Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломної роботи

магістра
(ступінь підготовки)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

напрям підготовки (спеціальність) *125 Кібербезпека*
(код і назва напряму підготовки)

спеціалізація (освітня програма) *Кібербезпека*
(код і назва спеціальності)

ступінь підготовки *магістр*
(назва освітнього рівня)

кваліфікація *професіонал із організації інформаційної безпеки*
(код і назва кваліфікації)

на тему: ***Управління обізнаністю персоналу в питаннях протидії методам соціальної інженерії***

Виконавець: студентка ***2*** **курсу, групи** ***125м-16-1***

_____ ***Легенченко Катерина Олегівна***
(підпис) (прізвище ім'я по-батькові)

Керівники	Прізвище, ініціали	Оцінка	Підпис
роботи	д.ф.-м.н., проф. Кагадій Т.С.		
розділів:			
спеціальний	ст.викл. Тимофєєв Д.С.		
економічний	к.е.н., доц. Волотковська Ю.О.		
Рецензент			
Нормоконтроль			

Дніпро
2018

Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

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

«_____»_____2018 року

ЗАВДАННЯ
на виконання кваліфікаційної роботи магістра

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту ***125м-16-1*** ***Легенченко Катерині Олегівні***
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи ***Управління обізнаністю персоналу в питаннях протидії методам соціальної інженерії***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора Державного ВНЗ «НГУ» від «26» грудня 2017 р. № 2127-л

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *процес управління обізнаністю персоналу*

Предмет досліджень *протидія методам соціальної інженерії*

Мета НДР *підготовка обґрунтованої методики підвищення рівня обізнаності персоналу у питаннях протидії методам соціальної інженерії*

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

3 ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна *полягає у розробці методики управління обізнаністю персоналу у питаннях протидії методам соціальної інженерії*

Практична цінність *полягає у розробці методичних вказівок для підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії, а також у розробці опитувальника для аналізу рівня обізнаності*

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Результати роботи мають відповідати вимогам чинного законодавства України та бути поданим у вигляді, що дозволяє безпосереднє використання для підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії на підприємстві

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт (початок-кінець)**
Аналіз нормативно-правової бази у сфері соціальної інженерії	1 вересня 2017 р. – 25 вересня 2017 р.
Дослідження існуючих методів підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії	26 вересня 2017 р. – 15 жовтня 2017 р.
Розробка методики підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії	16 жовтня 2017 р. – 5 листопада 2017 р.
Розробка методичних матеріалів для підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії та електронного опитувальника для аналізу ефективності методики на підприємстві	6 листопада 2017 р. – 20 грудня 2017 р.
Визначення капітальних та експлуатаційних витрат на реалізацію запропонованої методики підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії	21 грудня 2017 р. – 1 січня 2018 р.
Оформлення технічної документації	2 січня 2018 р. – 15 січня 2018 р.

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *від реалізації результатів роботи очікується позитивним завдяки зниженню можливого збитку підприємства від реалізованих методами соціальної інженерії загроз через застосування запропонованої у дипломній роботі методики підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії*

Соціальний ефект *дипломної роботи полягає у підвищенні впевненості керівництва та працівників підприємства у його надійності з точки зору протидії атакам методами соціальної інженерії*

7 ДОДАТКОВІ ВИМОГИ

Відповідність оформлення пояснювальної записки:
ДСТУ 3008-95. «Документація. Звіти у сфері науки і техніки. Структура і правила оформлення».
Бабенко Т.В. Методичні вимоги до підготовки та захисту дипломної роботи (проекту) для студентів галузей знань 1701 «Інформаційна безпека» та спеціальності 125 «Кібербезпека» / Бабенко Т.В., Корнєєв М.В., Кручінін О.В., Тимофєєв Д.С.; Нац. гірн. ун-т. – Д: НГУ, 2016. – 45 с.
Бабенко Т.В. Методичні вимоги до підготовки та захисту дипломної роботи

Завдання видала _____ Т.С. Кагадій
(підпис) (прізвище, ініціали)

Завдання прийняла
до виконання _____ К.О. Легенченко
(підпис) (прізвище, ініціали)

Дата видачі завдання: 01.09.2017

Термін подання дипломної роботи до ДЕК _____

РЕФЕРАТ

Пояснювальна записка: ___ с., __ рис., __ табл., __ додатків, __ джерел.

Об’єкт дослідження: процес управління обізнаністю персоналу.

Мета роботи: підготовка обґрунтованої методики підвищення рівня обізнаності персоналу у питаннях протидії методам соціальної інженерії.

Методи дослідження: порівняння, статистичний аналіз, моделювання.

У спеціальній частині досліджена теоретична база у сфері обізнаності персоналу в питаннях протидії методам соціальної інженерії. Проаналізовані загрози кібербезпеки та розглянута їх класифікація за різними ознаками. Виділено загрози кібербезпеки антропогенного характеру. З загроз антропогенного характеру виділено загрози методами соціальної інженерії. Проаналізовано методи соціальної інженерії та розглянуто існуючі методи протидії атакам соціальної інженерії.

У роботі розроблено методику управління обізнаністю персоналу у питаннях протидії методам соціальної інженерії. Для цього розроблено методичні вказівки для підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії та шаблон опитувальника як метрику для аналізу рівня обізнаності персоналу у питаннях протидії методам соціальної інженерії.

В економічній частині проведено розрахунок вартості розробки та впровадження методики управління обізнаністю персоналу у питаннях протидії методам соціальної інженерії і обґрунтовано її економічну доцільність.

Практичне значення роботи полягає у розробці методичних вказівок для підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії, а також у розробці опитувальника для аналізу рівня обізнаності.

Наукова новизна роботи полягає у розробці методики управління обізнаністю персоналу у питаннях протидії методам соціальної інженерії.

Ключові слова: СОЦІАЛЬНА ІНЖЕНЕРІЯ, АНТРОПОГЕННІ ЗАГРОЗИ, ОБІЗНАНІСТЬ ПЕРСОНАЛУ, МЕТОДИКА ПІДВИЩЕННЯ ОБІЗНАНОСТІ ПЕРСОНАЛУ.

РЕФЕРАТ

Пояснительная записка: ____ с., ___ рис., ___ табл., __ приложений, __ источников.

Объект исследования: процесс управления осведомленностью персонала.

Цель работы: подготовка обоснованной методики повышения уровня осведомленности персонала в вопросах противодействия методам социальной инженерии.

Методы исследования: сравнение, статистический анализ, моделирование.

В специальной части исследована теоретическая база в сфере осведомленности персонала в вопросах противодействия методам социальной инженерии. Проанализированы угрозы кибербезопасности и рассмотрена их классификация по разным признакам. Выделены угрозы антропогенного характера. Также выделены угрозы методами социальной инженерии. Проанализированы методы социальной инженерии и рассмотрены существующие методы противодействия атакам социальной инженерии.

В работе разработана методика управления осведомленностью персонала в вопросах противодействия методам социальной инженерии. Для этого разработаны методические указания для повышения осведомленности персонала и шаблон опросника как метрика для анализа уровня осведомленности персонала.

В экономической части проведен расчет стоимости разработки и внедрения методики и обоснована ее экономическая целесообразность.

Практическое значение работы заключается в разработке методических указаний для повышения осведомленности персонала в вопросах противодействия методам социальной инженерии, а также в разработке опросника для анализа уровня осведомленности.

Научная новизна работы заключается в разработке методики управления осведомленностью персонала в вопросах противодействия методам социальной инженерии.

Ключевые слова: СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ, АНТРОПОГЕННЫЕ УГРОЗЫ, ОСВЕДОМЛЕННОСТЬ ПЕРСОНАЛА, МЕТОДИКА ПОВЫШЕНИЯ ОСВЕДОМЛЁННОСТИ ПЕРСОНАЛА.

ABSTRACT

Explanatory note: ____ p., ___ fig., ___ tab, __ applications, __ sources.

Object of the study: the process of managing staff awareness.

The aim of research paper: to develop a justified methodology for raising the level of staff awareness in the issues of counteraction to social engineering methods.

Research methods: comparison, statistical analysis, modeling.

In a special part, the theoretical base in the sphere of personnel awareness in the issues of counteraction to methods of social engineering was explored. The threats of cybersecurity are analyzed and their classification is examined by different criteria. The threats of cyber-security of anthropogenic character are singled out. From threats of anthropogenic nature, threats by methods of social engineering are highlighted. The methods of social engineering are analyzed and the existing methods of counteracting social engineering attacks are considered.

In this paper, has been developed a methodology for managing staff awareness in the issues of countering social engineering methods. Guidelines have been developed to increase staff awareness in countering social engineering techniques and the questionnaire template as a metric for analyzing the level of staff awareness in countering social engineering techniques was done.

In the economic part, the calculation of the cost of developing and implementing a methodology for managing personnel awareness in countering social engineering methods has been carried out, and its economic feasibility has been justified.

The practical importance of the work is about guidelines for raising the awareness of personnel in combating social engineering techniques, as well as in developing a questionnaire for analyzing the level of awareness.

The scientific novelty of the work is to develop a methodology for managing staff awareness in the issues of counteraction to social engineering methods.

Key words: SOCIAL ENGINEERING, ANTHROPOGENIC THREATS, PERSONNEL AWARENESS, METHOD OF INCREASING PERSONNEL AWARENESS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизовані системи;

БД – база даних;

ЗУ – Закон України;

ІБ – інформаційна безпека;

ІСПДн – інформаційна система персональних даних;

ІТ – інформаційні технології;

НД ТЗІ – нормативний документ технічного захисту інформації;

ОС – операційна система;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

ПП – приватне підприємство;

СДН – система дистанційного навчання;

СІ – Соціальна інженерія;

ENISA – The European Union Agency for Network and Information Security;

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

ЗМІСТ

ВСТУП

Актуальність. В наш час усі підприємства пов’язані з процесами зберігання та обробки інформації. Ця інформація може містити конфіденційні дані, розкриття яких завдасть значної шкоди репутації підприємства, його роботоспроможності або фінансовому положенню.

Існує багато джерел загроз інформаційній та кібербезпеці підприємства. До процесу зберігання та обробки інформації завжди залучений персонал підприємства. Отже, важливо роздивлятись антропогенний фактор як реально існуючу уразливість у інформаційній безпеці підприємства. За статистичними даними [1] соціальна інженерія є найвагомішою загрозою, направленою на антропогенний фактор. Існує багато методів протидії методам соціальної інженерії. Одним з таких методів є підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії. Не всі підприємства приділяють належну увагу до підвищення обізнаності. Тому постає необхідним створення ефективної методики підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії.

Метою роботи є підготовка обґрунтованої методики підвищення рівня обізнаності персоналу у питаннях протидії методам соціальної інженерії.

У роботі були поставлені наступні завдання:

- аналіз нормативно-правової бази у сфері соціальної інженерії;

- дослідження існуючих методів підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії;

- розробка методики підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії;

- розробка методичних матеріалів для підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії та електронного опитувальника для аналізу ефективності методики на підприємстві;

- визначення капітальних та експлуатаційних витрат на реалізацію запропонованої методики підвищення обізнаності персоналу у питаннях

протидії методам соціальної інженерії та розрахунок економічної доцільності методики.

Об’єктом досліджень є процес управління обізнаністю персоналу.

Предметом досліджень є протидія методам соціальної інженерії.

Наукова новизна роботи полягає у розробці методики управління обізнаністю персоналу у питаннях протидії методам соціальної інженерії.

Практична цінність полягає в розробці методичних вказівок для підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії, а також у розробці опитувальника для аналізу рівня обізнаності.

РОЗДІЛ 1
ДОСЛІДЖЕННЯ ТЕОРЕТИЧНОЇ БАЗИ У СФЕРІ ОБІЗНАНОСТІ ПЕРСОНАЛУ В ПИТАННЯХ ПРОТИДІЇ МЕТОДАМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

1.1 Аналіз загроз кібербезпеки

Згідно Закону України (ЗУ) Про засади забезпечення кібербезпеки України [2], кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. [2]

Згідно НД ТЗІ 1.1-003-99 загроза – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків інформаційно-телекомунікаційній системі. [3]

Під загрозою в загальному сенсі розуміють потенційно можливу подію (вплив, процес або явище), яка може привести до нанесення збитків чиїмось інтересам, зокрема під загрозою безпеки автоматизованих систем (АС) обробки інформації розуміється можливість впливу на АС, що прямо або побічно може завдати шкоди її безпеці.

Перелік загроз, оцінки ймовірностей їх реалізації, а також модель порушника служать основою для аналізу ризику реалізації загроз і формулювання вимог до системи захисту інформації. Крім виявлення можливих загроз, доцільним є проведення аналізу цих загроз на основі їх

класифікації за рядом ознак. Кожна з ознак класифікації відображає одну з узагальнених вимог до системи захисту.

Необхідність класифікації загроз інформаційної безпеки обумовлена тим, що інформація в сучасних системах піддається впливу надзвичайно великого числа факторів, в силу чого стає неможливим формалізувати задачу опису повної множини загроз. Тому для системи, що захищається, зазвичай визначають не повний перелік загроз, а перелік класів загроз.

Згідно європейського центру експертизи кіберзбезпеки ENISA загрози кібербезпеці можна розділити за наступними групами, як показано на Рис. 1 [4]

Класифікація можливих загроз інформаційної безпеки АС може бути проведена за наступними базовим ознаками: [5]

За природою виникнення:

– природні загрози, викликані впливами на АС об'єктивних фізичних процесів або стихійних природних явищ;

– штучні загрози безпеки АС, викликані діяльністю людини.

За ступенем навмисності прояви:

– загрози, викликані помилками або халатністю персоналу, наприклад некомпетентне використання засобів захисту, введення помилкових даних і т.п.;

– загрози навмисних дій, наприклад дій зловмисників.

За джерелом загроз:

– природне середовище, наприклад стихійні лиха, магнітні бурі та ін.;

– людина, наприклад вербування шляхом підкупу персоналу, розголошення конфіденційних даних і т.п.;

– санкціоновані програмно-апаратні засоби, наприклад видалення даних, відмова в роботі операційних систем (ОС);

– несанкціоновані програмно-апаратні засоби, наприклад зараження комп'ютера вірусами з деструктивними функціями.

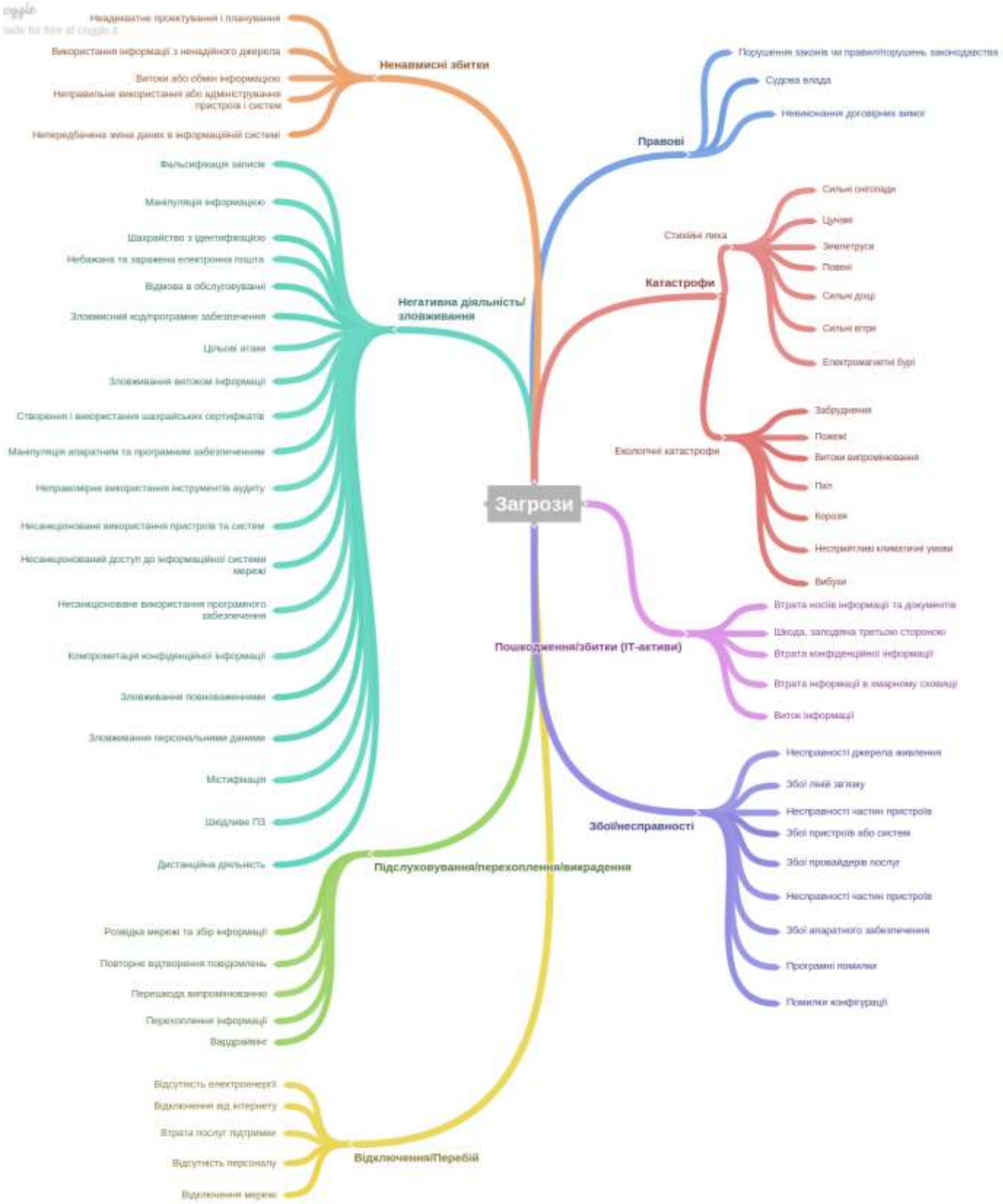

Рисунок 1.1 - Класифікація загроз кібербезпеки згідно ENISA

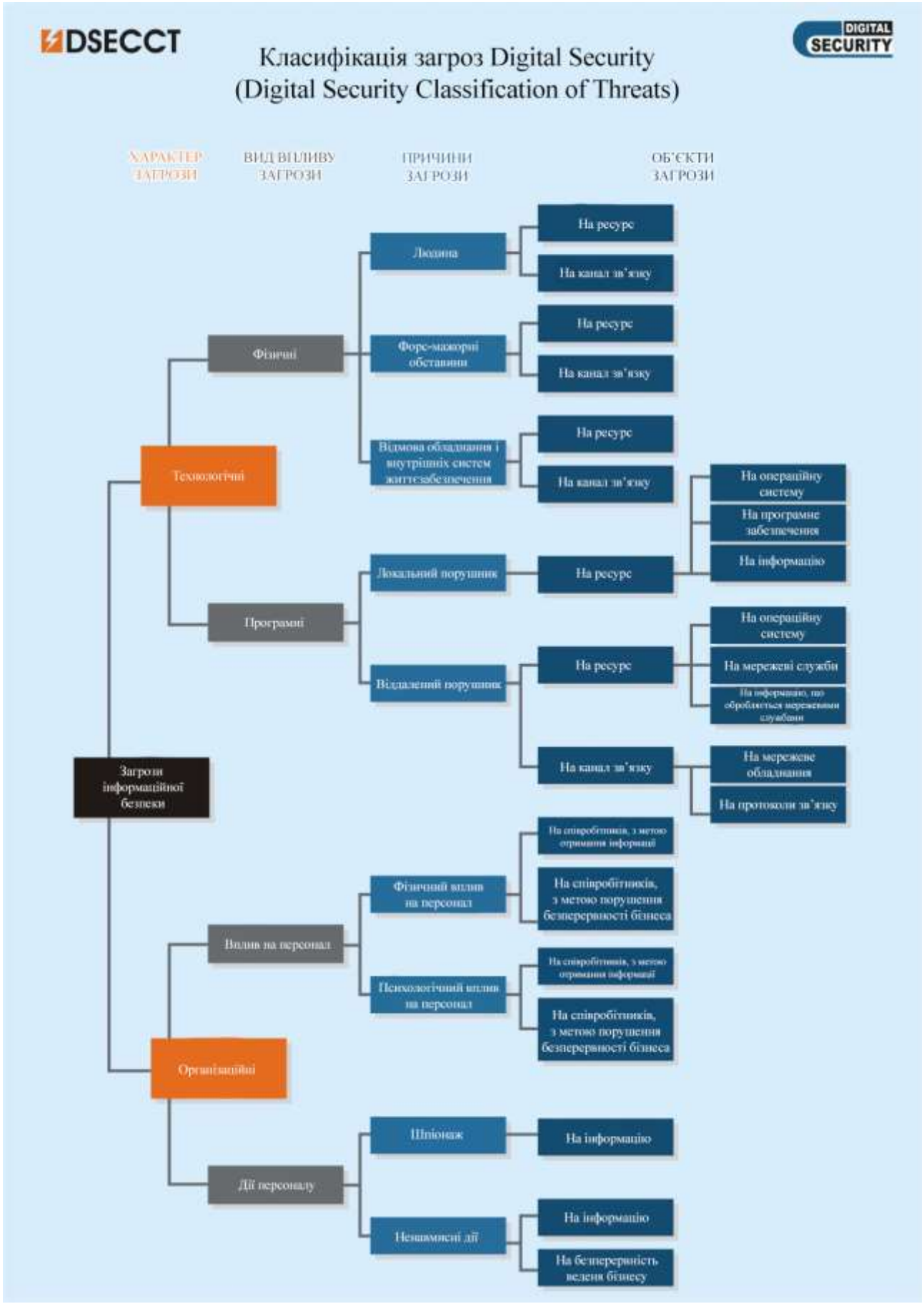

Рисунок 1.2 - Класифікація загроз згідно Digital Security

Відповідно до положення джерела загроз:

– поза межами контрольованої зони АС, наприклад перехоплення даних, переданих по каналах зв'язку, перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв;

– в межах контрольованої зони АС, наприклад застосування підслуховуючих пристроїв, розкрадання роздруківок, записів, носіїв інформації і т.п.;

– безпосередньо в АС, наприклад некоректне використання ресурсів АС.

За ступенем залежності від активності АС:

– незалежно від активності АС, наприклад розшифровування шифрів криптозахисту інформації;

– тільки в процесі обробки даних, наприклад загрози виконання і розповсюдження програмних вірусів.

За ступенем впливу на АС:

– пасивні загрози, які при реалізації нічого не змінюють у структурі та змісті АС, наприклад загроза копіювання секретних даних;

– активні загрози, які при впливі вносять зміни в структуру і зміст АС, наприклад впровадження троянських коней і вірусів.

За етапами доступу користувачів або програм до ресурсів:

– загрози, які проявляються на етапі доступу до ресурсів АС, наприклад загрози несанкціонованого доступу в АС;

– загрози, які проявляються після дозволу доступу до ресурсів АС, наприклад загрози несанкціонованого або некоректного використання ресурсів АС.

За способом доступу до ресурсів АС:

– загрози, які здійснюються з використанням стандартного шляху доступу до ресурсів АС;

– загрози, які здійснюються з використанням прихованого нестандартного шляху доступу до ресурсів АС, наприклад: несанкціонований

доступ до ресурсів АС шляхом використання недокументованих можливостей ОС.

За поточним місцем розташування інформації, що зберігається і оброблюється в АС:

– загрози доступу до інформації, що знаходиться на зовнішніх запам'ятовуючих пристроях, наприклад несанкціоноване копіювання секретної інформації з жорсткого диска;

– загрози доступу до інформації, що знаходиться в оперативній пам'яті, наприклад читання залишкової інформації з оперативної пам'яті, доступ до системної області оперативної пам'яті з боку прикладних програм;

– загрози доступу до інформації, що циркулює по лініях зв'язку, наприклад незаконне підключення до ліній зв'язку з подальшим введенням помилкових повідомлень або модифікацією переданих повідомлень, незаконне підключення до ліній зв'язку з метою прямої підміни законного користувача з подальшим введенням дезінформації та нав'язуванням неправдивих повідомлень;

– загрози доступу до інформації, яка відображається на терміналі або друкується на принтері, наприклад запис інформації, що відображається на приховану відеокамеру.

Небезпечні впливи на АС підрозділяються на випадкові і навмисні.

Причинами випадкових впливів при експлуатації АС можуть бути:

- аварійні ситуації через стихійні лиха і відключення електроживлення;
- відмови і збої апаратури;
- помилки в програмному забезпеченні;
- помилки в роботі обслуговуючого персоналу і користувачів;
- перешкоди в лініях зв'язку через впливи зовнішнього середовища. [6]

Помилки в програмному забезпеченні (ПЗ) є поширеним видом комп'ютерних порушень. ПЗ серверів, робочих станцій, маршрутизаторів і т.д. написано людьми, тому воно практично завжди містить помилки. Чим вище складність подібного ПЗ, тим більша ймовірність виявлення в ньому помилок і

уразливостей. Більшість з них не представляють ніякої небезпеки, деякі ж можуть привести до серйозних наслідків, таких як отримання зловмисником контролю над сервером, непрацездатність сервера, несанкціоноване використання ресурсів (використання комп'ютера як плацдарм для атаки і т.п.). Зазвичай подібні помилки усуваються за допомогою пакетів оновлень, що регулярно випускаються виробником ПЗ. Своєчасна установка таких пакетів є необхідною умовою безпеки інформації.

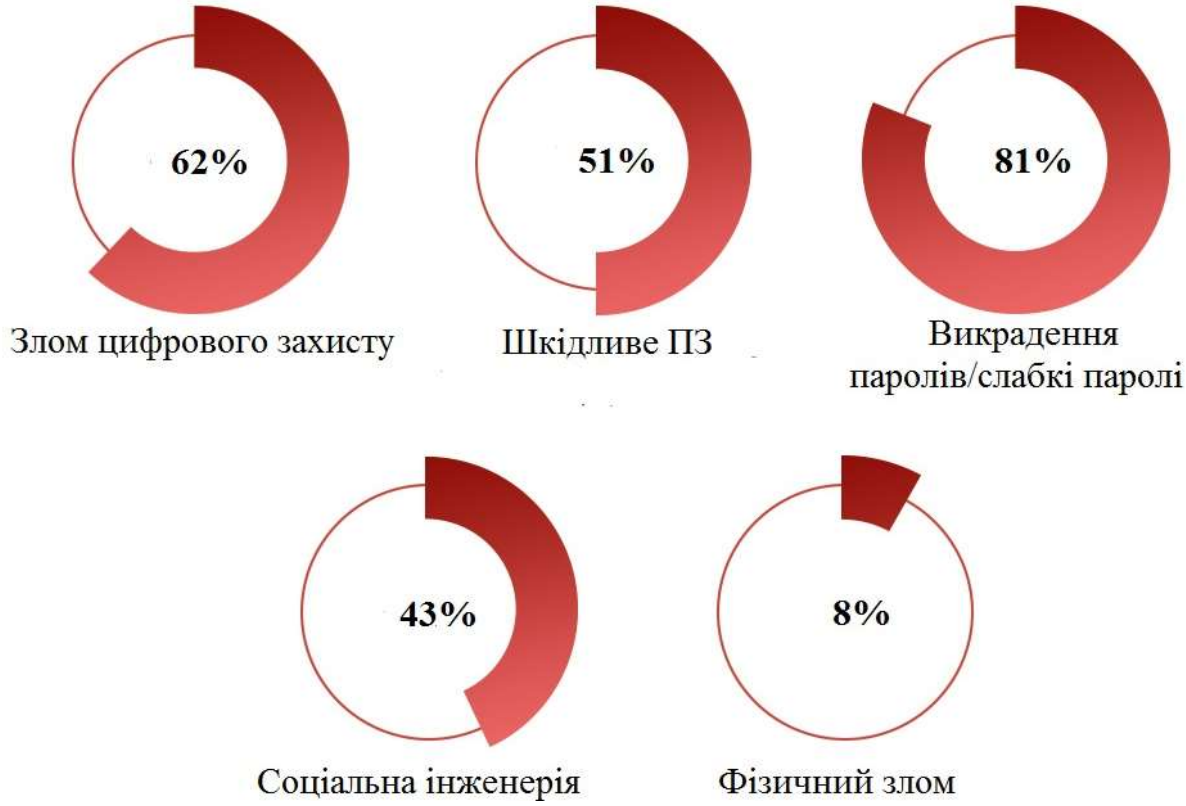

Рисунок 1.3 – Успішність реалізації методів, що використовували хакери у 2017 році

Навмисні загрози пов'язані з цілеспрямованими діями порушника. У якості порушника може виступати співробітник, відвідувач, конкурент, найманець і т.д. Дії порушника можуть бути обумовлені різними мотивами: невдоволенням службовця своєю кар'єрою, суто матеріальним інтересом (хабар), цікавістю, конкурентною боротьбою, прагненням самоствердитися будь-якою ціною і т.п.

Загрози порушення конфіденційності спрямовані на розголошення конфіденційної або секретної інформації. При реалізації цих загроз інформація стає відомою особам, які не повинні мати до неї доступ. У термінах комп'ютерної безпеки загроза порушення конфіденційності має місце щоразу, коли отримано несанкціонований доступ до деякої закритої інформації, що зберігається в комп'ютерній системі чи передається від однієї системи до іншої.

Загрози порушення цілісності інформації, що зберігається в комп'ютерній системі чи передається по каналу зв'язку спрямовані на її зміну або спотворення, що приводить до порушення її якості або повного знищення. Цілісність інформації може бути порушена навмисне, а також в результаті об'єктивних впливів з боку середовища, що оточує систему. Умисні порушення цілісності інформації не слід плутати з її санкціонованим зміною, яке виконується повноважними особами з обґрунтованою метою (такою зміною, наприклад, є періодична корекція деякої бази даних).

Загрози порушення доступності (відмова в обслуговуванні), спрямовані на створення таких ситуацій, коли певні навмисні дії або знижують працездатність АС, або блокують доступ до деяких її ресурсів. Наприклад, якщо один користувач системи запитує доступ до деякої службі, а інший робить дії по блокуванню цього доступу, то перший користувач отримує відмову в обслуговуванні. Блокування доступу до ресурсу може бути постійним або тимчасовим.

Ці види загроз можна вважати первинними або безпосередніми, оскільки реалізація цих загроз веде до безпосереднього впливу на інформацію, що захищається.

Серед перерахованих вище загроз велику частку мають загрози антропогенного характеру, що реалізовуються методами соціальної інженерії.

Рисунок 1.4 - Класифікація антропогенних джерел загроз

Важливим фактором захисту інформації на підприємствах є акцент на протидії методам соціальної інженерії. Будь-яка інформація, незалежно від її формату та стану - обробляється вона процесором, передається по каналах зв'язку, зберігається на диску - повинна входити в межі контролю системи забезпечення ІБ. Але технічні засоби, крім основного функціоналу, мають інтерфейси взаємодії з людиною, тому важливим елементом захисту інформації є сам співробітник компанії. Якщо по відношенню до технічних засобів завжди можна описати можливі ситуації, визначити і оцінити ризики, знайти способи захиститися (обмежити доступ, зашифрувати і т.п.), то в разі дій людини виникає проблема.

Виходячи з цього внутрішні загрози можуть утворюватися внаслідок:

– непрофесійних дій працівників;

– низького стану виховної та профілактичної роботи в організації;

– недосконалої системи заробітної плати та стимулювання праці персоналу;

– порушень правил кадрової роботи, невідповідності кадрової політики умовам роботи в організації;

– психологічних та комунікаційних особливостей працівників;

– відсутності нормативної бази організації, яка б установлювала режими їх діяльності та правила поведінки персоналу.

Участь співробітників у вирішенні питань ІБ дозволить підвищити захищеність активів компанії. Компетентність співробітників в питаннях ІБ, вміння застосовувати ці навички і знання в основній сфері діяльності значно підвищують довіру з боку клієнтів і партнерів компанії, сприяє більш стабільних відносин, оскільки помітно знижуються ризики. [7]

Загальний принцип всіх атак - введення жертви в оману. Для цього можуть використовуватися різні тактики, спрямовані на емоції, слабкості чи інші особливості особистості:

- кохання;
- співчуття і жалість;
- жадібність і бажання швидких результатів;
- страх перед начальством;
- недосвідченість;
- лінь.

Для розуміння ризиків вірогідності інцидентів соціальної інженерії важливо мати розуміння психологічного портрету персоналу, що працює на підприємстві.

Також слід зауважити, що існують критерії, що впливають на рівень обізнаності та вміння протистояти методам соціальної інженерії. До цих критеріїв відносяться:

- наявність та якість освіти;
- кваліфікація;

- наявність спеціальних прав доступу;
- наявність сертифікатів;
- наявність ліцензій;
- корпоративна та особиста мотивації.

1.2 Аналіз методів соціальної інженерії.

Соціальна інженерія - це сукупність підходів прикладних соціальних наук, які орієнтовані на цілеспрямовану зміну організаційних структур, що визначають людську поведінку і забезпечують контроль за нею, або - комплексний підхід до вивчення і зміни соціальної реальності, заснований на використанні інженерного підходу і наукомістких технологій .

Соціальна інженерія застосовується для:

- збору відомостей про мету підприємства;
- отримання конфіденційної інформації;
- прямого доступу до системи.

У сфері інформаційної безпеки термін «соціальна інженерія» використовується для опису науки і мистецтва психологічної маніпуляції. За статистикою аналітичного центру компанії Infowatch, 55% збитків, пов'язаних з порушеннями інформаційної безпеки, виникають з вини співробітників, що підпали під вплив соціальних інженерів. [1]

В освітній практиці ідеї соціальної інженерії реалізуються шляхом застосування сучасних освітніх технологій і активних методів навчання, а також за допомогою "насичення" навчального процесу дисциплінами соціоінженерного і організаційного циклу, у тому числі:

- теорія і методи соціальної інженерії;
- діагностика організацій;
- прогнозування і моделювання розвитку організацій;
- організаційне проектування і програмування;
- соціальне планування;

- впровадження соціальних нововведень в організації;
- практикум з соціальних технологій;
- методи вирішення конфліктів.

В основному інциденти соціальної інженерії, пов’язані з діями персоналу, відбуваються через низький рівень обізнаності користувачів. Таким чином, навчаючи своїх співробітників основним правилам в області інформаційної безпеки, організації можуть значно знизити ризик порушення інформаційної безпеки. Не дарма, навчання персоналу - одна з основних вимог міжнародного стандарту управління інформаційною безпекою ISO / IEC 27001.

Особливості атак з використанням людського фактору:

- не вимагають значних витрат;
- не вимагають спеціальних знань;
- можуть тривати протягом тривалого терміну;
- важко відслідковуються.

Людина часто набагато більш вразлива, ніж система. Саме тому соціальна інженерія спрямована на отримання інформації за допомогою людини, особливо в тих випадках, коли неможливо отримати доступ до системи (наприклад, комп'ютер з важливими даними відключений від мережі).

У соціальній інженерії є кілька технік, що використовуються для досягнення поставлених завдань. Всі вони засновані на помилках, що допускаються людиною в поведінці.

До технік соціальної інженерії відносяться:

1 Фішинг-атаки - це найпопулярніший вид шахрайства в соціальній інженерії. Фішингова є незаконне отримання конфіденційних даних користувачів (логіна і пароля). Часто фішингові листи написані погано і містять граматичні помилки. У цих листах зловмисники вказують гіперпосилання на копію сайту (наприклад, поштового клієнта) з формою, де необхідно ввести свій логін, пароль і іншу особисту інформацію. Наприклад, фішинг застосовується для збору логінів і паролів користувачів шляхом розсилки листів і повідомлень, що спонукають жертву повідомити необхідну

інформацію. Убезпечити себе від зловмисників можна ігноруванням листів від невідомих адресатів.

2 Претекстінг - це атака, проведена за заздалегідь підготовленим сценарієм. Такі атаки спрямовані на розвиток почуття довіри жертви до зловмисника. Атаки зазвичай здійснюються по телефону. Цей метод часто не вимагає попередньої підготовки і пошуку даних про жертви. Претекстінг полягає у видачі жертви себе за іншу людину для отримання бажаних даних. Отримати інформацію про людину можна через джерела відкритого доступу, в основному зі сторінок соціальних мереж.

3 Троянський кінь. Ця техніка використовує такі якості потенційної жертви, як цікавість і жадібність. Соціальний інженер відправляє e-mail з безкоштовним відео або оновленням антивірусу у вкладенні. Жертва зберігає вкладені файли, які насправді є троянськими програмами. Така техніка залишиться ефективною до тих пір, поки користувачі продовжують бездумно зберігати або відкривати будь-які вкладення.

4 Кви про кво. При використанні цього виду атаки зловмисники обіцяють жертві вигоду в обмін на факти. Наприклад, зловмисник дзвонить в компанію, представляється співробітником технічної підтримки і пропонують встановити «необхідне» програмне забезпечення. Після того, як отримано згоду на установку програм, порушник отримує доступ до системи і до всіх даних, що зберігаються в ній.

5 Tailgating або piggybacking має на увазі несанкціонований прохід зловмисника разом з законним користувачем через пропускний пункт. Такий спосіб не можна використовувати в компаніях, де співробітникам необхідно використовувати пропуски для входу на територію підприємства.

6 Однією з технік соціальної інженерії є плечовий серфінг. Він застосовується в транспорті, в кафе та інших громадських місцях, що дозволяють через плече жертви спостерігати за комп'ютерними пристроями і телефонами. Бувають ситуації, в яких користувач сам пропонує шахраєві

необхідну інформацію, будучи впевненим у порядності людини. У такому випадку говорять про зворотну соціальну інженерію.

7 Загрози при використанні служби миттєвого обміну повідомленнями. Користувачі швидко оцінили зручність обміну повідомленнями в режимі реального часу за допомогою мереж Skype, Viber, WhatsApp, Telegam та ін. Доступність і швидкість такого способу спілкування робить його відкритим для всіляких атак. Для безпеки варто ігнорувати повідомлення від невідомих користувачів, не повідомляти їм особисту інформацію, не переходити за надісланими посиланнями. [3]

Очевидно, що соціальна інженерія може завдати величезної шкоди будь-якій організації. Саме тому необхідно вживати всіх можливих заходів, щоб запобігти атак на людський фактор.

Спочатку завжди формулюється мета впливу на той чи інший об'єкт. Під "об'єктом" мається на увазі жертва, на яку націлена атака зловмисника.

Потім збирається інформація про об'єкт, з метою виявлення найбільш зручних мішеней впливу.

Після цього настає етап, який психологи називають атракцією. Атракція (від лат. attrahere - залучати, притягати) – це створення необхідних умов для впливу зловмисника на об'єкт.

Примушення до потрібної для соціального хакера дії зазвичай досягається виконанням попередніх етапів, тобто після того, як досягнута атракція, жертва сама створює необхідні зловмиснику дії. Однак в ряді випадків цей етап набуває самостійну значимість, наприклад, тоді, коли примушення до дії виконується шляхом введення в транс, психологічного тиску і т.д. [8]

Всі атаки соціальних хакерів укладаються в одну досить просту схему.

Соціальна інженерія спрямована не на комп'ютерну техніку, а на її користувача. Інтерес представляють всі платоспроможні особи, а також користувачі, що володіють цінною інформацією, співробітники підприємств і державних установ.

Рисунок 1.5 - Основна схема впливу в соціальній інженерії

Метод застосовується з метою виконання фінансових операцій, злому, крадіжки даних, наприклад, клієнтських баз, персональних даних і іншого несанкціонованого доступу до інформації. Соціальна інженерія допомагає конкурентам здійснювати розвідку, виявляти слабкі сторони організації, переманювати співробітників.

Таблиця 1.1 - TOP-10 найбільш поширених методів для отримання конфіденційної інформації за даними опитування компанії Balabit. [9]

№	USA	EU	Метод отримання конфіденційної інформації
1	81%	83%	Соціальна інженерія (наприклад, фішинг)
2	62%	63%	Скомпрометовані облікові записи (наприклад, слабкі паролі)
3	51%	54%	Веб-атаки (наприклад, ін'єкція SQL-кода)
4	33%	43%	Атаки на клієнтську частину (наприклад, на програми перегляду документів, веб-браузери)
5	23%	17%	Використання експлойтів для популярних серверних оновлень
6	21%	16%	Некеровані особисті засоби
7	15%	13%	Фізичне вторгнення
8	11%	10%	Тіньові IT (наприклад, використання користувачем особистих хмарних сервісів в робочих цілях)
9	9%	10%	Залучення поставників послуг третіх сторін (наприклад, аутсорсінг інфраструктури)
10	6%	6%	Викрадення даних, завантажених в хмарне сховище

Всі загрози, спрямовані на користувача за допомогою соціальної інженерії, можна розділити на кілька груп. Загрози, які виходять від використання телефону. Телефон є найпопулярнішим засобом спілкування, тому служить відмінним інструментом для впливу на людину. По телефону легко видати себе за іншу людину, тому, застосовуючи акторська майстерність, зловмисник легко переконує жертву перевести певну суму на банківський рахунок або повідомити дані. Поширені способи вивудження грошей за допомогою розсилки повідомлень і телефонних дзвінків про виграші в конкурсах, лотереях, проханнях перерахування грошей. Для безпеки рекомендується скептично ставитися до SMS сумнівного характеру, ігнорувати які приходять в них посилання. Необхідно перевіряти особистість абонента.

Зловмисники використовують соціальну інженерію для отримання матеріальної вигоди або для видобутку даних для перепродажу. Соціальна інженерія може використовуватися в якості одного з інструментів складних цільових кібератак. Джерелом загрози можуть бути електронні листи, текстові повідомлення в будь-яких месенджерах, смс-повідомлення і телефонні дзвінки. Шахраї можуть видавати себе за співробітників банків і інших фінансових

організацій, державних службовців, співробітників силових відомств, інтернет-провайдерів, представників поштових сервісів і великих веб-ресурсів і т.п. Аналіз ризику Для захисту компанії від шахрайства необхідно навчати персонал розпізнавати соціальну інженерію і правильно на неї реагувати, заборонити співробітникам обмінюватися паролями або мати один загальний, забезпечити захист клієнтських баз та іншої конфіденційної інформації, застосовувати особливу процедуру підтвердження для осіб, які звертаються до доступ до будь-яких даними. У браузерах з'явилася опція "антифішинг", що попереджає відвідувачів сайту про ненадійність даного ресурсу. Захиститися від загроз, які присилаються в електронних листах, допоможуть спам-фільтри. Існує послуга моніторингу, затребувана у компаній, найбільш часто піддаються атакам зловмисників. Знизять ризики більш складні методи авторизації.

Для захисту компанії від шахрайства необхідно навчати персонал розпізнавати соціальну інженерію і правильно на неї реагувати, заборонити співробітникам обмінюватися паролями або мати один загальний, забезпечити захист клієнтських баз та іншої конфіденційної інформації, застосовувати особливу процедуру підтвердження для осіб, які звертаються до доступ до будь-яких даних. У браузерах з'явилася опція "антифішинг", що попереджає відвідувачів сайту про ненадійність даного ресурсу. Захиститися від загроз, які присилаються в електронних листах, допоможуть спам-фільтри. Існує послуга моніторингу, затребувана у компаній, найбільш часто піддаються атакам зловмисників. Знизять ризики більш складні методи авторизації. [10]

Заходи протидії соціальної інженерії:

1 Розробка чіткого плану дій для працівників у разі виявлення атаки соціальної інженерії. Для запобігання атак з використанням методів соціальної інженерії необхідно розробити чіткі інструкції для всіх категорій співробітників, в яких будуть покроково розписано їхні дії в разі виявлення атак соціальної інженерії, і цю інформацію розмістити в доступному місці. Крім того, всі співробітники повинні бути інформовані про вжиті заходи щодо запобігання проникнення в інформаційні системи за допомогою соціальної

інженерії і протестовані на знання інструкцій і політик безпеки, прийнятих в даній організації.

2 Розробка для співробітників правил, що дозволяють визначати, яка інформація є важливою для компанії. Загальновідомо, що в організації повинні існувати правила доступу до конфіденційної інформації. Однак навіть ті відомості, які в більшості випадків не вважаються особливо важливими, можуть бути корисними соціальному інженеру, що збирає крихти інформації, зовні марної, але цілком придатної в професійних руках для створення атмосфери довіри і симпатії. Такою інформацією може бути робоча назва проекту, місце знаходження команди розробників, ім'я сервера, що використовують співробітники і т.д. Крім того, співробітники повинні знати правила знищення офісного сміття, який є для соціальних інженерів невичерпним джерелом інформації.

3 Навчити співробітників говорити «Ні!». Говорити «Ні!» Досить складно. Мало хто володіє цією якістю, не відчуваючи почуття незручності. Програма компанії з протидії атакам соціальної інженерії одним із завдань повинна ставити зміну норм ввічливості, а саме - розробку ввічливого відхилення запиту про надання важливої інформації, поки не буде встановлено особу яка подавала запит на її право на доступ до цієї інформації.

4 Розробити процедури для перевірки особистості людини і її авторизації. У будь-якій організації повинен бути розроблений процес перевірки особистості і авторизації людей, які звертаються за інформацією або вимагають якихось дій від співробітників компанії. При цьому не слід покладатися на особистий номер співробітника або інші схожі методи ідентифікації, так як такі номери часто використовуються і можуть бути легко отримані соціальним інженером від самих співробітників. З іншого боку, можна зобов'язати співробітників перевіряти особу, яка телефонувала, набравши її телефонний номер, який вказаний в телефонному довіднику компанії. Ця процедура не є дуже зручною у повсякденній роботі і не вирішує проблем з встановленням особи, але може захистити від багатьох атак.

5 Отримати підтримку керівництва компанії. Служба безпеки не зможе вводити заходи щодо запобігання атак без схвалення керівництва. Однак часто саме керівництво порушує прийняті ним самим політики безпеки. Тому співробітники ніколи не повинні отримувати від керівництва вказівок обійти протокол безпеки, і жоден співробітник не повинен бути покараний за те, що буде дотримуватися протоколу безпеки, навіть якщо отримав від керівництва вказівку його порушити. Причому ці положення слід задокументувати і запевнити підписами всіх керівників. Крім того, дієвими заходами протидії соціальної інженерії є тести на проникнення, які можуть проводитися регулярно. Тести дозволяють не тільки перевірити політики безпеки і правильність їх застосування, а й виявити ті недоліки захисту, які не були враховані при їх розробці.

6 Навчання і тренінг персоналу. Важливим є навчання персоналу навичкам протидії методам соціальної інженерії, розробка тренінгів по становленню пильності персоналу і періодична перевірка знань і навичок співробітників шляхом проведення спеціальних перевірок. Цей метод є дуже дієвим, тому необхідно розглянути його детальніше.

1.3 Аналіз підходів до підвищення обізнаності персоналу в питаннях, пов'язаних з інформаційною та кібербезпекою

Мета навчання персоналу - формування та підтримання необхідного рівня кваліфікації персоналу, з урахуванням вимог підприємства в сфері інформаційної безпеки та забезпечення високого рівня безпеки в інформаційній системі.

Завдання політики підприємства в галузі навчання питань інформаційної безпеки:

– вироблення і дотримання правил щодо захисту інформації;

– розробка і впровадження системи навчання, що включає виявлення потреби в навчанні, планування і бюджетування, організацію навчання і контроль його результативності;

– побудова навчання відповідно до специфікою бізнес-процесів підприємства;

– формування стандартів навчання;

– включення передового досвіду, знань, ефективних методів організації праці в процесі навчання персоналу інформаційної безпеки;

– мотивація співробітників до підвищення безпеки і забезпечення надійності роботи;

– регулярна перевірка знань в сфері інформаційної безпеки та їх застосування на практиці.

Програма підвищення обізнаності персоналу.

Під програмою обізнаності співробітників розуміється впровадження процесу, регулярного підвищення рівня знань співробітників підприємства в області ІБ.

Основні вимоги, яким все розглянуті рішення повинні задовольняти:

1) надавати можливість регулярного навчання співробітників незалежно від їх територіального місцезнаходження і без відриву від робочого процесу;

2) підносити матеріал користувачам в простій і зрозумілій формі;

3) вартість всіх впроваджуються рішень повинна бути адекватною, і не повинна бути в прямій залежності від кількості учнів.

Виходячи з перерахованих вище вимог, зрозуміло, що для вирішення даного завдання підходять різні системи корпоративного дистанційного навчання або ті чи інші «нестандартні» рішення.

Основним засобом для навчання великої кількості співробітників підприємства в даний час, безумовно, є різні системи дистанційного навчання (СДН). Зрозуміло, що СДН – більшою мірою не навчальна програма, а засіб доставки до кінцевого користувача інформації (навчальних матеріалів), яка в неї закладена. Тому при виборі СДО, як правило, слід звертати увагу на два

параметри: основний функціонал (управління процесом навчання співробітників, гнучкість формування звітів і т.п.) і набір навчальних матеріалів, які надаються разом з системою.

Під «нестандартними» засобами підвищення кваліфікації співробітників компанії в області ІБ розуміються різні методи і засоби, які, як правило, не використовуються для навчання, завдяки яким на емоційному і підсвідомому рівні співробітник запам'ятовує навчальний матеріал і розуміє важливість вимог ІБ. Деякими методами такого навчання є:

- скрінсейвер;
- фільми, мультфільми, ролики;
- новини по ІБ та інше.

Огляд методів навчання співробітників питань ІБ не можна було б назвати повним без розгляду можливих методів оцінки ефективності впровадженої в компанії програми навчання.

Одним із прикладів оцінки саме практичних, а не теоретичних знань співробітників, є використання соціальної інженерії, коли імітуються ситуації, в яких дії необізнаного користувача можуть призвести до порушення ІБ.

Навчені основним правилам в області ІБ співробітники підприємства і, особливо, що використовують отримані знання на практиці, істотно знижують ризик порушення ІБ і, як наслідок, зменшують можливі збитки підприємства. При це навчання співробітників в області ІБ при грамотному підході не вимагає значних матеріальних і тимчасових витрат.

В даний час існує велика кількість різних методів підвищення обізнаності співробітників в області ІБ.

Найбільша ж ефективність, досягається при комплексному використанні різних елементів.

Інститут SANS визначив п’ять основних моделей зрілості інформаційної безпеки, що характеризують рівень обізнаності персоналу підприємств з точки зору кібербезпеки: [11]

1 Неіснуючий: Програми не існує. Працівники не мають уявлення про свою роль у підтриманні кібербезпеки на підприємстві, що їх дії безпосередньо впливають на безпеку організації, не знають і не розуміють політику організації та легко стають жертвами методів соціальної інженерії.

2 Дотримання вимог: Програма призначена, перш за все, для задоволення конкретних критеріїв відповідності або аудиту. Навчання обмежується щорічною або спеціальною підготовкою. Працівники не знають організаційної політика та / або їх роль у захисті інформаційних активів їх організації.

3 Зміцнення поінформованості та зміни поведінки: програма визначає навчальні теми, що надають найбільший вплив на підтримку місії організації та зосереджена на цих ключових темах. Програма виходить за рамки простого щорічного навчання та включає постійне підкріплення протягом усього року. Програма впроваджується цікавим та позитивним способом, що сприяє зміні поведінки на роботі та вдома. В результаті люди розуміють політику організації, активно її дотримуються та визначають інциденти, запобігають їм й своєчасно повідомляють про них.

4 Довготривале заохочення та зміна культури: У програмі є процеси, ресурси та підтримка керівництва для довгострокового життєвого циклу, включаючи як мінімум щорічний огляд та оновлення програми. Таким чином, програма та кібербезпека є визначеною частиною культури організації.

5 Надійна структура метрик: Програма має надійну структуру метрик для відстеження прогресу та вимірювання впливу. Отже, програма постійно вдосконалюється і здатна продемонструвати рентабельність інвестицій. Показники є важливою частиною кожного етапу. Ця програма підкреслює, що для того, щоб по-справжньому мати зрілу модель інформаційної безпеки, підприємство повинне не тільки змінювати поведінку та культуру, але й мати структуру метрик для демонстрації цих змін.

Рисунок 1.6 - Ефективність моделей зрілості обізнаності про безпеку згідно SANS

Інститут SANS у 2017 році провів опитування, аналогічне минулому року. На рисунку нижче відображено яку модель зрілості обізнаності обирають респонденти у 2017 році. Загалом ці цифри були дуже схожі на торішні, у межах 3 відсоткових пунктів. Варто відмітити, що більше половини респондентів в даний час надають перевагу моделі зміцнення поінформованості та зміни поведінки та добре працюють над створенням довгострокових та стабільних програм.

Рисунок 1.7 - Наскільки є досконалою програма підвищення обізнаності згідно SANS

У рисунку нижче наведені основні проблеми безпеки, пов’язані з обізнаністю персоналу.

Основні проблеми	Відгуки	%
Комунікація	113	15,98
Залучення співробітників	101	14,29
Час	95	13,44
Культура	85	12,02
Ресурси	83	11,74
Підтримка вищого керівництва	80	11,32
Інше	66	9,34
Гроші	42	5,,94
Примусове виконання програми	31	4,38
Персонал	11	1,56
Підсумок	707	100%

Рисунок 1.8 - Основні проблеми безпеки, пов’язані з обізнаністю персоналу згідно SANS

Аналізуючи результати опитування можна зробити два висновки. По-перше, комунікація - це проблема з номером 1, а за нею слідує зацікавленість. Працюючи з організаціями по всьому світу, SANS виявили, що ці два фактори дуже тісно пов'язані між собою, тому що погана комунікація часто є основною причиною невдалого залучення людей.

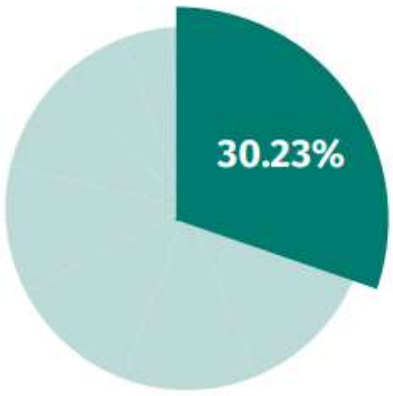

Рисунок 1.9 - Відсоток суми комунікації та зацікавленості персоналу у сукупності проблем соціальної інженерії

Друге зауваження - це ресурси. Хоча деякі респонденти просто писали "ресурси" як фактор, що обмежує подальший розвиток обізнаності, ті, хто представив більш детальний опис, визначили "час", а не "бюджет" як найбільш обмежений ресурс.

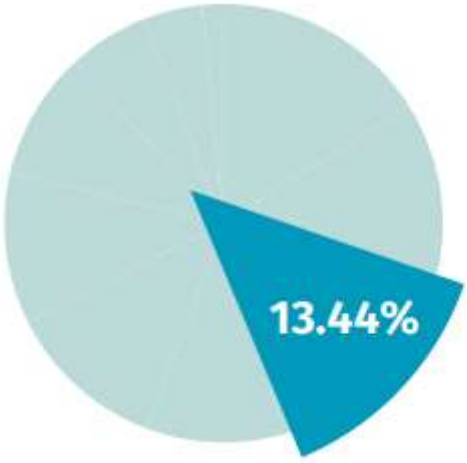

Рисунок 1.10 - Відсоток часу у сукупності проблем соціальної інженерії

Виходячи з цих даних, можна відмітити, що основними перешкодами підприємців на шляху до підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії є обмежені ресурси підприємства та нестача часу.

У 2017 році, як і у 2016, професіонали з обізнаності персоналу зробили висновки на основі статистичних даних. Компаніям, що брали участь у опитуванні, бракує ресурсів, необхідних для виконання роботи. 58% респондентів зазначають, що брак ресурсів перешкоджає зростанню програм з обізнаності в рамках їх організації.

Однак дослідження 2017 року показало, що також важливою перешкодою до зростання програм з обізнаності є брак часу. Чим більше часу у вас є, тим більшій кількості людей ви зможете приділити увагу і допомогти, тим успішніша ваша програма пізнання. Це має сенс. Важливо пам’ятати, що обізнаність - це не технічне рішення, це людське рішення. Фахівці з управління обізнаністю персоналу повинні спілкуватися, займатися і співпрацювати з іншими - і це займає багато часу.

Інформування частіше за все є не основною, а частковою роботою. На жаль, ця статистика залишилися майже такою ж, як у 2016 році. Лише 8% спеціалістів з обізнаності персоналу постійно займаються управлінням обізнаності. Натомість понад 75% фахівців з обізнаності витрачають 25% або менше свого часу на підвищення обізнаності. Це вражає. Неможливо уявити, щоб команда з реагування на інциденти, або відділ захисту інформації зосереджували свою увагу лише на такій малій частині своєї роботи. Наскільки надійною була б безпека такої організації?

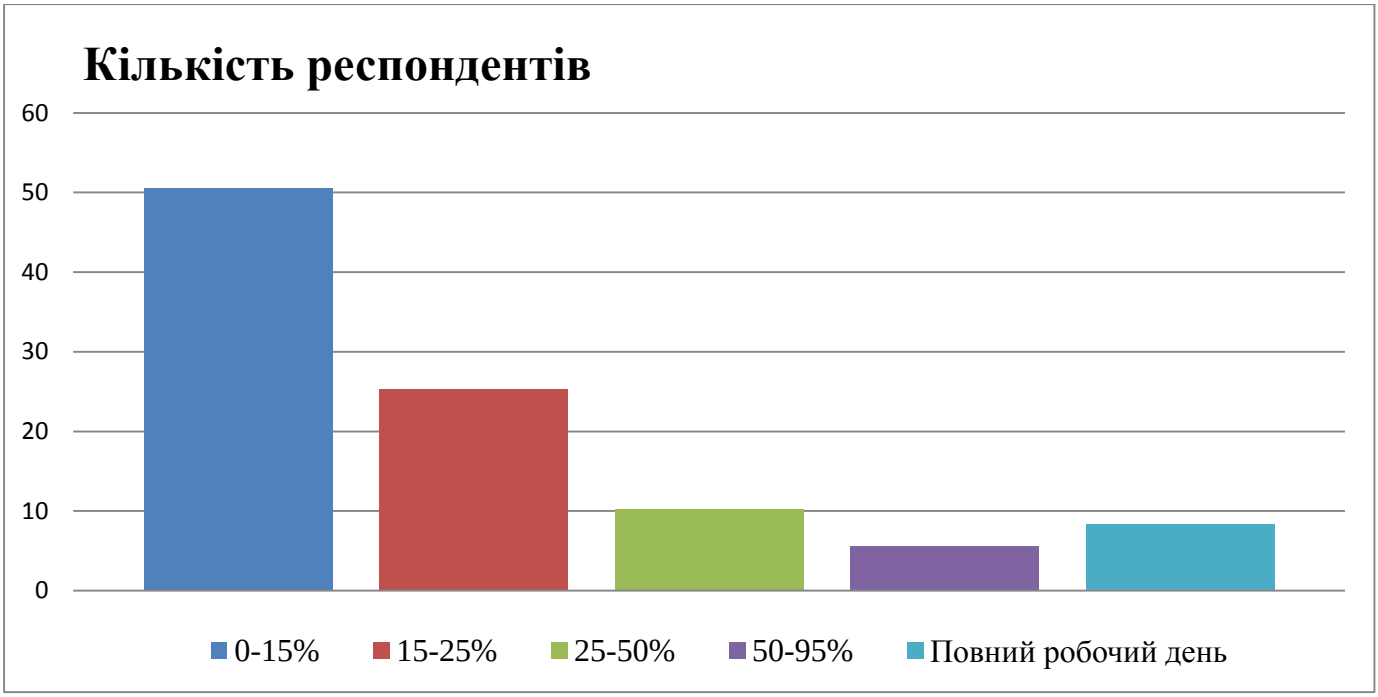

Рисунок 1.11 - Який відсоток часу респондентів зосереджено на обізнаності про безпеку згідно SANS

Необхідно також відмітити, що важливим фактором ефективності програми обізнаності персоналу є кількість працівників, що працюють над управлінням обізнаності персоналу цілий робочій день. Звичайно, що обов'язків працівників з інформаційної безпеки значно більше, аніж лише управління обізнаністю персоналу у питаннях протидії методам соціальної інженерії. Спеціалісти з інформаційної безпеки витрачають приблизно 15% робочого часу на обізнаність персоналу. Тому раціональним є розподілення

витрат часу на обізнаність між декількома спеціалістами. Аналітики SANS підрахували скільки спеціалістів мають працювати повний робочій день у організаціях з різною кількістю співробітників, щоб належним чином підтримувати обізнаність персоналу та підвищувати її.

Розмір підприємства (люд.)	Кількість робітників, що працюють цілий робочий день
1-500	1,28
500-1000	1,3
1000-5000	1,24
5000-25000	1,58
25000-100000	2,09
100000 >	2,45

Рисунок 1.12 - Кількість спеціалістів, що працюють повний робочий день у сфері обізнаності персоналу в залежності від кількості робітників підприємства згідно SANS

Це може здатися сміливим твердженням, але ніхто не можете просто виділити певну суму грошей - і проблема, пов’язана з персоналом, буде вирішена. Коли SANS опитували спільноту, вони хотіли дізнатися, наскільки великі бюджети респонденти виділили для програм підвищення обізнаності наступного року. Результати були демонстративними. Дані показують, що, хоча бюджет впливає на програму зрілості, співвідношення грошей та ефективності програми не є настільки ж важливим, як співвідношення між часом та ефективністю програми. Як висновок можна відмітити, якщо у вас немає часу, щоб зробити роботу, то не буде достатньо тільки грошей, щоб забезпечити успішну програму обізнаності.

Бюджет	Не існуючий	Дотримання вимог	Зміцнення поінформованості та зміни поведінки	Довготрив але заохочення та зміна	Надійна структура метрик

				культури	
Менше ніж 5000$	9.87%	27.63%	44.74%	6.58%	0.99%
5000-25000	2.65%	19.58%	59.79%	10.05%	0.00%
50000-100000	4.84%	20.97%	53.23%	12.90%	0.00%
100000% і більше	0,00%	16,92%	43,08%	24,62%	1,54%
Я не знаю	7,97%	25,90%	40,64%	5,58%	0,80%

Рисунок 1.13 - Бюджети за рівнем зрілості програми інформаційної безпеки згідно SANS

Загальні рекомендації щодо підвищення рівня обізнаності на підприємстві.

Занадто багато організацій вважають процес поінформованості про безпеку не вартим пильної уваги. Хтось (часто в IT) випадково покладає відповідальність на співробітників за контроль обізнаності персоналу без виділення часу або підтримки на це для високої якості процесу. Щоб створити безпечну культуру поведінки на підприємстві, фахівців з обізнаності про безпеку необхідно визнати як окрему професію у галузі безпеки, і надавати цим професіоналам ресурси (як персонал, так і бюджет), щоб робити процес підвищення обізнаності ефективним та успішним.

Для значного підвищення ефективності підвищення обізнаності персоналу у питання протидії методам соціальної інженерії необхідно створити партнерські відносини у колективі. Необхідно співпрацювати з іншими, щоб інші співпрацювали з вами. Тісне партнерство можливо зробити у своєму відділі комунікацій, оскільки він може допомогти розповсюдити інформацію про важливість програми зрілості обізнаності персоналу. Інші відділення підприємства також можуть принести значну користь у розповсюдженні програми. До таких відділів відносяться маркетинг, менеджмент, відділ кадрів, служба підтримки та інші. Не варто недооцінювати сили побудови відносин у

організації.

Бюджет корисно виділяти на придбання часу. А саме на раціоналізацію процесів обізнаності, щоб підвищувати їх ефективність. Корисним буде найняти сторонніх спеціалістів для налагодження деяких організаційних процесів на підприємстві. Також ефективним шляхом удосконалення процесу управління обізнаністю персоналу є використовування додаткових методичних та програмних матеріалів для навчання і атестації персоналу.

У минулому році було виявлено [11], що брак навичок комунікації був значним блокатором успішної програми обізнаності. Зрозуміло, що необхідними для фахівців є різні навички (співпраця, планування, управління проектами, навчальний дизайн та ін.). Однак не менш важливим є спілкування. Комунікація дає можливість спілкуватися з працівниками та залучати їх, а також мати можливість спілкуватися з лідерами та демонструвати важливість організації для обізнаності про безпеку.

Переважна більшість професіоналів з обізнаності виходять з технічного досвіду - 80%. Менш ніж 8% володіють такими навичками, як комунікація, маркетинг, навчання чи розподілення людських ресурсів. [11] Ті, хто має технічний досвід, мають перевагу, тому що вони володіють глибоким розумінням технічних та антропогенних ризиків. Вони знають, які моделі поведінки є найбільш ефективними в управлінні цими ризиками. Проте ці самі фахівці часто не мають навичок проведення тренінгів, необхідних для ефективного управління з цими ризиками та залучення працівників таким чином, щоб ефективно змінювати корпоративну поведінку.

Професіонали безпеки сприймають безпеку від методів СІ простою, адже ці знання є частиною їх повсякденного життя. Тому фахівці з безпеки вважають, що обізнаність у питаннях протидії методам соціальної інженерії повинна бути інтуїтивно зрозумілою усьому персоналу підприємства. Тому вони часто будують свою програму обізнаності на основі цих неправильних уявлень. Як наслідок, те, що вони освітлюють у програмі обізнаності, може призвести до повної невідповідності до того, що насправді потрібно людям в

організації.

Ще гірше, коли фахівець із безпеки, спілкуючись з керівництвом, використовує технічних терміни. Ця помилка призводить до непорозуміння. Професіонали з безпеки повинні розмовляти з лідерами доступною мовою, яка є зрозумілою не тільки фахівцям у сфері обізнаності персоналу.

Для проведення своїх атак зловмисники, які застосовують техніки соціальної інженерії, часто експлуатують довірливість, лінь, люб'язність і навіть ентузіазм користувачів і співробітників організацій. Захиститися від таких атак непросто, оскільки їхні жертви можуть не підозрювати, що їх обманули. Зловмисники, які використовують методи соціальної інженерії, переслідують, в загальному, такі ж цілі, що і будь-які інші зловмисники: їм потрібні гроші, інформація або IT-ресурси компанії жертви. Для захисту від таких атак потрібно вивчити їх різновиди, зрозуміти, що потрібно зловмисникові, і оцінити збиток, який може бути заподіяний організації. Володіючи всією цією інформацією, можна інтегрувати в політику безпеки необхідні заходи захисту.

1.4 Висновки до першого розділу. Постановка задачі.

У першому розділі було досліджено теоретичну базу у сфері обізнаності персоналу в питаннях протидії методам соціальної інженерії.

А саме, було проаналізовано загрози кібербезпеки та розглянуто їх класифікацію за різними ознаками. З загального списку загроз було виділено загрози кібербезпеки антропогенного характеру. З загроз антропогенного характеру було виділено загрози методами соціальної інженерії.

Далі було проаналізовано методи соціальної інженерії. Наступним етапом було розглянуто існуючі методи протидії атакам методами соціальної інженерії.

Виходячи з результатів аналізу висновків до першого розділу, було поставлено задачі на подальше дослідження.

Постає необхідним розробити методику управління обізнаністю персоналу у питаннях протидії методам соціальної інженерії. Для цього необхідно розробити методичні вказівки для підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії та шаблон опитувальника як метрику для аналізу рівня обізнаності персоналу у питаннях протидії методам соціальної інженерії.

Задля обґрунтування доцільності розробленої методики необхідно проаналізувати практичну та економічну ефективності запропонованої методики.

РОЗДІЛ 2
РОЗРОБКА МЕТОДИКИ ПІДВИЩЕННЯ ОБІЗНАНОСТІ ПЕРСОНАЛУ В ПИТАННЯХ ПРОТИДІЇ МЕТОДАМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

2.1 Розробка методики для підвищення обізнаності персоналу в питаннях протидії методам соціальної інженерії

Доведено, що навчання співробітників підвищує ефективність роботи всієї компанії, так як знижує ймовірність порушення інформаційної та кібербезпеки. Підприємствам завжди важливо, щоб навчання проводилося з максимальною віддачею і при цьому з мінімальними вкладеннями. Підприємствам потрібно, щоб співробітники були навчені, вміли застосовувати знання на практиці, вміли грамотно працювати з інформаційною системою. Крім цього, керівництво не хоче надовго відривати співробітників від виконання прямих обов'язків.

Крім застосування технічних заходів захисту інформації (розмежування доступу, мінімізації повноважень, моніторингу подій і трафіку і т.п.), які протидіють відомим шаблонами атак, основним заходом захисту від використання прийомів соціальної інженерії є метод «Безпека через навчання». Навчання має бути регулярним, простим і зрозумілим. Часто в організаціях до процесу навчання вимогам і практикам ІБ підходять формально. Тому виникає ситуація, коли працівники компаній мають низький рівень поінформованості та грамотності з питань інформаційної безпеки. Це тягне за собою їх халатне, неуважне ставлення до вхідних інформаційних потоків. Крім навчання, також варто підвищувати пильність співробітників шляхом їх періодичного тестування. Тому постає питання розробки простої та ефективної методики підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії.

Розробка методики підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії включає в себе такі складові:

1 Розробка методичних вказівок для підвищення рівня обізнаності персоналу у питаннях протидії методам соціальної інженерії.

2 Розробка шаблону опитувальника як метрики ефективності методики обізнаності та способу виявлення слабких сторін обізнаності персоналу для подальшого навчання їх у цьому напрямку.

Описати процес впровадження методики управління обізнаністю персоналу у питаннях протидії методам соціальної інженерії можна наступним чином:

Рисунок 2.1 – Процес розробки та впровадження методики

Першим етапом розробки та впровадження методики є проведення опитування на підприємстві для визначення рівня обізнаності персоналу у питаннях протидії методам соціальної інженерії.

Далі необхідно проаналізувати інциденти соціальної інженерії на підприємстві. Враховуючи результати аналізу інцидентів та специфіку підприємства (сферу його діяльності, кількість співробітників, процеси зберігання та обробки конфіденційної інформації), корегуємо методичні вказівки та опитувальник.

Наступним етапом є проведення інструктажу користування методикою для співробітників підприємства, що будуть займатися обізнаністю персоналу у питаннях протидії методам соціальної інженерії на підприємстві. Ввідний інструктаж включає:

– загальний опис методики (мета, складові методики, соціальна й економічна доцільності, методичний процес);

– ввідну лекцію, як приклад для подальших лекцій на підприємстві;

– правила користування опитувальником і метод аналізу результатів опитування;

– шляхи коректування подальших лекцій на основі аналізу результатів опитування для підвищення ефективності методики.

Далі процес буде відбуватися безпосередньо на підприємстві співробітниками, що уповноважені управляти процесом обізнаності персоналу у питаннях протидії методам соціальної інженерії.

Лекції за методичними вказівками рекомендовано проводити двічі на рік.

Після проведення лекції необхідно провести опитування персоналу, щоб зрозуміти на скільки підвищилась обізнаність і які моменти лекції не були достатньо зрозумілими для слухачів.

Через 3-6 місяців після проведення лекції на підприємстві проводиться аналіз інцидентів соціальної інженерії.

На основі аналізу опитування персоналу та інцидентів соціальної інженерії необхідно внести корективи до лекцій та опитувальника, щоб більш детально охопити питання, пов’язані з актуальними інцидентами соціальної інженерії на підприємстві.

Знову на підприємстві проводять лекцію і далі процес йде по колу.

Таким чином, навчання персоналу буде проходити кілька разів на рік. Завдяки аналізу результатів опитування та інцидентів соціальної інженерії на підприємстві буде представлена можливість корегування лекційного матеріалу для поступового підвищення рівня обізнаності персоналу та зниження кількості інцидентів СІ на підприємстві до мінімуму.

2.2 Розробка методичних вказівок для підвищення обізнаності персоналу в питаннях протидії методам соціальної інженерії

У даному підрозділі буде розроблено методичні вказівки, що дають достатньо повне уявлення про соціальну інженерію, пов’язані з нею загрози та методи протидії атакам у цій сфері. Методичні вказівки розроблено шляхом аналізу проблем безпеки інформації, викликаних антропогенним фактором, актуальних статистичних даних щодо методів та програм підвищення обізнаності персоналу.

Основною метою методичних вказівок є підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії.

Методичні вказівки виконують декілька функцій:

– несуть інформативний характер для персоналу: дають визначення основних понять соціальної інженерії, описують пов’язані з нею загрози та методи боротьби із ними;

– надають рекомендації для керівництва щодо налаштування організаційних процесів на підприємстві для зниження ймовірності реалізації загроз соціальної інженерії;

– є базою для проведення лекцій для персоналу для підвищення обізнаності у питаннях протидії методам соціальної інженерії.

На основі особливостей будови мережі, програмно-апаратного забезпечення, засобів захисту і теоретичних даних, сформовані загальні методичні рекомендації для адміністраторів і користувачів мережі.

Методичні рекомендації охоплюють питання:

- порядку доступу до конфіденційної інформації;
- роботи з криптографічними системами;
- фізичної безпеки (доступ в приміщення);
- розмежування прав доступу;
- роботи у глобальній мережі Інтернет;
- дублювання, резервування і зберігання конфіденційної інформації.

Методичні вказівки розподілені на такі частини:

1 Загальна термінологія

2 Вступ

3 Опис існуючих уразливостей та загроз у сфері соціальної інженерії і методи протидії ним

4 Рекомендації щодо протидії методам соціальної інженерії

2.3 Розробка шаблону опитувальника для аналізу рівня обізнаності персоналу протидії методам соціальної інженерії як метрики контролю обізнаності

Шаблон опитувальника розроблюється на базі даних, що були викладені у методичних вказівках для підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії.

Основною метою опитувальника є оцінювання та подальший аналіз рівня обізнаності персоналу у питаннях протидії методам соціальної інженерії.

Опитувальник поділяється на дві частини:

1 Основний блок питань, що включає питання:

- по теоретичній базі у сфері соціальної інженерії;
- видів загроз та уразливостей соціальної інженерії;
- основні методи протидії методам соціальної інженерії.

2 Спеціальний блок питань, що включає спеціальні питання, орієнтовані на специфіку сфери діяльності підприємства, його розміри та побажання керівництва.

По закінченню опитування підраховується відсоток правильних відповідей кожного співробітника, що дає підстави для аналізу рівня обізнаності окремих співробітників та персоналу в цілому у питаннях протидії методам соціальної інженерії.

Також шляхом аналізу опитування персоналу можна виявити теми, що виявилися недостатньо зрозумілими для персоналу, що прослухав лекцію. Таким чином, важливо передивитися матеріал, що викладається по цим темам та більш детально зупинитися на важких питаннях під час проведення наступної лекції.

2.4 Висновки до другого розділу

У другому розділі розроблено методику управління обізнаністю персоналу у питаннях протидії методам соціальної інженерії.

А саме:

– детально розкрито етапи процесу розробки та впровадження методики на підприємстві;

– розроблено методичні вказівки для підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії (методичні вказівки винесені у Додаток Б);

– розроблено шаблон опитувальника як метрику для аналізу рівня обізнаності персоналу у питаннях протидії методам соціальної інженерії.

РОЗДІЛ 3
ЕКОНОМІЧНА ЧАСТИНА

3.1 Вступ

Метою даного розділу є обґрунтування економічної доцільності застосування методики для підвищення кваліфікації персоналу у питаннях протидії методам соціальної інженерії на підприємстві.

Для визначення ефективності необхідно розрахувати:

1) витрати на розробку, впровадження та підтримку методики;

2) різницю вірогідності загроз у сфері соціальної інженерії шляхом визначення рівня обізнаності персоналу у питаннях протидії методам соціальної інженерії до та після впровадження методики на підприємстві (у відсотках за допомогою опитувальника);

3) економічну доцільність застосування методики на підприємстві.

3.2 Загальні відомості про підприємство

Приватне підприємство (ПП) «Море Турів» розташоване на 3ому поверсі ТРЦ «Материк» за адресою вул. Марії Кюрі 5 у м. Дніпро. Підприємство є франчайзинговим туристичним агентством, що займається продажем авіа білетів, страховок, пакетних турів у різні країни світу, допомогою у оформленні віз та закордонних паспортів. Кількість співробітників – 6.

До активів підприємства відносяться:

- офісні меблі (5 столів, 10 стільців, шафа) на суму 18 400 грн.;

- персональні комп’ютери (4 ноутбуки, 1 стаціонарний комп’ютер) на суму 50 000 грн.;

- програмне забезпечення (Windows 10, база даних, антивірус, спеціалізоване ПЗ) на суму 28 000 грн.

3.3 Витрати на розробку, впровадження та підтримку методики

Витрати на розробку методики є одноразовими та розраховуються за формулою:

$$К_1 = t * (З_{ЗП} + З_{МЧ}), \quad (3.1)$$

де t – загальна тривалість створення методики, год.;

$З_{ЗП}$ – заробітна плата виконавця за годину, грн./год.;

$З_{МЧ}$ – вартість витрат машинного часу за годину, грн./год.

Загальна тривалість створення методики розраховується за формулою:

$$t = t_{РМ} + t_{РО,} \quad (3.2)$$

де $t_{РМ}$ – тривалість розробки методичних вказівок, год.;

$t_{РО}$ – тривалість розробки опитувальника, год.

$$t = 320 + 40 = 360 \text{ год.}$$

Вартість 1 години машинного часу ПК визначається за формулою:

$$З_{МЧ} = P * C_E + \frac{Ф_{ПЕРВ} * Н_A}{F_р} + \frac{К_{ЛПЗ} * Н_{АПЗ}}{F_р}, \quad (3.3)$$

де P – встановлена потужність ПК, кВт;

C_E – тариф на електричну енергію, грн./кВт*година;

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

$Н_A$ – 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 $F_р$ = 1 920 год.).

$$З_{мч} = 0,5 * 1.67 + \frac{4500 * 0,25}{1920} + \frac{2000 * 0,5}{1920} = 1,94$$

грн./год.

Отже, витрати на розробку методики:

$$К_1 = 360 * (25 + 1,94) = 9\ 698 \text{ грн.}$$

Витрати на впровадження є одноразовими та розраховуються за формулою:

$$К_2 = К_1 + К_{ППЗ} + К_{НО} + К_{ВЛ}, \quad (3.4)$$

де $К_1$ - одноразові витрати на розробку методики, грн.;

$К_{ППЗ}$ - витрати на придбання програмного забезпечення для зберігання паролів, грн.;

$К_{НО}$ - налаштування опитувальника на персональних комп’ютерах співробітників, грн.;

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

$$К_2 = 9\ 698 + 1\ 800 + 350 + 1\ 000 = 12\ 848 \text{ грн.}$$

Витрати на підтримку методики (щорічні):

$$С_1 = К_{ПІ} + К_{ВП}, \quad (3.5)$$

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.

$$С_1 = 5\ 000 + 1\ 500 = 6\ 500 \text{ грн.}$$

Розраховуємо загальні річні витрати на застосування методики на підприємстві за формулою:

$$В_{ЗАГ} = К_2 + С_1, \quad (3.6)$$

$$В_{ЗАГ} = 12\ 848 + 6\ 500 = 19\ 348 \text{ грн.}$$

3.4 Розрахунок вірогідності реалізації загроз у сфері соціальної інженерії до та після впровадження методики на підприємстві

Слід зазначити, що чим нижче рівень обізнаності персоналу у питаннях протидії методам соціальної інженерії, тим вище рівень загрози у цій сфері.

Ймовірність реалізації загрози можна розглядати як функцію трьох змінних: ймовірності існування загрози безпеки ($Й_{ІЗ}$), ймовірності існування уразливості ($Й_{ІУ}$) і коефіцієнт наявності потенційних сил по цій загрозі для впливу на систему безпеки ($К_{НПС}$). Тоді ймовірність реалізації загрози можна розрахувати:

$$Й = Й_{ІЗ} * Й_{ІУ} * К_{НПС.} \quad (3.7)$$

Якщо будь-яка з цих змінних наближається до нуля, то і ймовірність реалізації загрози буде також прагнути до мінімуму. Розроблена методика

направлена на зменшення ймовірності існування уразливості шляхом підвищення обізнаності персоналу у питаннях протидії загрозам СІ.

Як було вказано у розділі 1.2 за статистикою аналітичного центру компанії Infowatch, 55% збитків, пов'язаних з порушеннями інформаційної безпеки, виникають з вини співробітників, що підпали під вплив соціальних інженерів. [7]

Отже:

$$Й_{ІЗ} = 55\%.$$

Ймовірність існування уразливості приймаємо як відсоток обізнаності, упущений персоналом. Тобто:

$$Й_{ІУ} = 100\% - О, \qquad (3.8)$$

де О – рівень обізнаності персоналу у питаннях протидії методам соціальної інженерії.

Для визначення рівня обізнаності персоналу у питаннях протидії методам соціальної інженерії до впровадження методики використаємо розроблений опитувальник, що автоматично підраховує відсоток правильних відповідей співробітника, що проходить тестування ($К_{1Д}$- $К_{6Д}$).

Для розрахунку середнього рівня обізнаності персоналу підприємства визначаємо середнє арифметичне значення для усіх співробітників (6 працівників):

$$О_{ДО} = (К_{1Д} + К_{2Д} + К_{3Д} + К_{4Д} + К_{5Д} + К_{6Д}) / 6, \qquad (3.9)$$

$$О_{ДО} = (42 + 38 + 53 + 41 + 47 + 37) / 6 = 43\%.$$

Аналогічно розрахунку рівня обізнаності персоналу у питаннях протидії методам соціальної інженерії до впровадження методики, розраховуємо рівень обізнаності персоналу після впровадження методики ($К_{1П}$- $К_{6П}$):

$$О_{ПІСЛЯ} = (К_{1П} + К_{2П} + К_{3П} + К_{4П} + К_{5П} + К_{6П}) / 6, \quad (3.10)$$

$$О_{ПІСЛЯ} = (79 + 73 + 92 + 68 + 83 + 67) / 6 = 77\%.$$

Коефіцієнт наявності потенційних сил приймаємо $Й_{НПС}$ = 0,03%.

Отже, розрахуємо ймовірність реалізації загрози до впровадження методики:

$$Й_{ДО} = Й_{ІЗ} * (100\% - О_{ДО}) * К_{НПС,} \quad (3.11)$$

$$Й_{ДО} = 55 * 57 * 0,03 = 94,05\%.$$

Та після впровадження методики:

$$Й_{ПІСЛЯ} = Й_{ІЗ} * (100\% - О_{ПІСЛЯ}) * К_{НПС,} \quad (3.12)$$

$$Й_{ПІСЛЯ} = 55 * 23 * 0,03 = 37,95\%.$$

3.5 Економічна доцільність застосування методики на підприємстві

Приймаємо річний можливий збиток ПП «Море Турів» від атак методами соціальної інженерії рівним З = 100 000 грн.

Отже, річний збиток до впровадження методики складав 94,05% від можливого збитку:

$$З_{ДО} = 94\ 050 \text{ грн.}$$

Річний збиток після впровадження методики складає 54,45% від можливого збитку:

$$З_{після} = 37\ 950 \text{ грн.}$$

Економічну доцільність застосування методики розраховуємо за формулою:

$$Е = З_{після} - З_{до} - С_1 – К_2 > 0, \quad (3.13)$$

$$Е = 94\ 050 – 37\ 950 – 6\ 500 – 12\ 848 = 36\ 752 \text{ грн.} > 0.$$

Визначаємо термін окупності капітальних інвестицій за формулою:

$$Т = К_2 / (З_{після} – З_{до} – С_1), \quad (3.14)$$

$$Т = 12\ 848 / 49\ 600 = 0,26 \approx 3 \text{ місяці.}$$

3.6 Висновки до економічної частини

В результаті розрахованих витрат на впровадження методики для підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії, було доведено, що застосування методики на приватному підприємстві «Море Турів» знизить ймовірність реалізації загроз соціальної інженерії на 56,1% і окупиться за 3 місяці.

ВИСНОВКИ

У дипломній роботі було розроблено методику підвищення рівня обізнаності персоналу у питаннях протидії методам соціальної інженерії.

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

– шляхом аналізу нормативно-правової бази у сфері соціальної інженерії та дослідження існуючих методів підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії було виявлено необхідність в розробці простої та ефективної методики управління обізнаністю персоналу у питаннях протидії методам соціальної інженерії;

– було розроблено методику підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії, до якої увійшли три складові:

1) розроблено процес впровадження методики на підприємстві;

2) розроблено методичні вказівки для підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії;

3) розроблено електронний опитувальник для аналізу ефективності методики на підприємстві та корегування лекційної програми;

– було обґрунтовано доцільність розробленої методики шляхом розрахунку витрат на розробку та впровадження методики для підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії на прикладі ПП «Море Турів» і обчислення зниження ймовірності реалізації загроз СІ на 56,1% і окупності методики, що склала 3 місяці.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Аналітичний центр компанії Infowatch [Електронний ресурс] – Режим доступу: https://www.infowatch.ru/analytics.
2. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Закон України від 01.06.2010 № 2297-VI. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2163-19.
3. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» [Електронний ресурс] – Режим доступу: http://iszzi.kpi.ua/images/Info_bezpeka/ND_TZI/4.
4. ENISA [Електронний ресурс] – Режим доступу: https://www.enisa.europa.eu/.
5. Класифікация загроз Digital Security [Електронний ресурс] – Режим доступу: http://www.infosecurity.ru/_eshop/detail/dsec_grif_ct.htm.
6. Бондарцев Р.А Класифікація загроз інформаційної безпеки [Електронний ресурс] – Режим доступу: https://studfiles.net/preview/6006132/page:2/.
7. Легенченко К. О., Тимофеев Д. С. Управління обізнаністю персоналу в питаннях протидії методам соціальної інженерії [Електронний ресурс] – Режим доступу: http://ir.nmu.org.ua/bitstream/handle/123456789/1667/14.pdf.
8. Шейнов В. П. Маніпулювання та захист від маніпуляцій. – 2014, 215 с. [Електронний ресурс] – Режим доступу: http://www.koob.ru/sheinov/against_manipulation.
9. State of Cybersecurity in Local, State & Federal Government [Electronic resource]: report, 2015, Ponemon Institute. – Access: http://www.ponemon.org/blog/the-state-of-cybersecurity-in-local-state-and-federal-government.

10. Блог A1Q1 Методи соціальної інженерії або атаки на людський фактор [Електронний ресурс] – Режим доступу: http://www.a1qa.ru/blog/sotsialnaya-inzheneriya-ili-ataki-na-chelovecheskiy-faktor/

11. SANS institute [Електронний ресурс]: security awareness report 2017. – Режим доступу: https://securingthehuman.sans.org/resources/reports-and-case-studies.

12. Microsoft TechNet Як захистити внутрішню мережу і співробітників компанії від атак, заснованих на використанні соціотехніки [Електронний ресурс] – Режим доступу: https://technet.microsoft.com/ru-ru/library/cc875841.aspx#EEAA

13. Портал Anti-Malware Соціальна інженерія [Електронний ресурс] – Режим доступу: https://www.anti-malware.ru/threats/social-engineering

14. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : Закон України від 19.04.2014, підстава 1170-18. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/80

15. Про захист персональних даних [Електронний ресурс] : Закон України від 01.06.2010 № 2297-VI. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2297-17

16. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD)

17. Про інформацію [Електронний ресурс] : Закон України від 02.10.1992 № 2657-XII. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2657-12

18. Міжнародний стандарт ISO/IEC 27005:2011 «Інформаційна технологія. Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки» [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/ru/catalogue_detail?csnumber=56742.

19. Будник М. М. ,Тимофєєв Д. С. Внутрішні загрози інформаційної безпеки та заходи по їх мінімізації [Електронний ресурс] – Режим доступу: http://ir.nmu.org.ua/bitstream/handle/123456789/1666/7.pdf?sequence=1

20. Резник Ю.М. Соціальна інженерія: предметна область і межі застосування // Соціологічні дослідження, 1994, № 2.

21. Соціальна інженерія // Сучасна західна соціологія: Словник. М., 2015.

22. Романенко Е. А., Тимофеев Д. С. Методы обучения персонала по вопросам информационной безопасности [Електронний ресурс] – Режим доступу: http://ir.nmu.org.ua/bitstream/handle/123456789/1667/14.pdf

23. Кургинян С.Е. Слабость силы / С.Е. Кургинян //Аналитика закрытых элитных игр и её концептуальные основания. – М.: ЭТЦ, 2006. – 388 с

24. Парсонс Т. Общетеоретические проблемы социологии / Т. Парсонс // Социология сегодня. Проблемы и перспективы. Американская буржуазная социология середины XX века. – М., 1965. – С. 25-67.

25. SANS institute [Електронний ресурс]: security awareness report 2015. – Режим доступу: https://securingthehuman.sans.org/resources/reports-and-case-studies

26. SANS institute [Електронний ресурс]: security awareness report 2016. – Режим доступу: https://securingthehuman.sans.org/resources/reports-and-case-studies

27. Резник Ю.М. Социальная инженерия как профессия / Ю.М. Рєзнік // Известия Томского политехнического университета. – 2011. – Т. 318. – № 6. – С.124-130.

28. Резник Ю.М. Соціально-гуманітарні технології управління: специфіка і можливості застосування // Вісник РГУ ім. С.А.Есенина. - 2010. - № 4 (29). - С. 91-105.

29. Автореферати дисертацій: електронна наукова бібліотека НБУВ [Електронний ресурс] – Режим доступу: http://www.nbuv.gov.ua/eb/. – Загол. з екрана

30. Укрепление безопасности компании через обучение сотрудников [Електронний ресурс] – Режим доступу: http://www.eos.ru/eos_delopr/eos_delopr_intesting/detail.php?ID=17058&SECTION_ID=668 – Загол. з екрана.

Додаток А

ПЕРЕЛІК ФАЙЛІВ НА ЕЛЕКТРОННОМУ НОСІЇ

1 Пояснювальна_записка.docx

2 Презентація.pptx

3 Опитувальник

Додаток Б

МЕТОДИЧНІ ВКАЗІВКИ

Для підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії

Методичні вказівки розподілені на такі частини:

1. Загальна термінологія
2. Вступ
3. Опис існуючих уразливостей та загроз у сфері соціальної інженерії і методи протидії ним
4. Рекомендації щодо протидії методам соціальної інженерії

Загальна термінологія

Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення.

Конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем.

Цілісність – означає неможливість модифікації неавторизованим користувачем.

Доступність – властивість інформації бути отриманою авторизованим користувачем, за наявності у нього відповідних повноважень, в необхідний для нього час.

Кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

Загроза – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків інформаційно-телекомунікаційній системі.

Уразливість – певні недоліки в системі, що створюють можливість реалізації загрози. Тобто, це нездатність системи протистояти реалізації певної загрози або сукупності загроз.

Вступ

Соціальна інженерія (СІ) – це метод несанкціонованого доступу до інформаційних систем, який був заснований на особливостях психологічної поведінки людини.

Соціальна інженерія застосовується для:

- збору відомостей про мету підприємства;
- отримання конфіденційної інформації;
- прямого доступу до системи.

У сфері інформаційної та кібербезпеки термін «соціальна інженерія» використовується для опису науки і мистецтва психологічної маніпуляції. За статистикою 55% збитків, пов'язаних з порушеннями інформаційної безпеки, виникають з вини співробітників, що підпали під вплив соціальних інженерів.

В основному інциденти соціальної інженерії, пов’язані з діями персоналу, відбуваються не через злого умислу, а просто через низький рівень обізнаності користувачів. Таким чином, навчаючи своїх співробітників основним правилам в області інформаційної безпеки, організації можуть значно знизити ризик порушення інформаційної безпеки.

Опис існуючих уразливостей та загроз у сфері соціальної інженерії і методів протидії ним

Атаки, засновані на методах соціальної інженерії, можна розділити на п'ять основних напрямків:

- мережеві атаки;

- телефонні атаки;
- пошук інформації у смітті;
- персональні підходи;
- зворотня соціальна інженерія.

Крім цього потрібно також розуміти, що розраховують отримати зловмисники. Зловмисниками рухають ті ж потреби, що і всіма людьми: гроші, соціальний статус і самооцінка. Іншими словами, зловмисники хочуть отримати чужі гроші або ресурси, домогтися визнання в суспільстві чи своїй групі і підняти себе в своїх очах. На жаль, зловмисники домагаються цих цілей незаконними методами, крадучи інформацію або завдаючи шкоди комп'ютерним системам. Будь-які атаки можуть завдати компанії шкоди у вигляді фінансових збитків, витрати ресурсів, витоку інформації, зниження працездатності компанії і шкоди її репутації.

Ступінь і прояви збитків від реалізації методів соціальної інженерії можуть бути різними:

1 Моральний і матеріальний збиток, нанесений фізичним особам, чия інформація була викрадена.

2 Фінансовий збиток, нанесений шахраєм в зв'язку з витратами на відновлення систем інформації.

3 Матеріальні витрати, пов'язані з неможливістю виконання роботи через зміни в системі захисту інформації.

4 Моральний збиток, пов'язаний з діловою репутацією компанії.

Мережеві загрози

У наш час персоналу компаній часто доводиться використовувати і обробляти електронні дані та запити, отримані з внутрішніх і зовнішніх джерел. Завдяки цьому зловмисники можуть налагоджувати відносини з співробітниками компаній через Інтернет, залишаючись при цьому анонімними. У пресі регулярно з'являються повідомлення про мережеві атаки, засновані на використанні електронної пошти, спливаючих додатків і служб миттєвого обміну повідомленнями. При проведенні таких атак для заподіяння шкоди або

несанкціонованого використання комп'ютерних ресурсів часто застосовуються троянські програми або віруси. Почати боротьбу з багатьма загрозами цього роду можна з впровадження надійних засобів захисту від вірусів.

Зловмисник, який використовує методи СІ, не намагається заразити корпоративну систему шкідливими програмами в ході прямої атаки. Замість цього він обманним шляхом переконує співробітника компанії надати йому потрібну інформацію, приводячи обґрунтовані правдоподібні аргументи. Співробітники компанії повинні знати, як найкраще визначати і блокувати мережеві атаки, засновані на методах СІ.

Загрози, пов'язані з електронною поштою.

Багато співробітників щодня отримують через корпоративні та приватні поштові системи десятки і навіть сотні електронних листів. Зрозуміло, при такому потоці кореспонденції неможливо приділити належну увагу кожному листу. Це значно полегшує проведення атак, заснованих на методах СІ. Більшість користувачів систем електронної пошти спокійно ставляться до обробки таких повідомлень, сприймаючи цю роботу як електронний аналог перекладання паперів з однієї папки в іншу. Коли зловмисник надсилає поштою простий запит, його жертва часто виконує те, про що її просять, не замислюючись про свої дії.

Наприклад, зловмисник може відправити співробітнику компанії лист, в якому йдеться про наказ начальника надіслати йому розклад вихідних днів для організації зустрічі, відправивши копію відповіді всім користувачам, включеним в доданий список. Зловмисник може легко включити в цей список зовнішній адресу і підробити ім'я відправника, щоб здавалося, що лист отримано з внутрішнього джерела. Підробити дані особливо легко, якщо у зловмисника є доступ до корпоративної комп'ютерної системі, тому що в цьому випадку йому не можуть перешкодити брандмауери, що захищають периметр мережі. Витік інформації про розклад вихідних днів не здається загрозою безпеці, але насправді таким чином зловмисник може дізнатися, хто із співробітників компанії і коли буде відсутній на своєму робочому місці. В цей

час зловмисник зможе видати себе за відсутнього співробітника з меншим ризиком викриття.

В останнє десятиліття використання електронної пошти в якості засобу проведення СІ атак набуло дуже високої популярності. Отримання особистої або конфіденційної інформації у користувачів за допомогою електронної пошти називають фішингом. З цією метою зловмисники можуть використовувати електронні листи, що імітують листи реальних закладів, зокрема банків та компаній-партнерів.

Таблиця 1 - Мережеві атаки, пов'язані з використанням електронної пошти, і можливий збиток від них

Мета атаки	Опис	Збиток
Крадіжка корпоративної інформації	Видаючи себе за внутрішнього користувача, зловмисник намагається отримати корпоративну інформацію.	Витік конфіденційної інформації Шкода репутації компанії
Крадіжка фінансової інформації	Використовуючи метод фітинга, зловмисник запрошує конфіденційну корпоративну інформацію (наприклад облікові записи).	Фінансові втрати Витік конфіденційної інформації Шкода репутації компанії
Завантаження шкідливого ПЗ	Зловмисник обманним шляхом переконує користувача клацнути на гіперпосилання або відкрити вкладення, що призводить до зараження корпоративної мережі.	Зниження робото спроможності компанії Шкода репутації компанії
Завантаження ПЗ зловмисника	Зловмисник обманним шляхом переконує користувача клацнути на гіперпосилання або відкрити вкладення, в результаті чого завантажується програма зловмисника, що споживає ресурси корпоративної мережі.	Втрата ресурсів Шкода репутації компанії Фінансові втрати

Як і у випадку з іншими різновидами шахрайства, найефективнішим способом захисту від атак зловмисників, заснованих на методах СІ, є скептичне ставлення до будь-яких несподіваних вхідних листів. Для поширення цього підходу в організації в політику безпеки слід включити конкретні принципи використання електронної пошти, що охоплюють перераховані нижче елементи:

- вкладення в документи;
- гіперпосилання в документах;
- запити особистої або корпоративної інформації, які виходять із середини компанії;
- запити особистої або корпоративної інформації, які виходять із-за меж компанії.

Спливаючі додатки і діалогові вікна

Щоб переконати користувача натиснути кнопку в діалоговому вікні, зловмисники найчастіше відображають попередження про проблему (наприклад реалістичне повідомлення про помилку операційної системи або програми) або пропонують додаткові послуги, такі як можливість безкоштовно завантажити програму, яка прискорює роботу комп'ютера.

Таблиця 2 - Мережеві атаки, пов'язані з використанням спливаючих додатків і діалогових вікон, і можливий збиток від них

Мета атаки	Опис	Збиток
Крадіжка особистої інформації співробітника	Зловмисник запитує у співробітника компанії особисту інформацію.	Витік конфіденційної інформації Фінансові втрати (для співробітника)
Завантаження шкідливого ПЗ	Зловмисник обманним шляхом переконує користувача клацнути на гіперпосилання або відкрити вкладення.	Зниження робото спроможності компанії Шкода репутації компанії

Завантаження ПЗ зловмисника	Зловмисник обманним шляхом переконує користувача клацнути на гіперпосилання або відкрити вкладення.	Втрата ресурсів Шкода репутації компанії Фінансові втрати

Захист користувачів від атак СІ, заснованих на використанні спливаючих додатків, зводиться переважно до інформування. Для усунення самих причин проблеми можна заблокувати у браузері спливаючі вікна і автоматичне завантаження файлів, однак повністю виключити відображення всіх спливаючих вікон в браузері не вийде. Тому краще переконати користувачів не клацати ніякі посилання у спливаючих вікнах без відома спеціалістів служби підтримки. Щоб цей підхід виправдав себе, співробітники служби підтримки не повинні засуджувати користувачів за підключення до Інтернету без службової потреби. На це можна вплинути, прийнявши відповідну корпоративну політику використання Інтернету в особистих цілях.

Служба миттєвого обміну повідомленнями

Миттєвий обмін повідомленнями набув широкої популярності серед корпоративних користувачів. Через швидкість і легкість використання цей спосіб комунікації відкриває широкі можливості для проведення атак СІ: користувачі ставляться до нього як до телефонного зв'язку і не пов'язують з потенційними програмними загрозами. Двома основними видами атак, заснованими на використанні служби миттєвого обміну повідомленнями, є вказівка в тексті листа посилання на шкідливу програму і доставка самої програми. Звичайно, миттєвий обмін повідомленнями - це ще й один із способів запиту інформації.

Миттєвий обмін повідомленнями має кілька особливостей, які полегшують проведення СІ атак. Одна з таких особливостей - його неформальний характер. У поєднанні з можливістю привласнювати собі будь-які імена цей фактор дозволяє зловмисникові набагато легше видавати себе за іншу людину і значно підвищує його шанси на успішне проведення атаки,

заснованої на підробці даних.

Видаючи себе за іншого відомого користувача, зловмисник відправляє лист або миттєве повідомлення, одержувач якого вважає, що отримав його від відомої йому людини. Це послаблює увагу одержувача, і він часто без всяких підозр клацає на посилання або відкриває вкладення, прислане зловмисником.

Таблиця 3 - Атаки, пов'язані з використанням служби миттєвого обміну повідомленнями, і можливий збиток від них

Мета атаки	Опис	Збиток
Крадіжка конфіденційної корпоративної інформації	Підроблюючи миттєві повідомлення, зловмисник видає себе за співробітника компанії, щоб запросити корпоративну інформацію.	Витік конфіденційної інформації Шкода репутації компанії
Завантаження шкідливого ПЗ	Зловмисник обманним шляхом переконує користувача клацнути на гіперпосилання або відкрити вкладення, що призводить до зараження корпоративної мережі.	Зниження робото спроможності компанії Шкода репутації компанії
Завантаження ПЗ зловмисника	Зловмисник обманним шляхом переконує користувача клацнути на гіперпосилання або відкрити вкладення, в результаті чого здійснюється завантаження програми зловмисника, що споживає ресурси корпоративної мережі.	Втрата ресурсів Шкода репутації компанії Фінансові втрати

Якщо компанія має намір використовувати можливості скорочення витрат і інші переваги, що забезпечуються миттєвим обміном повідомленнями, необхідно передбачити в корпоративних політиках безпеки механізми захисту від відповідних загроз. Для отримання надійного контролю над миттєвим обміном повідомленнями в корпоративному середовищі необхідно виконати п'ять таких вимог:

1. Обрати одну платформу для миттєвого обміну повідомленнями. Це полегшить роботу служби підтримки і зменшить ймовірність того,

що співробітники будуть користуватися аналогічними службами інших постачальників.

2. Визначити параметри захисту, що задаються при розгортанні служби миттєвого обміну повідомленнями.
3. Визначити принципи встановлення нових контактів. Запропонувати користувачам не брати за замовчуванням будь-які запрошення до спілкування.
4. Задати стандарти вибору паролів. Вимагати від співробітників, щоб їх паролі до служби обміну повідомленнями відповідали стандартам вибору надійних паролів, які прийняті для паролів, що слугують для входу в систему.
5. Скласти рекомендації по використанню служби миттєвого обміну повідомленнями. Сформулювати для користувачів служби миттєвого обміну повідомленнями оптимальні принципи роботи з нею, підкріпивши рекомендації обґрунтованими доводами.

Служба підтримки

Служба підтримки - один з головних механізмів захисту від звичайних зловмисників і в той же час це мішень для зловмисників, що використовують методи СІ.

Таблиця 4 - Телефонні атаки на службу підтримки і можливі збитки від них

Мета атаки	Опис	Збиток
Отримання інформації	Видаючи себе за легального користувача, зловмисник намагається отримати ділову інформацію.	Витік конфіденційної інформації
Отримання доступу	Видаючи себе за легального користувача, зловмисник намагається отримати доступ до корпоративних систем.	Витік конфіденційної інформації Шкода репутації компанії Зниження робото спроможності

		компанії Втрата ресурсів Фінансові втрати

Процедури забезпечення безпеки повинні виконувати в таких ситуаціях бути наступними:

- Служба підтримки повинна гарантувати, що всі дії користувачів, які звертаються за допомогою, реєструються. Якщо, звернувшись в службу підтримки, зловмисник здійснить спробу несанкціонованого доступу до даних і ресурсів, реєстрація його дій дозволить швидко заблокувати атаку і обмежити заподіяний збиток.
- Служба підтримки повинна затвердити структуровану процедуру обробки різних типів запитів. Наприклад, запит зміни прав доступу для співробітника повинен бути адресований керівнику по електронній пошті, це виключить несанкціоновані або неформальні зміни рівнів безпеки.

Загрози, пов'язані з утилізацією сміття

Несанкціонований аналіз сміття часто дозволяє зловмисникам отримати цінну інформацію. Паперові відходи компанії можуть містити відомості, які зловмисник може використовувати безпосередньо (наприклад номери облікових записів і ідентифікатори користувачів) або які полегшують йому проведення подальших атак (списки телефонів, схеми структури організації і т. д.). Для зловмисника, котрий використовує CI, відомості другого типу особливо цінні, тому що вони допомагають йому проводити атаки, не викликаючи підозри. Наприклад, знаючи імена та прізвища людей, що працюють в певному підрозділі компанії, зловмисник має набагато більше шансів при пошуку підходу до її співробітників, більшості з яких буде легко повірити, що людина, яка так багато знає про компанію, є їх колегою.

Електронні засоби зберігання інформації бувають для зловмисників ще більш корисними. Якщо в компанії не діють правила збору відходів, що

передбачають утилізацію списаних носіїв даних, на викинутих жорстких дисках, компакт-дисках і дисках DVD можна знайти найрізноманітніші відомості. Сучасні електронні носії даних надійні і довговічні, тому служби, що відповідають за захист IT-систем, повинні забезпечити дотримання політик, що передбачають знищення цих носіїв або стирання даних, що зберігаються на них.

Таблиця 5 - Атаки, засновані на пошуку інформації в смітті, і можливий збиток від них

Мета атаки	Опис	Збиток
Паперове сміття у контейнерах для сміття, що знаходяться поза межами організації	Вивчаючи документи, витягнуті з зовнішніх сміттєвих контейнерів, зловмисник дізнається важливу корпоративну інформацію.	Витік конфіденційної інформації Шкода репутації компанії
Паперове сміття у кошиках для сміття, що знаходяться всередині організації	Обходячи прийняті в організації принципи управління зовнішнім сміттям, зловмисник краде документи з сміттєвих кошиків, розташованих в самій організації.	Витік конфіденційної інформації Шкода репутації компанії
Викинуті електронні носії	Зловмисник краде дані і додатки, що зберігаються на викинутих електронних носіях, і самі носії.	Витік конфіденційної інформації Втрата ресурсів Шкода репутації компанії

Співробітники компанії повинні розуміти всі наслідки, до яких може привести викидання паперових документів або електронних носіїв інформації в сміттєву корзину. Як тільки сміття залишає територію компанії, її права можуть більше на нього не поширюватися. Саме по собі «пірнання в смітті» не завжди є чимось незаконним, тому співробітники компанії повинні знати, що потрібно робити зі сміттям. Паперове сміття завжди слід подрібнювати в

паперорізальних машинах, а електронний - знищувати або витирати записані на ньому дані. Якщо будь-які документи (наприклад телефонний довідник) через розміри або жорсткість неможливо подрібнити в паперорізальній машині або у користувача немає технічної можливості це зробити, потрібно визначити спеціальну процедуру позбавлення від них. Сміттєві контейнери слід розміщувати в захищеній області, недоступній стороннім особам.

При розробці політики утилізації сміття важливо переконатися в тому, що дотримані всі місцеві санітарні норми і норми безпеки. У міру можливості слід вибирати екологічно чисті способи утилізації сміття.

Персональні підходи

Найпростіший і дешевий для зловмисника спосіб отримати потрібну йому інформацію - безпосередньо запросити її. Яким би грубим і банальним цей спосіб не здавався, він незмінно залишається головним в арсеналі зловмисників, що використовують методи СІ. Для отримання інформації за допомогою цього способу зловмисники використовують чотири стратегії:

1. Залякування. Зловмисники, які обрали цю стратегію, часто змушують жертву виконати запит, видаючи себе за осіб, наділених владою.
2. Переконання. Найпопулярніші форми переконання - лестощі і посилання на відомих людей.
3. Виклик довіри. Цей підхід зазвичай вимагає досить тривалого часу і пов'язаний з формуванням довірчих відносин з колегою або начальником заради отримання у нього в кінцевому підсумку потрібної інформації.
4. Допомога. Зловмисник, який вибрав цей підхід, пропонує співробітникові компанії допомогу, для надання якої нібито потрібна особиста інформація співробітника. Отримавши цю інформацію, зловмисник краде ідентифікаційні дані жертви.

Захиститися від атак, заснованих на залякуванні, можна сприяючи формуванню корпоративної культури, яка виключає страх. Якщо співробітники компанії завжди поводяться чемно, залякування не дозволить зловмиснику

домогтися бажаного, тому що співробітник швидше за все повідомить про це начальству. Доброзичливе ставлення до співробітників з боку керівництва і нагляд за процедурою вирішення проблем і прийняття рішень - найгірше, з чим може зіткнутися зловмисник, який використовує методи СІ. Йому потрібно, щоб жертви атак приймали рішення швидко. Якщо в компанії прийнято доповідати про проблеми керівникам, зловмисник цього не доб'ється.

Переконання завжди було важливим способом досягнення особистих цілей. Повністю виключити ймовірність успішного проведення атак, заснованих на переконанні, не можна, але співробітникам можна дати чіткі вказівки з приводу того, що їм слід робити, а що не слід. Намагаючись отримати конфіденційну інформацію методом переконання, зловмисники завжди представляють той чи інший сценарій, який передбачає, що користувач повідомить її добровільно. Регулярне проведення інформаційних кампаній та визначення базових принципів використання паролів та інших засобів забезпечення безпеки - кращий захист від подібних атак.

Щоб увійти в довіру до співробітників компанії, зловмисникові потрібен час. Зловмисник повинен регулярно спілкуватися зі співробітниками, що значно легше, якщо він працює разом з ними. У більшості компаній середнього розміру основним джерелом таких загроз є працівники, які регулярно надають компанії будь-які послуги або працюють за контрактом. Тому відділ кадрів повинен приділяти підбору співробітників, що працюють за контрактом, не менше уваги, ніж найму постійних співробітників.

Нарешті, ймовірність успішного проведення атак, заснованих на зловживанні взаємодопомогою, можна звести до мінімуму, забезпечивши високу ефективність роботи служби підтримки. Найчастіше співробітники звертаються за допомогою до колег через незадоволеності послугами наявної служби підтримки. Щоб гарантувати, що в разі проблем співробітники будуть звертатися в службу підтримки, а не до колег або, гірше того, до зовнішніх фахівців, необхідно виконати дві умови:

1. Вказати в політиці безпеки, що при виникненні проблем користувачі

можуть робити запити тільки у фахівців служби підтримки і ні у кого більше.

2. Переконатися в тому, що для служби підтримки визначена процедура реагування на проблеми, в прийнятному для компанії рівня обслуговування. Регулярно проводити аудит ефективності роботи служби підтримки, перевіряючи, щоб користувачі отримували всю необхідну допомогу.

Служба підтримки - важливий механізм захисту від СІ атак, який не варто недооцінювати.

Фізичні методи

Ефективним для зловмисника способом підготовки до проведення атаки є встановлення безпосереднього особистого контакту з жертвою. Тільки недовірливі співробітники здатні поставити під сумнів щирість людини, що особисто просить допомоги у вирішенні комп'ютерних проблем або що пропонує таку допомогу. Хоча такі способи пов'язані для зловмисника з набагато більшим ризиком, вони забезпечують йому ряд переваг. У разі успіху він отримує вільний доступ до корпоративних систем зсередини компанії, обійшовши всі технічні засоби захисту периметра.

Іншою серйозною загрозою для компаній є поширення мобільних технологій, що дозволяють користувачам підключатися до корпоративних мереж в інших будівлях і в дорозі. Це робить можливими найрізноманітніші атаки: від зовсім простих, заснованих на спостереженні за тим, як користувач вводить в ноутбук ідентифікатор і пароль, до досить складних, при яких зловмисник, видаючи себе за співробітника служби підтримки, приносить і встановлює оновлення для пристрою читання карт або маршрутизатора, одночасно попросивши у користувача ідентифікатор і пароль для доступу до корпоративної мережі. Той, хто йде до кінця може навіть попросити і отримати від користувача електронний підпис, що використовується для перевірки його повноважень.

Хоча в більшості великих компаній є розвинена інфраструктура

обмеження доступу на корпоративні об'єкти, в компаніях малого і середнього розміру цим часто нехтують. Це забезпечує можливість проведення дуже простих CI атак, заснованих на несанкціонованому проникненні в офісну будівлю разом зі співробітником компанії, що має пропуск. Зловмисник притримує двері перед законним користувачем, заводить з ним розмову на якусь банальну тему і проходить разом з ним через пропускний пункт, не викликаючи підозри у контролерів. Для атак на великі компанії, співробітники яких можуть пройти в будівлю тільки через турнікети, зчитувальні дані з електронних карт, і малі організації, де всі один одного знають, цей підхід не годиться. Однак для атак на компанії, що налічують близько тисячі співробітників, далеко не завжди знайомих один з одним, він підходить якнайкраще. Якщо зловмисникові раніше вдалося отримати корпоративну інформацію, наприклад назви підрозділів, прізвища співробітників або дані з внутрішніх службових записок, йому буде простіше зав'язати розмову.

Забезпечення безпеки систем співробітників, що працюють вдома, зазвичай обмежується технічними засобами. Політика безпеки повинна вимагати, щоб домашні системи цих співробітників були захищені брандмауерами, блокуючими спроби зловмисників отримати доступ до мережі ззовні.

Таблиця 6 - Атаки, засновані на фізичному доступі, і можливий збиток від них

Мета атаки	Опис	Збиток
Крадіжка облікових даних мобільного користувача	Зловмисник підглядає, як легальний користувач вводить в систему облікові дані або інші відомості. Це може передувати крадіжці мобільного комп'ютера.	Витік конфіденційної інформації
Крадіжка облікових даних співробітника, що працює вдома	Зловмисник представляється службою технічної підтримки, щоб отримати доступ до мережі користувача, що працює вдома, і запитує у користувача ідентифікатор і пароль нібито для тестування оновленої конфігурації	Витік конфіденційної інформації

	системи.	
Вхід до корпоративної мережі через мережу співробітника, що працює вдома	Видаючи себе за представника служби підтримки, зловмисник отримує доступ до мережі співробітника, який працює вдома, і використовує її для підключення до корпоративної мережі. У разі успіху зловмисник отримує вільний доступ до мережі і ресурсів компанії.	Витік конфіденційної інформації Шкода репутації компанії Зниження роботоспроможності компанії Втрата ресурсів Фінансові втрати
Поточний доступ до мережі співробітника, який працює вдома	Зловмисник або локальний користувач отримує доступ в Інтернет, використовуючи для цього незахищену домашню мережу іншого користувача.	Втрата ресурсів
Доступ в офісну будівлю компанії без супроводу	Зловмисник проникає в офісну будівлю компанії слідом за авторизованим співробітником.	Витік конфіденційної інформації Шкода репутації компанії Зниження роботоспроможності компанії Втрата ресурсів Фінансові втрати
Доступ у офіс співробітника компанії	Зловмисник отримує доступ в офіс співробітника компанії, де намагається скористатися комп'ютерним обладнанням або знайти цікаві йому дані у паперових документах.	Витік конфіденційної інформації Втрата ресурсів Фінансові втрати

Можливість проникнення в будівлю або на об'єкт компанії без проходження авторизації повинна бути виключена. Взаємодіючи з

працівниками компанії, підрядчиками і відвідувачами, службовці приймальні повинні бути ввічливими, але непохитними. Включивши в корпоративну політику безпеки кілька простих принципів, ймовірність проведення СІ атак в будівлі можна звести практично до нуля. Ці принципи можуть визначати перераховані нижче вимоги:

1. Використання ідентифікаційних карт з фотографіями, що демонструються кожен раз при вході і виході з будівлі компанії
2. Ведення книги обліку відвідувачів, в якій відвідувач і співробітник, до якого він з'явився, повинні поставити свої підписи при прибутті відвідувача і його виходу
3. Застосування датованих пропусків відвідувачів, що прикріплюються на одяг у видному місці і повертаються службовцю приймальні при виході з будівлі
4. Ведення книги обліку підрядників, в якій підрядник і співробітник компанії, який затвердив його робоче завдання, повинні поставити свої підписи при прибутті підрядника і його виходу
5. Застосування датованих пропусків підрядників, що прикріплюються на одяг в видному місці і повертаються службовцю приймальні при виході з будівлі

Щоб гарантувати, що всі відвідувачі будуть представлятися службовцю приймальні, потрібно організувати бар'єри, що не дозволяють проникнути в будівлю компанії без його відома і без виконання реєстраційних процедур.

Протокол надання ІТ-послуг поза територією компанії повинен включати наступні правила:

1. Всі послуги технічної підтримки, в тому числі відновлення працездатності систем і оновлення їх конфігурації на місцях, повинні плануватися і затверджуватися службою підтримки
2. Підрядники і штатні співробітники, які встановлюють або обслуговуючі системи на місцях, повинні мати посвідчення, бажано з фотографією

3. Користувачі повинні повідомляти в службу підтримки час прибуття і від'їзду її представника
4. На кожне завдання має видаватися наряд на роботу, що підписується користувачем
5. Користувачі ніколи не повинні повідомляти спеціалістам зі служби підтримки своїх облікових даних або реєструватися в системі заради того, щоб вони могли отримати доступ до тих чи інших ресурсів.

Зворотня соціальна інженерія

Про зворотну СІ говорять тоді, коли жертва або жертви самі пропонують зловмисникові потрібну йому інформацію. Це може здатися малоймовірним, але насправді особи, що мають авторитет в технічній або соціальній сфері, часто отримують ідентифікатори і паролі користувачів і іншу важливу особисту інформацію просто тому, що ніхто не сумнівається в їх порядності. Наприклад, співробітники служби підтримки ніколи не запитують у користувачів ідентифікатор або пароль; їм не потрібна ця інформація для вирішення проблем. Проте багато користувачів заради якнайшвидшого усунення проблем добровільно повідомляють ці конфіденційні відомості. Зловмиснику навіть не треба питати про це. Проте, СІ атаки в більшості випадків ініціюються зловмисником.

Зазвичай зловмисник, який використовує методи СІ, створює проблемну ситуацію, пропонує рішення і надає допомогу, коли його про це просять. Розглянемо наступний простий сценарій.

Зловмисник, який працює разом з жертвою, змінює на її комп'ютері ім'я файлу або переносить його в інший каталог. Коли жертва зауважує пропажу файлу, зловмисник заявляє, що може все виправити. Бажаючи швидше завершити роботу або уникнути покарання за втрату інформації, жертва погоджується на цю пропозицію. Зловмисник заявляє, що вирішити проблему можна, тільки увійшовши в систему з обліковими даними жертви. Він навіть може сказати, що корпоративна політика забороняє це. Тепер вже жертва просить зловмисника увійти в систему під її ім'ям, щоб спробувати відновити

файл. Зловмисник неохоче погоджується і відновлює файл, а по ходу справи краде ідентифікатор і пароль жертви. Успішно здійснивши атаку, він навіть поліпшив свою репутацію, і цілком можливо, що після цього до нього будуть звертатися за допомогою і інші колеги.

Таблиця 7 - Атаки, засновані на методах зворотної СІ, і можливий збиток від них

Мета атаки	Опис	Збиток
Крадіжка облікових даних	Зловмисник отримує ідентифікатор та пароль авторизованого користувача.	Витік конфіденційної інформації Шкода репутації компанії Зниження роботоспроможності компанії Втрата ресурсів Фінансові втрати
Крадіжка інформації	Використовуючи ідентифікатор і пароль авторизованого користувача, зловмисник отримує доступ до файлів компанії.	Витік конфіденційної інформації Шкода репутації компанії Зниження роботоспроможності компанії Втрата ресурсів Фінансові втрати
Завантаження шкідливого ПЗ	Зловмисник обманним шляхом переконує користувача клацнути на гіперпосилання або відкрити вкладення, що приводить до зараження корпоративної мережі.	Шкода репутації компанії Зниження роботоспроможності

		компанії
Завантаження ПЗ зловмисника	Зловмисник обманним шляхом переконує користувача клацнути на гіперпосилання або відкрити вкладення, в результаті чого відбувається завантаження програми зловмисника, що споживає ресурси корпоративної мережі.	Шкода репутації компанії Втрата ресурсів Фінансові втрати

Захиститися від атак, заснованих на зворотній СІ, напевно, найскладніше. У жертви немає підстав підозрювати зловмисника в чому-небудь, так як при таких атаках створюється враження, що ситуація знаходиться під її контролем. Головним способом захисту від атак, заснованих на зворотній СІ, є включення в політику безпеки принципу, що вимагає, щоб всі проблеми вирішувалися тільки через службу підтримки. Якщо фахівці служби підтримки будуть компетентні, ввічливі і терпимі, у співробітників компанії не буде приводу звертатися за допомогою до будь-кого іншого.

Рекомендації щодо протидії методам соціальної інженерії

Розмежування доступу

З метою забезпечення захисту інформації, встановлюється наступний порядок допуску до роботи з конфіденційними джерелами:

1. Рішення про доступ працівника до потрібного моменту конфіденційної інформації приймається керівництвом.
2. Відповідальні особи, з числа штатних програмістів, забезпечують захист окремих файлів і програм від читання, видалення, копіювання особами, які не допущені до цього.
3. Доступ до комп'ютерної мережі здійснюється тільки з персональним паролем. Користувач повинен тримати в таємниці свій пароль. Повідомляти свій пароль іншим особам, а також користуватися чужими паролями забороняється. Ім'я користувача і пароль на вхід в БД повинні бути відмінні від імені користувача та пароля в загальну комп'ютерну мережу.

4. Категорично забороняється знімати несанкціоновані копії з носіїв банківської інформації, знайомити зі змістом електронної інформації осіб, не допущених до цього.

Криптографічні системи

До роботи з криптографічними системами (якщо такі є на підприємстві) допускаються тільки співробітники, які мають відповідний дозвіл від керівництва.

Секретні ключі електронно-цифрових підписів і шифрування повинні зберігатися в сейфах під відповідальністю уповноважених осіб. Доступ неуповноважених осіб до носіїв секретних ключів і шифрування повинен бути виключений.

Категорично забороняється:

- виводити секретні ключі і шифрування на дисплей комп'ютера або принтер;
- встановлювати в дисковод комп'ютера носій секретних ключів і шифрування в непередбачених режимах функціонування;
- записувати на носій секретних ключів і шифрування сторонню інформацію.

При компрометації секретних ключів, шифрування та іншої електронної інформації відповідальними особами вживаються заходи для припинення будь-яких операцій з використанням цих ключів та іншої інформації; вживаються заходи для зміни ключів і шифрування, паролів. За фактом компрометації організовується службове розслідування, результати якого відображаються в акті і доводяться до відома керівництва.

Фізична безпека

Всі критичні об'єкти з точки зору інформаційної безпеки (всі сервери баз даних, телефонна станція, основний маршрутизатор, брандмауер) знаходяться в окремому приміщенні, доступ до якого дозволений тільки співробітникам, які мають відповідний дозвіл від керівництва.

Вхід в приміщення здійснюється через металеві двері, що обладнані

замками (не менше двох).

Приміщення обладнане примусовою вентиляцією та пожежною сигналізацією. Вхід в приміщення контролюється системою відео спостереження з виходом на монітори охорони.

Ключові дискети, паролі та інша конфіденційна інформація зберігається в сейфах.

Доступ до приміщення стороннім особам заборонений. Технічний персонал, який здійснює прибирання приміщення, ремонт обладнання, обслуговування кондиціонера і т.п. може знаходиться в приміщенні тільки в присутності працівників, які мають право знаходитися в приміщенні у зв'язку з виконанням своїх посадових обов'язків.

Доступ до приміщення в позаурочний час або у вихідні та святкові дні здійснюється з письмового дозволу керівника підприємства або його заступників.

Розмежування прав доступу до програмного забезпечення і систем зберігання даних

Для входу в комп'ютерну мережу співробітник повинен ввести ім'я та пароль. Не допускається режими безпарольного (гостьового) доступу до будь-якої інформації.

З метою захисту конфіденційної інформації організаційно і технічно поділяються підрозділи підприємства, що мають доступ і працюють з різною інформацією (в розрізі її конфіденційності, секретності і смислової спрямованості). Дане завдання вирішується з використанням мережевої операційної системи, де в цілях забезпечення захисту даних доступ і права користувачів обмежуються персональними каталогами. Права призначаються відповідно з виробничою необхідністю, обумовленою начальником підрозділу.

Параметри входу в мережу, ім'я та пароль, користувачем не розголошуються. Копії на паперовому носії тримаються в недоступному для сторонніх місці. У разі компрометації пароля користувач повинен негайно звернутися до програмістів з заявкою про заміну.

При роботі з БД ім'я користувача і пароль повинні бути відмінні від імені користувача та пароля при вході у загальну комп'ютерну мережу. Пароль повинен бути не менше п'яти символів. Категорично забороняється повідомляти свій пароль іншим особам, а також користуватися чужими паролями. Всі дії користувача, що працює з БД протоколюються. Журнал операцій зберігатися не менше шести місяців.

Робота в глобальній мережі Інтернет

До роботи з ресурсами мережі Інтернет і електронної пошти допускаються співробітники, які отримали відповідний дозвіл від керівництва (достатньо усної форми).

Під час роботи з мережею Інтернет співробітникам заборонено:

1. Завантажувати та встановлювати на комп'ютер програмне забезпечення;
2. Відвідувати ресурси, які не мають безпосереднього відношення до роботи і службових обов'язків;
3. Передплачувати розсилку інформації невиробничого характеру;
4. Повідомляти адресу електронної пошти в невиробничих цілях;
5. Використовувати Інтернет для отримання матеріальної вигоди або у невиробничих цілях, в тому числі здійснюючи торгівлю через Інтернет;
6. Дублювання, резервування і роздільне зберігання конфіденційної інформації.

З метою захисту конфіденційної інформації від навмисного або ж ненавмисного її знищення, фальсифікації або розголошення забезпечити:

- щоденне обов'язкове резервування всієї інформації, що має конфіденційний характер;
- дублювання інформації з використанням різних фізичних і апаратних носіїв.

Відповідальність за зберігання і резервування інформації в електронному вигляді покласти на штатних програмістів.

УДК 007:658

Легенченко К. О., студентка групи 125м-16-1

Науковий керівник: Тимофєєв Д. С., ст. в. кафедри безпеки інформації та телекомунікацій

(ДВНЗ «Національний гірничий університет», м. Дніпро, Україна)

УПРАВЛІННЯ ОБІЗНАНІСТЮ ПЕРСОНАЛУ В ПИТАННЯХ ПРОТИДІЇ МЕТОДАМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Важливим фактором захисту інформації на підприємствах є акцент на протидії методам соціальної інженерії. Будь-яка інформація, незалежно від її формату та стану - обробляється вона процесором, передається по каналах зв'язку, зберігається на диску - повинна входити в межі контролю системи забезпечення ІБ. Але технічні засоби, крім основного функціоналу, мають інтерфейси взаємодії з людиною, тому важливим елементом захисту інформації є сам співробітник компанії. Якщо по відношенню до технічних засобів завжди можна описати можливі ситуації, визначити і оцінити ризики, знайти способи захиститися (обмежити доступ, зашифрувати і т.п.), то в разі дій людини виникає проблема.

Виходячи з цього внутрішні загрози можуть утворюватися внаслідок:

- непрофесійних дій працівників;
- низького стану виховної та профілактичної роботи в організації;
- недосконалої системи заробітної плати та стимулювання праці персоналу;
- порушень правил кадрової роботи, невідповідності кадрової політики умовам роботи в організації;
- психологічних та комунікаційних особливостей працівників;
- відсутності нормативної бази організації, яка б установлювала режими їх діяльності та правила поведінки персоналу. [1]

До сих пір не існує чіткої, всеосяжної математичної моделі, яка описує поведінку людей в різних ситуаціях, реакцію на той чи інший вплив або

сформовані умови, можливі помилки. Природно, що цей фактор відіграє на руку зловмисникам.

В атаках, що використовують методи соціальної інженерії, можна виділити 3 основних етапи: збір, профілювання і реалізація.

1. Збір даних про мету атаки є найбільш важливою стадією. Роботи полягають у визначенні характеристик об'єктів атаки, в тому числі шляхом зовнішнього впливу. Джерелом даних можуть бути соціальні мережі, публічно доступна інформація і ін. Також ефективними є спілкування з членами сім'ї, друзями і колегами, спостереження за діяльністю мети і навіть взаємодія з нею.
2. На етапі профілювання виконується аналіз зібраної інформації для побудови моделі атаки. Виділяються характеристики, що властиві цілі, а також її слабкості, на підставі чого вибираються канали взаємодії (пошта, телефонні дзвінки, особисте спілкування і т.п.), методи реалізації (вербування, неформальне спілкування, тиск і т.п.) і можливі вектори атаки, які можуть бути ефективними проти конкретної мети.
3. На етапі виконання атаки реалізується її модель, вироблена на стадії профілювання. Тут вступають в повну силу психологія, НЛП і технічні засоби. У разі вдалої реалізації першої хвилі атаки можна повернутися до етапу збору інформації з новими вхідними даними і ітеративно повторювати виконання етапів до тих пір, поки продовжує виявлятися нова інформація, або поки атака не досягне бажаної глибини. [2]

Активне використання Інтернету, крім плюсів, має ряд значних мінусів. Це і додаткові канали комунікації з жертвою, і залишені жертвою «сліди», вивчивши які, можна скласти портрет потенційної мети атаки. Інтернет дає зловмисникам можливість автоматизувати свою роботу, що значно скорочує «трудовитрати» на виконання атаки.

У той же час багато компаній і бояться, і не розуміють, навіщо їм потрібна оцінка свого персоналу, заснована на застосуванні методів соціальної інженерії. Бояться зазвичай внаслідок того, що такий процес не

регламентований законодавством або міжнародними стандартами. Він більшою мірою експертний, часто його результативність залежить від навичок конкретного виконавця. [3]

Крім застосування технічних заходів захисту інформації (розмежування доступу, мінімізації повноважень, моніторингу подій і трафіку і т.п.), які протидіють відомим шаблонами атак, основним заходом захисту від використання прийомів соціальної інженерії є метод «Безпека через навчання». Навчання має бути регулярним, простим і зрозумілим. Часто в організаціях до процесу навчання вимогам і практикам ІБ підходять формально. Тому виникає ситуація, коли працівники компаній мають низький рівень поінформованості та грамотності з питань інформаційної безпеки. Це тягне за собою їх халатне, неуважне ставлення до вхідних інформаційних потоків. Крім навчання, також варто підвищувати пильність співробітників шляхом їх періодичного тестування. [4]

На завершення необхідно відзначити, що гуманітарну проблему не можна вирішити виключно технічними методами. Тільки комплексний підхід може захистити від атак із застосуванням методів соціальної інженерії. Шляхом збору, обробки, порівняння та аналізу досліджень в сфері протидії атакам з використанням методів соціальної інженерії, необхідно описати і організувати систему заходів і методів підвищення кваліфікації персоналу в сфері протидії атакам з використанням методів соціальної інженерії.

Напрямок досліджень:

- вивчити раніше проведені дослідження в області протидії атакам з використанням методів соціальної інженерії;
- розробити теоретичну базу, де слід викласти основні поняття в сфері протидії атакам з використанням методів соціальної інженерії;
- класифікувати типи і види атак з використанням методів соціальної інженерії (з прикладами);
- проаналізувати існуючі методи протидії атакам даного типу;

- запропонувати унікальні методи протидії атакам з використанням соціальної інженерії;
- проаналізувати ефективність запропонованих методів протидії;
- розробити ряд методик для підвищення кваліфікації персоналу протидії методам соціальної інженерії;
- розробити спеціальне програмне забезпечення, що дозволяє дохідливо і ефективно піднести дані методики для персоналу підприємств.

Перелік посилань

1. Будник М. М. ,Тимофєєв Д. С. Внутрішні загрози інформаційної безпеки та заходи по їх мінімізації (Електрон. ресурс) / Спосіб доступу: URL: http://ir.nmu.org.ua/bitstream/handle/123456789/1666/7.pdf?sequence=1
2. Резник Ю.М. Соціальна інженерія: предметна область і межі застосування // Соціологічні дослідження, 1994, № 2.
3. Соціальна інженерія // Сучасна західна соціологія: Словник. М., 2015.
4. Романенко Е. А., Тимофеев Д. С. Методы обучения персонала по вопросам информационной безопасности (Електрон. ресурс) / Спосіб доступу: URL: http://ir.nmu.org.ua/bitstream/handle/123456789/1667/14.pdf