витрати на придбання програмного забезпечення, грн.;

$К_{вл}$ - ввідна лекція на використання методики, грн.

Отже, витрати на впровадження методики протидії складають:

$$К_в=72552 +1200+1500=75252 \text{ грн.}$$

Витрати на підтримку методики (щорічні) розраховуються за формулою:

$$С_п = К_{пі} + К_{вп}, \quad (3.5)$$

де $К_{пі}$ - витрати на заробітню плату співробітнику за проведення інструктажу 2 рази на рік;

$К_{вп}$ – витрати на внесення правок до методичних вказівок згідно актуальних проблем кібербезпеки у сфері соціальної інженерії.

Отже, витрати на підтримку методики протидії складають:

$$С_п=5\ 000 + 1\ 500 = 6\ 500 \text{ грн.}$$

Розраховуємо загальні річні витрати на застосування методики в організації за формулою:

$$В_{заг} = К_в + С_п, \quad (3.6)$$

Отже, загальні річні витрати на застосування методики в організації складають:

$$В_{заг} = 75252 + 6500 = 81752 \text{ грн.}$$

3.2 Розрахунок експлуатаційних витрат

Річні експлуатаційні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к , \quad \text{тис. грн.}, \quad (3.7)$$

де $С_в$ - витрати на Upgrade-відновлення й модернізацію системи інформаційної безпеки;

$С_к$ - витрати на керування системою інформаційної безпеки;

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{єв} + С_{ел} + С_{тос}, \text{ грн.}, \quad (3.8)$$

де $С_н$ - витрати на навчання адміністративного персоналу;

$С_а$ - річний фонд амортизаційних відрахувань;

$С_з$ - річний фонд заробітної плати інженерно-технічного персоналу;

$С_{єв}$ - розмір єдиного внеску (22% від фонду ЗП);

$С_е$ - вартість електроенергії;

$С_{тос}$ - витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки.

Річний фонд амортизаційних відрахувань (Са) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ):

$$С_а = \frac{К_{пз}}{2} = \frac{81752}{2} = 40\,876 \text{ грн.} \quad (3.9)$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки, складає:

$$С_з = (З_{зп} + 22\%) \cdot N \cdot m = 8200 \cdot 2 \cdot 12 = 196\,800 \text{ грн.} \quad (3.10)$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$) у відсотках від вартості капітальних витрат (1-3%).

Витрати на керування системою інформаційної безпеки складають:

$$С_к = 3000+40876+196800+1804+806,4+1635=243286 \text{ грн.}$$

Отже, річні експлуатаційні витрати на функціонування системи інформаційної безпеки складають:

$$С = 4200 + 243286 = 244\,921 \text{ грн.}$$

3.3 Оцінка можливого збитку від атаки (злому) на вузол або сегмент мережі

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = (П_п + П_в)\sum i \sum n, \quad (3.11)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_П \ , \quad (3.12)$$

де F – місячний фонд робочого часу (становить 160 ч);

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць;

tп – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин.

$$П_{п} = \frac{\sum 8200 \cdot 6}{160} \cdot 4 = 1230 \text{ грн.}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_{в} = П_{ви} + П_{пв} + П_{зч}, \quad (3.13)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_{с}$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} \ , \quad (3.14)$$

де $t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;

$$п_{ви} = \frac{\sum 8200 \cdot 6}{160} \cdot 12 = 3690 \text{ грн.}$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{ПВ} = \frac{\sum Зо}{F} \cdot t_В \ , \qquad (3.15)$$

де $t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$$П_{пв=} \frac{\sum 8200 \cdot 6}{160} \cdot 8 = 2460 \text{ грн.}$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе:

$$U = (1230+3690+2460+5000) \cdot 6 \cdot 10 = 742800 \text{ грн.}$$

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R – C, \qquad (3.16)$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

$$E = 742800 \cdot 0.4 – 244921 = 52199 \text{ грн.}$$

3.4 Оцінка економічної ефективності системи захисту інформації

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломного проекту, здійснюється на основі визначення та аналізу наступних показників:

а) коефіцієнт повернення інвестицій (ROSI) (Return on Investment for Security);

б) термін окупності капітальних інвестицій T_o.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,} \tag{3.17}$$

де Е – загальний ефект від впровадження системи інформаційної безпеки, тис. грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

$$\text{ROSI} = \frac{52199}{81752} = 0,\ 63$$

При цьому проект визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта:

$$\text{ROSI} > (N_{деп} - N_{інф})/100), \tag{3.18}$$

де $N_{деп}$ – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, 18%;

$N_{інф}$ – річний рівень інфляції, 13,7%.

$$0{,}63 > (18\text{-}13{,}7)/100$$

$$0{,}63 > 0{,}043$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = 1{,}5 \text{ роки} \qquad (3.19)$$

3.5 Висновки до третього розділу

Витрати на розробку методики є одноразовими і складаються з загальної тривалості створення методики, вартості одної години машинного часу ПК та заробітної плати за годину виконавця методики.

Загальні річні витрати на застосування методики, враховуючи впровадження та підтримку методики, в організації складають 81752 грн.

Збиток від простою складається з оплачуваних втрат робочого часу та простою співробітників атакованого вузла або сегмента корпоративної мережі і вартості відновлення працездатності вузла або сегмента корпоративної мережі.

Річні експлуатаційні витрати на функціонування системи інформаційної безпеки складають 244 921 грн.

Загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складає 742800 грн.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить 52199 грн.

Проект визнається економічно доцільним, розрахунковий коефіцієнт ефективності ROSI перевищує річний рівень прибутковості альтернативного варіанта.

ВИСНОВКИ

В даній дипломній роботі було розроблено методику протидії методам соціального інжинірингу та проаналізовано актуальні проблеми соціальної інженерії ТОВ «Азимут-Трейд».

В ході виконання поставлених в дипломній роботі задач були отримані наступні наукові та практичні результати:

– шляхом аналізу вимог нормативних документів у сфері соціальної інженерії та дослідження існуючих методів у питаннях протидії методам соціальної інженерії було виявлено необхідність в розробці простої та ефективної методики протидії методам соціальної інженерії;

– розроблено методику у питаннях протидії методам соціального інжинірингу. Методика спрямована на розробку політик і процедур безпеки, які повинні бути спрямовані на захист окремих співробітників і організації в цілому.

– розглянуто теоретичні аспекти створення методики протидії методам соціального інжинірингу, проаналізовано технічні засоби захисту від соціального інжинірингу.

– проаналізовано проблеми соціальної інженерії на прикладі організації ТОВ «Азимут-Трейд». Визначені вимоги політик безпеки, типи і рівні ризику. Після виявлення вразливостей визначено перелік вжитих заходів в організації.

– розкрито етапи процесу розробки та впровадження методики в організації, визначено методичні вказівки, необхідні дії та заходи дотримання правил у питаннях протидії методам соціального інжинірингу.

– обґрунтовано доцільність розробленої методики шляхом розрахунку витрат на розробку та впровадження методики для протидії методам соціальної інженерії на прикладі ТОВ «Азимут-Трейд», оцінки можливого збитку від атаки на вузол або сегмент мережі, експлуатаційних витрат на функціонування системи. Загальний ефект від впровадження системи інформаційної безпеки визнається економічно доцільним.

ПЕРЕЛІК ПОСИЛАНЬ

1 Кузнєцов Н.І. Підручник з інформаційно-аналітичної роботи: підручник для вузів / Н.І. Кузнєцов - М .: Яуза, 2011 - 217 с.

2 Шудрова К. Соціальна інженерія в інформаційній безпеці / К. Шудрова // Директор з безпеки. - 2012. - №10. - с. 13-17.

3 Ярочкин В.Г. Безпека інформаційних систем: підручник для вузів / В.Г. Ярочкин - М .: МІФІ, 2009. - 198 с.

4 Щокін Г.В. Основи кадрового менеджменту: підручник для вузів / Г.В. Щокін - К .: МАУП, 2010 - 280 с.

5 Кузнецов М.В. Соціальна інженерія та соціальні хакери: учеб.-метод. посібник / М.В. Кузнєцов - С.-Пб .: БХВ-Петербург, 2010 - 368 с.

6 Насакин Р. Ботнет / Р. Насакин // Комп'ютер. - 2007. - №17. - с. 50-61.

7 Касперски К. Секретна зброя соціальної інженерії / К. Касперски // Журнал мережевих рішень. - 2012. - №9 - с. 12-15.

8. Катальфамо Д. Протидія соціальної інженерії / Д. Катальфамо // SearchSecurity. - 2010. - №1. - с. 78-82.

9 Гаврилов А. Соціальний інжиніринг в дії // Безпека. - 2012. - №3.

10 Комаров А. TMS управляє життєвим циклів токенов / А. Комаров // CNews. - 2008. - №10. - с. 90-113.

11 Кучук Е. Сучасний гіпноз або соціальний інжиніринг. / Є. Кучук // Комп'ютерна газета. - 2009. - №4. - с. 46-51.

12 Прокоф'єв І.В. Введення в теоретичні основи комп'ютерної безпеки: навчальний посібник / І.В. Прокоф'єв - М .: МІФІ, 2008. - 287 с.

13 Шейнов В.П. Мистецтво управляти людьми: учеб.-метод. посібник / В.П. Шейнов - Мн .: Харвест. 2005 - 512 с.

14 Митник К.Д. Мистецтво обману: метод. посібник / К.Д. Митник - NYC: Wiley Books. 2008 - 273 с.

15 Ездаков А. Як захистити інформацію / А. Ездаков // Мережі. - 2010. - № 8. - с. 11-19.

16 Кузнецов Н. Інформаційна взаємодія як об'єкт наукового дослідження / Н. Кузнецов // Питання філософії. - 2011. - №1. - с. 21-29.

17 Лукацький О.В. Виявлення атак: учеб.-метод. посібник / А.В. Лукацький - С.-Пб .: БХВ-Петербург, 2009 - 624 с.

18 Вихорев С. Як визначити джерела загроз / С. Вихорев, Р. Кобцев // Відкриті системи. - 2012. - № 8. - с. 9-16.

19 Петраков А.В. Основи практичної захисту інформації: навчальний посібник / А.В. Петраков. - 3-е изд. - М .: Радио и связь, 2011. - 368с.

20 Хоффман Л. Сучасні методи захисту інформації: учеб.-методич. посібник / Л. Хоффман - М .: СР, 2010. - 269 с.

21 Гайковіч В.Ю. Основи безпеки інформаційних технологій: підручник для вузів / В.Ю. Гайковіч, Д.В. Єршов - М .: Тріумф. 2007. - 351 с.

22 Большаков А.А. Основи забезпечення безпеки даних в комп'ютерних системах і мережах / А.А. Большаков, А.Б. Петряев,- М .: РІЦ, 2008. - 528 с.

23 Хорошко В.О. Методи і засоби захисту інформації: підручник для вузів / В.А. Хорошко, А.А. Чекатков; - К .: Юніор, 2013. - 504с.

24 Долгин А.Є. Як захистити інформацію: учеб.-методич. посібник / А.Є. Долгін, М.Ю. Потанін. - М .: Фенікс, 2008. - 320 с.

25 Яремчук С.А. Захист вашого комп'ютера: учеб.-метод. посібник / С.А. Яремчук - С.-Пб .: Пітер, 2011 - 378 с.

26 Плетт В. Стратегічна розвідка: підручн. для вузів / В. Плетт - М .: МІФІ, 2007. - 310 с.

27 Ключко Н. Сучасні трансформації методів соціальної інженерії / Н. Ключко // Фінансова газета. - 2009. - №37. - с. 79-89

28 Лихоносов А.Г. Безпека серверних операційних систем: підручник для вузів / А.Г. Лихоносов - М .: МФПУ, 2010 - 210 с.

29 Інформаційна безпека державних організацій і комерційних фірм: навч. посібник / А. В. Волокітін - М .: НТЦ «ФІОРД-ІНФО», 2012. - 272с.

30 Чалдіні Р. Психологія впливу: підручн. для вузів / Р. Чалдіні – С.-Пб.: Санкт-Петербург, 2008 – 298 с.

31 Про затвердження Переліку відомостей, які містять конфіденційну інформацію : Наказ від 1.07.2016 р. №414

32 Співак В.А. Організаційна поведінка і управління персоналом: підручник для вузів / В.А. Співак - С.-Пб .: Санкт-Петербург, 2008 - 415 с.

33 Форсіф П.Є. Розвиток і навчання персоналу: підручник для вузів / П.Є. Форсіф - С.-Пб .: Нева, 2009 - 128 с.

34 Андрєєва Г.М. Соціальна психологія: підручник для вузів / Г.М. Андрєєва - М .: ЕЛІТ, 2003. - 270 с.

35 Трудовий кодекс України від 11.10.2018

36 Цивільний кодекс України від 02.08.2018

37 Баутов А. Економічний погляд на проблеми інформаційної безпеки А. Баутов // Відкриті системи. - 2012. - № 2. - с. 12-23.

38 Литвак М.Е. Психологічне айкідо: навчальний посібник / М.Є. Литвак – М.: Юніор, 2007. - 278 с.

ДОДАТОК А. Відомість матеріалів дипломної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	3	
5	А4	1 Розділ	28	
6	А4	2 Розділ	55	
7	А4	3 Розділ	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік файлів на електронному носії

1. Дипломна робота Сєрак Т.Г. 125м-17-2.docx – Пояснювальна записка

2. Сєрак Т.Г.pttx – Презентація

ДОДАТОК В. Відгук керівника економічного розділу

Керівник: _____ к.е.н., доц. Пілова Д.П.
(підпис)

ДОДАТОК Г. Відгук
на дипломну роботу магістра на тему:
Розробка методики протидії методам соціального інжинірингу.
студента групи 125м-17-2
Сєрак Тетяни Геннадіївни

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 113 сторінках та містить 11 рисунків, 13 таблиць, 38 джерел та 4 додатка.

Актуальність теми полягає в необхідності розробки методики протидіям методам соціального інжинірингу, який набув свого значення завдяки розвитку інформаційного простору. Незважаючи на динамічний розвиток сектора кібербезпеки в країнах світу головним аспектом шкідливих атак на інформаційні системи залишається людський фактор. У зв'язку з цим у ряді країн набув поширення соціальний інжиніринг як метод несанкціонованого доступу.

Зміст та структура дипломної роботи дозволяють розкрити поставлену тему повністю.

Студент показав добрий рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота виконана самостійно. У роботі було розглянуто актуальність розробки методів соціального інжинірингу, що значно підвищить надійність функціонування і захищенність об’єктів.

Робота оформлена та написана відповідно до вимог щодо написання дипломних проектів. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому дипломна робота задовольняє усім вимогам і може бути допущена до захисту, а її автор Сєрак Тетяна Геннадіївна заслуговує на оцінку «відмінно».

Керівник дипломної роботи,
к.ф.-м.н., доцент Гусєв О.Ю.

Керівник спеціального розділу,
ас. кафедри БІТ Ю.В. Ковальова