Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
« » червня 2021 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього рівня)

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

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Методи та засоби захисту від кібершпигунства та кіберсталкінгу»

Виконавець: студент IV курсу, групи КБ-42

_____ Андрусенко Кирило Валерійович
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Мирутенко Л. В.	

Нормоконтроль	Зюбіна Р. В.	

Київ 2021

Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____Н.В. Лукова-Чуйко
«10» жовтня 2020 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студенту **КБ-42** (група) **Андрусенку Кирилу Валерійовичу** (прізвище ім'я по-батькові)

Тема дипломної роботи Методи та засоби захисту від кібершпигунства та кібersталкінгу

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №2 від 08.10.2020 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Концепція кіберпростору; методи кібершпигунства та кібersталкінгу; сучасні технології протидії кібершпигунству та кібersталкінгу.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Ознайомитися з поняттям кіберпростору, його ознаками та видами; дослідити існуючі методи кібершпигунства та кібersталкінгу, їх законодавчого регулювання; проаналізувати методи запобігання переслідуванню у кіберпросторі;

розробити перелік рекомендацій щодо захисту громадян від кіберсталкінгу.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблені рекомендації щодо протидії кіберсталкінгу можуть бути застосовані фізичними особами та сприяють зниженню рівня кримінальної активності, пов'язаної з переслідуваннями, домаганнями, вандалізмом, наклепом та крадіжками персональних даних.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 12 жовтня 2020 року

Завдання видала	_____	Л. В. Мирутенко
	(підпис)	(ініціали, прізвище)
Завдання прийняв до виконання	_____	К. В. Андрусенко
	(підпис)	(ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	25.01.2021 – 27.01.2021	*виконано*
2	Аналіз літератури	28.01.2021 – 11.02.2021	*виконано*
3	Аналіз та опис проблематики	12.02.2021 – 15.02.2021	*виконано*
4	Дослідження концепції кіберпростору	16.02.2021 – 04.03.2021	*виконано*
5	Дослідження методів та засобів кібершпигунства та кіберсталкінгу	05.03.2021 – 21.03.2021	*виконано*
6	Визначення найефективнішого методу кіберсталкінгу	22.03.2021 – 08.04.2021	*виконано*
7	Дослідження та агрегація існуючих методів запобігання кіберсталкінгу	09.04.2021 – 10.05.2021	*виконано*
8	Розробка рекомендацій щодо захисту громадян від кіберсталкінгу	11.05.2021 – 22.05.2021	*виконано*
9	Оформлення пояснювальної записки	23.05.2021 – 08.06.2021	*виконано*
10	Підготовка до захисту дипломної роботи	09.06.2021 – 21.06.2021	*виконано*

Завдання видала	_____	Л. В. Мирутенко
	(підпис)	(ініціали, прізвище)
Завдання прийняв до виконання	_____	К. В. Андрусенко
	(підпис)	(ініціали, прізвище)

Термін подання дипломної роботи до ЕК 08 червня 2021 року

РЕФЕРАТ

Дипломна робота на тему «Методи та засоби захисту від кібершпигунства та кіберсталкінгу» складається зі вступу, основної частини, що містить 3 розділи, висновків, списку літератури та джерел. Загальний обсяг роботи – 51 сторінка. Робота містить 4 рисунки, 2 таблиці. Список використаних джерел включає 70 джерел.

Метою даної роботи є оцінка поточного стану захищеності користувачів інтернету від кіберсталкінгу та розробка комплексу рекомендацій щодо ефективного упередження спроб переслідування особистості у кіберпросторі.

У роботі проаналізована існуюча література та електронні джерела, що стосуються кібершпигунства та кіберсталкінгу. Введено поняття цифрової особистості та крадіжки цифрової особистості. Експериментальним чином визначено, що крадіжка цифрової особистості є найефективнішим методом кіберсталкінгу.

Розроблено комплекс рекомендацій щодо упередження та захисту від спроб кіберсталкінгу. Практичне значення розроблених рекомендацій полягає у формуванні багажу знань та вмінь, націлених на захист особистості від кіберсталкінгу, реалізація яких буде сприяти зниженню рівня кримінальної активності, пов’язаної з переслідуваннями, домаганнями, вандалізмом, наклепом та крадіжками чутливих персональних даних.

Комплекс рекомендацій передбачає можливість масштабування шляхом імплементації нових методів та засобів захисту, які будуть актуальні у випадку масового поширення нових інформаційно-комунікаційних технологій. Результати здійснених досліджень можуть бути впроваджені у процес інформаційної підготовки школярів, студентів, працівників державних та комерційних установ.

Ключові слова: кібершпигунство, кіберсталкінг, захист персональних даних, крадіжка особистості, цифровий слід, цифрова особистість, переслідування, шантаж.

ЗМІСТ

ВСТУП

Не підлягає сумніву той факт, що віртуальний простір став невід'ємною частиною людського сьогодення. З поширенням інтернету доступ до віртуального середовища став доступним мільярдам людей з будь-яких куточків планети. Важко собі уявити сучасну людину, яка б ніколи в житті не користувалась пристроями, під'єднаними до глобальної мережі, і так само важко уявити людину, яка б не залишила там свій слід.

Новонароджені діти, самі того не розуміючи, потрапляють до віртуального середовища швидше, ніж з пологового будинку до батьківського дому, адже реєстрація їх народження відразу заноситься до великої об'єднаної мережі, створюючи їх перше віртуальне представлення у кіберпросторі. До того моменту, коли дитина навчиться ходити, її цифровий слід вже сягне значних розмірів: історія хвороб, карта щеплень, реєстраційні записи, та безліч її фотографій, які батьки викладуть до соціальних мереж – усе це стане частиною кіберпростору.

Чим дорослiше стає людина, тим складніше їй стає контролювати особисту інформацію, яка потрапляє до віртуального простору. Ситуація ускладняється ще й тим, що наразі кіберпростір є основним середовищем комунікації між людьми та одним з найголовніших інструментів для успішної соціалізації, а отже кожного дня в мережу потрапляє незліченний об'єм приватної інформації, видалити яку звідти практично неможливо.

Отримання доступу до приватної інформації особи або організації без її згоди – це основна мета кібершпигунства. Отримані дані злочинці можуть використовувати для особистої, економічної, політичної чи військової переваги, та для інших протизаконних та аморальних діянь, таких як кіберсталкінг.

Актуальність даної дипломної роботи визначається тією обставиною, що наразі використання електронних пристроїв відкриває можливості для реалізації безлічі тактик кіберсталкінгу, таких як переслідування, залякування, домагання, примус, викрадення особистості, тощо.

Мета даної дипломної роботи – розробити комплекс рекомендацій, які допоможуть захиститися від найбільш популярних методів кібершпигунства, задля упередження кіберсталкінгу та крадіжки особистості.

Об'єкт дослідження: процес кібершпигунства та кіберсталкінгу.

Предмет дослідження: технології та методи упередження спроб кіберсталкінгу.

Методи дослідження: спостереження, прикладне дослідження, комплексний аналіз, структурний аналіз.

РОЗДІЛ 1
МЕТОДИ КІБЕРШПИГУНСТВА ТА КІБЕРСТАЛКІНГУ

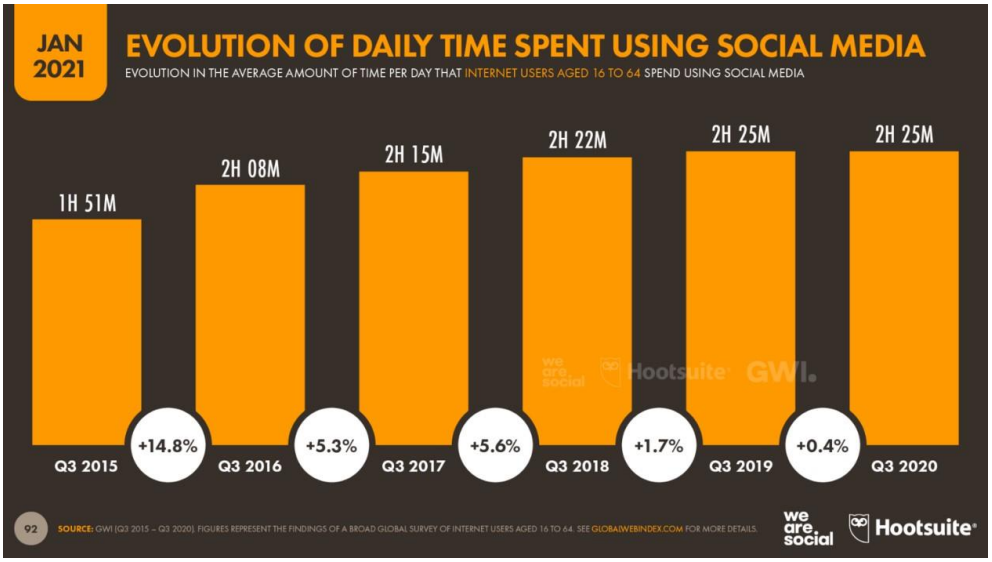
1.1 Дослідження актуальності проблеми кіберсталкінгу

З кожним роком кількість людей, які користуються інтернетом та соціальними мережами стрімко зростає. Згідно даних, зібраних дослідницьким товариством We Are Social, у 2021 році 5,22 мільярдів людей мають власний мобільний пристрій (66,6 % світового населення), 4,66 мільярдів людей регулярно користуються інтернетом, а соціальні мережі налічують близько 4,20 мільярдів користувачів.

В цілому середній користувач тепер проводить майже 7 годин в день в інтернеті зі всіх пристроїв – більше 48 годин на тиждень, 2 повних дні з 7.

Якщо припустити, що середньостатистична людина спить від 7 до 8 годин на день, це означає, що зараз ми проводимо приблизно 42% нашого часу неспання в інтернеті. Ми знаходимося онлайн приблизно стільки ж часу, скільки витрачаємо на сон.

На діаграмі нижче (Рисунок 1.1) представлена динаміка середньої кількості



часу, який користувачі проводять у соціальних мережах [1]:

Рисунок 1.1 – динаміка середньої кількості часу, який користувачі проводять у соціальних мережах

Як видно з діаграми, кількість часу, яку люди проводять в інтернеті та соціальних мережах на день, значно зростає. В умовах карантину, пов'язаного з епідемією COVID-19, люди все більше стали покладатися на інтернет та соцмережі як на основний спосіб комунікації, а отже і чутливої персональної інформації у кіберпросторі стало більше. Чим більше персональної інформації знаходиться у віртуальному просторі, тим більше поширюються випадки атак на цю інформацію, які відкривають можливості кіберсталкінгу [7].

Так само, як і переслідування у реальності, кіберсталкінг може спричинити широкий спектр фізичних та емоційних наслідків для тих, на кого він націлений. Наприклад, нерідкі випадки, коли ті, кого переслідують в Інтернеті, відчувають гнів, страх і розгубленість. Вони також можуть мати проблеми зі сном і навіть скаржитися на проблеми зі шлунком. Є навіть повідомлення про те, що цілі кіберсталкінгу можуть відчувати посттравматичний стресовий розлад та суїцидальні наміри [2].

Проблема кіберсталкінгу на сьогоднішній день як ніколи актуальна: згідно дослідженням, проведеним товариством Cyberbullying Research Center, близько 36,5 відсотків з 5 тисяч опитаних людей сказали, що вважають, що вони були жертвами кіберсталкінгу протягом свого життя, а 17,4 % опитаних сказали, що були жертвами кіберсталкінгу протягом останніх 30 днів з моменту опитування [3].

Таким чином, розробка методів боротьби з кіберсталкінгом – це актуальне і комплексне завдання, що має на меті покращення взаємовідносин між людьми у кіберпросторі та зниження кримінальної активності, пов'язаної з онлайн-переслідуваннями, крадіжками, домаганнями, примусом, тощо. А враховуючи швидкість розвитку інтернету та популярність його використання, можна припустити, що в майбутньому методи кіберсталкінгу будуть лише удосконалюватись та спричиняти ще більше негативного впливу на людей та їх власність.

1.2 Дослідження концепції кіберпростору

У 1980-х роках почався повсюдний перехід від аналогових технологій до цифрових, який був названий «Цифровою революцією». Цифрова революція проголосила початок нової Інформаційної ери, яка характеризується можливістю людини вільно й миттєво передавати і приймати інформацію.

У 1982 році американський письменник Вільям Гібсон ввів у вжиток термін «кіберпростір». *Кіберпростір* — інтерактивне інформаційне середовище, яке функціонує за допомогою комп'ютерних систем та надає можливості для здійснення комунікацій та/або реалізації суспільних відносин.

Сьогодні кіберпростір все більше стає схожим на проекцію реальності, де майже у кожного реального об’єкту та процесу є своя цифрова репрезентація. Електронні кошти, цифрові посвідчення, онлайн-школи, електронний документообіг, месенджери – це лише кілька з багатьох проекцій реальності у віртуальність. Ціллю даних проекцій є спрощення та пришвидшення рутинних процесів життєдіяльності людини, зменшення обсягів роботи працівників на підприємствах та мінімізація обмежень, пов’язаних з матеріальними ресурсами.

1.3 Розробка поняття цифрової особистості

Цифрова особистість – це віртуальна репрезентація реальної особи, яка представляє її у кіберпросторі.

Цифрова особистість складається з відкритих та приватних ідентифікаційних відомостей, які належать реальній особі.

Відкриті ідентифікаційні відомості – це набір даних, доступних до перегляду іншим користувачам інформаційного сервісу або системи, за якими вони можуть знаходити акаунт конкретної особи.

Приватні ідентифікаційні відомості – це набір даних, прихований від інших користувачів сервісу/системи, що використовується у технічних цілях (наприклад як унікальний ідентифікатор при автентифікації користувача у системі). Зазвичай користувач сам обирає, які дані він бажає зробити відкритими або приватними.

Традиційно, відкритими є такі ідентифікаційні відомості:

- ім’я та прізвище;
- нікнейм;
- дата народження;
- місце навчання.

До приватних відомостей зазвичай відносять:

- номер мобільного телефону;
- адресу електронної пошти;
- перелік персональних паролів.

Якщо проводити аналогію з реальною особою, то номер мобільного телефону можна вважати аналогом паспорту для цифрової особистості. Номер телефону у комбінації з персональними паролями використовуються у більшості інформаційних систем як типові облікові дані для автентифікації користувачів, та як основний інструмент скидання паролю у випадках, коли користувач забуває свої дані для входу.

1.4 Цінність цифрової особистості у розрізі кіберсталкінгу

Оскільки цифрова особистість репрезентує реальну особу, то для зловмисників, які займаються кіберсталкінгом, отримання контролю над цифровою особистістю жертви є одним з найефективніших способів реалізації їх намірів. Так, маючи доступ до приватних ідентифікаційних відомостей жертви, зловмисники мають змогу переглядати усі її приватні дані (листування, фотографії, робочі записи,

тощо), фінансові рахунки, та відслідковувати переміщення жертви, що відкриває безліч можливостей до переслідування, шантажу та приниження цілі кіберсталкінгу.

1.5 Кібершпигунство як передумова кібersталкінгу

Кібершпигунство або комп'ютерний шпіонаж – це термін, який позначає несанкціоноване отримання інформації з метою отримання особистої, економічної, політичної чи військової переваги, здійснюваний з використанням обходу (злому) систем комп'ютерної безпеки, з застосуванням шкідливого програмного забезпечення.

Кіберсталкінг – це процес використання Інтернету для переслідування або домагань людини, групи людей або організації. До кібersталкінгу також часто відносять неправдиві звинувачення, плітки і наклеп. Одними з найрозповсюдженіших прикладів кібersталкінгу є викрадення особистості, загрози, вандалізм або збирання інформації, яка може бути використана для залякування або домагань.

Протягом багатьох років корпорації намагалися шукати переваги, вписуючись у бізнес-плани своїх конкурентів. Однією з тактик є підсилання працівників, які намагаються отримати доступ до даних або проектів, де розробляються нові технології. Ця тактика забезпечила еволюційний шлях для цієї діяльності і призвела до народження кібершпигунства.

Підсилання працівників-шпигунів під прикриттям все ще є корисною тактикою, але зараз незахищена робоча станція набагато привабливіша. Людина може використовувати USB-накопичувач для завантаження програми-шпіону або вірусу за лічені секунди. Метою може бути виявлення та відкриття порталу безпеки або пошук експлойту, на який можна націлитися пізніше [23].

Бізнес-веб-сайти можуть пропонувати такий самий тип відкриття, а досвідчені хакери можуть використовувати вразливий веб-сайт для здійснення атаки. Електронні листи можуть надсилатися певним особам з вищими мережевими привілеями, яких можна заманити, натиснувши посилання, яке завантажує код, що відкриває можливість подальшої атаки. Цей тип атаки називається фішинговим.

Сучасне програмне забезпечення браузера складається з тисяч рядків коду. Нові рядки коду додають нові функції в міру розвитку програмного забезпечення. Іноді новий код випадково або через недогляд (або відсутність такого) порушує маловідомі функції або вступає у протиріччя з засобами забезпечення безпеки, які раніше були ефективними. Коли нова функція або нова частина програмного забезпечення потрапляє на ринок, вона аналізується та досліджується за допомогою реверс-інжинірингу безліччю людей та зацікавлених сторін у всьому світі.

Кібершпигуни найчастіше намагаються отримати доступ до таких активів:

- Дані та дослідження досліджень та розробок
- Дані академічних досліджень
- Інтелектуальна власність, наприклад формули продукту або креслення
- Зарплати, преміальні структури та інша фінансова інформація
- Списки клієнтів та структури платежів
- Бізнес-цілі, стратегічні плани та тактика маркетингу
- Політичні стратегії, приналежності та комунікації
- Військова розвідка

Кібершпигунство, націлене на конкретну фізичну особу (на її персональні дані, дані банківських рахунків, деталі персонального життя, тощо) часто є передумовою кіберсталкінгу. Зловмисник використовує отримані під час процесу кібершпигунства дані про жертву для того, щоб встановити психологічний або фізичний контроль над нею та її інтелектуальними або матеріальними активами.

Кіберсталкінг поділяється на дві категорії згідно мети зловмисника:

- Відкритий кіберсталкінг
- Прихований кіберсталкінг

Відкритий кіберсталкінг включає відкрите переслідування жертви, вимагання грошей/послуг або шантаж, та має на меті отримання матеріальної або моральної вигоди, або встановлення домінації над жертвою.

Прихований кіберсталкінг часто залишається непоміченим жертвою, він часто використовується зловмисниками з психологічними відхиленнями для втручання у персональне життя жертви, перегляду її особистих фотографій, листувань, робочих записів, тощо. Такий тип кіберсталкінгу не має на меті встановлення контролю над реальною особою, а тільки над її цифровою особистістю та її активами.

Крадіжка особистості – особливий вид переслідування, який можна віднести як до відкритого, так і до закритого кіберсталкінгу. У першому випадку цифрова особистість викрадається для отримання активів реальної особи та викривається нею після здійснення модифікації, знищення або крадіжки активів, а у другому випадку цифрова особистість викрадається для непомітного отримання приватної інформації, що належить жертві, тобто ціллю кіберсталкінгу стає подальше кібершпигунство.

Візуальне представлення кібершпигунства та кіберсталкінгу проілюстроване на Рисунку 1.2.

Рисунок 1.2 – візуальне представлення процесу кібершпигунства та кіберсталкінгу у часі

1.6 Типові тактики кібершпигунства та кіберсталкінгу

Більшість видів кібершпигунства класифікуються як розвинена стійка загроза. Це складна, тривала кібератака, в якій зловмисник проявляє невизначену присутність у мережі, щоб викрасти конфіденційні дані протягом тривалого періоду часу. Дана атака ретельно спланована і розроблена для уникнення існуючих заходів безпеки протягом тривалого періоду часу.

Кібершпигунство вимагає вищого рівня налаштування та витонченості, ніж традиційна атака. Зловмисники, як правило, добре фінансуються та являються досвідченими командами кіберзлочинців, які націлені на високоцінні організації. Вони витрачають значний час та ресурси на дослідження та виявлення вразливостей в організації. З іншого боку, кібершпигунство, націлене на конкретну фізичну особу зазвичай не вимагає високого рівня кваліфікації, так як індивідуальні фізичні особи дуже рідко використовують передові технології захисту своїх приватних даних. Для отримання приватних даних фізичної особи дуже часто використовуються такі методи, як перенаправлення на шкідливі посилання, завантаження шкідливого програмного забезпечення до комп’ютеру жертви або сплата фальшивих квитанцій.

Більшість кібершпигунських атак також включають певну форму соціальної інженерії, щоб стимулювати активність або збирати необхідну інформацію від цілі для просування атаки. Ці методи часто використовують такі людські емоції, як хвилювання, допитливість, емпатія або страх діяти швидко або необдумано.

Методи соціальної інженерії зазвичай використовуються під час особистого спілкування зловмисниками з жертвою з фейкових акаунтів у соцмережах. Таким чином, просто ведучі бесіду з жертвою, вони можуть приховано викрасти чутливі приватні дані про жертву, такі як відповіді на контрольні запитання для скидання паролей, адресу проживання, номера телефонів жертви та її знайомих, тощо.

Кібершпигунство, особливо коли воно організоване та здійснюється великими державами, є зростаючою загрозою безпеці. Незважаючи на безліч звинувачень та законодавчих актів, спрямованих на стримування такої діяльності, більшість злочинців залишаються на волі через відсутність угод про екстрадицію між країнами та труднощі із забезпеченням міжнародного права, пов'язаного з цією проблемою.

Деякі держави на законодавчому рівні підтримують та спонсорують кібершпигунство, націлене на фізичних осіб, з метою виявлення екстремізму та упередження терористичних діянь проти держави. Деякі форми кібершпигунства, пов'язаних з аналізом цифрового сліду користувачів інтернету, використовуються державними установами для оцінки політичних настроїв соціальних груп та для попередніх прогнозів під час урядових виборів.

Етична сторона питання державного кібершпигунства, націленого на конкретних громадян – це тема активних дискусій серед політичних представників та верств влади.

Таблиця 1.1

Типова категоризація тактик кібершпигунства

Watering hole (з англійської – «Полив»)	Зловмисники можуть заражати легальні веб-сайти, які часто відвідує жертва або її знайомі, шкідливим програмним забезпеченням з явною метою компрометації користувача.
Цільовий фішинг	Хакер націлений на конкретних осіб, та відсилає їм шахрайські електронні листи, текстові повідомлення та робить телефонні дзвінки, щоб викрасти облікові дані для входу або іншу конфіденційну інформацію.
Експлойт «першого дня»	Кіберзлочинці використовують невідому вразливість системи безпеки або недолік програмного забезпечення перед виявленням та виправленням розробником програмного забезпечення або IT-командою замовника.
Інсайдерська загроза	Зловмисник переконує працівника або підрядника поділитися або продати інформацію або доступ до системи неавторизованим користувачам. До інсайдерських загроз також відносять процес отримання приватних даних індивідуальної фізичної

	особи від її друзів або знайомих.

Кібersталкінг не завжди пов’язаний з викраденням персональних даних жертви та зламом її акаунтів у соцмережах. Ті, хто займається кібersталкінгом, використовують різноманітні тактики та техніки для переслідування, приниження, залякування та контролю своїх цілей. Насправді багато з тих, хто бере участь у кібersталкінгу, володіють технологічною кмітливістю та креативом і придумують безліч способів мучити та переслідувати свої цілі.

Ось кілька прикладів того, що можуть робити люди, які займаються кібersталкінгом:

- Публікація в Інтернеті грубих та образливих коментарів.
- Переслідування цілі в Інтернеті, приєднуючись до тих самих груп та форумів.
- Надсилання цілі погрожуючих або непристойних повідомлень.
- Використання технологій, щоб погрожувати або шантажувати ціль.
- Позначання цілі у публікаціях надмірно, навіть якщо вони не мають до них нічого спільного.
- Коментування або «вподобання» (лайки) усього, що ціль розміщує в Інтернеті.
- Створення підроблених акаунтів, щоб відслідковувати ціль в соцмережах.
- Злам або викрадення онлайн акаунтів та фінансових рахунків цілі.
- Спроба вимагання сексу або приватних фотографій.
- Надсилання небажаних подарунків цілі.
- Розголошення конфіденційної інформації цілі в Інтернеті.
- Розміщення або поширення реальних або фальшивих фотографій цілі.
- «Бомбардування» цілі явно вираженими непристойними фотографіями.
- Створення фейкових дописів, призначених для присоромлення жертви.

- Відстеження онлайн-переміщення цілі, встановлюючи пристрої відстеження.
- Злам камери цілі на її ноутбуці чи смартфоні для слідкування за нею.

Усі ці дії націлені на приниження жертви або втручання у її особисте життя, що може призвести до значних збитків як моральному, так фінансовому стану жертви.

У наступному розділі проведено аналіз основних тактик кіберсталкінгу та визначено найефективніший метод здобуття контролю над цифровою особистістю реальної особи.

1.7 Законодавче регулювання проблем кіберсталкінгу

Кіберсталкінг, як і переслідування у реальності, не розглядається правоохоронцями як певний вид правопорушення (злочину), але у даному діянні існує як потерпіла сторона, так і сторона, яка певним чином створює для потерпілої сторони умови, при яких вона відчуває страх, приниження, та ін. Кіберсталкерами можуть бути будь-хто, навіть просто угруповання тих, хто робить це для розваги.

Сучасні юридичні проблеми у сфері електронно-інформаційної комунікації пов’язані з тим, що техніко-технологічна взаємодія з реальним світом здійснюється через віртуальний простір за допомогою певного програмно-апаратного комплексу.

У зв’язку зі швидким розвитком ІТ-технологій та повільним розвитком законодавства щодо сфери комп’ютерних технологій маємо реальну ситуацію, коли злочинці діють безкарно, за умов недосконалості законодавства.

Складність вияву злочинця та отримання допомоги від кіберполіції, відсутність законодавчого визначення понять «кіберсталкінг» та «кібербуллінг» разом з визначенням механізмів протидії, надає злочинцям можливість безкарно виконувати дії, які вони обирають за певним сценарієм. Саме велика кількість варіацій дій злочинця не дає можливості чітко визначити ступінь його вини, а потерпілій стороні – навіть можливості на мінімальний захист від зловмисника.

Зокрема це стосується відсутності сталих механізмів взаємодії та нормативних важелів щодо банківських структур, які зобов'язують забезпечувати більше тісну взаємодію з правоохоронними структурами у частині розслідування втрати коштів з розрахункового рахунку потерпілих.

Як висновок, масштаб та поява нових способів і методів кіберсталкінгу зумовлює потреби подальших досліджень з цієї тематики, спрямованих на удосконалення та розвиток національного законодавства, створення спеціальних програмних засобів захисту прав людини та відповідного методичного забезпечення для сфери протидії кіберзлочинності.

Висновки за розділом 1

У даному розділі було розглянуто основні методи та засоби кібершпигунства та кіберсталкінгу.

За результатами проведеної роботи було зроблено наступні висновки:

1. Проблема кіберсталкінгу на сьогоднішній день є актуальною.
2. Існує безліч методів та засобів, за допомогою яких може реалізовуватись кібершпигунство та кіберсталкінг, а саме: переслідування, примус, наклеп, домагання, викрадення цифрової особистості, тощо.
3. Проблема захисту цифрової особистості є найбільш критичною у контексті збитків, які можуть бути нанесені фізичній особі під час кіберсталкінгу.
4. Кібершпигунство є передумовою кіберсталкінгу та відкриває можливість викрадення цифрової особистості.

Таким чином в даній роботі, згідно досліджуваної мети, треба розглянути наступні задачі:

1. Визначити найефективніші методи кіберсталкінгу.
2. На основі визначених методів провести експериментальне дослідження з метою підтвердження їх ефективності.
3. Дослідити засоби та заходи для протидії визначеним методам.

4. Розробити комплекс рекомендацій щодо упередження та захисту від спроб кіберсталкінгу.

РОЗДІЛ 2
ВИЗНАЧЕННЯ НАЙЕФЕКТИВНІШОГО МЕТОДУ КІБЕРСТАЛКІНГУ

2.1 Викрадення особистості як основний інструмент кіберсталкерів

У першому розділі даної дипломної роботи були наведені найпопулярніші методи кіберсталкінгу. Було визначено, що найбільш значних збитків фізичній особі може завдати кіберсталкінг, пов’язаний з викраденням та маніпуляцією цифровою особистістю жертви. Маючи контроль над цифровою особистістю цілі, кіберсталкер має можливість реалізувати усі інші методи кіберсталкінгу, такі як погрози, вимагання, наклеп, залякування, шантаж, тощо.

Викрадення особистості – це процес, при якому зловмисник використовує особисту ідентифікаційну інформацію іншої особи, як її ім’я, ідентифікаційний номер або номер кредитної картки, без її дозволу для вчинення шахрайства чи інших злочинів.

Кіберсталкери все частіше використовують комп’ютерні технології для отримання персональних даних інших людей для шахрайства. Щоб знайти таку інформацію, вони можуть здійснювати пошук на жорстких дисках викрадених або викинутих комп’ютерів, зламувати комп’ютери або комп’ютерні мережі,

отримувати доступ до комп'ютерних публічних записів, використовувати зловмисне програмне забезпечення для збору інформації та зараження комп’ютерів, переглядати сайти соціальних мереж або використовувати оманливі електронні листи чи текстові повідомлення.

Є кілька служб захисту від викрадення особистості, які допомагають людям уникати та пом’якшувати наслідки крадіжки особистих даних. Як правило, такі послуги надають інформацію, яка допомагає людям захищати свої особисті дані, відстежувати державні записи та приватні записи, такі як кредитні звіти, щоб попередити своїх клієнтів про певні операції та зміни статусу.

Ресурсний центр з викрадення особистих даних (Identity Theft Resource Center) виділяє п’ять основних типів викрадення особистості, які представлені у таблиці нижче.

Таблиця 2.1

Типи викрадення особистості згідно даним Identity Theft Resource Center

Кримінальне викрадення особистості	Використовується зловмисниками під час скоєння кримінальних дій задля приховання власних ідентифікаційних даних.
Фінансове викрадення особистості	Використання особистих даних іншої особи для отримання кредиту, товарів, послуг чи вигод. Це найпоширеніша форма викрадення особистості.
Клонування особистості	Вдавання себе за іншу реально існуючу (або існувавшу) особу у повсякденному житті для ухилення від будь-якої персональної відповідальності.
Медичне викрадення особистості	Використовується зловмисниками для здобуття безкоштовної медичної допомоги від страхових компаній.

Викрадення дитячої особистості	Використання особистості дитини для різних форм особистої вигоди. Діти часто не мають пов'язаної з ними інформації, яка могла б створити перешкоди для винного. Шахрай може використовувати дані дитини для отримання місця проживання, працевлаштування, позик або уникнення арешту за непогашеними ордерами.

У даній дипломній роботі було введено поняття «Викрадення цифрової особистості», яке означає викрадення мережевих облікових даних жертви задля отримання доступу до її персональних облікових записів в інтернеті з метою реалізації цілей кіберсталкінгу.

2.2 Основні методи викрадення цифрової особистості

Нижче наведено приклади основних методів та засобів, які використовують зловмисники для викрадення цифрової особистості жертви. Як було зазначено раніше, деякі з цих методів використовують кібершпигунство як основний інструмент отримання персональних даних жертви.

- Отримання персональних даних зі старого IT-обладнання та носіїв інформації, включаючи ПК, сервери, КПК, мобільні телефони, накопичувачі USB та жорсткі диски, які необережно утилізувались на загальнодоступних звалищах, віддавались або перепродавались без належної очистки.
- Загальновідомі схеми опитування, які пропонують перевірку облікового запису, наприклад, "Яке дівоче прізвище вашої матері?", "Якою була ваша перша модель автомобіля?" або "Як звали вашого першого улюбленця?".
- Shoulder-Surfing – це процес, під час якого особа непомітно спостерігає або чує, як інші надають цінну особисту інформацію. Це зазвичай робиться в місцях,

де багатолюдно, оскільки порівняно легко спостерігати за кимось, коли він заповнює форми, вводить PIN-коди в банкоматах або навіть паролі на смартфонах.

- Викрадення особистої інформації з комп'ютерів через використання порушень систем безпеки браузера чи шкідливих програм, таких як програми реєстрації натискань клавіш, Трояни або інші види шпигунського програмного забезпечення.
- Злом комп'ютерних мереж, систем та баз даних для отримання персональних даних, часто у великих кількостях.
- Використання інсайдерського доступу та зловживання правами привілейованих користувачів ІС на доступ до персональних даних у системах своїх роботодавців.
- Брутфорс атаки на слабкі паролі та використання натхненних здогадок для компрометації питань щодо скидання слабких паролів.
- Вдавання себе за жертву для обману людей, представників служби обслуговування клієнтів та працівників довідкової служби, щоб вони розкрили особисту інформацію та дані для входу або змінили паролі користувачів.
- Налагодження контакту з жертвою в соціальних мережах та користування їх довірою для отримання приватної інформації.
- Вдавання себе за довірені організації в електронних листах, текстових SMS-повідомленнях, телефонних дзвінках або інших формах спілкування, щоб обдурити жертв, розкриваючи їх особисту інформацію або дані для входу, як правило, на підробленому корпоративному веб-сайті або у формі збору даних.

2.3 Номер мобільного телефону як ключова цінність цифрової особистості

Будь-яка сучасна людина користується послугами мобільних операторів для отримання послуг стільникового зв'язку та мобільного інтернету. На сьогоднішній день майже усі інформаційні платформи надають можливість використовувати номер мобільного телефону як основний персональний ідентифікатор для входження у облікові записи користувачів. Більше того, велика кількість інтернет

сервісів та платформ надають можливість скидання паролів облікових записів за допомогою SMS-підтверджень.

Для цифрової особистості номер мобільного телефону – це аналог паспорту для реальної фізичної особи, оскільки це дуже зручний персональний ідентифікатор, він унікальний, та майже завжди доступ до нього можливий у будь-який час.

Істотна вада мобільного номеру телефону як унікального ідентифікатора полягає в тому, що ідентифікація особи – це не основна його функція. На момент створення, мобільні номери мали одну основну функцію – комунікаційну, вони використовувалися для дзвінків та коротких SMS-повідомлень, їх використання замість персональних ідентифікаторів розпочалося вже після поширення інтернету. Головна відмінність такого ідентифікатора від паспорта полягає в тому, що паспортні дані прийнято тримати в таємниці та пред'являти лише у регламентованих законом випадках, у той час як відношення до мобільного номеру телефону зазвичай більш вільне – це один з основних засобів комунікації, який має на меті поширення серед друзів, знайомих та організацій.

Таку двоїстість використання мобільних номерів можна вважати дуже сильною вразливістю інформаційної безпеки, оскільки отримавши контроль над мобільним номером, можна отримати майже необмежений контроль над цифровою особистістю.

Для доведення даного твердження було проведено опитування серед близького кола знайомих, та експериментально підтверджено вищезазначену позицію.

Опитування включало три питання:

1. Скільки мобільних номерів телефону ви маєте та активно використовуєте?
2. У випадку, якщо у вас два чи більше номерів – чи використовуєте ви різні номери для комунікації та ідентифікації у веб-просторі?
3. На вашому основному фінансовому номері встановлено контрактний чи передплатний тариф?

Як видно з графіків, наведених нижче, кількість осіб, які користуються одним номером телефону, приблизно дорівнює кількості осіб, які мають два або більше номерів, але більшість осіб з декількома номерами все одно використовують лише один номер як свій основний для комунікації і веб-ідентифікації.

Зі всіх опитаних, лише у 8-ми відсотків осіб були контрактні фінансові номери, а це означає, що інші 92 відсотки опитаних знаходяться під загрозою викрадення номеру телефону (а як наслідок – цифрової особистості) шляхом блокування номера оператором та відновлення його сторонньою особою.

Кількість опитаних осіб – 107. На ілюстрації нижче (Рисунок 2.1) зображено діаграми, які висвітлюють результати опитування.

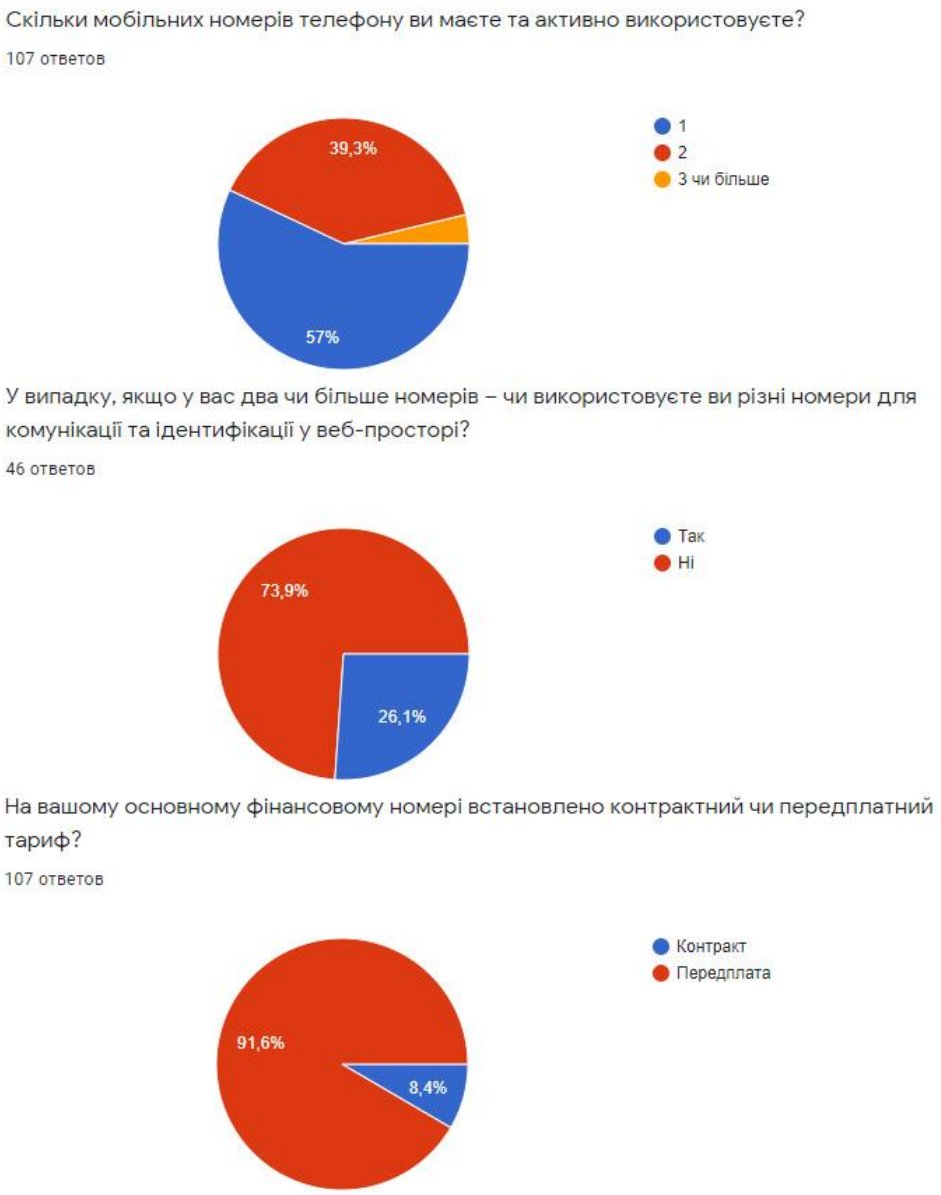


Рисунок 2.1 – діаграми з розподілом результатів опитування щодо користування мобільними номерами телефонів

2.4 Експериментальна перевірка методу викрадення цифрової особистості

Після отримання статистичних даних про користування мобільними номерами, була розпочата експериментальна частина дослідження: перевірка теорії про те, що отримавши контроль над номером телефону жертви, можна взяти повне управління її цифровою особистістю.

Для проведення експерименту було використано метод вдавання себе за жертву для обману представників служби обслуговування клієнтів. Нижче представлені кроки експерименту.

Підготовка:

1. Обрання цілі: було обрано особу з найближчого кола знайомих з відомим номером телефону.

2. Здобуття інформації про ціль та її оточення: за допомогою вищезгаданого опитування було визначено, що ціль користується двома мобільними номерами, але лише один з них основний та підключений до передплатного тарифного плану. Також методом спостереження було отримано інформацію про близькі контакти цілі, та здобуто номери телефонів двох її друзів.

3. Підготовка технічного обладнання: для проведення експерименту було використано окремий мобільний телефон з новою SIM-карткою.

Хід експерименту:

1. Протягом місяця з різними інтервалами на номер телефону жертви здійснювалися дзвінки від імені працівників університету, нібито для уточнення деталей щодо академічної успішності. Жертві також необхідно було передзвонювати на зазначений номер. Усього за час експерименту було здійснено 6 вихідних і 5 вхідних дзвінків.

2. Після завершення першого кроку експерименту, було розпочато ключовий момент атаки: був здійснений дзвінок до підтримки мобільного оператора

жертви та сказано, що мобільний телефон жертви було викрадено для того, щоб залишити заявку на блокування номеру. Під час того, як оператор підтримки попросив назвати викрадений номер – було названо номер жертви. Для того, щоб заблокувати номер, агент підтримки мобільного оператора попросив назвати 3 інших номера, на які здійснювалися вихідні та вхідні виклики. Мною було названо власний експериментальний номер, та номери двох друзів жертви. Цього виявилося достатньо для того, щоб заблокувати мобільний номер.

3. Наступним кроком був похід до центру обслуговування мобільного оператора, де була залишена заявка на відновлення SIM-карти з номером телефону жертви. Оператор знову попросив назвати 3 номери, на які здійснювалися вихідні та вхідні виклики, після чого було видано нову SIM-карту з номером жертви.

4. Вставивши отриману SIM-карту у старий телефон, мною був розпочатий процес викрадення цифрової особистості. Першим чином, було скинуто пароль до облікового запису жертви у Google. Для цього було необхідне лише SMS-підтвердження, яке було успішно отримано на SIM-карту з номером жертви. Увійшовши до даного облікового запису у браузері Google Chrome, усі дані браузера жертви були синхронізовані з моїм комп'ютером, у тому числі історія перегляду веб-сторінок, закладки та паролі (які мене цікавили найбільше).

5. Отримавши доступ до списку паролів, який зберігався у браузері жертви, було розпочато процес автентифікації до її облікових записів. У ході даного крока, вдалося отримати доступ до фінансового акаунту жертви у Privat24 та таких соціальних мереж як Telegram, Instagram і Twitter.

6. Було отримано можливість читати особисті листування жертви, завантажувати її приватні фотографії собі на комп'ютер, знімати кошти з її банківських рахунків та робити провокаційні дописи в соцмережах від її імені.

Висновок експерименту: гіпотеза про те, що здобуття контролю над мобільним номером телефону жертви є ключовим фактором для викрадення її цифрової особистості, підтвердилася. Маючи контроль над номером мобільного телефону жертви, зловмисники можуть отримати необмежений доступ до усіх її активів. Отримані у ході експерименту приватні дані жертви могли бути

використані для подальшого процесу кіберсталкінгу, який включає вимагання, шантаж, примус, тощо.

Після проведення даного експерименту стало зрозуміло, наскільки критичну роль відіграє мобільний номер телефону фізичної особи в розрізі її безпеки у кіберпросторі. Було доведено, що викрадення цифрової особистості – це найефективніший метод кіберсталкінгу, який необхідно упереджувати у першу чергу.

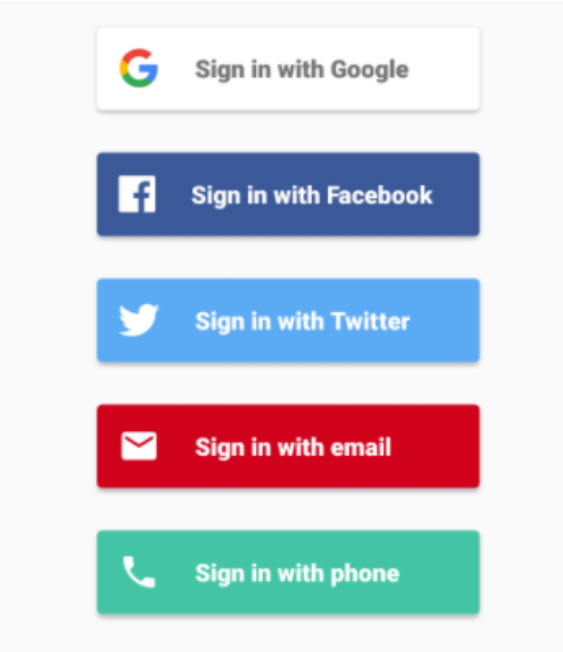
Представлений експеримент – це не єдиний спосіб отримання контролю над номером мобільного телефону особи. Кількість способів реалізації даної задачі обмежена лише фантазією та креативністю зловмисника. Іншими прикладами є викрадення фізичної SIM-карти з телефону жертви, приховане перехоплення SMS-сповіщень, підглядання верифікаційних номерів, тощо.

2.5 Огляд основних персональних ідентифікаторів цифрової особистості

Як було зазначено, номер мобільного телефону – це ключова цінність цифрової особистості, але існує безліч інших засобів та сервісів, які можуть виконувати роль персональних ідентифікаторів у кіберпросторі.

Другим за популярністю універсальним ідентифікатором є адреса електронної пошти. Спільна риса мобільного номеру телефону та адреси електронної пошти полягає у тому, що обидва ідентифікатори мають іншу основну функцію – комунікаційну, а отже надійність такого ідентифікатора є дуже сумнівною.

Останнім часом багато веб-сайтів та сервісів почали надавати можливість авторизації за допомогою акаунтів у соцмережах. Все частіше на веб-сайтах та платформах можна побачити кнопки Sign in with Google, Facebook, Twitter, тощо



(Рисунок 2.2).

Рисунок 2.2 – приклад опцій, які можуть використовуватися на веб-сайтах та веб-сервісах для авторизації користувачів

Дані засоби авторизації використовують протокол під назвою OAuth, який дозволяє надати третій стороні обмежений доступ до захищених ресурсів користувача без необхідності передавати їй (третій стороні) логін і пароль.

Зазвичай веб-сайти та веб-сервіси пропонують створити у них обліковий запис, для цього потрібно вказати ім’я користувача (логін) та зазначити електронну адресу, на яку вони можуть надіслати повідомлення-підтвердження – лише для того, щоб переконатися, що ви справжня людина. Використовуючи Google, Facebook, Twitter, або інший сервіс для входу, користувачі пропускають вищезазначену процедуру. Натомість вони покладаються на ці сервіси, щоб підтвердити свою особу та керувати обліковим записом. Важлива деталь полягає в тому, що веб-сайт чи веб-сервіс ніколи не отримує пароль користувача.

OAuth – це протокол авторизації, що дозволяє видати одному сервісу (або додатку) права на доступ до ресурсів користувача на іншому сервісі. Протокол позбавляє від необхідності довіряти сервісу або додатку логін і пароль користувача, а також дозволяє видавати обмежений набір прав, а не всі права відразу.

2.6 Дослідження вразливостей протоколу авторизації OAuth

OAuth – це стандарт, що знаходиться у процесі розвитку. Це означає, що його специфікація ще не усталилася і постійно змінюється (іноді досить помітно).

Безпека OAuth багато в чому заснована на SSL. Це сильно спрощує життя розробникам, але вимагає додаткових обчислювальних ресурсів і адміністрування. Це може бути суттєвим питанням в високо навантажених проектах.

Наразі чинним стандартом є OAuth 2.0, але деякі веб-сайти все ще використовують застарілу версію OAuth 1.0. OAuth 2.0 був написаний з нуля, а не розроблявся безпосередньо з OAuth 1.0. Як результат, ці два стандарти дуже різні. У даній роботі термін OAuth стосується виключно OAuth 2.0.

OAuth 2.0 спочатку був розроблений як спосіб спільного доступу до певних даних між програмами. Протокол працює, визначаючи серію взаємодій між трьома різними сторонами, а саме клієнтською програмою, власником ресурсу та постачальником послуг OAuth.

Клієнтська програма – веб-сайт або веб-сервіс, який хоче отримати доступ до даних користувача.

Власник ресурсу – користувач, до даних якого хоче отримати доступ клієнтська програма.

Постачальник послуг OAuth – веб-сайт або веб-сервіс, який контролює дані користувача та доступ до них. Вони підтримують OAuth, надаючи API для взаємодії як із сервером авторизації, так і з сервером ресурсів.

Існує безліч різних способів реалізації фактичного процесу OAuth. Вони відомі як «потоки OAuth» або «надання доступу/грантів». У даній дипломній роботі

розглянуто другий спосіб реалізації процесу OAuth, оскільки він є найпоширенішими. Загалом, надання доступу/грантів включає такі етапи:

1. Клієнтська програма вимагає доступ до підмножини даних користувача, вказуючи, який тип надання вона хоче використовувати і який доступ їй потрібен.

2. Користувачеві пропонується увійти до служби OAuth і чітко дати свою згоду на запитуваний доступ.

3. Клієнтська програма отримує унікальний маркер доступу, який підтверджує, що він має дозвіл від користувача на доступ до запитуваних даних.

4. Клієнтська програма використовує маркер доступу для здійснення викликів API для отримання відповідних даних із сервера ресурсів.

Автентифікація за допомогою OAuth зазвичай реалізується наступним чином:

1. Користувач вибирає можливість входу за допомогою свого акаунта в соціальних мережах. Потім клієнтська програма використовує службу OAuth сайту соціальних мереж для запиту доступу до деяких даних, які вона може використовувати для ідентифікації користувача. Наприклад, це може бути електронна адреса, зареєстрована в його обліковому записі.

2. Отримавши маркер доступу, клієнтська програма запитує ці дані від сервера ресурсів, як правило, від виділеної/кінцевої точки користувацької інформації.

3. Отримавши вищезазначені дані, клієнтська програма використовує їх замість імені користувача для входу. Маркер доступу, який програма отримує від сервера авторизації, часто використовується замість традиційного пароля.

Вразливості автентифікації OAuth частково виникають через те, що специфікація OAuth є відносно розмитою та гнучкою за дизайном. Хоча існує декілька обов’язкових компонентів, необхідних для базової функціональності кожного типу гранту, переважна більшість реалізацій є абсолютно необов’язковою. Сюди входить безліч налаштувань конфігурації, необхідних для захисту даних користувачів. Як висновок, виникає багато можливостей для виникнення вразливостей.

Однією з інших ключових проблем OAuth є загальна відсутність вбудованих функцій безпеки. Безпека майже повністю покладається на розробників, які використовують правильну комбінацію параметрів конфігурації та реалізують власні додаткові заходи безпеки, наприклад, надійну перевірку вводу. Розробникам систем, які реалізують методи автентифікації OAuth, досить легко помилитися, якщо у них немає досвіду роботи з даним протоколом.

Залежно від типу надання доступу, високочутливі дані також надсилаються через браузер, що представляє різні можливості для зловмисника перехопити їх.

Клієнтські програми часто використовують надійну, загартовану службу OAuth, яка добре захищена від широко відомих експлойтів. Однак їх власна сторона реалізації може бути менш безпечною.

Як вже було зазначено, специфікація OAuth є відносно розмитою. Особливо це стосується реалізації клієнтських програм. У потоці OAuth є багато рухомих частин, безліч необов'язкових параметрів і налаштувань конфігурації в кожному типі надання, що означає, що існує багато можливостей для неправильних конфігурацій.

Мабуть, найбільш сумнозвісною вразливістю, заснованою на OAuth, є та, що дозволяє зловмисникам красти коди авторизації або отримувати доступ до маркерів, пов'язаних з обліковими записами інших користувачів. Викравши дійсний код або маркер, зловмисник може отримати доступ до даних жертви. Зрештою, це може повністю скомпрометувати їх обліковий запис – зловмисник потенційно може увійти в систему як користувач-жертва в будь-якій клієнтській програмі, зареєстрованій у цій службі OAuth.

Залежно від типу надання, код або маркер надсилаються через браузер жертви до кінцевої точки, зазначеної в параметрі запиту авторизації. Якщо службі OAuth не вдається перевірити цей URI належним чином, зловмисник може створити атаку, подібну до CSRF, обманувши браузер жертви на ініціювання потоку OAuth, який надішле код або маркер контрольованому зловмисником Redirect URI.

На додаток до відкритих переадресацій, існують інші уразливості, які дозволяють витягти код або маркер і відправити його на зовнішній домен. Нижче наведені приклади таких вразливостей:

- Небезпечний JavaScript, який обробляє параметри запиту та фрагменти URL-адрес. Наприклад, незахищені сценарії обміну повідомленнями в Інтернеті можуть для цього чудово підходити. У деяких сценаріях зловмиснику може знадобитися довший ланцюжок гаджетів, які дозволяють передавати маркер через ряд сценаріїв, перш ніж врешті-решт відправити його у зовнішній домен.
- Уразливості XSS. Незважаючи на те, що атаки XSS можуть мати величезний вплив самі по собі, зазвичай існує невеликий часовий проміжок, коли зловмисник має доступ до сеансу користувача. Викравши код OAuth або маркер, зловмисник може отримати доступ до облікового запису користувача у власному браузері. Це дає йому набагато більше часу для вивчення даних користувача та здійснення шкідливих дій, значно збільшуючи ступінь вразливості XSS.
- Вразливості HTML-ін’єкцій. Якщо зловмисник зможе вказати параметр Redirect URI на сторінку з власним вмістом HTML, можливо, що він зможе отримати токен через заголовок Referer. Наприклад, розглянемо такий елемент img: <img src = "evil-user.net">. При спробі отримати це зображення деякі браузери (наприклад, Firefox) надішлють повну URL-адресу в заголовку Referer запиту, включаючи рядок запиту.

Також під час автентифікації користувачів за допомогою OAuth, клієнтська програма робить неявне припущення, що інформація, що зберігається постачальником OAuth, є достовірною. Це може бути небезпечним припущенням. Деякі веб-сайти, що надають послугу OAuth, дозволяють користувачам реєструвати обліковий запис, не перевіряючи всі свої дані, в деяких випадках включаючи адресу електронної пошти. Зловмисник може скористатися цим, зареєструвавши обліковий запис у постачальника OAuth, використовуючи ті самі дані, що і цільовий користувач, наприклад відому електронну адресу, після чого клієнтські програми можуть дозволити зловмиснику ввійти в систему як жертва.

Вплив вразливостей автентифікації може бути дуже серйозним. Як тільки зловмисник обійшов автентифікацію або ввійшов до облікового запису іншого користувача, він отримує доступ до всіх даних та функціональних можливостей, які має скомпрометований обліковий запис. Якщо зловмисник зможе зламати високопривілейований обліковий запис, наприклад, системного адміністратора, він може взяти повний контроль над усією програмою та потенційно отримати доступ до внутрішньої інфраструктури.

Навіть компрометуючи низькопривілейовані облікові записи, зловмисник може отримати доступ до даних, яких він не повинен мати, наприклад, до комерційно-конфіденційної ділової інформації. Навіть якщо обліковий запис не має доступу до будь-яких конфіденційних даних, він все одно може дозволити зловмисникові отримати доступ до додаткових сторінок, які забезпечують подальші рівні атаки. Часто певні атаки високої серйозності неможливі з загальнодоступних сторінок, але вони можуть бути можливі з внутрішньої сторінки.

Підбиваючи підсумки, можна сказати, що використання OAuth зовсім не є безпечним способом авторизації на веб-сайтах та веб-сервісах. Загалом, усі рішення, пов’язані з захистом персональних даних користувачів повністю покладаються на постачальника послуг OAuth. Отже, використовуючи кнопки Sign in with Google, Facebook, Twitter (та інші), користувачі повинні самі визначати, який рівень довіри вони мають до того чи іншого постачальника послуг OAuth, та наскільки добре вони захищені від спроб зламу своїх акаунтів на сайтах цих самих постачальників.

Висновки за розділом 2

У даному розділі було проведено ряд досліджень та отримано наступні практичні результати:

1. Проаналізовано методи викрадення особистості, у тому числі цифрової.

2. Проведено огляд основних персональних ідентифікаторів цифрової особистості та їх вразливостей.

3. Зібрано статистичні дані про користування мобільними номерами телефонів.

4. Проведено експеримент з використанням одного з методів викрадення цифрової особистості.

5. Доведено критичну важливість захисту мобільного номеру телефону у розрізі кіберсталкінгу.

6. Доведено, що викрадення цифрової особистості є найефективнішим методом кіберсталкінгу.

РОЗДІЛ 3
РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ВІД ТИПОВИХ МЕТОДІВ КІБЕРСТАЛКІНГУ

3.1 Формування вимог щодо переліку методів упередження та захисту від кіберсталкінгу

Спираючись на дослідження, проведені у попередніх розділах даної дипломної роботи, основною ціллю захисту від кіберсталкінгу повинна бути цифрова особистість фізичної особи, оскільки неправомірний контроль над нею є критичним інструментом для скоєння будь-яких злочинних дій.

Процес упередження кіберсталкінгу повинен включати наступне:

1. Мінімізація цифрового сліду фізичної особи.
2. Приховання критичних персональних відомостей про особу.
3. Обмеження можливостей витоку приватних облікових даних особи.
4. Запобігання типовим методам кібершпигунства.

Процес захисту від кіберсталкінгу повинен включати наступне:

1. Розпізнавання та швидке реагування на спроби кіберсталкінгу.
2. Перелік першочергових дій під час кіберсталкінгу.
3. Можливості державного регулювання спроб кіберсталкінгу.
4. Мінімізація збитків, заподіяних під час кіберсталкінгу.
5. Формування моделі поведінки, якої треба дотримуватися під час кіберсталкінгу.

3.2 Рекомендації щодо упередження кіберсталкінгу

Як було зазначено у попередніх розділах, зазвичай кіберсталкінгу передує процес кібершпигунства, під час якого зловмисник отримує необхідну особисту інформацію жертви, яку згодом він може використати для реалізації кіберсталкінгу.

- Першим кроком на шляху до захисту від кібершпигунства є мінімізація цифрового сліду. Це може бути важко для деяких людей, особливо для тих, хто потребує використання онлайн-платформ для самореклами чи діяльності, пов’язаної з бізнесом. Тим не менш, багато користувачів можуть отримати вигоду з того, щоб

трохи пом’якшити ситуацію. Необхідно завжди уникати розміщення особистих даних, таких як власна адреса та номер телефону.

- Хорошим способом протидії кібершпигунству є уникнення використання справжнього імені в онлайн-профілях. Хоча це важко для будь-яких питань, пов’язаних з роботою, це цілком можливо для таких речей, як форуми, дошки оголошень та певні акаунти в соціальних мережах. Наприклад, можна використовувати псевдонім в Instagram або Twitter.
- Якщо потрібно зберегти своє справжнє ім’я та фотографію, необхідно бути дуже обережними щодо того, від кого приймаються запити на з’єднання та повідомлення. Якщо це не друг, родич чи колега, треба зробити деякі перевірки, перш ніж рухатися вперед.
- У деяких випадках практично неможливо уникнути розголошення особистої інформації та зв’язку з незнайомими людьми, наприклад, на веб-сайтах знайомств. На жаль, вони популярні серед шахраїв, і це навіть може призвести до спілкування в чаті з потенційним кіберсталкером. З цієї причини найкраще дотримуватися авторитетних веб-сайтів, провести деякі дослідження щодо залицяльника, перш ніж розкривати особисту інформацію або зустрічатися особисто, і повідомляти адміністраторам сайту про будь-яку діяльність, яка викликає почуття дискомфорту.
- Чутливі приватні дані особи можуть знаходитись на ресурсах, які вона більше не використовує. Хорошою ідеєю є видалення профілів (або приватної інформації з них), які не були у користуванні більше двох місяців. У разі потреби завжди можна створити новий обліковий запис.
- Оновлення програмного забезпечення може бути не першим, що спадає на думку, коли мова йде про запобігання кібершпигунству. Однак регулярні оновлення програмного забезпечення мають вирішальне значення для запобігання витоку інформації. Багато оновлень розроблено для виправлення вразливих місць безпеки та забезпечення захисту вашої інформації. Це особливо важливо для мобільних пристроїв, які містять цінні дані та відстежують точне місцезнаходження особи.

- Багато програм та служб розкривають особисту IP-адресу людині, з якою ведеться спілкування. Це може здатися неважливим, але ця інформація безпосередньо пов'язана з персональними даними. Кіберсталкери можуть починати розвідку з IP-адреси цілі та використовувати її для пошуку даних кредитної картки та фізичної адреси.

Щоб замаскувати IP-адресу, можна використовувати віртуальну приватну мережу (VPN). Це приховує справжню IP-адресу та замінює її на інше вибране місце. VPN також шифрує весь інтернет-трафік, захищаючи його від сторонніх очей хакерів.

Інший варіант – використання браузера Tor. Він також шифрує трафік, хоча це може привернути увагу правоохоронних органів, оскільки даний браузер зазвичай використовують самі злочинці. Для максимальної конфіденційності та анонімності можна поєднати Tor та VPN. Не рекомендується використовувати веб-проксі або безкоштовну послугу VPN, оскільки це часто може нашкодити безпеці в Інтернеті більше, ніж допомогти їй.

- Необхідно підтримувати цифрову гігієну. «Цифрова гігієна» – це відносно новий термін, але він представляє дуже важливу тему, особливо щодо соціальних мереж. Забезпечення належної цифрової гігієни допомагає захиститися від переслідувань в Інтернеті, знущань та переслідування.

Налаштування параметрів конфіденційності – це один із перших кроків, який необхідно зробити, щоб «очистити» свої облікові записи. Більшість платформ соціальних медіа та деякі інші типи облікових записів в Інтернеті дозволять налаштувати, хто може бачити профіль і зв'язуватися з його власником.

- Також непогано закрити такі речі, як історії, публікації та повідомлення, від негативних коментарів. Окрім того, що вони можуть спричинити більше негативу з боку інших, вони можуть мати значний емоційний вплив, під час їх перечитування. Наприклад, психологічна підтримка регулярно надається модераторам веб-сайтів, оскільки вони серйозно страждають від читання агресивних повідомлень, навіть тих, які не надсилаються їм особисто.

- Необхідно уникати розкриття чутливої інформації. Багато людей постійно діляться особистою інформацією про себе: заповнюючи анкети або подаючи заявки на купони, люди збільшують ймовірність того, що хтось доторкнеться до їх особистих даних і, можливо, зроблять кіберсталкінг більш доступним. Не треба відчувати зобов'язання заповнювати всі поля під час реєстрації в Інтернеті або надавати ідентифікаційну інформацію, таку як дата народження та місце проживання в обов'язкових полях.
- Бажано створювати різні облікові записи електронної пошти для реєстрації на сайтах соціальних мереж та інших інтернет-просторах. Це допоможе уникнути спаму, і особиста електронна адреса не буде розкрита, якщо онлайн-служба не має належної практики конфіденційності.
- Якщо відбулося розлучення з інтимним партнером – особливо якщо він або вона жорстокі, неспокійні або злі – скиньте паролі усіх ваших облікових записів.
- Необхідно контролювати, яку інформацію розміщують родичі та друзі. Треба повідомити їх про занепокоєння щодо конфіденційності та допомогти їм захистити себе теж.
- Бажано регулярно виконувати пошук свого імені в інтернеті та стежити за тим, де ви з'являєтесь. Якщо було знайдено небажану інформацію про себе в мережі, необхідно зв'язатися з модератором веб-сайту та попросити її видалити.
- Номер мобільного телефону особи – це її найбільша цінність, коли мова йде про її цифрову особистість. Необхідно докласти максимум зусиль для того, щоб забезпечити надійний захист мобільного номера. По-перше, найкращий варіант – це використання різних номерів телефонів для комунікацій та для автентифікації на веб-ресурсах. Використовуйте один номер виключно для входження у ваші онлайн-профілі, не діліться ним, не виконуйте з нього дзвінки та не залишайте його на сайтах інтернет-магазинів. Відноситься до нього так, немов це ваш реальний паспорт.
- Обов'язково треба змінити пін-код SIM-карти зі стандартного на власний. Це допоможе уникнути ситуацій, коли при втраті телефону можна втратити ще й контроль над своєю цифровою особистістю.

- Багато мобільних операторів пропонують оформлення контрактного тарифу. Бажано скористатися даною послугою, адже це не дозволить злочинцям заблокувати та відновити номер мобільного телефону без вашої особистої присутності у відділі обслуговування клієнтів.
- Треба запам’ятати перелік типових контрольних питань для скидання паролей на веб-ресурсах, ці питання можуть задавати злочинці під час товариської бесіди на віддалені теми, тож необхідно уважно слідкувати за тим, що саме вас питають та завжди оцінювати питання відкидаючи контекст розмови.
- Не треба користуватися корпоративними комп’ютерами у особистих цілях та для зберігання особистої приватної інформації.
- Не бажано співпрацювати з організаціями, які мали прецеденти з розголошенням персональних даних своїх клієнтів без їх згоди.
- Бажано використовувати багатофакторну автентифікацію де це можливо.
- Не можна переходити за підозрілими посиланнями на незнайомих веб-сайтах та ні в якому разі не треба завантажувати або відкривати файли, які ви не мали намір здобути.
- Зберігати паролі у браузері можна тільки у тому випадку, якщо вони не синхронізуються між вашими пристроями шляхом входження у обліковий запис браузера.
- Необхідно регулярно видаляти листування, зміст яких вже не знадобиться.

Виконуючі усі вищезазначені рекомендації, особа може значно знизити ризик спроб кіберсталкінгу відносно неї. Варто пам’ятати, що технології швидко розвиваються, а разом з тим розвиваються і методи кіберсталкінгу, тож важливо завжди пам’ятати про те, що зловмисники ніколи не зможуть здобути з кіберпростору тільки ту персональну інформацію, якої там немає, тож треба уважно слідкувати за тим, яка інформація надсилається до глобальної мережі.

3.3 Рекомендації щодо захисту під час кіберсталкінгу

Стати жертвою кіберсталкінгу може кожен, але особливу категорію ризику складають медійні особи, політики, працівники великих корпорацій та володарі цінних активів. Чим більше ваших активів знаходиться у віртуальному просторі, тим значнішої шкоди ви можете зазнати під час кіберсталкінгу. Нижче представлені рекомендації щодо методів захисту під час кіберсталкінгу. Дані методи, крім заходів активної протидії, включають формування правильної психологічної моделі поведінки у критичних ситуаціях та настанови щодо мінімізації збитків після атаки.

Деякі види кіберсталкінгу не пов'язані з викраденням персональних даних, а мають на меті переслідування цілі у соцмережах, надмірну активність та спроби виявитися поміченим. Нижче представлено перелік рекомендацій, що стосуються даного виду кіберсталкінгу:

- Необхідно заблокувати профіль докучливого користувача, якщо людина вас сильно турбує своїми повідомленнями. Зазвичай веб-сервіси надають можливість заблокувати будь-кого. Ви припините отримувати повідомлення від цієї людини.
- Залиште скаргу на профіль користувача. Майже кожна платформа соціальних мереж дозволяє залишати скаргу на профіль. Якщо існує якийсь інший спосіб звітування, то вам слід також використовувати його.
- Подайте скаргу до поліції. Після того, як ви зробили перші два кроки, вам слід подати скаргу в поліцію. Якщо ви відчуваєте, що переслідувач може заподіяти вам шкоду, вам слід негайно повідомити про це охоронні служби. Можливо, ви не маєте багато інформації про сталкера. Однак після подання скарги ви отримаєте пораду щодо кращого вирішення ситуації.

Найбільш небезпечним методом кіберсталкінгу є викрадення цифрової особистості. Нижче приведений перелік пунктів, які допоможуть ідентифікувати спроби кіберсталкінгу, пов'язаного з викраденням цифрової особистості:

- Повідомлення про оплату кредитними або дебетовими картками товарів чи послуг, про які ви не знаєте, включаючи несанкціоноване зняття коштів з вашого рахунку.

- Дзвінки з відділу контролю за шахрайством стосовно кредитних або дебетових карток із попередженням про можливу підозрілу активність на рахунку вашої кредитної картки.
- Отримання інформації про те, що було проведено розслідування за кредитним балом. Вони часто робляться, коли подається заявка на позику або телефонну підписку.
- Деякі сервіси дозволяють переглядати історію автентифікації у ваші акаунти: наявність підозрілих спроб входу може свідчити про те, що ви стали ціллю кіберсталкерів.
- Серед ваших вихідних повідомлень у соцмережах та інших веб-сервісах з'явились ті, які ви не відсилали.
- У вашому списку контактів з'явились невідомі особи.
- Вам прийшло повідомлення про спробу скидання паролю від вашого облікового запису на будь-якому веб-порталі.
- Дзвінки від невідомих осіб з проханням передзвонити.
- Аномальна активність на ваших дописах у соцмережах.
- Ви отримуєте відкриті погрози, домагання, непристойні медіа-файли чи шантажуючі матеріали.

Нижче представлений перелік рекомендацій щодо того, як треба діяти в умовах явного зловмисного кіберсталкінгу та викрадення персональних даних:

- Якщо ви стали жертвою викрадення цифрової особистості – перше, що треба зробити, це докласти максимум зусиль для заспокоєння, адже паніка у даному випадку може призвести до необдуманих дій та наслідків.
- Змініть паролі до усіх веб-сервісів, до яких ви маєте доступ. У першу чергу зробіть це для вашої електронної пошти. Якщо зловмисник взяв контроль над вашими обліковими записами, якнайшвидше скористайтеся формами скидання паролю.
- Повідомте друзів та близьких про те, що відбулося. Попередьте їх не відповідати на будь-які повідомлення, відправлені з ваших акаунтів.

- Якщо діяльність кіберсталкера пов’язана з вашими фінансовими даними чи активами – негайно подзвоніть у банк та попросіть заблокувати ваші рахунки, після чого зверніться до поліції та повідомте їх про дану ситуацію.
- Якщо сталкер вступає у комунікацію з вами – зберігайте, записуйте або робіть скріншоти усіх повідомлень сталкера. Не редагуйте та не змінюйте їх жодним чином. Дані докази можуть допомогти у випадку долучення правоохоронних органів.
- Зберігайте записи про ваші зв’язки з адміністраторами веб-сервісів або працівниками правоохоронних органів, якщо ви повідомляєте владу про переслідувача. Ведення діловодства є надзвичайно важливим, тому зберігайте все, навіть якщо безпосереднім бажанням може бути видалення повідомлень сталкера та намагання забути про нього. Створіть резервну копію цих повідомлень на іншому комп’ютері, знімній картці пам'яті або зовнішньому жорсткому диску.
- Якщо мета кіберсталкінгу – це шантаж чи примус, то ні в якому разі не намагайтеся вступити в угоду зі сталкером чи платити викуп. Чим більше ви будете спілкуватися з ним, тим більше впливу та контролю він отримає над ситуацією. Насправді сталкери можуть сприймати ваші відповіді як ознаку того, що ви – легка жертва, яка дотримується їхніх вимог. Як тільки вони це знають, вони можуть висувати все більш агресивні вимоги. Заблокуйте акаунт сталкера та відправте на нього скаргу.
- Грайте на випередження. Якщо сталкер шантажує вас оприлюдненням приватних даних, таких як особисті фото- або відео-матеріали, листування, тощо – відразу зробіть публікації в усіх соціальних мережах про те, що ви стали жертвою кіберсталкера. Якщо приватні дані включають фото або відео інтимного характеру – вкажіть у дописі, що вас намагаються шантажувати підробленими матеріалами, це знизить соціальний вплив на вас у тому випадку, якщо ваші дані все ж таки будуть оприлюднені.
- Перевстановіть систему на вашому комп’ютері задля впевненості у тому, що атака кіберсталкера не була зумовлена активністю шкідливого ПЗ.

Після атаки необхідно мінімізувати збитки та привести свою цифрову особистість у належний стан. Якщо атака кіберсталкера стосувалася викрадення ваших активів, то правоохоронні органи повинні провести розслідування даної справи. Якщо ваші кошти були викрадені, але ви вчасно звернулися до банку та до поліції – висока вірогідність того, що ваші гроші вам повернуть, так як більшість банків має функцію реверсу транзакцій.

Що стосується оприлюднення приватних даних – то даний тип кіберсталкінгу може заподіяти значної шкоди психологічному стану жертви. Найкращим рішенням буде звернутися до спеціаліста у області психології, який допоможе пережити даний інцидент. Головне – пам'ятати про те, що життя продовжується та з часом дана ситуація стане просто спогадом.

Якщо ж репутації особи було заподіяно значної шкоди, що призвело до звільнення, втрати близьких контактів або руйнування інших важливих складових вашого життя – розумним рішенням буде зміна місця проживання на абсолютно нове та встановлення нових соціальних зв'язків.

3.4 Оцінка цінності розроблених рекомендацій

У даній дипломній роботі було проаналізовано велику кількість наукових джерел та викладено найбільш комплексну стратегію упередження та протидії кіберсталкінгу, розроблену згідно рішень до сучасних проблем кібербезпеки. Стратегія охоплює усі основні сфери діяльності людини у кіберпросторі та може використовуватися фізичними особами для захисту себе, своїх приватних даних та активів.

Частина розроблених рекомендацій була апробована під час проходження науково-дослідної практики на підприємстві. Втілення даних рекомендацій допомогло покращити рівень захищеності персональних даних працівників, ліквідувавши знайдені шляхи витоку цінної приватної інформації.

Висновки за розділом 3

У даному розділі було виконано наступну роботу:

1. Формування вимог, які стосуються рекомендацій щодо упередження та захисту від кібершпигунства та кіберсталкінгу.
2. Розробка рекомендацій щодо упередження та протидії різним сценаріям кіберсталкінгу.
3. Розробка інструкцій для формування правильної психологічної моделі при зіткненні з кіберсталкінгом.
4. Формування тактики мінімізації збитків, заподіяних кіберсталкінгом.

ВИСНОВКИ

У даній дипломній роботі було висвітлено процес дослідження та аналізу такого поняття як кіберсталкінг, його зв’язку з кібершпигунством. Були визначені основні цілі та методи кіберсталкінгу.

Було впроваджено новий термін – «цифрова особистість», та описаний її зв’язок з кіберсталкінгом. Було експериментально визначено, що найефективнішим методом кіберсталкінгу є викрадення цифрової особистості.

Спираючись на дослідження, проведені у даній роботі, було розроблено комплекс рекомендацій щодо упередження та захисту від кібершпигунства та кіберсталкінгу.

Розроблені рекомендації були апробовані під час науково-дослідної практики.

Таким чином можна зазначити, що усі задачі, сформовані у даній дипломній роботі, були виконані, що дало можливість досягнути поставленої мети.

Дослідження та розробки, викладені у даній роботі можна використовувати для поширення серед громадян України задля зниження рівня кримінальної активності у кіберпросторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Digital 2021. *We are social*: веб-сайт. URL: https://wearesocial.com/digital-2021

2. What Is Cyberstalking? *VeryWellMind*: веб-сайт. URL: https://www.verywellmind.com/what-is-cyberstalking-5181466

3. 2019 Cyberbullying Data. *Cyberbullying*: веб-сайт. URL: https://cyberbullying.org/2019-cyberbullying-data

4. Online harassment 2017. *Pew Research Center*: веб-сайт. URL: https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

5. Begotti T., Acquadro Maran D. Characteristics of cyberstalking behavior, consequences, and coping strategies: наукова робота, 2019. 120 с.

6. Short E., Linford S., Wheatcroft J. M., Maple C. The impact of cyberstalking: the lived experience - a thematic analysis: наукова робота, 2014. 199 с.

7. Increased time spent on media consumption due to the coronavirus outbreak among internet users worldwide as of March 2020, by country. *Statista*: веб-сайт. URL: statista.com/statistics/1106766/media-consumption-growth-coronavirus-worldwide-by-country/

8. Parenting Children in the Age of Screens. *Pew Research Center*: веб-сайт. URL: pewresearch.org/internet/2020/07/28/parenting-children-in-the-age-of-screens/

9. YouTube, Netflix and Gaming: A Look at What Kids Are Doing With Their Increased Screen Time. *Morning Consult*: веб-сайт. URL: morningconsult.com/2020/08/20/youtube-netflix-and-gaming-a-look-at-what-kids-are-doing-with-their-increased-screen-time/

10. U.S. internet users who have experienced cyber bullying 2020. *Statista*: веб-сайт. URL: statista.com/statistics/333942/us-internet-online-harassment-severity/

11. Stop Cyberbullying Before it Starts. *National Crime Prevention Council*: веб-сайт. URL: archive.ncpc.org/resources/files/pdf/bullying/cyberbullying.pdf

12. Tween Cyberbullying in 2020. *Cyberbullying Research Center*: веб-сайт. URL: i.cartoonnetwork.com/stop-bullying/pdfs/CN_Stop_Bullying_Cyber_Bullying_Report_9.30.20.pdf

13. *Wired Safety*: веб-сайт. URL: http://www.wiredsafety.org/cyberstalking_harassment/context.html

14. Alexis A. Moore. Cyberstalking and Women – Facts and Statistics. *About.com*: веб-сайт. 2009.

15. Bocij, Paul. Cyberstalking: Harassment in the Internet Age and how to Protect Your Family. Greenwood Publishing Group.

16. Ellison Louise, Akdeniz Yaman. Cyber-stalking: the Regulation of Harassment on the Internet" Criminal Law Review. December 1998 Special Edition: Crime, Criminal Justice and the Internet. 1998. 29–48 с.

17. Meloy, J. The Psychology of Stalking. Reid. Academic Press. 2009.

18. Mullen, Paul E., Pathé Michele; Purcell Rosemary. Stalkers and Their Victims. Cambridge University Press. 2009.

19. Hitchcock, J.A. Net Crimes & Misdemeanors: Outmaneuvering the Spammers, Swindlers, and Stalkers Who Are Targeting You Online. CyberAge Books. 2006.

20. "PDF article on Cyberstalking in the United Kingdom". Archived from the original PDF on March 15, 2007.

21. Crime Library: Cyberstalking. 2017.

22. Craig Lee and Patrick Lynch. Cyberstalking – Is it Covered by Current Anti-Stalking Laws? 2009.

23. *Identity Theft Resource Center*: веб-сайт. URL: idtheftcenter.org.

24. Medical Identity Theft: What to Do if You are a Victim. World Privacy Forum.

25. Identity Theft Reported by Households. Bureau of Justice Statistics. 2011.

26. Ahlgrim and Terrance, B. Ahlgrim, C. Terrance, Perceptions of cyberstalking: impact of perpetrator gender and Cyberstalker/victim relationship, J. Interpers. Violenc. 2018.

27. G. Vaia, W.H. DeLone, M. Waheed, Two decades of research on business intelligence system adoption, utilization and success: наукова робота. 2019.

28. Cattaneo, L., Cho, S., & Botuck, S. Describing intimate partner stalking over time. Journal of Interpersonal Violence. 2011.

29. Cox, L., & Speziale, B. Survivors of stalking. 2009.

30. Fox, R. Someone to watch over us: Criminology and Criminal Justice. 2001.

31. Harrison, C. Cyberspace and child abuse images. 2006.

32. Henson, B., Reyns, B. W., & Fisher, B. S. Security in the 21st century. Criminal Justice. 2011.

33. Kamphuis, J. H., & Emmelkamp, P. M. G. 20 years of research into violence and trauma. Journal of Interpersonal Violence. 2005.

34. Kohm, S. A., & Greenhill, P. Pedophile crime films as popular criminology: A problem of justice? Theoretical Criminology. 2011.

35. Logan, T., & Walker, R. Partner stalking. Trauma, Violence, & Abuse. 2009.

36. Marcum, C. D., Ricketts, M. L., & Higgins, G. E. Assessing sex experiences of online victimization: An examination of adolescent online behaviors using routine activity theory. Criminal Justice Review. 2010.

37. Miller, S. L., & Smolter, N. L. "Paper abuse": When all else fails, batterers use procedural stalking. Violence against Women. 2011.

38. Mitchell, K. J., Wolak, J., & Finkelhor, D. Police posing as juveniles online to catch sex offenders: Is it working? Sexual Abuse: A Journal of Research and Treatment. 2005.

39. Peak, K. J., Barthe, E. P., & Garcia, A. Campus policing in America. Police Quarterly. 2008.

40. Prins, H. Mental disorder and violent crime: A problematic relationship. Probation Journal. 2005.

41. Reyns, B. W., Henson, B., & Fisher, B. S. Being pursued online: Applying cyberlifestyle – routine activities theory to cyberstalking victimization. Criminal Justice and Behavior. 2011.

42. Southworth, C., Finn, J., Dawson, S., Fraser, C., & Tucker, S. Intimate partner violence, technology, and stalking. Violence against Women. 2007.

43. Spitzberg, B. H. The tactical topography of stalking victimization and management. Trauma, Violence, & Abuse. 2002.

44. Van Wilsem, J. Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. European Journal of Criminology. 2011.

45. Wykes, M. Constructing crime: Culture, stalking, celebrity and cyber. Crime, Media, Culture. 2007.

46. P. Bocij. "Corporate cyberstalking: An invitation to build theory,". 2002.

47. P. Bocij and L. McFarlane. "Online harassment: Towards a definition of cyberstalking,". 2002.

48. P. Bocij and L. McFarlane. "Cyberstalking: Genuine problem or public hysteria?" Prison Service Journal. 2002.

49. P. Bocij, M. Griffiths and L. McFarlane. "Cyberstalking: A new challenge for criminal law," Criminal Lawyer. 2002.

50. T. Budd, J. Mattinson and A. Myhill. The extent and nature of stalking: Findings from the 1998 British Crime Survey. London: Home Office Research, Development and Statistics Directorate, U.K. 2000.

51. W.A. Burgess and T. Baker. "Cyberstalking," In: J. Boon and L. Sheridan (editors). Stalking and psychosexual obsession: Psychological perspectives for prevention, policing and treatment. 2002.

52. L. Cohen, L. Manion and K. Morrison. Research methods in education. Fifth edition. London: Routledge Falmer. 2000.

53. A. Cooper, C. Scherer and R. Mathy. "Overcoming methodological concerns in the investigation of online sexual activities," CyberPsychology and Behaviour. 2001.

54. D. Dillman, R. Tortora and D. Bowker. "Principles for constructing Web surveys,". 1999.

55. D. Dillman, R. Tortora, J. Conradt and D. Bowker. "Influence of plain vs. fancy design on response rates for Web surveys,". 1998.

56. J.H. Kamphuis and P.M.G. Emmelkamp. "Stalking: A contemporary challenge for forensic and clinical psychiatry," British Journal of Psychiatry. 2000.

57. L. McFarlane and P. Bocij, forthcoming. "Cyberstalking: Defining the invasion of cyberspace," Forensic Update.

58. M. McGrath and E. Casey. "Forensic psychiatry and the Internet: Practical perspectives on sexual predators and obsessional harassers in cyberspace," Journal of the American Academy of Psychiatry and the Law. 2002.

59. J.R. Meloy. "Stalking: An old behavior, a new crime," Forensic Psychiatry. 1999.

60. J.R. Meloy (editor). The psychology of stalking: Clinical and forensic perspectives. London: Academic Press. 1998.

61. P. Mullen, M. Pathé and R. Purcell. Stalkers and their victims. Cambridge: Cambridge University Press. 2000.

62. E. Mustaine and R. Tewksbury. "A routine activity theory explanation for women's stalking victimization," Violence Against Women. 1998.

63. M. Pathé and P. Mullen. "The impact of stalkers on their victims," British Journal of Psychiatry. 1997.

64. W. Petherick. "Cyber-stalking: Obsessional pursuit and the digital criminal". 1999.

65. R. Purcell, M. Pathé and P. Mullen. "The prevalence and nature of stalking in the Australian community," Australian and New Zealand Journal of Psychiatry. 2002.

66. J. Reno. "Cyberstalking: A new challenge for law enforcement and industry". 1999.

67. R. Saunders. "The legal perspective on stalking," In: J.R. Meloy (editor). The psychology of stalking: Clinical and forensic perspectives. 1998.

68. L. Sheridan, G. Davies and J. Boon. "The course and nature of stalking: A victim perspective," Howard Journal. 2002.

69. B.H. Spitzberg and G. Hoobler. "Cyberstalking and the technologies of interpersonal terrorism," New Media and Society. 2002.

70. D. Thomas and B. Loader (editors). Cybercrime: Law enforcement, security and surveillance in the information age. London: Routledge. 2000.