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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Гончарова Данила Олеговича*

академічної групи *125м-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Організація протидії кібершахрайству, що використовує фішингові веб-ресурси*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.ф.-м.н., проф. Кагадій Т.С.			
розділів:				
спеціальний	ст. викл. Тимофєєв Д.С.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2018

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту *Гончаров Д.О.* **академічної групи** ***1**25м-17-2*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Організація протидії кібершахрайству, що використовує фішингові веб-ресурси*

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

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

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *Кібератаки з використанням фішингу*

Предмет досліджень *Механізми протидії кібершахрайству*

Мета *Вдосконалення сучасних методів протидії кібершахрайству, надання і впровадження рекомендацій*

Вихідні дані для проведення роботи *Вітчизняна та міжнародна правова база у сфері інформаційної та кібербезпеки, наукові публікації вітчизняних та іноземних авторів, статистичні дані , результати науково-дослідницької та переддипломної практики*

3 ОЧІКУВАНІ РЕЗУЛЬТАТИ

Наукова новизна *полягає у покращенні ефективності застосування актуальних методів протидії кібершахрайству*

Практична цінність *полягає у розробці та впровадженні рекомендацій для користувачів щодо протидії кібершахрайству, що використовує фішингові веб-ресурси*

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Результати роботи мають відповідати вимогам чинного законодавства України та мають підвищити рівень обізнаності користувачів у питанні протидії кібершахрайству

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт** (початок-кінець)
Аналіз статистичної інформації України та світу щодо випадків кібершахрайства	25.09.18-19.10.18
Дослідження існуючих методів фішингових атак та методів протидії	20.10.18-17.11.18
Розробка рекомендацій для покращення ефективності роботи методів протидії кібершахрайству та впровадження рекомендацій для користувачів	18.11.18-28.11.18
Визначення капітальних та експлуатаційних витрат на впровадження запропонованих рекомендацій	29.11.18-07.12.18
Оформлення пояснювальної записки	08.12.18-10.12.18

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *від реалізації результатів роботи очікується позитивним завдяки зниженню можливих збитків через фішингові атаки завдяки створенню та впровадженню рекомендацій для користувачів щодо протидії кібершахрайству, що запропоновані у дипломній роботі*

Соціальний ефект *дипломної роботи полягає у підвищенні обізнаності керівництва та працівників підприємства у питаннях протидії кібершахрайству та ефективності забезпечення безпеки інформації*

7 ДОДАТКОВІ ВИМОГИ

Відповідність оформлення пояснювальної записки:

ДСТУ 3008-95. «Документація. Звіти у сфері науки і техніки. Структура і правила оформлення»;

Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека, 172 Телекомунікації та радіотехніка / О.Ю. Гусєв, О.В. Герасіна, О.М. Алексєєв, О.В. Кручінін – Дніпро:НГУ, 2018. – 52с;

Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: І.В. Шереметьєва, Д.П. Пілова, Н.М. Романюк. – Дніпро: Національний технічний університет "Дніпровська політехніка", 2017. – 17 с.

Завдання видано _____ Тимофєєв Д.С.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 03.09.18р.

Дата подання до екзаменаційної комісії: 14.12.18р.

Прийнято до виконання _____ Гончаров Д.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 59 с., 5 рис., 2 табл., 4 додатки, 32 джерел.

Об’єкт дослідження: кібератаки з використанням фішингу.

Мета дипломної роботи: вдосконалення сучасних методів протидії кібершахрайству, надання і впровадження рекомендацій.

В першому розділі розглянуті основні проблеми, які пов’язані з кібершахрайством та фішинговими атаками. Розглянуто статистичні дані щодо фішингових атак та завданої ними шкоди Україні та країнам світу. Була проаналізована нормативно-правова база щодо безпеки персональних даних користувачів.

У другому розділі були розглянуті основні типи фішингових атак, розглянуті методи протидії ним, їх сильні та слабкі сторони. Розроблені рекомендації щодо посилення ефективності роботи механізмів протидії кібершахрайству та рекомендації для користувачів щодо мінімізування ризиків потрапляння під вплив фішингової атаки та її наслідків.

Новизна очікуваних результатів полягає у впровадженні адаптованих рекомендацій для користувачів щодо питання кібершахрайства, що використовує фішингові веб-ресурси.

ІНФОРМАЦІЙНА БЕЗПЕКА, ПЕРСОНАЛЬНІ ДАНІ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, ФІШИНГ, КІБЕРШАХРАЙСТВО, РЕКОМЕНДАЦІЇ ДЛЯ КОРИСТУВАЧІВ

РЕФЕРАТ

Пояснительная записка: 59 с., 5 рис., 2 табл., 4 приложения, 32 источников.

Объект исследования: кибератаки с использованием фишинга.

Цель дипломной работы: совершенствование современных методов противодействия кибермошенничестве, предоставление и внедрение рекомендаций.

В первом разделе рассмотрены основные проблемы, связанные с кибермошенничеством и фишинговыми атаками. Рассмотрены статистические данные по фишинговым атакам и причиненного ими ущерба Украине и странам мира. Была приведена нормативно-правовая база по безопасности персональных данных пользователей.

Во втором разделе были рассмотрены основные типы фишинговых атак, рассмотрены методы противодействия им, их сильные и слабые стороны. Разработаны рекомендации по усилению эффективности работы механизмов противодействия кибермошенничеству и рекомендации для пользователей по минимизации рисков попадания под влияние фишинговой атаки.

Новизна ожидаемых результатов заключается во внедрении новых рекомендаций для пользователей по вопросу кибермошенничества, что использует фишинговые веб-ресурсы.

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ, ЛИЧНЫЕ ДАННЫЕ, НЕСАНКЦИОНИРОВАННІЙ ДОСТУПА, ФИШИНГ, КИБЕРМОШЕННИЧЕСТВО, РЕКОМЕНДАЦИИ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ

ABSTRACT

Explanatory slip: 59 p., 5 images, 2 tab., 4 appendices, 32 sources.

Object of the research: cyber attacks using phishing.

Subject of the development: the improvement of modern methods of countering cyber fraud, the provision and implementation of recommendations.

The first section covers the main problems associated with cyber fraud and phishing attacks. Statistic data on phishing attacks and damage caused by them to Ukraine and countries of the world are considered. The regulatory framework for the security of personal user data was provided.

In the second section, the main types of phishing attacks were considered, methods to counter them, their strengths and weaknesses were considered. Recommendations on enhancing the effectiveness of cyber fraud prevention mechanisms and recommendations for users on minimizing the risks of falling under the influence of a phishing attack were developed.

The novelty of the expected results lies in the introduction of new recommendations for users on the issue of cyber fraud, which uses phishing web resources.

SECURITY INFORMATION, PERSONAL DATA, UNAUTHORIZED ACCESS, FISHING, CYBER FRAUD, RECOMMENDATIONS FOR USERS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІБ	–	інформаційна безпека
ПЗ	–	програмне забезпечення
СЦ	–	сертифікаційний центр
2FA	–	двухфакторна аутентифікація
SSL	–	Secure Sockets Layer
API	–	Application Programming Interface
APWG	–	Anti Phishing Work Group
CPNI	–	Centre for the Protection of National Infrastructure
DMARC	–	Domain-based Message Authentication, Reporting and Conformance
DNS	–	Domain Name System
DKIM	–	DomainKeys Identified Mail
NCSC	–	National Cyber Security Centre
SPF	–	Sender Policy Framework
URL	–	Uniform Resource Locator

ЗМІСТ

ВСТУП

З розвитком інтернет-технологій і розширенням інтернет-простору збільшується ймовірність зіткнення з шахрайством. Останнього часу популярність набув фішинг — різновид шахрайської діяльності, метою якої є отримання несанкціонованого доступу до конфіденційної інформації (логінів, паролів, банкових рахунків, тощо).

Найпопулярнішим методом шахрайства є фішингові електронні повідомлення. Фішингові повідомлення спонукають до негайних дій, не залишаючи часу на роздуми. Шахрайські повідомлення найчастіше надходять від імені відомих компаній та брендів і впливають на емоційне сприйняття інформації. Найчастіше в них йдеться про дуже вигідні фінансові угоди, стан банкового рахунку, розіграші грошей та цінних призів, фінансову допомогу хворим дітям і т.д.

Для отримання інформації про клієнтів банків та електронних платіжних систем або для поширення вірусів у мережі шахраї використовують не лише розсилку листів на електронні адреси, але й онлайн-оголошення, результати запитів у пошукових системах, імітацію спливаючих вікон з системними повідомленнями, розповсюдження інформації у соціальних мережах. Є багато прикладів поширення вірусних програм у таких соціальних мережах як VK, Facebook та Instagram, які успішно збирали відомості про користувачів. За оцінками фахівців, 70% фішингових атак в соціальних мережах мають успіх. Це обумовлено тим, що більшість користувачів інтернету не надають належної уваги кібербезпеці та не знають як відрізнити фішингову атаку від заходу на авторитетному ресурсі.

РОЗДІЛ 1.
СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз статистики кіберінцидентів повязаних з фішинговими атаками.

За даними української міжбанківської асоціації членів платіжних систем ЕМА, в 2017 році було зафіксовано 174 фішингові сайти. За перше півріччя 2018 року - вже 79 шахрайських веб-ресурсів.

Якщо тенденція збережеться, то до кінця року злочинці створять, як мінімум, 160 шахрайських ресурсів. Але є підстави припускати, що і цей показник буде перевищений. Адже помічено, що в період свят шахраї активізуються - тільки в листопаді-грудні 2017 року було розкрито діяльність 42 фішингових веб-сервісів.

Тільки за один день «роботи» фішингових сайтів в святкові дні конфіденційні реквізити своїх карт на ньому залишили 2 600 користувачів. Всі вони могли втратити свої гроші, але фішинговий сайт був вчасно виявлений і банки встигли заблокувати рахунки клієнтів, які ледь не стали жертвами шахраїв.

За місяць існування фішингових ресурсу, його відвідують до 35 тисяч користувачів, кожен з яких може бути пограбований шахраями.

З 79 виявлених (на 1 липня 2018 року) фішингових сайтів 41 - це підроблені сервіси грошових переказів з картки на картку. Крім того, 48 з 79 фішингових ресурсів пропонували неіснуючі послуги поповнення мобільного телефону.

Два шахрайських веб-сервісу «займалися» кредитуванням (виманювали дані карти під приводом видачі кредиту онлайн). Ще чотири сайту пропонували працевлаштуватися - працювати на державне підприємство «Укрпошта» у віддаленому доступі.

Один з виявлених в 2017 році фішингових веб-ресурсів пропонував користувачам брати участь у відмиванні грошей (працювати дропом), але насправді, виманював дані карт тих людей, які вирішили «легко заробити».

Два шахрайських сайти «продавали» неіснуючі дешеві авіаквитки - покупець навіть міг отримати квиток на руки та проїзний документ був недійсним, зате шахрай отримував доступ до карти клієнта.

Фахівці відзначають, що в 2017 році зросла кількість фішингових сайтів, що імітують сервіси грошових переказів, які крадуть гроші з карти в режимі реального часу.

Такі сайти пропонують зробити переклад, а після того, як клієнт ввів дані своєї карти і номер картки одержувача, спеціальна програма переадресовує операцію на легітимний ресурс грошових переказів, однак підміняючи номер картки одержувача грошей, а іноді — і суму переказу.

Також, фішинг один з найефективніших засобів вилучення персональних даних користувачів мережі Інтернет та веб-ресурсів. Співробітники компанії Google провели дослідження, де вивчили дані про продаж інтернет-акаунтів на чорному ринку. Вони з'ясували, що найпоширеніша причина витоку персональних даних — це фішинг.

Результати даного дослідження були представлені на конференції в Далласі «Conference on Computer and Communication Security». З'ясувалося, що 15% всіх користувачів мінімум раз стикалися з шахраями в мережі, і втрачали дані своїх акаунтів і навіть інформацію про платіжні картки.

І хоча кожен намагається убезпечити як себе, так і своїх користувачів від шахраїв і хакерів, не завжди це виходить. Знаходяться нові способи, але як виявилося, найпродуктивніші старі і прості. Більше 800 тисяч паролів були втрачені людьми через програми-кейлогери (програмне забезпечення або апаратний пристрій, що реєструє різні дії користувача - натискання клавіш на клавіатурі комп'ютера, руху і натиснення клавіш миші і т. д.). За допомогою фішингу зловмисники вкрали не менше 12 мільйонів акаунтів.

У деяких країнах ЄС онлайн-шахрайство та фішинг вийшли на принципово новий рівень розповсюдження. Згідно зі звітом британського Національного бюро по боротьбі з шахрайством (NAO), онлайн-шахрайство — найчастіше злочин в Англії і Уельсі. У 2016 році окремі особи втратили близько 10 млрд фунтів стерлінгів через шахрайство, тоді як збитки приватного бізнесу досягли 144 млрд.

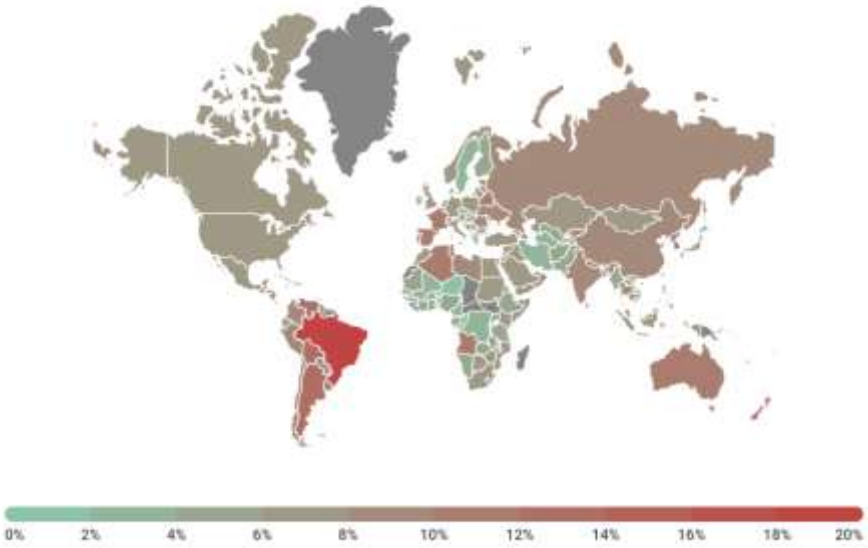
У Великобританії на кібершахрайство довелося на 16% всіх злочинів в минулому році. Втрати через інтернет-злочинців ростуть, а в агентстві вважають, що

уряд приймає недостатні заходи для вирішення цієї проблеми. За статистикою, онлайн-шахраї крадуть невеликі суми, але в більших масштабах. У 40% випадків потерпілі повідомляли про втрати в розмірі 250 фунтів стерлінгів і вище.

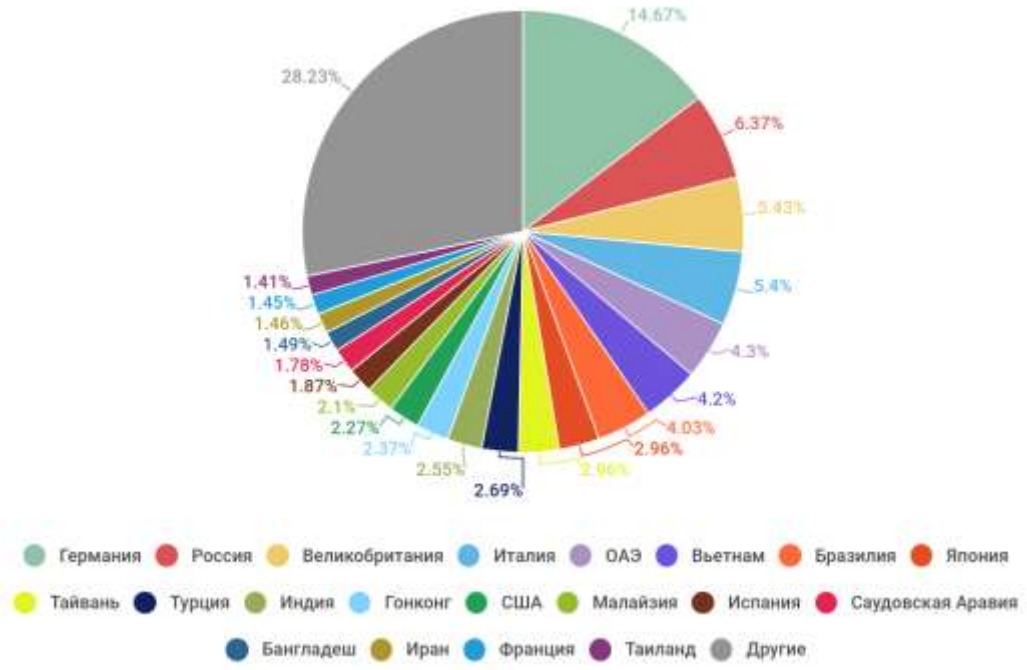
Тим часом, інтернет-шахрайство «без карт» в період з 2011 по 2014 почастішало на 103%. У доповіді також говориться, що споживачі погано інформовані про ризики і можуть легко стати жертвами кіберзлочинців.

Не задовго до цього повідомлялося про те, що в Європі підрахували збитки від онлайн-шахрайства з банківськими картами. Сукупні збитки від шахрайства з картами в минулому році в 19 європейських країнах склали приблизно 1,8 млрд євро.

Приведемо статистику щодо фішингових атак у світі за перше півріччя 2018 року.



Риснок 1.1 — Країни з найбільшою часткою атакованих фішерами користувачів в першому кварталі 2018 року



Риснок 1.2 — Країни як об'єкти для шкідливих розсилок електронної пошти у першому кварталі 2018 року

Не слід обходити стороною таку актуальну проблему, як вішинг (англ. Vishing — voice + phishing). Вішинг - це одна з різновидів фішингу, при якому також використовуються методи соціальної інженерії, але вже за допомогою телефонного дзвінка.

Також при вішингу може бути запропонована вигідна покупка з величезною знижкою або озвучена інформація про виграш у будь-якої акції. Не можна відразу ж вірити словам зловмисників, завжди варто зайвий раз перевірити ще раз інформацію, звернувшись до офіційних ресурсів.

Нижче наведені діаграми зі статистикою щодо жертв шахрайства, сум шахрайських операцій та дохід шахраїв (рисунок 1.1, рисунок 1.2, рисунок 1.3).

Можна зробити висновок, що питання онлайн-шахрайства в Україні та світі дуже актуальне. З інформації наведеної вище, користувачі мережі Інтернет та банківських карток постійно стикаються зі спробами незаконного заволодіння особистими даними та даними фінансовою інформацією досить часто, тож тема дослідження моєї дипломної роботи досить актуальна та важлива. Жертвами шахрайства можуть стати як великі компанії так і звичайні користувачі платіжних

систем, соціальних мереж, сервісів електронної пошти, тощо. Наша мета розглянути існуючі методи протидії кібершахрайству, посилити деякі з них та розробити ефективні рекомендації для користувачів для розпізнавання фішингових веб-ресурсів, електронних листів і т.д.

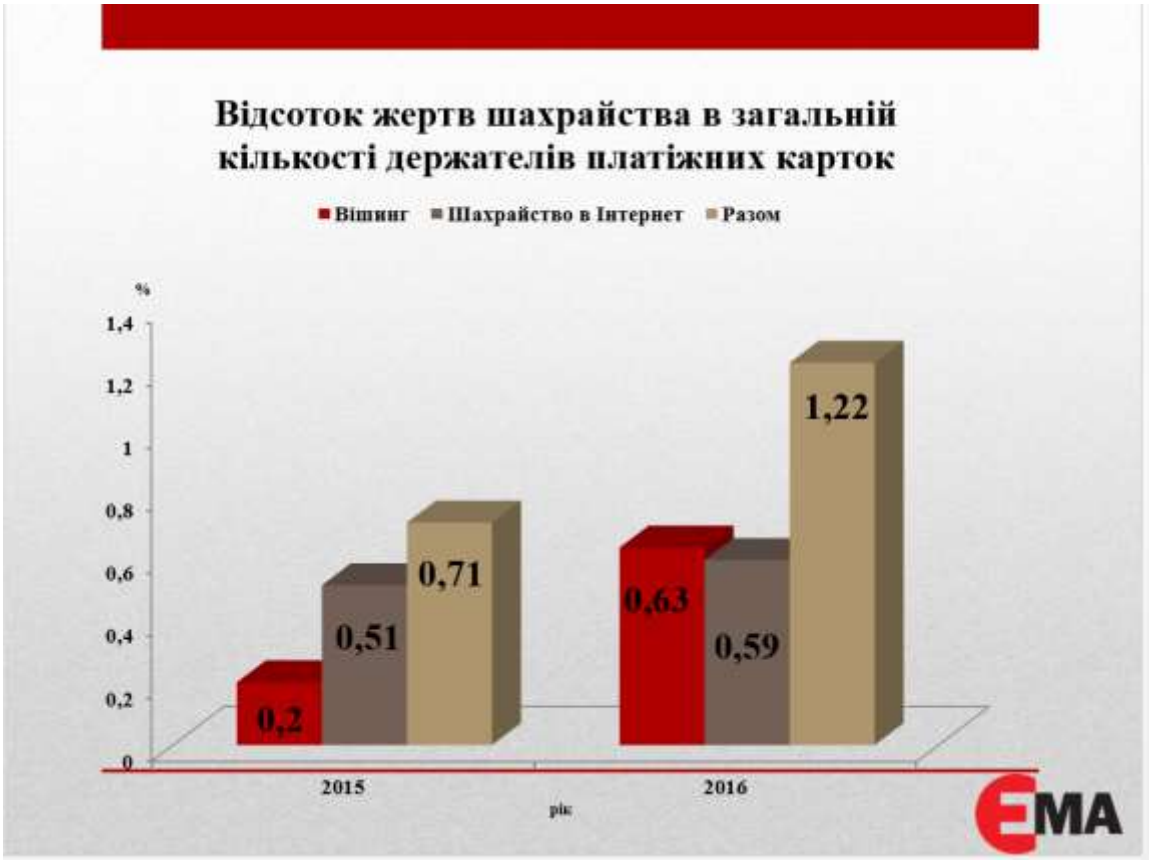


Рисунок 1.1 – Відсоток жертв шахрайства в загальній кількості держателів платіжних карток

Рисунок 1.2 – Середня сума шахрайської операції

Рисунок 1.3 – Сукупний розрахунковий дохід шахраїв

1.2 Аналіз нормативно-правової бази у сфері захисту інформації

Основними складовими інформаційної законодавчої бази України є Конституція України, інформаційні положення міжнародного права і ратифіковані в Україні законодавчі акти про окремі види і розділи інформації.

Основою інформаційної законодавчої бази є закон України «Про інформацію» [1], який регулює інформаційні відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони і захисту інформації а також визначає права громадянина на інформацію яка потрібна для реалізації його прав, свобод і законних інтересів. Також, дуже важливими складниками інформаційної нормативно-правової бази України є закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [2] який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, закон України «Про електронні документи та електронний документообіг» [3] який встановлює основні організаційно-правові засади електронного документообігу та використання електронних документів та закон України про «Про захист персональних даних» [4] який регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних, закон України «Про основні засади забезпечення кібербезпеки України» що визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі. Ці закони формують статуси їх суб’єктів та об’єктів, дозволяють опиратися на них у регулюванні будь-яких інформаційних відносин та дозволяють визначити права кожного учасника інформаційних відносин.

Усі наведені вище закони та документи нормативно-правової бази необхідні для обґрунтування прав громадянина у мережі Інтернет та захист його персональних даних в ній.

Вимоги до захисту інформації регламентує державний стандарт України ДСТУ 3396.0-96. Цей стандарт установлює вимоги до порядку проведення робіт з ТЗІ.

Вимоги стандарту обов`язкові для підприємств та установ усіх форм власності й підпорядкування, громадян, суб`єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

В цьому стандарті йдеться що до заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціювання засобів (систем) забезпечення ІД та засобів (систем) забезпечення ТЗІ.

У процесі розроблення і реалізації організаційних заходів потрібно:

- визначити окремі задачі захисту ІзОД;

- обґрунтувати структуру і технологію функціювання системи захисту інформації;

- розробити і впровадити правила реалізації заходів ТЗІ;

- визначити і встановити права та обов`язки підрозділів та осіб, що беруть участь в обробленні ІзОД;

- придбати засоби забезпечення ТЗІ та нормативні документи і забезпечити ними підприємство;

- установити порядок упровадження захищених засобів оброблення інформації, програмних і технічних засобів захисту інформації, а також засобів контролю ТЗІ;

- установити порядок контролю функціювання системи захисту інформації та її якісних характеристик;

- визначити зони безпеки інформації;

- установити порядок проведення атестації системи захисту інформації і, її елементів і розробити програми атестаційного випробування;

- забезпечити керування системою захисту інформації.

Оперативне вирішення задач ТЗІ досягається організацією керування системою захисту інформації, для чого необхідно:

- вивчати й аналізувати технологію проходження ІзОД у процесі ІД;
- оцінювати схильність ІзОД до впливу загроз у конкретний момент часу;
- оцінювати очікувану ефективність застосування засобів забезпечення ТЗІ;
- визначати (за необхідності) додаткову потребу в засобах забезпечення ТЗІ;
- здійснювати збирання, оброблення та реєстрацію даних, які відносяться до ТЗІ;
- розробляти і реалізовувати пропозиції щодо коригування плану ТЗІ в цілому або окремих його елементів.

Вимоги до захисту в системі інформації, що становить державну таємницю, визначаються [20]. Згідно з [18] державна таємниця (секретна інформація) - вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою.

Забезпечення охорони державної таємниці відповідно до вимог режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, діяльність яких пов'язана з державною таємницею, покладається на керівників зазначених органів, підприємств, установ і організацій.

Необхідно надавати відповідний гриф секретності рішенням про віднесення інформації до державної таємниці та про скасування цих рішень залежно від важливості їх змісту. Інформація вважається державною таємницею з часу опублікування Зводу відомостей, що становлять державну таємницю, до якого включена ця інформація, чи зміни до нього у порядку, встановленому цим Законом.

До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої

завдає шкоди особі, суспільству і державі. Віднесення інформації до категорії таємних відомостей, які становлять державну таємницю, і доступ до неї громадян здійснюється відповідно до [1].

Правила, що розглянені у [19] визначають загальні вимоги та організаційні засади забезпечення захисту таємної інформації або інформації, вимога щодо захисту якої встановлена законом:

- відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій;
- усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією;
- модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі;
- під час обробки службової і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення;
- доступ до службової інформації надається тільки ідентифікованим та автентифікованим користувачам;
- у системі здійснюється обов'язкова реєстрація результатів ідентифікації та автентифікації, результатів виконання користувачем операцій з обробки інформації, спроб НСД, фактів надання та позбавлення користувачів права доступу до інформації, результатів перевірки цілісності ЗЗІ. Ідентифікація та автентифікація користувачів, надання та позбавлення їх права доступу до інформації та її обробки, контроль за цілісністю засобів захисту в системі здійснюється автоматизованим способом;
- передача службової і таємної інформації з однієї системи до іншої здійснюється у зашифрованому вигляді або захищеними к-аналами зв'язку згідно з вимогами законодавства з питань технічного та криптографічного ЗІ;
- у системі здійснюється контроль за цілісністю ПЗ, яке використовується для обробки інформації, програмних та технічних ЗЗІ;
- для забезпечення захисту інформації в системі створюється КСЗІ;

- організація та проведення робіт із захисту інформації в системі здійснюється службою захисту інформації;

- якщо для створення СЗІ необхідно провести роботи з криптографічного

- захисту інформації, виконавець повинен мати ліцензії на провадження виду робіт у сфері криптографічного захисту інформації або залучати співвиконавців, що мають відповідні ліцензії;

- захист інформації від несанкціонованих дій, у тому числі від комп'ютерних вірусів, забезпечується в усіх системах.

Конфіденційна інформація — це відомості, що перебувають у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

- Згідно з [26] об’єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься інформація з обмеженим доступом, що не становить державної таємниці, підлягають обов’язковому категоріюванню.

- ЗІ від НСД в Україну на сьогоднішній день регламентують нормативні документи [3-12].

- На вимоги до захисту інформації від НСД впливає клас АС, який має на увазі обробку інформації різних категорій, а також важливість об'єкта та цінність інформації.

- Однією з вимог забезпечення ЗІ в АС згідно [8] є те, що обробка в АС конфіденційної інформації повинна здійснюється з використанням захищеної технології.

- У наведеному НД ТЗІ також наведені вимоги до забезпечення конфіденційності, цілісності, доступності та спостережності оброблюваної інформації. Дані вимоги розглядаються для захисту конфіденційнох та службової інформації зокрема.

Загальні вимоги передбачають:

- наявність переліку конфіденційної інформації, яка підлягає автоматизованій обробці;

- наявність визначеного (створеного) відповідального підрозділу, якому надаються повноваження щодо організації і впровадження технології захисту інформації, контролю за станом захищеності інформації;

- створення КСЗІ;

- розробку плану захисту інформації в АС;

- наявність атестата відповідності КСЗІ в АС нормативним документам із захисту інформації;

- можливість визначення засобами КСЗІ декількох ієрархічних рівнів повноважень користувачів та декількох класифікаційних рівнів інформації;

- обов'язковість реєстрації в АС всіх користувачів і їхніх дій щодо конфіденційної інформації;

- можливість надання користувачам тільки за умови службової необхідності санкціонованого та контрольованого доступу до конфіденційної

- інформації, яка обробляється в АС;

- заборона несанкціонованої та неконтрольованої модифікації конфіденційної інформації в АС;

- здійснення з допомогою СЗІ обліку вихідних даних, отриманих під час вирішення функціональної задачі, у формі віддрукованих документів, які містять конфіденційну інформацію;

- заборона несанкціонованого копіювання, розмноження, розповсюдження конфіденційної інформації в електронному вигляді;

- забезпечення з допомогою СЗІ контролю за санкціонованим копіюванням, розмноженням, розповсюдженням конфіденційної інформації в електронному вигляді;

- можливість здійснення однозначної ідентифікації і аутентифікації кожного зареєстрованого користувача;

- забезпечення КСЗІ можливості своєчасного доступу зареєстрованих користувачів АС до конфіденційної інформації.

Наведені вимоги є базовими і застосовуються при захисті інформації від НСД в усіх типах АС.

Системи безпеки повинні не лише обмежувати допуск користувачів до інформаційних ресурсів, а також визначати і делегувати їх повноваження в сумісному вирішенні завдань, виявляти аномальне використання ресурсів, прогнозувати аварійні ситуації та усувати їх наслідки, адаптуючи структуру в умовах відмов, часткової втрати або тривалого блокування ресурсів.

Також важлива економічна доцільність застосування тих чи інших заходів забезпечення безпеки інформації, які мають бути адекватні існуючим загрозам. У ТЗ викладаються вимоги до функціонального складу і порядку розробки і впровадження технічних засобів, що забезпечують безпеку інформації в процесі її обробки в обчислювальній системі ІТС, а також вимоги до організаційних, фізичних та інших заходів захисту, що реалізуються поза обчислювальної системи ІТС на додаток до комплексу програмно-технічних ЗЗІ.

1.3 Постановка задачі

З урахуванням виконаного аналізу та виявлених тенденцій зростання кіберзлочинів з використанням фішингових атак, з метою організації протидії на всіх рівнях забезпечення кібербезпеки доцільним є виконання наступних задач:

- проаналізувати загальні відомості про механізми протидії кібершахрайству, що використовує фішингові веб-ресурси, виявити сильн та слабкі сторони.
- створити рекомендації для користувачів безпеки щодо організації протидії кібершахрайству, що використовує фішингові веб-ресурси.

Висновки до першого розділу

З огляду на раніше наведене можна зробити висновок, що організація протидії кібершахрайству та фішингу – це дуже важливий крок для збереження захищеності особистої інформації користувача та запобігання її витоку. Посилення методів протидії кібершахрайству дозволить знизити ризики та загрози інформації користувачів в мережі Інтернет до мінімуму та посилити ефективність моделі забезпечення захисту інформації від несанкціонованого доступу. Поява таких проблем виявляє необхідність перегляду деяких правил користування онлайн-

сервісами та поведінки користувачів у мережі, тож створення рекомендацій для користувачів та їх впровадження можна вважати доцільним та актуальним.

РОЗДІЛ 2.
СПЕЦІАЛЬНА ЧАСТИНА

2.1 Дослідження методів протидії кібершахрайству, що використовує фішинг

Головний вектор атаки фішингу спрямований на найслабкішу ланку будь-якої сучасної системи безпеки — на людину. Далеко не завжди клієнт банку може відрізнити оригінальну веб-адресу його банку від фішингової копії, наприклад: mybank.account.com або account.mybank.com. Зловмисники можуть використовувати і той факт, що в деяких шрифтах рядкова буква “i” прописна “L” виглядають однаково (I = l). Такі способи дозволяють обдурити людини за допомогою схожою на справжню посилання в електронному листі, при цьому навіть наведення курсору миші на таке посилання (з метою побачити справжню адресу) не допомагає.

В арсеналі зловмисників є й інші засоби: від банальної підміни в локальній базі IP-адреси реальної адреси на підроблену (в ОС Windows, наприклад, для цього достатньо відредагувати файл hosts) до фармінгу (pharming — це процедура таємного перенаправлення жертви на хибну IP-адресу).

Ще один вид шахрайства - підміна веб-сторінки локально. Спеціальний вірус-троян, що заразив комп'ютер користувача, може додавати у зображений браузером сайт додаткові поля, відсутні на оригінальній сторінці. Наприклад, номер кредитної картки. Звичайно, для успішного проведення такої атаки треба знати банк або платіжну систему, якими користується жертва. Саме тому тематичні бази електронних адрес користуються великою популярністю і є на чорному ринку ліквідним товаром.

Не бажаючи нести додаткові витрати фішери просто спрямовують свої атаки на найбільш популярні сервіси — аукціони, платіжні системи, великі банки - в надії на те, що випадковий одержувач спам-листів має там обліковий запис. На жаль, надії зловмисників найчастіше виправдовуються.

Отже, можна виділити наступні види атак з використанням фішингу:

- Класичний фішинг. Фішингові листи, відправлені від імені відомих дійсно існуючих компаній, які практично не відрізняються від листів, які

користувачі зазвичай отримують від цих компаній. Єдина відмінність може полягати в проханні пройти по посиланню, щоб виконати якусь дію.

- Цілеспрямована фішингова атака. Персоналізовані фішингові листи, спрямовані на конкретну людину. Такі листи містять ім'я, посаду потенційної жертви, а також будь-які інші особисті дані.
- Фішинг проти топ-менеджменту. Фішинг-листи націлені на отримання доступу до облікового запису глави компанії, генерального директора, технічного директора і т.д. Після отримання доступу до таких облікових записів фахівці з фішингу можуть продовжувати використовувати їх для зв'язку з іншими відділами, наприклад, підтверджувати шахрайські банківські перекази будь-якому фінансовій установі за власним вибором.
- Фішинг розсилки від Google і Dropbox. Відносно новий напрямок фішингових атак, метою яких є імена користувачів і паролі для входу в хмарні сховища даних.
- Фішингові листи з прикріпленими файлами. Фішинг-листи з вкладеннями, що містять віруси.
- Фармінг. Прихована переадресація на шахрайський сайт, виконаний за допомогою зміни кеша DNS на локальному комп'ютері або мережевому обладнанні.

Тепер визначемо основні методи боротьби з фішинговими сайтами та іншими видами онлайн-шахрайства.

Перший з них це створення унікального дизайну веб-сайту для кожного користувача. Суть цього методу така: клієнт, наприклад, у банку чи на веб-сайті при укладанні договору вибирає одне із запропонованих зображень. Надалі при вході на сайт банку йому буде показуватися саме це зображення. У разі якщо користувач його не бачить або бачить іншого, він повинен покинути підроблений сайт і негайно повідомити про це службі безпеки. Передбачається, що зловмисники, які не були присутні при підписанні договору, не зможуть вгадати правильне зображення і обдурити клієнта.

Однак на практиці цей спосіб не витримує критики. По-перше, для того щоб показати користувачеві його картинку, його спочатку треба ідентифікувати,

наприклад, за логіном, який він ввів на першій сторінці сайту банку. Зловмиснику не складає труднощів підготувати підроблений сайт, щоб дізнатися цю інформацію, а для самого користувача — емулювати помилку зв'язку. Тепер достатньо звернутися на реальний сервер, ввести вкрадений логін і підглянути правильне зображення.

Саме через невелику надійність зараз цей метод зустрічається доволі рідко, на заміну цьому при детальній перевірці користувача на сайті потрібно ввести дівоче прізвище матері, яке користувач вказав при оформленні картки чи при відкритті рахунку у банку. Проте, навіть цей метод аутентифікації користувача вже не забезпечує повноцінний захист від шахраїв.

Наступний метод це використання одноразових паролів. Класичні паролі є багаторазовими: користувач вводить один і той же пароль кожного разу при проходженні процедури аутентифікації, не змінюючи його часом роками. Перехоплений зловмисником, цей пароль може неодноразово використовуватися без відома господаря.

На відміну від класичного, одноразовий пароль використовується тільки один раз, тобто при кожному запиті на надання доступу користувач вводить новий пароль.

Для цього використовуються, зокрема, спеціальні пластикові картки з нанесеним захисним шаром. Клієнт банку кожен раз стирає чергову смужку і вводить потрібний одноразовий пароль. Всього на картку стандартного розміру поміщається близько 100 паролів, що при інтенсивному використанні послуг телебанкінгу вимагає регулярної заміни носія.

Більш зручними, але, правда, і дорогими представляються спеціальні пристрої — генератори одноразових паролів. В основному розрізняють два типи створення: за часом, коли поточний одноразовий пароль відображається на екрані і періодично змінюється (наприклад, раз в дві хвилини); за подією, коли нове значення генерується кожен раз при натисканні користувачем на кнопку пристрою.

Будучи більш безпечним, ніж класична парольна аутентифікації, такий метод, проте, залишає зловмисникові певні шанси на успіх. Наприклад, аутентифікація з використанням одноразових паролів не захищена від атаки "людина посередині".

Суть її полягає у "вклинювання" в інформаційний обмін між користувачем і сервером, коли зловмисник "представляється" користувачу сервером, і навпаки. Серверу передається вся інформація від користувача, в тому числі і введений нею одноразовий пароль, але вже від імені зловмисника. Сервер, отримавши правильний пароль, дозволяє доступ до закритої інформації. Не викликаючи підозр, зловмисник може дозволити користувачеві попрацювати, наприклад, зі своїм рахунком, пересилаючи йому всю інформацію від сервера і назад, але при завершенні користувачем свого сеансу роботи не розривати зв'язок з сервером, а зробити потрібні транзакції нібито від імені користувача.

Щоб не витрачати час в очікуванні завершення сеансу користувача, зловмисник може просто імітувати помилку зв'язку і не дозволяти легальному користувачеві працювати зі своїм рахунком. Залежно від використовуваного методу генерації перехоплений одноразовий пароль буде діяти або протягом короткого часу, або тільки для першого сеансу зв'язку, але в будь-якому випадку це дає зловмиснику можливість успішно провести крадіжку даних або грошей користувача.

На практиці аутентифікація за допомогою одноразових паролів сама по собі використовується рідко, для підвищення безпеки застосовується встановлення захищеного з'єднання ще до аутентифікації, наприклад, з використанням протоколу SSL.

Третій відомий метод це одностороння аутентифікація користувача. Використання протоколу безпечних з'єднань SSL (Secure Sockets Layer) забезпечує захищений обмін даними між Web-сервером і користувачами. Незважаючи на той факт, що протокол дозволяє аутентифікувати не тільки сервер, але і користувача, на практиці найчастіше застосовується тільки одностороння аутентифікація.

Для встановлення SSL-з'єднання необхідно, щоб сервер мав цифровий сертифікат, який використовується для аутентифікації. Сертифікат зазвичай видається і засвідчується третьою довіреної стороною, в ролі якої виступають центри сертифікації (ЦС). Роль ЦС полягає у тому, щоб підтверджувати оригінальність Web-сайтів різних компаній, дозволяючи користувачам, "повіривши"

одному єдиному ЦС, автоматично мати можливість перевіряти справжність тих сайтів, власники яких зверталися до цього ж самого ЦС.

Список довірених центрів, що засвідчують зазвичай зберігається в реєстрі операційної системи або в настройках браузера. Саме ці списки і піддаються атакам з боку зловмисника. Дійсно, видавши фішинговому сайту сертифікат від підробленого ЦС, що засвідчує, і додавши цей ЦС в довірені, можна, не викликаючи жодних підозр у користувача, успішно здійснити атаку.

Звичайно, такий спосіб потребує від шахраїв більше зусиль і відповідно витрат, але користувачі, на жаль, часто самі допомагають у крадіжці своїх даних, не бажаючи розбиратися в тонкощах і особливостях використання цифрових сертифікатів. В силу звички або некомпетентності нерідко ми натискаємо кнопку "Так", не особливо беручи до уваги в повідомлення браузера про відсутність довіри до організації, що видала сертифікат.

До речі, дуже схожий спосіб використовують деякі засоби з контролю SSL-трафіку. Справа в тому, що останнім часом почастішали випадки, коли сайти, заражені троянськими програмами, і самі трояни використовують протокол SSL з тим, щоб уникнути шлюзові системи фільтрації трафіку — адже шифровану інформацію ні антивірусне ядро, ні система захисту від витоку даних перевірити не в стані. Втручання в обмін між Web-сервером і призначеним для користувача комп'ютером дозволяє таким чином замінити сертифікат Web-сервера на виданий, наприклад, корпоративним СЦ і без видимих змін в роботі користувача сканувати трафік користувача при використанні протоколу SSL.

Четвертий та доволі ефективний метод протидії це URL-фільтрація. У корпоративному середовищі фільтрація сайтів застосовується для обмеження нецільового використання мережі Інтернет співробітниками і як захист від фішерських атак. У багатьох антивірусних засобах захисту даний спосіб боротьби з підробленими сайтами взагалі є єдиним.

Виявленням фішерських сайтів і внесенням їх в чорні листи займаються багато компаній - від виробників антивірусних рішень до банків, платіжних систем і

правоохоронних органів. Зокрема, створюються спеціальні організації для боротьби з фішерами, такі як Anti Phishing Work Group (APWG - http://www.apwg.org).

Спільні заходи зацікавлених сторін в тісній співпраці з реєстраторами та хостингових компаній дозволяють оперативно закривати підроблені сайти. Спільні зусилля спрямовані на максимально швидке оновлення чорних списків і блокування роботи сайтів зловмисників. Не можна не відзначити певні успіхи в цьому напрямку — середній час життя фішерських сайту складає всього 49,5 годин.

Однак далеко не всі виробники засобів антивірусного захисту можуть похвалитися такою високою оперативністю в оновленні баз, до того ж багато користувачів не використовують ніяких засобів захисту на своїх комп'ютерах або вводять номери кредитних карт і іншу конфіденційну інформацію з випадкових робочих місць. Наостанок не слід забувати: реальні атаки можуть завдавати шкоди конкретному користувача або компанії, можливо, ставлячи їх на межу банкрутства.

Отже можна зробити висновок, що методи протидії кібершахрайству діють та попереджують деяку частину правопорушень, проте, спираючись на зростаючий рівень веб-злочинів саме через недостатній рівень обізнаності користувачів можна зазначити що основною задачею є підвищення саме рівня підготовки користувачів до фішингових атак та махінацій.

2.2 Рекомендації для посилення заходів безпеки щодо протидії кібершахрайству, що використовує фішингові веб-ресурси

У попередньому розділі ми розглянули основні методи кібершахрайства, що використовує фішингові веб-ресурси та аналізуючи кожний окремий метод зіштовхувались з тим, що найслабкішою частиною захисту від атаки є сам користувач та його недостатня обізнаність у питаннях онлайн-шахрайства та захисту власних персональних даних.

На мою думку, сама необхідність посилення заходів безпеки щодо протидії кібершахрайству полягає, зокрема, у посиленні рівня навичок звичайних користувачів мережі Інтернет та фінансових сервісів, адже саме вони становляться жертвами шахрайства. Тож надалі необхідно створити рекомендації для посилення заходів безпеки щодо протидії кібершахрайству та рекомендації для користувачів.

Розглянемо кращі існуючі практики покращення ефективності роботи методів протидії фішинговим аткам.

Захист Gmail була додатково покращена за допомогою більш уважного відстеження входу в сервіси Google через сторонні додатки. Саме так працювала атака через Google Docs - замість хмарного офісного пакету користувачі входили в підроблену програму, яка запитувала логін і пароль свого облікового запису Google. Також додана вдосконалена система фільтрації спаму. Крім цього, у компанії вже є ряд заходів по боротьбі з фішингом - виявлення шахрайства на основі машинного навчання, режим Safe Browsing, сканування вкладень електронної пошти і додаткові заходи безпеки при підозрілому вході в сервіси Google.

Додатково Google підкреслює, що остання атака не завдала великих збитків — було зачеплено менш, ніж 0,1 відсотка користувачів. Але навіть така невелика частина призначеної для користувача бази Google представляє величезну кількість акаунтів, на які було скоєно напад. Посилені заходи по боротьбі з фішингом будуть вкрай необхідні для запобігання черговій подібній небезпечній ситуації.

Також Google використовує власну розробку Safe Browsing API (API безпечного пошуку, інтерфейс програмування застосунків, інтерфейс прикладного програмування, англ. Application Programming Interface, API) дозволяє додаткам зі сторони клієнта перевіряти, чи знаходиться URL в чорному списку, який постійно оновлюється Google. Хоча протокол все ще експериментальний, більшість браузерів використовують його. Список ведеться на стороні клієнта і періодично оновлюється; однак якщо URL-адреса буде змінена навіть незначно, то її вже не буде в чорному списку.

Оскільки життя цих, фішингових атак дуже коротке, великий обсяг даних використовується для зберігання цих URL, занесених до чорного списку та домену, від яких не буде користі у найближчому майбутньому. Крім того, складність порівняння кожного URL користувача з даними чорного списку дуже висока.

Найбільш частою вразливістю методів протидії фішинговим атакам за допомогою чорних списків URL-адрес є те, що інформаційна безпека все ще

стикається з тим, що зловмисники все ще можуть отримати доступ на сайт просто змінивши IP-адресу або використовуючи ботів для підробки домену.

До нових методів протидії кібершахрайству також можна занести впровадження засобів захисту електронної пошти, які вже містять необхідні механізми - SPF, DKIM, DMARC та інші. За версією Gartner, в Топ-5 відповідного сегмента ринку сьогодні входять такі компанії: Barracuda Networks, Cisco, Mimecast, Proofpoint та The Email Laundry.

Другою лінією оборони зазвичай вважаються засоби контролю доступу в Інтернет - локальні або хмарні. Вони дозволяють блокувати переходи по посиланнях, отриманим поштою, SMS або MMS (в останніх двох випадках потрібно хмарне рішення - можливо, на стороні мобільного оператора або спеціального постачальника послуг інформаційної безпеки). Серед лідерів цього сегменту можна назвати компанії Bluecoat, Cisco, Websense і Zscaler.

Останнім часом добре себе зарекомендувало використання чорного списку на основі DNS (Доменна система імен (англ. Domain Name System — ієрархічна розподілена система перетворення імені хоста (комп'ютера або іншого мережевого пристрою) в IP-адресу) розгортає протокол DNS для контролю фішингових електронних листів. Але через велику кількість учасників чорного списку сервери вимушені мати обмеження щодо ресурсу та продуктивності, якщо це не так оптимальний метод обробки великої кількості записів DNS. Чорні списки повинні оновлюватись з певною періодичністю, що потребує інтерактивне втручання, чим і можуть скористуватися злочинці, якщо вони мають доступ до комп'ютера який не знаходиться у чорному списку або через зміну IP-адреси комп'ютера.

2.3 Розробка рекомендацій для користувачів

Рекомендації необхідно розбити на чотири основні етапи протидії фішинговим атакам, на яких ви можете побудувати свій захист:

- Ускладнення доступу зловмисників до користувачів;
- Допомога користувачам у визначенні та швидкому повідомленні про підозрілі фішингові листи;

- Захист себе чи організації від впливу невиявлених фішингових листів та атак;
- Швидке реагування на інциденти та вжиття заходів.

Почнемо з першого пункту, у якому описується застосування мір захисту, які можуть ускладнити зловмисникам доступ до кінцевих користувачів.

Не можна дозволити зловмисникам використовувати адреси електронної пошти користувачів як ресурс.

Сценарій атаки:

Зловмисники «підробляють» довірені електронні листи, роблячи їх дуже схожими на ті, які були відправлені авторитетними організаціями. Ці підробні електронні листи можуть бути використані для атаки на клієнтів або людей у вашій організації.

Рекомендації для застосування:

- Зробити підробку електронної пошти з ваших доменів більш складною, використовуючи засоби захисту від «підроблення»: DMARC (Domain-based Message Authentication, Reporting, and Conformance — технологія, що дозволяє отримувачу електронної пошти перевірити справжність її відправника), SPF (Sender Policy Framework, SPF інфраструктура політики відправника — розширення для протоколу відправки електронної пошти), DKIM (DomainKeys Identified Mail — технологія, що об'єднує декілька існуючих методів антифішингу і антиспаму, з метою підвищення якості класифікації та ідентифікації легітимної електронної пошти), і заохочуйте ваші контакти робити те ж саме.
- Додаткову інформацію про реалізацію поглибленного захисту від «підроблювання» можна знайти в керівництві NCSC (National Cyber Security Centre) щодо захисту електронної пошти.

Наступне що треба зробити це скорочення об'єму інформації, яка може бути доступна зловмисникам.

Сценарій атаки:

Зловмисники використовують загальнодоступну інформацію про вашу організацію і користувачів, щоб зробити свої фішингові повідомлення більш

переконливими. Це часто виходить з вашого веб-сайту і з соціальних мереж (інформація, відома як «цифровий слід»).

Рекомендації для застосування:

- Оцінити вплив інформації, поширюваної на веб-сайті вашої організації і сторінках соціальних мереж. Що потрібно знати відвідувачам вашого сайту, і які деталі не потрібні (але можуть бути корисні зловмисникам)?
- Бути в курсі того, що ваші партнери, підрядники та постачальники повідомляють про вашу організацію в Інтернеті.
- Допоможіть своїм співробітникам та користувачам зрозуміти, як обмін їх особистою інформацією може вплинути на них і вашу організацію, і розробіть чітку політику використання цифрових технологій для всіх користувачів. Мова йде не про те, щоб очікувати від людей видалення з Інтернету всіх своїх слідів. Замість цього підтримайте їх, оскільки вони керують своїм цифровим слідом, формуючи свій профіль так, щоб це працювало для них і організації.

Не варто забувати про фільтрацію або блокування фішингових повідомлень до того, як вони потраплять до користувачів. Це не тільки знижує ймовірність фішинг-інциденту, а й зменшує кількість часу, який користувачі повинні витрачати на перевірку і складання звітів по електронній пошті.

Рекомендації для застосування:

- Перевірте всю вхідну електронну пошту на предмет спаму, фішингу та шкідливих програм. Підозрілі фішингові листи повинні бути відфільтровані або заблоковані до того, як вони потраплять до користувачів. В ідеалі це має бути зроблено на сервері, але це також може бути зроблено на пристроях кінцевого користувача (тобто в поштовому клієнті). Ваша служба фільтрації / блокування може бути вбудованою послугою хмарного поштового провайдера або замовною окремою послугою для вашого власного поштового сервера.
- Для вхідних повідомлень електронної пошти повинна існувати антипідробна політика домену відправника. Якщо у відправника є політика DMARC з політикою карантину або відхилення, то вам слід вчинити так, як цього потребує політика відправника, якщо ваш лист не пройшов перевірку.

- Якщо ви використовуєте хмарного провайдера електронної пошти, переконайтеся, що його служба фільтрації / блокування достатня для ваших потреб і включена за замовчуванням для всіх ваших користувачів. Якщо ви розміщуєте свій власний поштовий сервер, переконайтеся, що працює перевірена служба фільтрації / блокування. Це може бути реалізовано локально або може бути придбаним як хмарна послуга.
- Служби фільтрації зазвичай відправляють електронну пошту в папки спаму або небажаної пошти, а служба блокування гарантує, що вони ніколи не потраплять до користувачів. Правила, що визначають блокування або фільтрацію, повинні бути точно адаптовані до потреб вашої організації. Якщо ви відфільтруєте всі підозрілі електронні листи у папки зі спамом або небажаною поштою, користувачам доведеться керувати великою кількістю електронних листів, збільшуючи своє робоче навантаження та підвищуючи можливість помилки через людський фактор. Однак, якщо ви заблокуєте всі підозрілі електронні листи, деякі дозволені і потрібні електронні листи можуть бути втрачені. Можливо, вам доведеться з часом змінити правила, щоб забезпечити кращу взаємодію.
- Фільтрація електронної пошти на пристроях кінцевих користувачів може забезпечити додатковий рівень захисту від шкідливих електронних листів. Однак це не повинно компенсувати неефективні заходи на основі сервера, які можуть повністю блокувати велику кількість вхідних фішингових листів.
- Листи електронної пошти також можуть бути відфільтровані або заблоковані з використанням різних методів, включаючи: IP-адреси, імена доменів, білий / чорний список адрес електронної пошти, публічні чорні списки спаму, типи вкладень і виявлення шкідливих програм.

Перейдемо до другого пункту — допомога користувачам у визначенні та швидкому повідомленні про підозрілі фішингові листи. У цьому розділі ми виділимо необхідні заходи, які допоможуть користувачам виявляти фішингові електронні листи та поліпшать вашу культуру звітності.

Навчання ваших користувачів — особливо в формі фішинг-симуляції — це метод, який часто переоцінюється у захисті від фішингових атак. Ваші користувачі

можуть зробити цінний внесок в захист вашої організації, але вони не можуть компенсувати недоліки в інших місцях. Ось чому важливо дотримуватися цілісного підходу з відповідними технічними заходами і змінами у культурі безпеки організації.

Рекомендації для застосування:

- Користувачі повинні розуміти, що фішингові повідомлення важко виявити. Замість власноручного виявлення фішингових листів, користувачі мають знати коли можна попросити подальших вказівок або підтримки, коли щось здається підозрілим, несподіваним або незвичайним.
- Переконайтеся, що користувачі розуміють природу загрози фішингу. По можливості використовуйте реальні приклади і тематичні дослідження, щоб зробити загрозу відчутною, не пригнічуючи людей.
- Допоможіть своїм користувачам визначити загальні риси фішингових повідомлень, такі як терміновість або сигнали довіри, які змушують користувача діяти. Ресурс CPNI (Centre for the Protection of National Infrastructure) надає широкий спектр матеріалів для розуміння основних принципів.
- Є багато підходів, які ви могли б розглянути для анти-фішингових тренувань користувачів. Ваші користувачі можуть знайти практичні підходи, такі як тести або семінари, де вони створюють свої власні фішингові повідомлення, більш цікаві та інформативні.
- Деякі області вашої організації можуть бути більш уразливі для фішингу. Відділи, що працюють з клієнтами, можуть отримувати великі обсяги небажаних електронних листів, в той час як співробітники, уповноважені отримувати доступ до конфіденційної інформації, управляти фінансовими активами або керувати IT-системами, представлятимуть великий інтерес для зловмисника (і можуть стати метою складної фішингової атаки). Переконайтесь, що ці співробітники інформовані про ризики, і запропонуйте їм додаткову підтримку.
- Ретельно усе зважте, перш ніж використовувати фішингові симуляції. Вони можуть допомогти вам зрозуміти сприйнятливість до конкретних типів фішингових повідомлень (або більш чітку картину вразливих областей у вашій

організації), але «фішинг ваших користувачів» може мати непередбачені наслідки. Наприклад, це може вплинути на продуктивність, створюючи невизначеність щодо того, чи відповідати вам на звичайні електронні листи або користувачів, які відчувають себе «обдуреними» вашою організацією.

- Підтримуйте зв'язок з відділом кадрів, щоб переконатися, що моделювання відповідає політиці HR (Human resources — людські ресурси) вашої організації.

Наступне що треба зробити це спростити розпізнавання шахрайських запитів для ваших користувачів.

Сценарій атаки:

Зловмисники можуть втручатися в процеси, щоб змусити користувачів передавати інформацію (включаючи паролі) або проводити несанкціоновані платежі.

Визначте, які процеси можуть бути імітовані зловмисниками, а також про важливість їх аналізу і поліпшення, щоб фішингові атаки було легше виявити (при цьому дозволяючи вашій організації функціонувати).

Рекомендації для застосування:

- Переконайтеся, що всі користувачі знайомі з вашими поточними процесами, щоб вони могли розпізнавати незвичні запити.
- Зробіть процеси більш стійкими до фішингу, переконавшись, що всі важливі запити електронної пошти перевірені з використанням другого типу повідомлень (SMS / веб-сайт / телефон / пошта / особисто). Інші приклади зміни процесів включають використання іншого методу входу в систему або спільне використання файлів через хмарний обліковий запис з контрольованим доступом, а не відправлення файлів у вигляді вкладень.
- Потрібно визначити оригінальний вигляд ваших вихідних повідомлень для постачальників і клієнтів. Наприклад, ви відправляєте небажані електронні листи з проханням грошей або паролів? Чи будуть ваші електронні листи помилково прийняті за фішингові електронні листи, або люди будуть уразливі для атаки, яка була розроблена, щоб виглядати як електронний лист від вас?

- Повідомте своїх постачальників або клієнтів про те, на що їм слід звертати увагу (наприклад, «ми ніколи не запитаємо ваш пароль» або «наші банківські реквізити не змінюються ні за яких умов»).

Наступний не менш важливий крок у цьому пункті який потрібно зробити це створити середовище, яке дає користувачам можливість звертатися за допомогою. Формування оптимальної культури звітності дозволяє користувачам звертатися за допомогою і дає важливу інформацію про те, які типи фішингових атак націлені на вашу організацію. Обидва з них можуть допомогти вам поліпшити ваш захист. Ви також можете дізнатися, які типи електронних листів помилково приймають за фішинг і який вплив це може мати на вашу організацію.

Рекомендації для застосування:

- Розробіть ефективний процес надання звітів користувачам, якщо вони вважають, що спроби фішингу, можливо, перевершили технічні засоби захисту вашої організації. Чи є процес зрозумілим, простим і зручним у використанні? У користувачів є впевненість, що звіти будуть оброблені?
- Надайте відгук про те, які дії були зроблені, і поясніть, що їхній внесок має значення. Зворотній зв'язок буде більш ефективним, якщо він буде швидким та конкретним.
- Подумайте про те, як ви можете використовувати неформальні канали зв'язку (через колег, команди або внутрішні дошки оголошень), щоб створити середовище, в якій користувачам буде легко «голосно питати» про підтримку в керівництва, коли вони можуть зіткнутися зі спробою фішингу.
- Уникайте створення культури покарання або звинувачення в провині. Важливо, щоб користувачі відчували підтримку, навіть якщо вони щось натиснули, і пізніше вважають, що це щось може бути підозрілим.

Тепер розглянемо третій пункт, а саме захист себе чи організації від впливу невиявлених фішингових листів та атак. Оскільки неможливо зупинити всі атаки, в цьому пункті ми розглянемо як мінімізувати вплив невиявлених фішингових листів.

Захистіть свої пристрої від шкідливих програм. Шкідливе ПЗ часто ховається в електронних листах або підроблених веб-сайтах, на які спрямований користувач.

Добре налаштовані пристрої і хороший захист кінцевих точок можуть зупинити встановлення шкідливого ПЗ, навіть якщо програма вже потрапила на пристрій користувача.

Рекомендації для застосування:

- Запобігайте використання відомих вразливостей, використовуючи тільки ліцензійне програмне забезпечення та сертифіковані пристрої. Слідкуйте за тим, щоб програмне забезпечення та пристрої завжди були оновленими останніми версіями від розробників програмного забезпечення, постачальників обладнання та постачальників.
- Запобігайте випадкове встановлення користувачами шкідливих програм з фішингових електронних листів, обмеживши облікові записи адміністраторів тими, кому потрібні ці привілеї. Люди з обліковими записами адміністратора не повинні використовувати ці облікові записи для перевірки електронної пошти або перегляду веб-сторінок.
- Є і багато інших способів захисту від шкідливих програм, і вам необхідно враховувати свої потреби в області безпеки і способи роботи, щоб забезпечити найбільш відповідний підхід. Деякі засоби захисту специфічні для конкретних загроз (наприклад, відключення макросів), а деякі можуть не підходити для всіх пристроїв (на деяких пристроях програмне забезпечення для захисту від шкідливих програм може бути попередньо встановлено, а на інших не потрібне).

Важливим є і захист користувачів від шкідливих сайтів. Посилання на шкідливі сайти часто є ключовою частиною фішингу. Однак, якщо посилання не може відкрити сайт, атака не може бути продовжена.

Рекомендації для застосування:

- Більшість сучасних сучасних браузерів блокують відомі фішингові та шкідливі сайти. Зверніть увагу, що це не завжди так на мобільних пристроях.
- Організації повинні запускати проксі-сервіс, як у власному, так і в хмарному сховищі, щоб блокувати будь-які спроби доступу до веб-сайтів, які були визначені як хостинг шкідливих програм або фішингових атак.

- Публічні організації повинні використовувати службу DNS державного сектора, яка не дозволить користувачам потрапляти на домени, які, як відомо, є шкідливими.

Останній обов'язковий крок у цьому пункті це захист облікових записів за допомогою ефективної аутентифікації і авторизації. Паролі є ключовою метою для зловмисників, особливо якщо вони призначені для облікових записів з такими привілеями, як доступ до конфіденційної інформації, управління фінансовими активами або адміністрування IT-систем. Ви повинні зробити процес входу в систему для всіх облікових записів більш стійким до фішингу та обмежити кількість облікових записів з привілейованим доступом до абсолютного мінімуму.

Рекомендації для застосування:

- Збільшіть рівень безпеки вашого процесу входу в систему, налаштувавши двухфакторну аутентифікацію (2FA), яка також називається «Двохетапна перевірка» в деяких веб-сервісах. 2FA підтримується багатьма веб-сервісами, причому деякі пропонують корпоративні рішення на додаток до базових опцій. Наявність другого фактора означає, що зловмисник не може отримати доступ до облікового запису, використовуючи тільки вкрадений пароль.
- Паролі часто крадуть, обманюючи користувача при введенні його пароля на фальшивому веб-сайті. Деякі менеджери паролів можуть розпізнавати реальні веб-сайти і не можуть автоматично заповнюватися на підроблених веб-сайтах. Точно так само ви можете використовувати метод єдиної реєстрації (коли пристрій розпізнає і автоматично входить в реальний веб-сайт). Використання цих методів означає, що введення паролів вручну стає незвичайним, і користувач може легше розпізнати підозрілий запит.
- Можна використовувати альтернативні механізми входу, які вимагають більше зусиль для крадіжки, таких як біометричні дані або смарт-карти.
- Збиток, який може нанести зловмисник, пропорційний привілеям, присвоєним вкраденим обліковим даним. Чим більше ваші користувачі можуть зробити, тим більше шкоди може завдати зловмисник. Надавайте привілейований доступ тільки тим людям, які цього потребують. Регулярно перевіряйте

користувачів, яким були надані привілейовані права доступу, щоб переконатися, що вони як і раніше необхідні. Якщо це більше не так, то привілейований доступ повинен бути анульований. Привілейований доступ повинен бути винятком, а не нормою, і надаватися тільки до тих пір, поки він необхідний.

- Потрібно видалити або призупинити облікові записи, які більше не використовуються, наприклад, коли член вашої організації її залишає або переходить на нову посаду.
- Розгляньте оцінку ваших існуючих політик. Наприклад, політика паролів повинна знизити ймовірність повторного використання робочого пароля в особистий обліковий запис (де він може бути більш вразливий для фішингу).

Розглянемо останній пункт рекомендацій — швидке реагування на інциденти та вжиття заходів. Всі організації будуть стикатися з інцидентами безпеки в якийсь момент, тому переконайтеся, що ви в змозі швидко їх виявити і реагувати на них в запланованому порядку. Знаючи про інцидент раніше, ніж пізніше, ви зможете обмежити шкоду, яку він може спричинити.

Рекомендації для застосування:

- Користувачі повинні знати заздалегідь, як вони можуть повідомити про інцидент. Майте на увазі, що вони можуть бути не в змозі отримати доступ до звичайних засобів зв'язку, якщо їх пристрій взламано.
- Можливість моніторингу безпеки дозволяє виявляти інциденти, про які ваші користувачі не знають, хоча це підходить не для всіх організацій, оскільки вимагає значних ресурсів. У якості відправної точки ви можете отримати уявлення про ваших системах / мережах, збираючи журнали (наприклад, історію отриманих електронних листів, відвіданих веб-адрес і з'єднань із зовнішніми IP-адресами). Для тих, у кого достатньо ресурсів і гострої необхідності в безпеці, це може бути розширено до реактивного моніторингу відомих загроз. Щоб зібрати цю інформацію, ви можете використовувати інструменти моніторингу, вбудовані в ваші готові сервіси (такі як хмарні панелі захисту електронної пошти), створити власну команду або передати службу в керований сервіс моніторингу безпеки. Сума, яку ви

збираєте і зберігайте, буде залежати від вашого бюджету, обсягу журналів і обсягу аналізу.

- Після налаштування можливості моніторингу її необхідно постійно оновлювати, щоб забезпечити її ефективність.

Що ще досить важливо, це мати план реагування на інциденти. Після того, як інцидент виявлений, ви повинні знати, що робити, щоб якомога швидше запобігти подальшій шкоді.

Рекомендації для застосування:

- Переконайтеся, що ваша організація знає, що робити в разі різних типів інцидентів. Наприклад, як ви будете примусово скидати пароль, якщо пароль зламаний? Хто несе відповідальність за видалення шкідливих програм з пристрою, і як вони будуть це робити?

- Переконайтеся, що ваш план реагування відповідає юридичним та нормативним обов'язкам вашої організації.

- Плани реагування на інциденти повинні бути протестовані до того, як інцидент станеться. Як мінімум, переконайтеся, що всі знайомі з їхніми обов'язками і знають до кого звертатися за подальшою підтримкою.

Висновки до другого розділу

У другому розділі було проведено аналіз загальних відомостей про організацію протидії кібершахрайству, що використовує фішингові веб ресурси, детально розглянули існуючі методи протидії і їх сильні та слабкі сторони, спираючись на недоліки існуючих методів протидії провели обґрунтування необхідності посилення заходів безпеки щодо протидії кібершахрайству. Після цього було розглянуто рекомендації для посилення заходів безпеки щодо організації протидії кібершахрайству і можливі засоби та інструменти для посилення їх ефективності були проаналізовані.

Останнім пунктом другого розділу були створені рекомендації для користувачів щодо захисту від фішингових атак у мережі Інтернет, були розглянуті методи уникнення фішингових розсилок електронної пошти та надані рекомендації

керівникам організацій щодо безпечного функціонування їх компаній і правила поводження для співробітників.

РОЗДІЛ 3
ЕКОНОМІЧНА ЧАСТИНА

3.1 Обґрунтування витрат на впровадження рекомендацій для користувачів

Розглянувши статистичні дані першого та другого розділів, можемо зробити висновок про недостатній рівень обізнаності користувачів у питаннях кіберзлочинів та протидії ним, тож можемо вважати розробку та впровадження рекомендацій для користувачів доцільною та соціально важливою. Рекомендації у впорядкованому вигляді надаються користувачу шляхом використання системи підтримки прийняття рішень (СППР). Виконаємо розрахунок витрат на розробку програмного забезпечення відповідної СППР.

3.2 Розрахунки витрат

Нормування праці в процесі створення рекомендацій істотно ускладнено через творчій характер праці програмістів. Проте трудомісткість розробки і опрацювання ПЗ може бути розрахована на основі системи моделей з певною точністю оцінки.

Трудомісткість створення ПЗ визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного програміста):

$$t = t_{тз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{б}\text{ , годин,} \qquad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку ПЗ;

$t_{в}$ – тривалість вивчення ТЗ, літературних джерел за темою тощо;

$t_{а}$ – тривалість розробки блок-схеми алгоритму;

$t_{пр}$ – тривалість програмування за готовою блок-схемою;

$t_{опр}$ – тривалість опрацювання програми на ПК;

$t_{б}$ – тривалість підготовки технічної документації на ПЗ.

Підрахуємо трудомісткість:

$t_{тз}$ = 14 годин;

$t_{в}$ = 22 години;

$t_а$ = 6 годин;

$t_{пр}$ – 8 годин;

$t_{опр}$ – 2 години;

$t_б$ – 4 години.

Використовуючи формулу (3.1) обчислюємо трудомісткість створення ПЗ:

$$t = 14 + 22 + 6 + 8 + 2 + 4 = 56 \text{ годин}$$

Витрати на створення програмного продукту $К_{пз}$ складаються з витрат на заробітну плату виконавця програмного забезпечення $З_{зп}$ і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК $З_{мч}$:

$$К_{пз} = З_{зп} + З_{мч}, \text{ тис. грн.} \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{зп} = t \text{ x } З_{пр}, \text{ грн,} \quad (3.3)$$

де t – загальна тривалість створення ПЗ, годин;

$з_{пр}$ – средньогодинна заробітна плата програміста з нарахуваннями, грн/годину.

Використовуючи формулу (3.3) обчислюємо заробітну плату виконавця:

$$З_{зп} = 56 \text{ x } 141 = 7896 \text{ , грн.}$$

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t_{опр} \text{ x } С_{мч} + t_б, \text{ грн,} \quad (3.4)$$

де $t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

$t_б$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = Р \times t_{нал} \times С_е + (Ф_{зал} \times Н_а) / F_р + (К_{лпз} \times Н_{апз}) / F_р \text{ , грн,} \quad (3.5)$$

де Р – встановлена потужність ПК, кВт;

$t_{нал}$ – кількість ПК;

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

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

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

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

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

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

Використовуючи формулу (3.5) обчислюємо вартість 1 години машинного часу ПК:

$$С_{мч} = 0,2 \times 2 \times 1,67 + (4000 \times 0,5) / 1920 + (5000 \times 0,25) / 1920 = 2,36 \text{ грн.}$$

Використовуючи формулу (3.4) обчислюємо вартість машинного часу для налагодження програми на ПК:

$$З_{мч} = 5 \times 2,36 + 4 = 15,8 \text{ грн.}$$

Використовуючи формулу (3.2) обчислюємо витрати на створення програмного продукту:

$$К_{пз} = 7896 + 15,8 = 7911,8 \text{ грн.}$$

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_н, \text{ грн.} \quad (3.6)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн (2000 грн вартість розробки проекту та 3000 грн вартість послуг залучених зовнішніх консультантів);

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн (Windows 10 Pro — 3000 грн на рік, антивірус 360 Total Security — 900 грн ліцензія на рік, Visual Studio та Microsoft Office — 1100 грн);

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн (для проекту ну потребується створення ПЗ);

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн (твердотільний диск SSD 128 GB — 1200 грн);

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн (послуги навчання персоналу — 1000 грн);

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн (послуги спеціаліста зі встановлення обладнання — 1200 грн).

Використовуючи формулу (3.6) обчислюємо витрати на капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки:

$$К = 5000 + 5000 + 0 + 1200 + 1000 + 1200 = 13400 \text{ грн.}$$

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

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

$$С = С_{в} + С_{к} + С_{ак} \text{ , тис. грн.} \qquad (3.7)$$

де $С_{в}$ – витрати на Upgrade-відновлення й модернізацію системи інформаційної безпеки (20% від капітальних витрат);

$С_{ак}$ – витрати, викликані активністю користувачів системи інформаційної безпеки (46% від капітальних витрат);

$С_к$ – керування системою інформаційної безпеки, визначається за формулою:

$$С_к = С_{ел} + С_{тос} \quad (3.8)$$

де $С_{ел}$ – Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року;

$С_{тос}$ – Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки;

$С_{ел}$ визначається за формулою:

$$С_{ел} = Р \text{ x } F_р \text{ x } Ц_е \text{ , грн} \quad (3.9)$$

Використовуючи формулу (3.9) обчислюємо вартість електроенергії, що споживається апаратурою системи інформаційної безпеки протягом року:

$$С_{ел} = 0,2 \text{ x } 1920 \text{ x } 1,67 = 641,28 \text{ грн.}$$

Використовуючи формулу (3.8) обчислюємо витрати на керування системою інформаційної безпеки $С_к$:

$$С_к = 641,28 + (13400 \text{ x } 0,02) = 909,28 \text{ грн.}$$

Використовуючи формулу (3.7) обчислюємо річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки:

$$С = 0,21 \text{ x } 13400 + 909,28 + 0,46 \text{ x } 13400 = 9887,28 \text{ грн}$$

де $С_в$ – витрати на Upgrade-відновлення й модернізацію системи інформаційної безпеки (20% від капітальних витрат);

$С_{ак}$ – витрати, викликані активністю користувачів системи інформаційної безпеки (46% від капітальних витрат);

$С_к$ – керування системою інформаційної безпеки.

Тепер розглянемо можливі втрати через припинення роботи корпоративного вузла чи через виток інформації.

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

$$П_{ви} = \sum З_о / F \text{ x } t_в = 101 \text{ x } 10 = 1010 \text{ грн}$$

Де середньогодинна заробітня плата обслуговуючого персоналу — 101 грн, а час відновлення після атаки $t_в = 10$ годин.

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

$$E = B \cdot R – C, \quad (3.10)$$

Де В – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн (врахуємо 2080 годин на рік);

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

С – щорічні витрати на експлуатацію системи інформаційної безпеки (як вже підрахували 9887,28 грн).

Підрахуємо загальний ефект від впровадження системи інформаційної безпеки:

$$E = (101 \text{ x } 2080) \text{ x } 0{,}3 – 9887{,}28 = 53137 \text{ грн.}$$

Розрахуємо також оцінку економічної ефективності системи захисту інформації. Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

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

$$ROSI = E / K , \quad (3.11)$$

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

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, (приблизно 80000 тис. грн)

Підрахуємо коефіцієнт ROSI:

$$ROSI = 53137 / 80000 = 0,66$$

Можемо зробити висновок, що коефіцієнт повернення інвестицій вказує на перспективність інфвестицій.

Висновки

У розділі були підраховані суми капітальних (фіксованих) витрат на проектування та впровадження проектного варіанта системи інформаційної безпеки та річних поточних (експлуатаційних) витрат на функціонування системи інформаційної безпеки, які склали 13400 та 9887,28 грн відповідно, коефіцієнт ROSI становить 0,66.

Розробку і впровадження рекомендацій для користувачів можна назвати доцільним, адже спираючись на статистичні дані збитків через фішингові атаки, витрачені кошти на створення СППР видачі рекомендацій дозволять суттєво зменшити поточні витрати організацій на ліквідацію наслідків порушень ІБ.

ВИСНОВКИ

В першій частині був проаналізований стан справ України та світу щодо питання кібершахрайства та фішингових атак, були наведені статистичні дані та приклади інцидентів витоку персональної інформації користувачів.

Була обґрунтована основа розробки рекомендацій для користувачів щодо протидії кібершахрайству, що використовує фішингові веб-ресурси.

В спеціальній частині були проведені обстеження сучасних методів протидії кібершахрайству, були проведено аналіз щодо виявлення їх сильних та слабких сторін.

Після цього було надане обґрунтування створення рекомендацій для посилення ефективності роботи існуючих методів протидії кібершахрайству.

Для мінімізування ймовірності виникнення та реалізації кіберінцидентів були розроблені рекомендації для посилення ефективності роботи методів протидії фішинговим атакам та рекомендації для користувачів щодо уникнення кібершахрайства та виявлення фішингових атак.

В економічній частині були проведені розрахунки капітальних (фіксованих) та річних поточних (експлуатаційних) витрат на розробку СППР та впровадження політики безпеки інформації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Про інформацію [Електронний ресурс] : закон України від 02.10.1992 № 2657-XII. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12.

2. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : закон України від 05.07.1994 № 80/94-ВР. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/80/94-вр.

3. Про електронні документи та електронний документообіг [Електронний ресурс] : закон України від 22.05.2003 № 851-IV. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/8515.

4. Про захист персональних даних . [Електронний ресурс] : закон України від 01.06.2010 № 2297-VI. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2297-51.

5. Постанова Кабінету міністрів України №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006

6. НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі»

7. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»,

8. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»

9. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»

10. International Intellectual Property Alliance Special Report 2016 [Електронний ресурс]. – Режим доступу: http://www.iipawebsite.com/

11. Wu, M., Miller, R. and Garfinkel, S., 2005. Do Security Toolbars Actually Prevent Phishing Attacks?, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Montreal, Quebec, Canada, 22 - 27April 2006.

12. Kirlappos, I. and Sasse, M.A., 2012. Security education against phishing: A modest proposal for a major rethink. IEEE Security and Privacy Magazine, 10(2), pp.24-32.

13. Aggarwaly, A., Rajadesingan, A. and Kumaraguru, P., 2012. PhishAri:Automatic Realtime Phishing Detection on Twitter, Seventh IEEE APWG eCrime Researchers Summit (eCRS), Las Croabas, Puerto Rico, pp. 22-25, Available at: , (Accessed 25 November 2016)

14. Krieg, G.and Kopan, T. 2016. CNN News, Is this the email that hacked John Podesta's account?, Available at: , (Accessed 19 November 2016)

15. G. Bottazzi et al., "MP-Shield: A Framework for Phishing Detection in Mobile Devices", in Proceedings of the 3rd IEEE International Workshop on Cybercrimes and Emerging Web Environments, Liverpool, UK, October 2015.

16. Випадки витоку конфіденційної інформації в українських компаніях [Електронний ресурс]. – Режим доступу: https//:searchinform.com.ua/

17. Конеев И. Р., Беляев А. В. Информационная безопасность предприятия: учеб. пособие. – СПб.: БХВ-Петербург, 2003.- 752с.

18. Методичні рекомендації до підготовки та захисту дипломної роботи (проекту) для студентів галузі знань 1701 «Інформаційна безпека» та спеціальності 125 «Кібербезпека» / Т.В. Бабенко, М.В. Корнєєв, О.В. Кручінін, Д.С. Тимофєєв ; Нац. гірн. ун-т. – Д. : НГУ, 2016. – 44 с.

19. Методичні вказівки до виконання економічної частини дипломного проекту (для студентів напряму підготовки 1701 Інформаційна безпека)/ Упорядн.: О.Г. Вагонова, І.В. Шереметьєва, Ю.О. Волотковська, Н.М. Романюк. – Дніпропетровськ: ДВНЗ "Національний гірничий університет", 2013. – 17 с.

20. Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F. and Hong, J., 2008. Lessons from a real world evaluation of anti-phishing training, eCrime Researchers Summit, 15-16 October, pp.1–12

21. Marforio, C., Masti, R.J., Soriente, C., Kostiainen, K. and Capkun, S., 2016, October. Hardened Setup of Personalized Security Indicators to Counter Phishing Attacks

in Mobile Banking. In Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices (pp. 83-92). ACM.

22. Rachna Dhamija, and J.D. Tygar, “The Battle against Phishing - Dynamic Security Skins,” Proceeding SOUPS '05 Proceedings of the 2005 symposium on Usable privacy and security, PP 77 – 88, 2005.

23. Neil Chou, Robert Ledesma, Yuka Teraguchi, Dan Boneh, and John C. Mitchell, “Client-side defence against web-based identity theft,” in NDSS. The Internet Society, 2004.

24. GARTNER. “Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks”, December 17,2007, available: “http://www.gartner.com/it/page.jsp?id=565125”

25. Zhao, M., An, B. and Kiekintveld, C., 2016, February. Optimizing personalized email filtering thresholds to mitigate sequential spear phishing attacks. In Proceedings of the 30th AAAI Conference on Artificial Intelligence (AAAI).

26. G. Tally, R. Thomas, T. V. Vleck, “Anti-Phishing : Best Practices for Institutions and Consumers” Mcafee research technical report, September 2004.

27. Arachchilage, N. A. G. (2015). User-Centred Security Education: A Game Design to Thwart Phishing Attacks. arXiv preprint arXiv:1511.03459.

28. Srivastava; B. B. Gupta; A. Tyagi; A. Shamn; A. Mishra, “Recent Survey on DDoS Attacks and Defence Mechanisms,” Advances in Parallel Distributed Computing, Communications in Computer and Information Science, vol. 203, pp. 570-580.

29. Wu, M., Miller, R. and Garfinkel, S., 2005. Do Security Toolbars Actually Prevent Phishing Attacks?, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Montreal, Quebec, Canada, 22 - 27April 2006.

30. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Generation Computer Systems, vol.29, no.7, pp. 1645–1660, 2013.

31. FireEye, “Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign”, Available at: https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html

32. Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F. and Hong, J., 2007. Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer, APWG eCrime Researchers Summit, 4-5October 2007, Pittsburgh, PA, USA.

ДОДАТОК А. Відомість матеріалів дипломного проекту

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Зміст	2	
3	А4	Вступ	2	
4	А4	1 Розділ	16	
5	А4	2 Розділ	23	
6	А4	3 Розділ	8	
7	А4	Висновки	1	
8	А4	Перелік посилань	1	
9	А4	Додаток А	1	
10	А4	Додаток Б	1	
11	А4	Додаток В	1	
12	А4	Додаток Г	1	

ДОДАТОК Б. Відгук керівника економічного розділу

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

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

(підпис)

ДОДАТОК В. Відгук керівника дипломної роботи

ВІДГУК

на дипломну роботу магістра

студента групи 125м-17-2

Гончарова Данила Олеговича

на тему: «Організація протидії кібершахрайству, що використовує фішингові веб-ресурси»

Метою дипломної роботи є вдосконалення сучасних методів протидії кібершахрайству, надання і впровадження рекомендацій.

Тема дипломного проекту безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в дипломному проекті вирішуються наступні задачі: аналіз теоретичної бази в сфері сучасних кіберзлочинів; досліджено існуючі методи фішингових атак; проаналізовано сучасні механізми протидії кібершахрайству, виявлено їх сильні та слабкі сторони .

Розроблено рекомендації щодо покращення ефективності роботи механізмів протидії кібершахрайству та рекомендації для користувачів щодо уникнення фішингових атак. Практичне значення результатів дипломного проекту полягає у розробці рекомендацій для вибору відповідної методики протидії кібершахрайству, що використовує фішингові веб-ресурси.

Недостатньо повно виконано аналіз програмно-технічних методів протидії фішинговим атакам.

Оформлення пояснювальної записки до дипломної роботи виконано з незначними відхиленнями від стандартів. Допускалось порушення графіку виконання роботи.

За час дипломування Гончаров Д.О. проявила себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння звання магістра та кваліфікації професіонала з організації інформаційної безпеки.

Дипломна робота заслуговує оцінки «добре».

Оцінка роботи_____

Керівник дипломної роботи д.ф.-м.н., проф. Кагадій Т.С.

Керівник спец. розділу ст. викл. Тимофєєв Д.С.

ДОДАТОК Г. Перелік файлів на електронному носії

Дипломний проект Гончаров Д.О. 125М-17-2 – Пояснювальна записка.

Гончаров Д.О. 125М-17-2.pttx – Презентація.