Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Технологія впливу соціальних мереж на забезпечення інформаційної безпеки.

Виконав: студент 6 курсу, групи СБм-62
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) *Турчиняк М.А.* (прізвище та ініціали)

Керівник (підпис) *Скарга-Бандурова І.С.* (прізвище та ініціали)

Нормоконтроль (підпис) *Лобур Т.Б.* (прізвище та ініціали)

Завідувач кафедри (підпис) *Загородна Н.В.* (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль
2022

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н. В.
(підпис) (прізвище та ініціали)
«____» _____ 2022 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр
(назва освітнього ступеня)

за спеціальністю 125 кібербезпека
(шифр і назва спеціальності)

студенту Турчиняку Мирону Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Технологія впливу соціальних мереж на забезпечення інформаційної безпеки.
Керівник роботи Скарга-Бандурова Інна Сергіївна, докт. техн. наук, професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «___» _____ 20__ року № _____

2. Термін подання студентом завершеної роботи _____

3. Вихідні дані до роботи _____

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. РОЗДІЛ 1. Аналіз особливостей соціальних мереж та потенційних загроз інформаційній безпеці. 1.1 Соціальна мережа як феномен сучасного цифрового суспільства. 1.2 Огляд сучасних соціальних мереж та загроз інформаційній безпеці.1.3 Ландшафт загроз. РОЗДІЛ 2. Технології підвищення інформаційної безпеки та боротьби з дезінформацією. 2.1 Технології боротьби з кожним із впливів. 2.2 Роль штучного інтелекту (ШІ) у просуванні та потенційній боротьбі з дезінформацією. РОЗДІЛ 3. Рекомендації щодо забезпечення інформаційної безпеки. 3.1 Правила безпеки для користувачів соціальних мереж. 3.2 Автоматизовані інструменти для користувачів соціальних мереж. 3.3 Рекомендації щодо інституційних змін в організаціях та країнах. РОЗДІЛ 4. Охорона праці та безпека в надзвочайних ситуаціях. 4.1 Охорона праці. 4.2 Фактори, що впливають на функціональний стан користувачів комп'ютерів. Висновки. Перелік використаних джерел

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Галина Михайлівна, к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик Василь Михайлович, старший викладач		

7. Дата видачі завдання 14 листопада 2022р

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Аналіз предметної галузі	15.09.2022	Виконано
2	Огляд існуючих методів	24.09.2022	Виконано
3	Основна частина	09.10.2022	Виконано
4	Підготовка пояснювальної записки	19.11.2022	Виконано
5	Спецчастина	24.11.2022	Виконано
6	Підготовка презентації та доповіді	27.11.2022	Виконано
7	Попередній захист	29.11.2022	Виконано
8	Нормоконтроль, рецензування	14.12.2022	Виконано
9	Занесення диплома в електронний архів	20.12.2022	Виконано
10	Допуск до захисту у зав. кафедри	21.12.2022	Виконано
11	Захист кваліфікаційної роботи	22.12.2002	Виконано

Студент _____ Турчиняк М.А.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Скарга-Бандурова І.С.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Технологія впливу соціальних мереж на забезпечення інформаційної безпеки.// Турчиняк Мирон Андрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем та програмної інженерії, кафедра кібербезпеки, група СБм–62 // Тернопіль, 2022 // с. - 64, рис. -3, бібліогр. – 25.

Ключові слова: ІНТЕРНЕТ-ЗАГРОЗА, СОЦІАЛЬНІ МЕРЕЖІ, ДЖЕРЕЛО ЗАГРОЗИ, TWITTER, FACEBOOK,LINKEDIN,TELEGRAM, ВРАЗЛИВОСТІ СОЦ. МЕРЕЖ.

Кваліфікаційна робота присвячена дослідженню технології впливу соціальних мереж на забезпечення інформаційної безпеки на основі аналізу вразливостей соціальних мереж. В роботі проведений аналіз чотирьох популярних соціальних мереж, на підставі якого виявлено їхні вразливості. Розглянуто методи захисту облікових записів користувачів, які вирішують задачу виявлення та захисту користувача від виявлених вразливостей.

ANNOTATION

The technology of the influence of social networks on ensuring information security.// Myron Andriyovych Turchynyak // Ivan Pulyuy Ternopil National Technical University, Faculty of Computer and Information Systems and Software Engineering, Department of Cyber Security, SBm-62 group // Ternopil, 2022 // p . - 64, fig. -3, bibliography - 25.

Keywords: INTERNET THREAT, SOCIAL NETWORKS, SOURCE OF THREAT, TWITTER, FACEBOOK, LINKEDIN, TELEGRAM, SOCIAL VULNERABILITIES. NETWORK

The qualification work is devoted to the study of the influence of technology of social networks on ensuring information security based on the analysis of vulnerabilities of social networks. In the work, an analysis of four popular social networks was carried out, on the basis of which their vulnerabilities were identified. The methods of protecting user accounts, which solve the problem of detecting and protecting the user from detected vulnerabilities, are considered.

ЗМІСТ

ВСТУП

Науково-технічна революція початку XXI сторіччя спричинила в усьому світі глибокі системні перетворення. Передусім завдяки поєднанню досягнень у сфері новітніх інформаційно-комунікаційних технологій (ІКТ) із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем (ІТС), сформувалися принципово нові глобальні субстанції — інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу. Зі збільшенням доступності Інтернету і стрімкого розвитку засобів комунікації, потреби в доступності до інформаційно-телекомунікаційних ресурсів, незалежно від місця їх надходження, постійно зростають. Тому цілком природно постала необхідність контролю та подальшого врегулювання відповідних ресурсів, а отже, і невідкладного створення надійної системи кібернетичної безпеки. Натомість відсутність такої системи може призвести до втрати політичної незалежності будь-якої держави світу, бо йтиметься про фактичний програш нею змагання невійськовими засобами та підпорядкування її національних інтересів інтересам протиборчої сторони. Оскільки саме ці обставини відіграють останнім часом важливу роль у геополітичній конкуренції більшості країн світу, то забезпечення кібербезпеки та злагоди в кіберпросторі стає головним завданням нашої інформаційної епохи.

РОЗДІЛ 1. АНАЛІЗ ОСОБЛИВОСТЕЙ СОЦІАЛЬНИХ МЕРЕЖ ТА ПОТЕНЦІЙНИХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

1.1 Соціальна мережа як феномен сучасного цифрового суспільства

Сьогодні соціальні медіа та мережі онлайн стали невід'ємною частиною життя кожного. Соціальна мережа – це практика розширення контакту з іншими особами здебільшого через сайти соціальних медіа, такі як Facebook, Twitter, Instagram, LinkedIn та багато інших. Її можна використовувати як для особистих, так і для ділових цілей. Це об'єднує людей, щоб поговорити, поділитися ідеями та інтересами та знайти нових друзів. По суті, це допомагає людям із різних географічних регіонів співпрацювати.

Платформи соціальних мереж завжди вважалися простими у використанні. Саме тому популярність і чисельність соціальних мереж зростає в геометричній прогресії. На рис.1 показано основні складові соціальних мереж і сфери, в яких вони відіграють важливу роль.

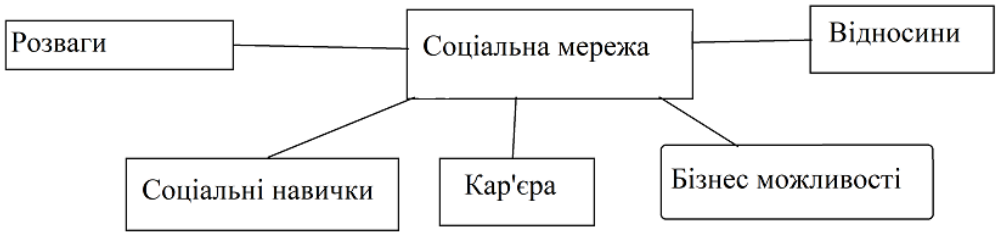

Рисунок 1 – Складові онлайн соціальних мереж

Як показано на рис.1, соціальні мережі можна використовувати для розваг, створення можливостей для бізнесу, створення кар'єри, вдосконалення своїх соціальних навичок і налагодження стосунків з іншими людьми. Facebook і Twitter є одними з найбільш улюблених сайтів

соціальних мереж. Оскільки значна частина користувачів Інтернету використовує платформу соціальних мереж, вона стала важливим засобом просування бізнесу та кампанії поінформованості.

Із зростанням репутації цих соціальних сайтів зростають і ризики їх використання. Вільне спілкування не є безкоштовним. Зменшивши вартість інформації, ми знизили її цінність і сприяли її фальсифікації. Щоб відновити здоров'я нашої інформаційної екосистеми, необхідно зрозуміти вразливі місця перевантаженого розуму та те, як можна використати економіку інформації, щоб захистити людей від введення в оману.

1.2 Огляд сучасних соціальних мереж та загроз інформаційній безпеці

Загрози інформаційної безпеки можуть бути класифіковані за різними ознаками:

- За аспектом інформаційної безпеки, на який спрямовані загрози:
- Загрози конфіденційності (неправомірний доступ до інформації).
- Загрози цілісності[1] (неправомірна зміна даних).
- Загрози доступності (дії, які дозволяють неправомірний доступ до ресурсів інформаційної системи).

Згідно матеріалів The New York Post щодня лише у Facebook зламують 160 000 облікових записів, а дослідники Університету Фенікса що близько 66% облікових записів громадян США було хоч раз зламано (це означає, що якщо ви знаєте ім'я собаки свого менеджера соціальних мереж, ви на півдорозі до брут форсінгу облікового запису вашої організації). На відміну від інших активів, служби безпеки не можуть відключити зламаний обліковий запис у соціальних мережах, тобто зловмисник може зберігати

контроль протягом годин, якщо не днів. Вартість? Кожна секунда, коли ви не контролюєте свій обліковий запис, спричиняє каскад вірусної інформації, що призводить до шкоди стосункам із брендом і клієнтом, втрати бізнесу, кошмарів зі зв'язків із громадськістю та витрат на підтримку клієнтів.

Використання «соціальної тактики» в глобальних кібератаках почало зростати в 2010 році, а самі атаки в соціальних мережах стрімко зросли в останні роки. До них належать:

- фішинг,
- викрадення особистих даних,
- розповсюдження зловмисного програмного забезпечення,
- соціальна інженерія та компрометація облікових даних банківського або системного входу.

Експерти з безпеки погоджуються: за даними Northon[8], лише 1 із 10 співробітників відкриває небажаний електронний лист, але майже третина працівників приймає небажані запити друзів у соціальних мережах. McAfee повідомляє, що співробітники частіше стикаються з кіберзлочинністю в соціальних мережах, ніж на будь-якій іншій бізнес-платформі, включаючи електронну пошту та обмін файлами.

Річний звіт Cisco[9] про безпеку за 2016 рік показав, що Facebook зараз є найпоширенішим способом зламу вашої мережі. Згідно зі звітом PandaSecurity[10], 20% підприємств заражаються шкідливим програмним забезпеченням безпосередньо через соціальні мережі. Дослідження TrendMicro показують, що 5,8% твітів є шкідливими; це 29 000 000 шкідливих твітів на день. На початку 2017 року журнал TIME виявив, що 10 000 службовців уряду США отримали зловмисне програмне забезпечення у спеціалізованих твітах, надісланих російським агентом. Зловмисне програмне забезпечення, зокрема HAMMERTOSS і ZeuS, використовує соціальні мережі як C&C або для масового розповсюдження.

Список можна продовжувати нескінченно. Ці ризики можуть мати значні фінансові наслідки. Згідно з даними Kaspersky, глобальна річна вартість фішингових атак у соціальних мережах становить 1,2 мільярда доларів. За оцінками ZeroFox, лише фінансові афери, виявлені в Instagram, обходяться брендам приблизно в 420 мільйонів доларів щороку. За один рік Міністерство юстиції США підрахувало 17,5 мільйонів людей, особисті дані яких викрали кіберзлочинці в Інтернеті. 90% респондентів нещодавнього опитування Symantec[12] повідомили, що середня вартість організації інциденту в соціальних мережах становить неймовірні 3 588 611 доларів США. Зрештою, соціальні медіа знижують бар'єр доступу для кожного зловмисника — навіть недосвідчений зловмисник може створити підроблену онлайн-персону, знайти цілі та поширити шкідливе програмне забезпечення чи фішингове посилання мільярдам людей по всьому світу. Найгірше те, що цілі ще ніколи не були численнішими чи більш довірливими.

Багато нападників координують свої зусилля серед білого дня. Відомо, що атаки розподіленої відмови в обслуговуванні (DDoS) використовують певний хештег Twitter для координації атаки. Зловмисники, особливо хактивісти, краудсорсингують учасників атак через кампанії з хештегами та керують DDoS-атакою в Twitter, публікуючи IP-адреси, домени, інструменти атаки, час атаки та бажану ціль. Оскільки атаки використовують громадські місця для участі, команди безпеки можуть підготувати стратегію захисту, наприклад, ховати вхідні запити або координувати дії з мережевими командами, професійними службами та постачальниками послуг Інтернету (ISP). Команди безпеки також можуть стежити за розмовами учасників загрози, щоб виявити, чи згадується їх організація. Це одні з найчистіших, найдешевших, найактивніших і доступних у реальному часі даних про загрози. Дивно, але така публічна балаканина досить поширена. Аналізуючи, хто говорить і контекст

ключової фрази, служби безпеки можуть отримати вирішальну систему раннього попередження проти атак. Зловмисники часто афішують або хваляться своїми успіхами в соціальних мережах. Вони також рекламують викрадені дані, які можуть продавати. Подібно до того, як соціальні медіа є основною рушійною силою діяльності легального ринку, ними також користуються продавці на чорному ринку. Організації можуть інтегрувати конфіденційну інформацію, виявлену на сайтах соціальних мереж, у фреймворки DLP, щоб швидше визначати, коли стався злом, і ефективніше починати дії з усунення. Витоку або викрадених даних частіше торгують у відкритому доступі, ніж усвідомлюють. Якщо облікові дані співробітників або конфіденційні файли виявлені в соціальних мережах або цифрових каналах, наприклад на сайтах вставлення, служби безпеки можуть оновити тренінги компанії, скинути облікові дані співробітників або відстежити, де заходи запобігання потенційній втраті даних (DLP) не змогли запобігти конфіденційним файлам, таким як медичні записи, інтелектуальну власність або інформацію облікового запису від виходу з мережі.

Методи безпеки можуть зменшити інші бізнес-ризики соціальних медіа

Соціальні медіа також можуть викликати головний біль в інших частинах організації. Ці бізнес-ризики можуть зашкодити організації, наприклад :

- викрадення хештегів,
- видавання себе за іншу компанію,
- шахрайство клієнтів (загальні річні витрати становлять майже 4 мільярди доларів США),
- підписники ботів,
- контрафактні товари,
- рекламне шахрайство,

- онлайн-піратство (загальні річні витрати становлять понад 70 мільярдів доларів США),
- тролі,
- фальшиві представники служби підтримки клієнтів,
- фізичні погрози тощо.

Для шахрая соціальні медіа є новим потужним інструментом для використання дуже специфічної масової групи користувачів, наприклад підписників певного бренду. Соціальні мережі дозволяють шахраям націлюватися на цих користувачів, оскільки списки підписників бренду та залучення користувачів до фірмового хештегу є загальнодоступними. Таким чином, шахрай має безпрецедентну можливість отримати список жертв і розпочати цілеспрямовану атаку. Шахрайство, орієнтоване на клієнтів, зазвичай обіцяючи винагороду за певну вартість участі та використовує фальшиві логотипи бренду або історії успіху з інших облікових записів маріонеткових учасників, які вказують на те, що шахрайство є «законним». Ці шахрайства процвітають у соціальних мережах, тому що їх дуже легко створити та поширювати серед цільової аудиторії у великих масштабах. Навіть нетехнічний шахрай може створити групу фальшивих облікових записів, створених для коментування один одного та надання довіри, маючи лише підключення до Інтернету з будь-якої точки світу.

Використовуючи методи для виявлення та пом’якшення ризиків інформаційної безпеки, групи безпеки можуть допомогти у вирішенні різноманітних загроз, які охоплюють інформаційну безпеку, фізичну корпоративну безпеку, дотримання вимог, отримання прибутку та маркетинг. Постійно відстежуючи соціальні медіа на наявність зловмисних дій, служби безпеки та маркетингу можуть ідентифікувати профілі, що рекламують піратський вміст або контрафактні товари, заощаджуючи таким чином організації потенційно мільйони втрачених доходів. Це чудова

можливість для команд служби безпеки вийти за рамки блокування активів і зміцнення стін, надавши можливість іншим відділам виконувати свою роботу безпечніше та ефективніше. Крім того, фінансова вигода відразу відчутна та піддається кількісному виміру.

Соціальні медіа є неминучою константою для ведення бізнесу в сучасному світі. Оскільки маркетологи, рекрутери, продавці та рекламодавці постійно розширюють свою присутність, групи безпеки повинні працювати разом з ними, щоб гарантувати, що це робиться безпечно та надійно. Щоб усунути ризики соціальних мереж, служби безпеки повинні тісно співпрацювати з кількома іншими відділами. Усі інші департаменти стикаються з ризиками в соціальних мережах, і тепер командам безпеки доручено усунути ризики, одночасно забезпечуючи безпечне використання каналів соціальних мереж. Найголовніше, що команди безпеки повинні очолити цю ініціативу. Ризики в соціальних мережах залишаються.

ДЕЗІНФОРМАЦІЯ – спотворена, свідомо неправдива, провокаційно-тенденційна інформація, поширена як правдива з метою введення в оману громадськості, політичних опонентів, конкурентів тощо. Дезінформацією також називають сам процес поширення у соц мережах чи у інших середовищах викривлених або свідомо неправдивих відомостей. Так, за доби рад. тоталітаризму стала складовою державно-політичної стратегії СРСР. Щоб приховати реалії внутрішнього і світового розвитку та утримувати народ в інформаційному вакуумі.

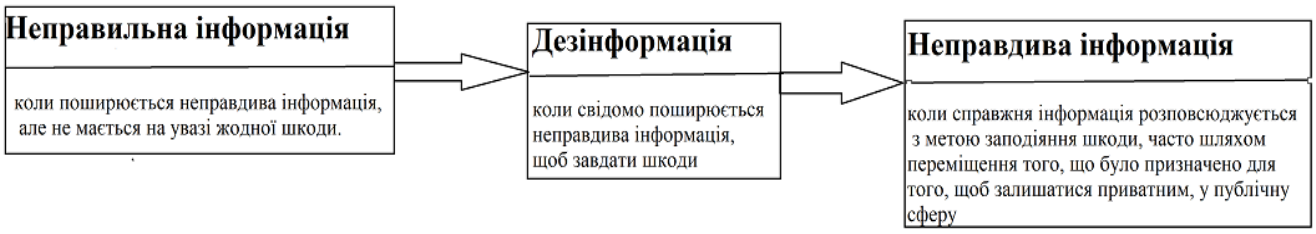

Рис. 2 - види інформації

Види дезінформації:

- введення в оману конкретної особи чи групи людей (навіть цілої нації);
- маніпулювання;
- Клікбейт;
- створення потрібної громадської думки.

У сучасній соціальній психології проблема дезінформації розглядається переважно у зв'язку свідченнями свідків, ставленням до соціально значимих проблем (таким, як ризики вакцинації, використання ГМО, міжетнічні конфлікти), а також у зв'язку з іншими загрозами: тероризмом, екстремізмом, гібридними війнами, стихійними лихами. Одиницею аналізу є в основному індивіди, які виступали як дезінформатори або об'єкти дезінформування як у реальному спілкуванні, так і за допомогою комунікаційних технологій (Мережі, Інтернет, СМЯ). Дослідження, в яких використовується груповий рівень аналізу, поки що вкрай нечисленні.

У вітчизняній соціальній психології можна виділити кілька перспективних підходів до вивчення дезінформації: по-перше, дослідження впливу дезінформації на міжособистісне спілкування [7]; по-друге, вивчення впливу дезінформації на групові захисні механізми, у тому числі на механізми захисту позитивної групової ідентичності; по-третє, дослідження динаміки колективних переживань у процесі впливу СМЯ на масову свідомість .

Ставлення особистості до дезінформації у соціальних мережах тісно пов'язано з особливостями антиципації, переживання та осмислення інтернет-спільнотою спільної діяльності представників своєї та чужих груп, спрямованої на створення, використання або запобігання дезінформації.

У структурі ставлення особистості до дезінформації виділяються когнітивні, емоційно-оціночні, ціннісно-смислові та поведінкові компоненти.

Когнітивні компоненти включають:

- оцінку частоти використання дезінформації у ЗМІ та соціальних мережах;
- Уявлення про джерела дезінформації;
- уявлення про цілі дезінформації;
- Уявлення про способи реалізації дезінформації;
- Уявлення про зв'язки з іншими ризиками;
- уявлення про засоби захисту від дезінформації;
- Уявлення про способи протидії на рівні держави, організацій;
- уявлення про очікувані та фактичні наслідки використання дезінформації;
- уявлення про тих, хто може використати наслідки дезінформації у своїх цілях.

Емоційно-оціночні компоненти включають:

- значимість загрози дезінформації в порівнянні з іншими видами загроз;
- Оцінку використання брехні в ЗМІ;
- Оцінку джерел дезінформації.

Цінно-смислові компоненти включають:

- Допустимість використання дезінформації;
- цінності, яким суперечить використання дезінформації та цінності, якими виправдовується використання дезінформації.

Поведінкові компоненти включають:

- відмінні способи реагування на дезінформацію;

- Готовність особистими діями підтримати громадські та державні ініціативи, спрямовані на боротьбу з дезінформацією;
- Швидкість реагування на дезінформацію;
- готовність обговорювати дезінформацію з іншими людьми.

Ставлення особистості[7] до дезінформації тісно пов'язане з психологічними механізмами, серед яких на внутрішньо-особистісному рівні виділяються: ціннісні орієнтації, соціальна довіра, рівень тривожності, обсяг соціального капіталу, соціальна ідентичність.

1.2.1 LinkedIn

LinkedIn (lɪŋktɪn) — соц. мережа для знаходження нових робочих контактів та зв'язків. У LinkedIn створено більше 774 мільйонів акаунтів (станом на 2021р.), які охоплюють 150 різноматних видів бізнесу близько 200 країн. Є великий вибір мов інтерефейсу включаючи українську, іспанську, португальську, італійську, німецьку, французьку, англійську та інші мови.

Мережа LinkedIn заснована у 2002 році, працює з травня 2003року. Компанія власник соціальної мережі LinkedIn компанія Microsoft.

Більше 50% акаунтів LinkedIn створені у США і ще близько 11 в Європі. В Україні створено близько 2,5 мільйонів акаунтів.

LinkedIn забезпечує можливість створення робочих контактів. Вони можуть знаходиться як на сайті, так і ззовні, проте LinkedIn потребує наявності поперенього знайомства між контактами. .

Акаунт LinkedIn може використовувати контактів для різних завдань:

- збільшувати кількість зв'язків та представлятись через них;
- Шукати компанії, акаунти, групи за інтересами;
- Поширюватисвої резюме і займатись пошуком роботи;

- Формувати рекоментації та потрапляти в них;
- Викладати вакансії.

Для підтвердження особи необхідно завантажити на сайт чітку фотографію дійсного посвідчення особи державного зразка, посвідчення водія або паспорта.

LinkedIn відноситься до забезпечення конфіденційності з усією серйозністю і використовує відомості, що надаються, виключно для підтвердження особи. У процесі підтвердження застосовується технологія обробки зашифрованих фотографій документів, що посвідчують особу. Отримані від фотографії та пов'язані з ними персональні дані зберігаються лише на період часу, доки вирішуються проблеми з обліковим записом. Як правило, вони віддаляються протягом 14 днів без можливості відновлення. Можливо зберігати знеособлені дані з документа, що посвідчує особу, з метою запобігання шахрайству.

Алгоритм LinkedIn визначає інтереси користувача на основі груп, сторінок, хештегів і людей, на яких він стежить. Якщо у публікації згадуються теми чи компанії, які відповідають інтересам користувача, що ж, це дуже гарна новина! Відповідно до блогу LinkedIn Engineering, алгоритм також розглядає кілька інших факторів.

Алгоритм LinkedIn вимірює ряд факторів, щоб здогадатися, наскільки будь-яка публікація може бути релевантною для аудиторії.

Він відсортує вміст за однією з трьох категорій: спам, низькоякісний або високоякісний.

Низька якість: ці публікації не є спамом. Але вони також не дотримуються найкращих практик щодо вмісту. Якщо ви не можете зробити свою публікацію привабливою, алгоритм вважає її низькою якістю.

Висока якість: ці публікації відповідають усім рекомендаціям щодо вмісту LinkedIn:

- Пост легко читається.

- Заохочує відповіді запитанням.
- Використовує три або менше хештегів.
- Містить сильні ключові слова.
- Позначає лише тих, хто дійсно відповість.

Коли алгоритм LinkedIn встановить, що не опублікувано щось надто спамне, він передасть публікацію невеликій кількості ваших підписників.

Якщо відразу буде багато залучених (лайків! коментарів! ділиться!), LinkedIn підштовхне це до більшої кількості людей.

Але якщо на цьому етапі ніхто не реагує (або, що ще гірше, якщо аудиторія позначить ваш допис як спам або вирішить приховати його зі своїх каналів), LinkedIn не буде турбуватися про те, щоб ділитися ним далі. Усе це відбувається протягом першої години після того, як був поширений допис.

Якщо публікація привертає увагу, потужний алгоритм почне надсилати вміст ширшій аудиторії.

Хто зможе побачити публікацію звідси, залежить від трьох сигналів рейтингу:

- Наскільки тісно ви пов’язані.

Чим тісніше пов’язані з підписником, тим більша ймовірність, що він побачить вміст.

- Інтерес до теми.

Алгоритм LinkedIn визначає інтереси користувача на основі груп, сторінок, хештегів і людей, на яких вони підписані.

Якщо у публікації згадуються теми чи компанії, які відповідають інтересам користувача, що ж, це дуже хороша новина!

Відповідно до блогу LinkedIn Engineering, алгоритм також розглядає кілька інших факторів. До них належать мова публікації та компанії, люди та теми, згадані в ній.

- Імовірність залучення.

Фактор «ймовірності залучення» вимірюється двома способами.

По-перше, наскільки ймовірно, що користувач зацікавиться публікацією? (Це базується на їхній попередній поведінці та тому, що вони взаємодіяли з публікаціями в минулому.)

Другий сигнал: наскільки залученою є сама публікація в цілому? Якщо це гаряча-гаряча-гаряча публікація, яка викликає багато розмов, більше людей, ймовірно, також захочуть долучитися.

Основні загрози інформаційній безпеці:

- витік даних;
- надання зловмисникам розвідувальної інформації ;
- дезінформація;
- Зловмисне програмне забезпечення.
- Відмова в обслуговуванні (DoS).
- Атака "людина посередині" (MITM).
- Фішингові атаки.

З правильним паролем кіберзловмисник отримує доступ до великої кількості інформації. Соціальна інженерія — це тип атаки на пароль, яку Data Insider визначає як «стратегію, яку використовують кібер-зловмисники, яка значною мірою залежить від взаємодії людей і часто передбачає обманом змусити людей порушити стандартні методи безпеки». Інші типи атак на паролі включають доступ до бази даних паролів або пряме вгадування.

Якщо соцмережа, розглянувши скаргу, вирішує, що контент порушує її стандарти, публікацію видаляють із платформи. Водночас, що більше користувачів звернуться з відповідними скаргами про порушення правил спільноти, то вище шанс подальшого видалення допису.

LinkedIn може бути інструментом для проведення розвідки цільової організації. Наприклад, ця мережа заохочує своїх користувачів публікувати повідомлення про свої посади та обов'язки, щоб спілкуватися зі своїми колегами по всьому світу, однак ця інформація може бути небезпечною в нечесних руках.

Зловмисник може дізнатися, які співробітники мають доступ до критично важливих систем або хто має повноваження фінансового підпису на основі описів ролей, що дозволяє йому створити більш точну атаку.

Подібним чином, якщо мережевий інженер повідомляє, що він сертифікований для певних брандмауерів, це може надати зловмисникам інформацію, необхідну для визначення того, що існує висока ймовірність того, що цільова організація використовує цей продукт.

1.2.2 Telegram

Telegram є однією з трох найпоширеніших платформ соціальних мереж, які підтримують інформаційну екосферу Росії. В перші три тижні повномасштабної війни Росії проти України, кількість користувачів Telegram збільшилася на 46% і з лютого по квітень 2022, додаток Telegram став найбільш завантажувальним з 4.4 мільйонів завантажень.

Telegram створювався як тестовий майданчик для роботи з технологією шифрування листування MTProto на великих навантаженнях.

Доступний по всьому світу мультиплатформовий захищений месенджер. Він може створювати наскрізь зашифровані чати (секретні чати). Створено веб додатки Telegram WebK та WebZ, Telegram має відритий вихідний код своїх компонентів, тому існують неофіційні клієнти на базі його протоколів.

Основний функціонал соціальної мережі Telegram це прямий обмін повідомленнями між користувачами.

Алгоритми підвищення певних публікацій не використовуються

Основні загрози інформаційній безпеці :

- витік даних.
- Дезинформація.
- Зловмисне програмне забезпечення/
- Фішингові атаки.

З правильним паролем кіберзловмисник отримує доступ до великої кількості інформації. Соціальна інженерія — це тип атаки на пароль, яку Data Insider визначає як «стратегію, яку використовують кібер-зловмисники, яка значною мірою залежить від взаємодії людей і часто передбачає обманом змусити людей порушити стандартні методи безпеки». Інші типи атак на паролі включають доступ до бази даних паролів або пряме вгадування.

Немає офіційної політики цензури чи видалення будь-якого контенту

Висновки за результатами аналізу мережі:

Telegram — це зашифрований сервіс обміну повідомленнями, який створив і належить російському технічному мільярдеру Павлу Дурову, який використовується на війні для всього: від маніпулювання українськими біженцями [17] до передачі особистих даних українських військових чи активістів кремлівським телеграм-каналам[18].

Важливо, що у боротьбі з дезінформацією Telegram немає офіційної політики цензури чи видалення будь-якого контенту.

Незважаючи на те, що деякі канали в Telegram закриті, компанія не публікує офіційних заяв про те, чому і в цілому дозволяє більшості вмісту, опублікованого користувачами, продовжувати циркулювати незалежно від його характеру. Це дозволяє Telegram служити в основному нефільтрованим джерелом дезінформації в Росії та Україні і включати аудиторію, від якої західні соціальні медіа-платформи були відрізані.

Хоча Telegram не фільтрує вміст, як і багато інших платформ, він також не використовує алгоритм підвищення певних публікацій і покладається на прямий обмін повідомленнями між користувачами. Така конструкція ускладнює ефективне посилення дезінформації інструментами штучного інтелекту. Навпаки, на інших платформах, таких як Twitter і Facebook, ШІ сприяє швидкому поширенню дезінформації про війну.

1.2.3 Facebook

Facebook[19] — популярна мережа, створена 4 лютого 2004 року для американських студентів певних університетів. Facebook належить корпорації Meta Platforms. Засновником та головою сервісу є Марк Цукерберг.

У 2017 року була різка хвиля рєстрації українських акаунтів, оскільки російські аналоги були заблоковані владою України, тому загальна кількість користувачів з України у Facebook подолала відмітку в 10 млн.[19] У липні того ж року Facebook став найпопулярнішою соцмережею в Україні.

За останні пів року українська аудиторія Facebook зросла на 800 тис. і складає 16,8 млн користувачів, з них 16,4 млн — аудиторія 18+.

Яку інформацію користувач соціальної мережі розміщує про себе у мережі:

- ім’я, основна світлина та світлина обкладинки.
- Відомості про стать.
- Перелік мереж (наприклад, школа, місце роботи).
- Ім’я та ID користувача (наприклад, номер облікового запису) входять до URL-адреси профілю.
- Відомості про віковий діапазон.
- Відомості про мову та країну проживання.

Як соціальна мережа підтверджує оригінальність облікового запису користувача**:**

Двофакторна аутентифікація - використовується пароль для входу та код підтвердження, отриманий через мобільний пристрій. Це допомагає зменшити ризик зламу облікового запису та запобігає викраденню зловмисником законного облікового запису та розміщенню шкідливого вмісту.

Алгоритм Facebook[20] визначає, які публікації люди бачать щоразу, коли переглядають свою стрічку Facebook, і в якому порядку ці публікації відображаються.

По суті, алгоритм Facebook оцінює кожну публікацію. Він підраховує дописи, а потім розташовує їх у спадному нехронологічному порядку, що цікавить кожного окремого користувача. Цей процес відбувається щоразу, коли користувач — а їх 2,9 мільярда — оновлює свою стрічку.

Невідомо, як алгоритм Facebook вирішує, що показувати людям (а що ні). Але як і всі алгоритми рекомендацій у соціальних мережах, одна з цілей — утримати людей на платформі, щоб вони бачили більше реклами.

Насправді Facebook зіткнувся з спекою у 2021 році, оскільки алгоритм віддавав пріоритет суперечливому контенту. Суперечка часто викликає найбільше залучення та може навіть спровокувати «вимушене використання» платформи.

І ще в 2018 році критики побоювалися, що алгоритм посилює обурення, розбіжності та політичну поляризацію, одночасно просуваючи дезінформацію та межовий контент.

Зі свого боку, Facebook каже, що алгоритм допомагає користувачам «відкривати новий контент і спілкуватися з історіями, які їх найбільше цікавлять», водночас «утримуючи спам і оманливий контент». Нижче

подані нещодавні зміни в алгоритмі Facebook спрямовані на вирішення проблем щодо вмісту та конфіденційності.

Алгоритм Facebook не є статичним. У Meta є ціла команда людей, які працюють над штучним інтелектом і машинним навчанням. Частиною їх роботи є вдосконалення алгоритмів, які з'єднують користувачів Facebook із найціннішим для них вмістом.

З роками сигнали ранжирування алгоритмів додавали, видаляли та змінювали їх важливість. Все залежить від того, що, на думку Facebook, хочуть бачити користувачі.

Ось деякі з найбільш помітних моментів і змін у розвитку алгоритму Facebook:

- 2009: Facebook представляє свій перший алгоритм для переміщення публікацій із найбільшою кількістю лайків у верхню частину стрічки.
- 2015: Facebook[20] починає знижувати рейтинг сторінок, які публікують занадто багато рекламного контенту. Вони вводять функцію «Побачити першим», щоб дозволити користувачам вказати, що вони хочуть, щоб публікації сторінки були пріоритетними в їхній стрічці.
- 2016: Facebook додає рейтинговий сигнал «витрачений час», щоб оцінити цінність публікації на основі часу, який користувачі провели з нею, навіть якщо вони не поставили лайк або не поділилися нею.
- 2017: Facebook починає зважувати реакції (наприклад, сердечка чи сердите обличчя) більше, ніж класичні лайки. Для відео додано ще один рейтинговий сигнал: коефіцієнт завершення. Іншими словами, відео, які змушують людей дивитися до кінця, показуються більшій кількості людей.
- 2018: Новий алгоритм Facebook надає пріоритет «дописам, які викликають розмови та значущі взаємодії». Публікації від друзів, родини та груп у Facebook були пріоритетні над звичайним вмістом зі сторінок.

Брендам тепер потрібно залучити набагато більше, щоб сигналізувати про цінність алгоритму.

- 2019: Facebook надає пріоритет «високоякісному оригінальному відео», яке глядачі дивляться довше 1 хвилини, особливо відео, яке утримує увагу довше 3 хвилин. Facebook також починає збирати вміст від «близьких друзів»: тих, з ким люди спілкуються найбільше. Представлено інструмент «Чому я бачу цю публікацію».
- 2020: Facebook розкриває деякі деталі алгоритму, щоб допомогти користувачам зрозуміти, як він обслуговує вміст, і дозволяє користувачам контролювати свої дані, щоб надати алгоритму кращий відгук. Алгоритм починає оцінювати достовірність і якість новинних статей, щоб просувати обґрунтовані новини, а не дезінформацію.
- 2021: Facebook[20] публікує нові відомості про свій алгоритм і надає людям кращий доступ до їхніх даних. Ось їхнє пояснення алгоритму в 2021 році.

Отже, де все це залишить нас у 2023 році? По-перше, стрічки новин більше немає. Те, що ви бачите під час прокручування Facebook, тепер називається просто Feed.

Facebook каже, що Feed «показує вам історії, які є значущими та інформативними». Починаючи з 2023 року, алгоритм Facebook може визначити, що можуть бути в цих історіях, використовуючи три основні сигнали рейтингу:

- Хто це опублікував: швидше за все, побачите вміст із джерел, з якими взаємодієте, зокрема друзів і компаній.
- Тип вмісту: якщо найчастіше взаємодієте з відео, побачите більше відео. Якщо взаємодієте з фотографіями, побачите більше фотографій.

- Взаємодія з дописом: стрічка віддаватиме пріоритет дописам із великою зацікавленістю, особливо від людей, з якими багато спілкуєтеся.

Кожна публікація оцінюється на основі цих основних сигналів, щоб визначити, де вона з'являється у вашій стрічці.

Facebook[20] також надає користувачам параметри, які допомагають їм навчити алгоритм і налаштувати свій канал:

- Вибране: користувачі можуть вибрати до 30 людей і сторінок для додавання до вибраного (раніше відоме як «Переглянути спочатку»). Публікації з цих облікових записів відображатимуться вище в стрічці. Щоб отримати доступ до вибраного, клацніть стрілку вниз у верхньому правому куті Facebook, потім натисніть «Налаштування та конфіденційність», а потім «Параметри стрічки новин».

- Параметри в стрічці: клацніть будь-яку публікацію, і побачите опцію Я не хочу це бачити. Потім виберіть «Приховати публікацію», щоб повідомити Facebook[20], що хочете, щоб у стрічці було менше публікацій такого характеру. Для реклами еквівалентною опцією є Сховати рекламу. Тоді Facebook надасть набір параметрів, щоб вказати, чому хочете приховати рекламу. Це допоможе Facebook зрозуміти, яких рекламодавців хочете почути, а яких краще уникати.

І, нарешті, Facebook буде видаляти вміст, який суперечить стандартам спільноти. Вони також можуть «видалити або обмежити аудиторію для певних видів конфіденційного контенту», наприклад, зображення оголеного тіла, насильства та графічного вмісту».

Основні загрози інформаційній безпеці**:**

- витік даних;
- надання зловмисникам розвідувальної інформації ;
- дезінформація;
- Зловмисне програмне забезпечення.

- Відмова в обслуговуванні (DoS).
- Атака "людина посередині" (MITM).
- Фішингові атаки.

З правильним паролем кіберзловмисник отримує доступ до великої кількості інформації. Соціальна інженерія — це тип атаки на пароль, яку Data Insider визначає як «стратегію, яку використовують кібер-зловмисники, яка значною мірою залежить від взаємодії людей і часто передбачає обманом змусити людей порушити стандартні методи безпеки». Інші типи атак на паролі включають доступ до бази даних паролів або пряме вгадування.

Зловмисник може дізнатися, які співробітники мають доступ до критично важливих систем або хто має повноваження фінансового підпису на основі описів ролей, що дозволяє йому створити більш точну атаку.

Подібним чином, якщо мережевий інженер повідомляє, що він сертифікований для певних брандмауерів, це може надати зловмисникам інформацію, необхідну для визначення того, що існує висока ймовірність того, що цільова організація використовує цей продукт.

У середньому кожні 60 секунд на Facebook публікується 510 000 коментарів, оновлюється 298 000 статусів і завантажується 136 000 фотографій. Оскільки на Facebook завантажується величезна кількість даних, існує висока ймовірність загроз безпеці. Будь-хто може публікувати шкідливий вміст, прихований у мультимедійних даних або за допомогою скорочених уніфікованих покажчиків ресурсів (URL). Існує близько 83 мільйонів підроблених профілів, які можуть належати нелегітимним користувачам або професіоналам, які проводять тестування та дослідження. Близько 1 млн веб-сайтів щодня зламується.

1.2.4 Twitter

Твіттер[21] — соціальна мережа, яка є мережею мікроблогів, дає змогу користувачам надсилати короткі текстові повідомлення (до 280 символів, до 2017 року — до 140 символів), використовуючи SMS, служби миттєвих повідомлень і сторонні програми-клієнти. Літературний сегмент твіттера породив такий різновид короткотекстової літератури, як твіттература. Одна з найбільших соціальних медіа-платформ у світі за кількістю активних користувачів щомісяця (близько 463 мільйонів).

28 жовтня 2022 року Ілон Маск викупив Twitter за 44 млрд доларів,. Оскільки Twitter перейшла до приватних рук, акції соцмережі будуть зняті з торгів на Нью-Йоркській фондовій біржі.

Мета Twitter[22] – обслуговувати публічну дискусію. Насильство, переслідування та інші подібні види поведінки перешкоджають людям висловлюватись і, зрештою, зменшують цінність глобальної публічної дискусії. Правила полягають у тому, щоб усі люди могли вільно та безпечно брати участь у публічній бесіді.

- Безпека:
  - Насильство: не можна погрожувати насильством окремій особі чи групі людей. Заборонено прославляти насильство.
  - Тероризм/насильницький екстремізм: не можна погрожувати чи пропагувати тероризм чи насильницький екстремізм.
  - Сексуальна експлуатація дітей: не допускається сексуальна експлуатації дітей у Twitter.
  - Жорстоке поводження/переслідування: не можна брати участь у цілеспрямованих переслідуваннях когось або підбурювати інших людей до цього. Це включає в себе бажання або надію, що хтось зазнає фізичної шкоди.

- Ненависницька поведінка: не можна пропагувати насильство, погрожувати або переслідувати інших людей на основі раси, етнічного походження, національного походження, касти, сексуальної орієнтації, статі, гендерної ідентичності, релігійної приналежності, віку, інвалідності чи серйозної хвороби.
- Винуватці насильницьких атак: видаляються будь-які облікові записи, які ведуть окремі виконавці терористичних, насильницьких екстремістських або масових насильницьких атак, а також твіти, що поширюють маніфести, або інший вміст, створений зловмисниками.
- Самогубство або самоушкодження[22]: не можна пропагувати або заохочувати до самогубства чи самоушкодження.
- Делікатні медіа, зокрема зображення насильства та вміст для дорослих: не можна публікувати надто криваві медіа або ділитися насильницьким чи дорослим вмістом у відео в прямому ефірі, на зображеннях профілю чи заголовку. ЗМІ, що зображують сексуальне насильство та/або напади, також заборонені.
- Незаконні або певні регульовані товари чи послуги: не можна використовувати сервіс із будь-якою протизаконною метою або для сприяння незаконній діяльності. Це включає продаж, купівлю або сприяння транзакціям із незаконними товарами чи послугами, а також певними типами регульованих товарів чи послуг.

- Конфіденційність:
  - Приватна інформація: не можна використовувати чи публікувати особисту інформацію інших людей (наприклад,

домашній номер телефону та адресу) без їх явного дозволу та дозволу також заборонено погрожувати розголошенням приватної інформації або заохочувати інших до цього. Вивчайте більше.

- Оголення без згоди: не можна публікувати чи ділитися інтимними фотографіями чи відео когось, створеними чи розповсюдженими без їхньої згоди.

- Автентичність:
  - Маніпуляції[22] на платформі та спам: не можна використовувати служби Twitter у спосіб, призначений для штучного розширення чи приховування інформації або брати участь у поведінці, яка маніпулює чи порушує роботу людей у Twitter.
  - Громадянська доброчесність: не можна використовувати служби Twitter з метою маніпулювання або втручання у вибори чи інші громадські процеси. Це включає публікацію або поширення вмісту, який може перешкоджати участі або вводити людей в оману щодо того, коли, де чи як брати участь у громадському процесі.
  - Оманливі та оманливі особи: не можна видавати себе за окремих осіб, групи чи організації, щоб ввести в оману, заплутати чи обманювати інших, а також використовувати підроблену особу таким чином, щоб порушити роботу інших у Twitter.
  - Синтетичні та оброблені медіа: не можна оманливо ділитися синтетичними чи маніпуляційними носіями, які можуть завдати шкоди. Крім того, ми можемо позначати твіти, що

містять синтетичні та підроблені медіа, щоб допомогти людям зрозуміти їх автентичність і надати додатковий контекст.

- Авторське право та торгова марка: не можна порушувати права інтелектуальної власності інших осіб, зокрема авторські права та торговельну марку. Дізнайтеся більше про нашу політику щодо торговельних марок і політику щодо авторських прав.

Алгоритм Twitter[23] мало чим відрізняється від алгоритмів, які використовуються іншими гігантами соціальних мереж, як Facebook наприклад.

Ці платформи мають використовувати алгоритми, щоб показувати вміст своїм користувачам, оскільки інакше немає логічного способу встигати за всім цим.

Алгоритм Twitter[23] ґрунтується на активності на платформі.

Коли спілкуєтесь у Twitter, подобаються певні твіти, підписуються на певні облікові записи та ретвітуються певні речі, які подобаються. Twitter використовує все це, щоб показувати твіти, які, на його думку, захочете побачити.

Важливо пам’ятати, що користувачі бачать вміст не завжди з облікових записів, на які вони підписані.

Twitter також може показувати твіти з облікових записів, схожих на облікові записи, за якими стежать користувачі. Алгоритм визначає, який вміст він показуватиме з цих джерел на основі облікових записів, на які ви стежите, і типів твітів, які вам часто подобаються.

Для користувача все це виглядає так: коли користувачі вибирають головну часову шкалу, вони побачать вміст алгоритму Twitter, розділ «Якщо ви пропустили» з останніми твітами облікових записів, на які вони підписані, а потім усі інші «звичайні» твіти з облікових записів, на які вони стежать.

Користувачі можуть увімкнути перемикач алгоритму, щоб вимкнути припущення Twitter щодо їхніх інтересів, і перейти в режим «Останні твіти», щоб побачити у зворотному хронологічному порядку список усіх останніх твітів з облікових записів, на які вони підписалися.

Коли намагаєтеся оптимізувати вміст свого Twitter, щоб його побачила найбільша кількість користувачів, яких вважаєте ідеальними для свого акаунту, потрібно працювати в рамках алгоритму платформи.

Twitter шукатиме певні речі у вмісті, щоб визначити, чи він «гідний» розміщення вище в стрічці аудиторії.

Ось що алгоритм[23] «зважатиме», вирішуючи, де розмістити вміст:

- Як давно було створено твіт.
- Наскільки твіт відповідає темі чи ринковій ніші порівняно з тим, що говорять інші в цьому просторі.
- Наскільки зацікавлені користувачі конкретним твітом та іншими твітами з облікового запису.
- Чи містить твіт візуальні елементи, такі як зображення, відео, gif-файли чи інші засоби масової інформації (усі вони, як правило, більш привабливі, ніж просто текст).

Політичні резонанси в Твіттері настільки екстремальні, що політичні уподобання окремих користувачів можна передбачити з високою точністю: ви маєте ті самі думки, що й більшість ваших зв’язків.

1.3 Ландшафт загроз

Загрози можна умовно поділити на три категорії: звичайні загрози, сучасні загрози та цільові загрози. Звичайні загрози включають загрози, з якими користувачі стикаються з самого початку соціальної мережі. Сучасні загрози – це атаки, які використовують передові методи для компрометації

облікових записів користувачів, а цільорві атаки – це атаки, націлені на певного користувача, які можуть бути вчинені будь-яким користувачем з метою різноманітної особистої помсти.

Традиційні загрози:

- Спам-атака.

Спам — це термін, який використовується для масових електронних повідомлень [3]. Хоча електронна пошта є звичайним способом розповсюдження спаму, платформа соціальних мереж є більш успішною в поширенні спаму . Деталі зв’язку законних користувачів можна легко отримати на веб-сайтах компаній, у блогах і групах новин . Неважко переконати цільового клієнта читати спам-повідомлення та довіряти його захисту . Більшість спаму є комерційною рекламою, але він також може використовуватися для збору конфіденційної інформації від користувачів або може містити віруси, зловмисне програмне забезпечення або шахрайство.

- Атака шкідливих програм.

Шкідливе програмне забезпечення - це шкідливе програмне забезпечення, яке явно розроблено для зараження або доступу до комп’ютерної системи, як правило, без інформації користувача . Зловмисник може використовувати численні способи розповсюдження шкідливих програм і зараження пристроїв і мереж . Наприклад, зловмисне програмне забезпечення може бути встановлено, клацнувши зловмисну URL-адресу в системі клієнта, або воно може перенаправити клієнта на фальшивий сайт, який намагається отримати особисті дані від клієнта. Зловмисник може вставити якийсь шкідливий сценарій в URL-адреси, і натискання на ці URL-адреси може змусити цей сценарій запускатися в системі, яка може збирати конфіденційну інформацію з цієї системи [3]. На платформах соціальних мереж зловмисне програмне забезпечення використовує структуру онлайн-соціальної мережі (OSN), щоб

розповсюджувати себе, наприклад кількість вершин, кількість ребер, середній найкоротший шлях і найдовший шлях.

- Фішинг.

Фішингова атака – це різновид атаки соціальної інженерії, коли зловмисник може отримати конфіденційну та конфіденційну інформацію, як-от ім’я користувача, пароль і дані кредитної картки користувача, через підроблені веб-сайти та електронні листи, які здаються справжніми . Зловмисник може видати себе за справжнього користувача та використовувати його/її особистість для надсилання фальшивих повідомлень іншим користувачам через платформу соціальної мережі, яка містить шкідливу URL-адресу. Ця URL-адреса може перенаправляти споживача на фальшивий веб-сайт, де він запитує особисту інформацію. У випадку SNS зловмиснику необхідно залучити клієнта на фальшиву сторінку, де він зможе здійснити фішингову атаку. Щоб досягти цього, нападник використовує різні методи соціальної інженерії. Наприклад, він може надіслати користувачеві повідомлення: «Ваші особисті зображення розміщені на цьому веб-сайті, перевірте!». Натискаючи цю URL-адресу, користувач перенаправляється на підроблений веб-сайт, який виглядає як якийсь законний сайт соціальної мережі.

- Крадіжки особистих даних.

У цьому виді нападу нападник використовує чужу особу, як-от номер соціального страхування, номер мобільного телефону та адресу, без їхнього дозволу для вчинення нападників . За допомогою цих деталей зловмисник може легко отримати доступ до списку друзів жертви та вимагати від неї конфіденційну інформацію за допомогою різних методів соціальної інженерії [3]. Оскільки зловмисник видає себе за законного користувача, він може використовувати цей профіль будь-яким можливим способом, що може серйозно вплинути на автентичних клієнтів.

Сучасні загрози:

- Міжсайтова сценарна атака.

Міжсайтовий скриптинг є дуже поширеним вектором атак серед зловмисників. Атака скорочено називається XSS і також відома як «Self-XSS» [3]. По суті, атака виконує шкідливий JavaScript у браузері жертви за допомогою різних методів. Вони класифікуються як постійні, відображені та XSS-атаки на основі DOM . Браузер може бути зламаний лише одним натисканням кнопки, що може надіслати шкідливий сценарій на сервер . Цей скрипт бумерангом повертається до жертви та виконується у браузері. Привабливі посилання та кнопки в популярних соціальних мережах, таких як Twitter і Facebook, можуть обманом змусити користувача перейти за URL-адресами. Що ще гірше, деякі користувачі можуть відчувати потребу скопіювати та вставити посилання, що містять JavaScript, в адресний рядок свого браузера. Ці атаки можуть викрасти інформацію або діяти як шпигунське програмне забезпечення. Такі атаки також можуть захопити комп’ютери для здійснення атак на нічого не підозрюючих користувачів. Справжній виконавець атаки ховається за скомпрометованою машиною.

- Атака клонування профілю.

Під час цієї атаки зловмисник клонує профіль користувача, про який він має попередні знання. Зловмисник може використовувати цей клонований профіль на тій самій або іншій платформі соціальної мережі, щоб створити довірливі стосунки з друзями реального користувача [3]. Після встановлення з’єднання зловмисник обманом змушує друзів жертви повірити в достовірність фальшивого профілю та успішно перехоплює конфіденційну інформацію, яка не розповсюджується в їхніх публічних профілях. Цю атаку також можна використовувати для вчинення інших типів кіберзлочинів, таких як кіберзалякування, кіберпереслідування та шантаж [3].

- Викрадення.

Під час викрадення зловмисник компрометує або бере контроль над обліковим записом користувача для здійснення онлайн-шахрайства . Сайти без багатофакторної автентифікації та облікові записи зі слабкими паролями більш вразливі до викрадення, оскільки паролі можна отримати за допомогою фішингу . Якщо у нас немає багатофакторної автентифікації, то нам бракує вторинної лінії захисту. Після викрадення облікового запису зловмисник може надсилати повідомлення, ділитися шкідливим посиланням і змінювати інформацію облікового запису, що може завдати шкоди репутації користувача .

- Атака логічного висновку.

Атака інференції робить висновок про конфіденційну інформацію обробника, яку користувач може не захотіти розголошувати, через іншу статистику, яку користувач розміщує на певному сайті соціальної мережі (SNS). Він використовує процедури інтелектуального аналізу даних на видимих даних, таких як список друзів користувача та топологія мережі. Використовуючи цю техніку, зловмисник може знайти секретну інформацію організації або географічну та освітню інформацію користувача.

- Атака Sybil.

Під час атаки Sybil вузол претендує на кілька ідентифікацій у мережі [3]. Це може бути шкідливим для платформ соціальних мереж, оскільки вони містять величезну кількість користувачів, які підключені через однорангову мережу . Однорангові комп’ютери — це комп’ютерні структури, які пов’язані один з одним за допомогою Інтернету, і вони можуть прямолінійно обмінюватися записами без потреби в центральному сервері. Одна онлайн-суб’єкт може створювати кілька підроблених ідентифікацій і використовувати їх для розповсюдження небажаної інформації, зловмисного програмного забезпечення або навіть для впливу на репутацію та популярність організації. Наприклад, веб-опитуванням

можна маніпулювати, використовуючи різні Інтернет-протоколи (IP), щоб подати величезну кількість голосів, і агресор може перевершити справжнього клієнта.

- Клікджекінг.

Клікджекінг — це процедура, за якої зловмисник обманює користувача, щоб він клацнув на сторінці, яка відрізняється від тієї, на якій він збирався клацнути [3]. Це також відоме як атака відшкодування інтерфейсу користувача. Зловмисник використовує вразливість браузерів для виконання цієї атаки. Він завантажує іншу сторінку поверх сторінки, до якої користувач хоче отримати доступ, як прозорий шар. Дві відомі різновиди клікджекінгу — це джекінг і джекінг курсору. Лицьовий шар показує речовину, якою можна приманити клієнта. У той момент, коли клієнт натискає цей вміст, він фактично натискає кнопку «подобається». Чим більше людей лайкає публікацію, тим більше вона поширюється.

У cursorjacking зловмисник замінює фактичний курсор власним зображенням курсору. Фактичний курсор зсувається від фактичного положення миші. Таким чином зловмисник може змусити споживача натиснути на шкідливий сайт за допомогою розумного позиціонування елементів сторінки.

- Атака деанонімізації.

На багатьох сайтах соціальних мереж, таких як Twitter і Facebook, користувачі можуть приховувати або захищати свою справжню особу перед оприлюдненням будь-яких даних, використовуючи псевдонім або вигадане ім’я [3]. Але якщо третя сторона хоче з’ясувати справжню особу користувача, це можна зробити, просто зв’язавши інформацію, яку витікає з цих сайтів соціальних мереж . Вони використовують такі стратегії, як відстеження файлів cookie, мережеві топології та реєстрація груп користувачів, щоб розкрити справжню особу клієнта . Це свого роду метод видобутку інформації, в якому таємнича інформація перехресно

посилається на інші джерела інформації для повторного розпізнавання невідомої інформації. Зловмисник може збирати інформацію про членство користувача в групі, викрадаючи історію з його браузера та поєднуючи цю історію із зібраними даними. Таким чином зловмисник може деанонімізувати користувача, який відвідує веб-сайт цього зловмисника.

- Кібершпигунство.

Кібершпигунство — це акт, який використовує кіберможливості для збору конфіденційної інформації або інтелектуальної власності з наміром передати її протиборчим сторонам. Ці напади мотивуються жадібністю до грошової вигоди та широко використовуються як невід'ємна частина військової діяльності або як демонстрація незаконного залякування. Це може спричинити втрату конкурентної переваги, матеріалів, інформації, фондів або кількість загиблих. Соціальний інженер може виконувати напади соціальної інженерії за допомогою сайтів соціальних мереж. Він може отримати важливі дані, такі як завдання працівника, адреса електронної пошти тощо, використовуючи сайти соціальних мереж.

Цільові загрози:

- Кіберзалякування.

Кіберзалякування – це використання електронних засобів масової інформації, таких як електронні листи, чати, телефонні розмови та соціальні мережі в Інтернеті, для залякування чи переслідування людини [3]. На відміну від традиційного булінгу, кібербулінг є безперервним процесом. Він постійно підтримується через соціальні мережі. Зловмисник неодноразово надсилає залякуючі повідомлення, сексуальні зауваження, публікує чутки, а іноді публікує незручні фотографії чи відео, щоб переслідувати людину. Він також може опублікувати особисту чи приватну інформацію про жертву, що спричинить збентеження чи приниження. Кіберзалякування також може статися випадково. Дуже важко дізнатися тон відправника в текстових повідомленнях, миттєвих повідомленнях і

електронних листах. Але повторювані моделі таких електронних листів, текстових повідомлень і публікацій в Інтернеті рідко бувають випадковими.

- Кібергрумінг.

Кібергрумінг — це встановлення інтимних та емоційних стосунків із жертвою (зазвичай дітьми та підлітками) з наміром спонукати до сексуального насильства [3]. Основна мета кібер-догляду полягає в тому, щоб завоювати довіру підлітка та за допомогою чого можна отримати інтимну та індивідуальну інформацію від дитини. Дані часто мають хтивий характер через розмови сексуального характеру, фотографії та відео, що дає зловмиснику перевагу погрожувати та шантажувати дитину. Зловмисники часто звертаються до підлітків або дітей через підроблені ідентифікаційні дані на сайтах, орієнтованих на дітей, залишаючи їх уразливими та не поінформованими про той факт, що їх наблизили з кінцевою метою кібергрумінгу. Однак жертва також може неусвідомлено ініціювати процес догляду, коли отримує винагородні пропозиції, наприклад, готівку в обмін на контактні дані або особисті фотографії. У деяких випадках жертва знає про те, що вона розмовляє з дорослим, що може спонукати до подальших сексуальних дій. Однак це стосується особи, яка не досягла віку згоди, і таким чином є злочином. Анонімність і доступність передових засобів масової інформації дозволяють грумерам рухатися до різних молодих людей одночасно, експоненціально збільшуючи випадки кібер-грумінгу. Незважаючи на те, що можна було очікувати, у всьому світі є кілька випадків почуття почуття до злочину кібер-грумінгу, оскільки 66% країн світу не мають конкретних законів щодо кібер-грумінгу дітей.

- Кіберпереслідування.

Кіберпереслідування – це спостереження за особою за допомогою Інтернету, електронної пошти чи будь-якого іншого типу електронного листування, яке призводить до страху перед насильством і втручається в психічний спокій цієї особи [3]. Це передбачає вторгнення в право особи на

приватне життя. Зловмисник відстежує особисту або конфіденційну інформацію жертв і використовує її, щоб погрожувати їм, надаючи безперервні та постійні повідомлення протягом дня. Така поведінка змушує потерпілого надзвичайно хвилюватися за власну безпеку та викликає у нього певний тип занепокоєння, страху чи занепокоєння. Більшість людей сьогодні діляться своєю особистою інформацією, як-от номер телефону, місце проживання, район і розклад, у своїх профілях соціальних мереж. Крім того, вони також діляться своїми даними про місцезнаходження. Зловмисник може зібрати ці дані та використати їх для кіберпереслідування.

1.3.1 Як платформи соціальних медіа використовуються для поширення конкуруючих наративів та дезінформації

Рисунок 3 – вектори атак.

1.3.2 Вплив з точки зору загроз безпеці користувачів

Соціальні медіа звертаються до одного з найбільш унікальних, неструктурованих і нерегульованих набору даних у розвиненому світі, і ця ситуація швидко поширюється по всьому світу . Щодня мільйони людей

завантажують свої фотографії та інший мультимедійний вміст у соціальні мережі, щоб поділитися ним зі своїми друзями. Це спонукає до розвитку цифрового моніторингу ризиків [3]. Розвиток веб-медіа представив нові стандарти безпеки, які ставлять клієнтів (представників, клієнтів і партнерів) у поле зору агресора. Соціальна мережа стала новою цифровою віхою, де зловмисники вважають, що легко націлитися на жертв. Він представляє одну з найбільших, найпотужніших небезпек для авторитетної безпеки. Зловмисники впливають на соціальні мережі з трьох супутніх причин:

- Масштаби соціальних мереж: оскільки величезна маса людей проводить свій час у соціальних мережах з різними цілями, атаки можуть поширюватися, як і будь-яка інша вірусна тенденція. Зловмисник може використовувати хештеги, клікбейт і популярні теми, щоб оголосити про своє зловмисне програмне забезпечення, яке може бути спрямоване на всіх або на певне зібрання людей. Це становить величезну проблему для експертів із безпеки, яку необхідно фізично подолати.
- Довірчий характер[3] соціальних медіа: зловмисники користуються довірчим характером соціальних медіа. Люди іноді приймають невідомий запит про друзі на основі спільних друзів, які мають той, хто запитує. Вони легко переходять за посиланням, розміщеним їхніми друзями, не замислюючись про можливе порушення безпеки. Понад одна третина загальної кількості користувачів соціальних медіа погоджуються з невідомими запитами друзів, що робить онлайн-медіа, мабуть, найкращим способом завоювати довіру об’єкта.
- Невидимість для команди безпеки: більшість людей у світі проводять більшу частину свого часу в соціальних мережах. Спостерігати за цією величезною масою людей надзвичайно складно, оскільки служби безпеки не мають інструментів, щоб розширити свою видимість за межі

певної межі в соціальні мережі, де співробітники інтенсивно вразливі до злому.

1.3.3 Вплив з точки зору загроз безпеці організації

Найбільш поширені ризики соціальних мереж для компаній і організацій:

- Втрата інтелектуальної власності або конфіденційних даних.

Витік або викрадення даних[25], несвоєчасне оприлюднення конфіденційної інформації, стратегічної для діяльності організації, і викрадення інтелектуальної власності, наприклад кодів, можуть призвести до серйозних фінансових втрат і навіть призвести до закриття компанії. Такі події не завжди є результатом складних кібератак; у багатьох випадках вони є результатом людської помилки, викликаної фішинговими атаками, соціальною інженерією та видаванням себе за іншу особу.

- Втрата репутації.

Думки споживачів можуть дуже швидко поширюватися в соціальних мережах. А негативні огляди та відгуки мають набагато більшу тенденцію стати вірусними. Через це компанії повинні бути дуже обережними щодо своєї онлайн-репутації[25]. Втрата репутації також може бути спричинена власними силами, наприклад через нечутливі твіти чи повідомлення, нереалістичні обіцянки щодо продуктів чи послуг або невідповідну поведінку співробітників в Інтернеті.

Якщо компанія не уважно ставиться до своєї присутності в Інтернеті або не звертає уваги на негативні відгуки, потенційні наслідки негативної реклами в соціальних мережах можуть бути дуже серйозними. Соціальні медіа мають таку силу, що одна негативна подія може знищити роки розбудови бренду та всю добру волю за лічені миті.

- Порушення цілісності або витік даних.

Соціальні медіа-платформи, особливо сайти знайомств, можуть бути використані для захоплення співробітників або керівників. Така тактика

використовується для залучення осіб, які мають доступ до конфіденційної інформації, до фальшивих стосунків, як правило, в Інтернеті. Потім зловмисник збирає інформацію або облікові дані облікового запису, щоб отримати несанкціонований доступ до конфіденційних даних з наміром викрасти або розкрити дані з метою фінансової вигоди.

- Порушення відповідності.

Якщо облікові записи в соціальних мережах не регулюються суворо політикою компанії, бізнес може опинитися під загрозою передачі інформації, яка порушує нормативні вимоги та закони про конфіденційність. Існує низка потенційних ризиків залежно від галузі та послуг, включаючи порушення торгових марок або авторських прав, порушення HIPAA[25] або CCPA, збереження даних або порушення прав на конфіденційність тощо.

Масштабні порушення та витоки даних призвели до посилення уваги до конфіденційності, що призвело до появи більшої кількості нормативних актів і вимог для компаній. Тому організації повинні бути дуже обережними щодо своєї присутності в Інтернеті та залучення користувачів щодо безпеки та конфіденційності даних.

1.3.4 Вплив з точки зору загроз безпеці країні.

Соціальні мережі є інструментом двосторонньої комунікації між владою та суспільством, який сприяє прозорості влади та розвитку демократичного суспільства. Прозорості в управлінні[24] можна досягти шляхом встановлення механізму зворотного зв’язку у відносинах між урядом та громадянами (G2C). Впровадження новітніх технологій, додатків у соціальних медіа (таких як блоги у Facebook чи Twitter) дозволяє урядам скористатися новими інструментами спілкування та взаємодії. З іншого боку, соціальні медіа стають платформою, що надає кожному легкий доступ до Інтернету, і уряд приєднується до них, щоб зв’язатися зі своїми громадянами, щоб підвищити рівень залученості та відданості громадян.

Мережеві суспільства можуть функціонувати одночасно в кількох напрямках: об'єднання людей для досягнення певної мети, поширення інформації, гнучкі механізми регулювання політичного курсу, відносини громадянин-влада тощо. Особливу увагу слід приділити застосуванню ключових компонентів електронного урядування в соціальних мережах, що найбільш динамічно розвиваються, у сфері сучасних соціальних комунікацій у контексті наявних досліджень, а також виявлення потенційних ризиків і негативних тенденцій у процесі обміну контентом. . Дослідження показують, що за останні кілька років з'явилася низка актуальних напрямків досліджень із застосуванням технологій Web 2.0 в електронному урядуванні. Дослідження Web 2.0, соціальних медіа, соціальних мереж та їх використання в державному секторі показують, що такі питання, як формування соціальних медіа та роль соціальних мереж у державному управлінні, були широко вивчені. Ключові напрямки досліджень включають роль соціальних мереж у побудові зворотного зв’язку між електронним урядуванням та громадянами, питання безпеки, встановлення взаємодії з органами державної влади за допомогою соціальних мереж, трансформацію соціальної культури та форм управління у використанні соціальних медіа в електронному урядуванні.

Окрім[24] загрози маніпулювання персональними даними, соціальні мережі є інструментом масових протестів у контексті загроз суспільній безпеці. Деструктивні виклики в соціальних мережах піддаються зовнішньому втручанню, викликаючи конфлікти між владою та громадянами, протести за короткий проміжок часу. Зазначу, що соціально довірені соціальні мережі досить успішно використовуються в сегменті електронного урядування для захисту інтересів влади, досягнення прозорості у відносинах між владою та громадянами, підвищення ефективності прийняття рішень та вдосконалення механізмів електронної участі.

РОЗДІЛ 2. ТЕХНОЛОГІЇ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА БОРОТЬБИ З ДЕЗІНФОРМАЦІЄЮ

2.1 Технології боротьби з кожним із впливів

2.1.1 З боку власників соціальних мереж.

Багато дослідників як у наукових колах, так і в промисловості постійно намагаються знайти рішення для загроз у соціальних мережах. Вони запропонували багато рішень і деякі підходи для боротьби з цими загрозами. Тут описано різні методи та підходи, запропоновані різними дослідниками для вирішення цих загроз.

- Механізм автентифікації.

Щоб переконатися, що лише законний користувач входить або реєструється в соціальній мережі, а не соціальні роботи, деякі OSN використовують процедури автентифікації, такі як CAPTCHA, багатофакторна автентифікація та ідентифікація за фотографіями друзів. Наприклад, провідні соціальні мережі, такі як Twitter і Facebook, використовують принципи двофакторної аутентифікації. Цей принцип використовує пароль для входу та код підтвердження, отриманий через мобільний пристрій. Це допомагає знизити ризик зламу облікового запису та запобігає викраденню зловмисником законного облікового запису та розміщенню шкідливого вмісту.

- Налаштування безпеки та конфіденційності.

Багато сайтів соціальних мереж надають параметри безпеки та конфіденційності, які можна налаштувати, щоб клієнт міг захистити свою особисту інформацію від небажаного доступу сторонніх осіб або програм. Наприклад, клієнт Facebook може змінити налаштування безпеки та вибрати аудиторію (наприклад, друзів, друзів друзів і всіх) у мережі, які можуть бачити їхні деталі, зображення, публікації та іншу конфіденційну інформацію. Крім того, Facebook додатково дозволяє своїм користувачам

підтверджувати або відхиляти доступ сторонніх додатків до їх особистої інформації. Багато сайтів соціальних мереж оснащено внутрішніми засобами безпеки системи. Вони захищають користувачів мережі від спаму, підроблених профілів, спамерів і різних ризиків.

- Повідомлення про підозрілих користувачів.

Соціальні мережі в Інтернеті захищають молоде покоління та підлітків від утисків, надаючи можливість повідомляти про будь-яку форму зловживання чи порушення політики будь-яким користувачем у їхній мережі. Наприклад, якщо користувач бачить у Facebook щось, що є неприйнятним для настроїв особи, але це не порушує умови Facebook, тоді користувач може використати посилання для звіту, щоб надіслати повідомлення тому, хто це опублікував, із проханням прийняти це або видалити.

- Виявлення фішингу.

Фішинг порушує конфіденційність і безпеку багатьох традиційних веб-додатків, таких як веб-сайти, сайти соціальних мереж, електронні листи та блоги. Отже, було розроблено кілька методів захисту від фішингу для виявлення фішингових атак. Багато дослідників запропонували процедури боротьби з фішингом, які базуються на техніках, які намагаються ідентифікувати фішингові веб-сайти та фішингові URL-адреси. Оскільки фішингові атаки стають все більш поширеними на веб-сайтах соціальних мереж, дослідницьке співтовариство запропонувало спеціальні рішення для фішингових атак у середовищі соціальних мереж. Наприклад, Aggarwal et al. запропонував техніку PhishAri для ідентифікації фішингових атак у режимі реального часу в Twitter. Він використовував спеціальні функції Twitter, такі як вік облікового запису та кількість підписників, щоб визначити, чи опублікований твіт є фішинговим чи безпечним [3].

- Виявлення кіберзалякування.

Хоча виявлення кіберзалякування складніше, ніж виявлення расистської лексики та спаму, деякі дослідники намагалися виявити це за допомогою більш складного представлення документів і додаткової інформації про жертв і хуліганів [3].

Для виявлення кіберзалякування можна застосовувати методи машинного навчання. Замість того, щоб використовувати лише слова та смайли, які виражають образи, непристойність і типові слова кібербулінгу, він також може використовувати деяку додаткову інформацію, як-от стать і особистість учасників підозрюваної події кібербулінгу. Щоб мати справу з невизначеністю та неточністю, можна використовувати нечітку систему на основі правил, яка є математичним інструментом. Для оптимізації результатів використовуються генетичні алгоритми прямим і стохастичним методами.

- Кібергрумінг.

Ефективним заходом для вирішення проблеми онлайн-кібердогляду є методи машинного навчання. Міхалопулос та ін. [3] представили систему розпізнавання атак грумінгу (GARS) — техніку розпізнавання, аналізу та контролю атак грумінгу, щоб діти могли бути захищені від онлайн-атак. Він розраховує загальне значення ризику, яке визначає загрози догляду, яким піддається дитина, аналізуючи розмови дитини. Порогове значення попередньо визначено для значення ризику, і коли загальне значення ризику перетинає попередньо визначений поріг, спрацьовує механізм тривоги. Цей механізм сигналізації також одночасно передає попереджувальне повідомлення на місці батькам. Виробляється кольоровий сигнал, який попереджає дитину про ступінь небезпеки розмови. Було оцінено використання та ефективність профілю для виявлення сексуальних хижаків. За допомогою цієї оцінки також досліджували агресивні текстові повідомлення.

- Клікджекінг.

Було спроектовано і розроблено автоматизовану систему, яка може аналізувати веб-сторінки, щоб захистити користувача від атак зловмисників. Вона складається з коду, який може виявляти накладання елементів, які можна натиснути. І на додаток до цього рішення, також застосовано інструмент NoScript, який містить функцію захисту від клікджекінгу. Запропоновано рішення, до якого додано інші візуальні компоненти, які гарантують, що користувач не зможе продовжити свої дії, доки він не матиме видимості над наявним елементом керування. Щоб забезпечити роботу цього рішення, було забезпечено існування об’єкта HyperText Markup Language (HTML), що містить шаблон. Деякі контрольні точки генеруються на основі взаємодії користувача. Користувач повинен дотримуватися цих контрольних точок без жодного клацання мишею. На додаток до нього, область панелі показує ідентифікатор третьої сторони. А для забезпечення цілісності дій використовується контроль перевірки інтерфейсу користувача. Цю техніку можна застосувати двома способами: один полягає в генеруванні випадкових шаблонів, за якими користувач повинен слідувати цьому шаблону, щоб далі поширювати свою дію, а інший спосіб полягає в тому, щоб попросити користувача намалювати той конкретний шаблон, який він уже зареєстрував. Корпорація Майкрософт представила X-FRAME-OPTIONS, заголовок протоколу передачі гіпертексту (HTTP), який надсилається у відповідь HTTP, як захист від блокування фреймів і клікджекінга в Internet Explorer 8. JavaScript також можна використовувати як захист від клікджекінга [3].

- Кіберпереслідування.

Методи шифрування доступні для пристроїв на останніх версіях Android та iOS. Якщо пристрій викрадено, злодій не зможе прочитати вміст, якщо ввімкнено шифрування. Крім того, будь-які спроби прочитати інформацію з внутрішньої або зовнішньої пам'яті перешкоджають наявності пароля пристрою [3]. Існують різні технології, які можна

використовувати проти сталкерів, як-от антивірус для блокування відбитків пальців на смартфоні, спеціалізоване програмне забезпечення для виявлення сталкерів, брандмауери та засоби захисту конфіденційності. Шифрування пристрою можна використовувати проти шпигунського ПЗ, додатків сталкерів і крадіжки пристрою.

- Кібершпигунство.

Кібершпигунство є різновидом цілеспрямованої атаки. Описано концепцію системи виявлення АТА та введено контрольний список проектування системи який явно призначений для ідентифікації цілеспрямованих атак [3]. Організації можуть створити власну команду для боротьби з цілеспрямованими атаками та аналізу вразливостей у своєму та коді інших компаній. У Google є власна команда для аналізу вразливостей і помилок у коді. Кожна компанія має свій профіль, який відрізняється один від одного. Отже, кожна компанія повинна вжити відповідних заходів відповідно до свого профілю для впровадження заходів безпеки, щоб розробити та запровадити засоби контролю безпеки для усунення різноманітних ризиків безпеки. Організації також можна певною мірою захистити від цілеспрямованих атак за допомогою систем автентифікації. Раніше для захисту даних використовувався лише пароль, але тепер використовується двофакторна система автентифікації, яка являє собою комбінацію пароля та деяких пін-кодів або біометричних даних. Це безпечніше, ніж використання одного фактора, наприклад пароля. Дані, які більше не потрібні для комерційних цілей, повинні бути видалені з мережі компанії. Зберігання таких записів може створити ризик несанкціонованого доступу до конфіденційної інформації в організації [3].

- Фейковий профіль.

Існує модель для розрізнення підроблених облікових записів і профілів. Злочинці видобули деякий вміст профілів користувачів із платформи LinkedIn і обробили цей вміст профілів, щоб отримати різні

функції. Після попередньої обробки профілів через головний компонент створюється навчальний набір із використанням стійкого алгоритму зворотного поширення в нейронній мережі. Для визначення характеристик профілю використовуються опорні векторні машини (SVM). запропоновано модель, яка виявляє бот-мережу за допомогою адаптивного багаторівневого підходу машинного навчання. У запропонованій роботі була представлена структура виявлення ботів на основі дерев рішень, яка ефективно виявляє ботнети P2P. Крім того, запропоновано модель ансамблевої класифікації для виявлення фейкових новин, яка досягла кращої точності порівняно з іншими сучасними моделями. Запропонована модель витягує важливі функції з наборів даних фейкових новин, а витягнуті функції потім класифікуються за допомогою моделі ансамблю, що складається з трьох популярних моделей машинного навчання, а саме дерева рішень, випадкового лісу та класифікатора додаткового дерева. Крім того, представлено систематичний огляд літератури щодо існуючих схем виявлення вузлів-клонів з деяким теоретичним та аналітичним оглядом існуючих централізованих і розподілених схем для виявлення вузлів-клонів у середовищі статичних WSN.

- Виявлення Сибіл.

Аль-Куріші запропонували нову систему виявлення Sybil, яка використовує модель глибокого навчання для точного прогнозування атаки Sybil. Ця модель складається з трьох модулів, а саме: одного модуля збору даних, одного модуля вилучення ознак і моделі глибокої регресії. Усі ці три модулі працюють у систематичній формі разом для аналізу профілю користувача в Twitter. Рахман представив модель під назвою SybilTrap, яка є напівконтрольованою системою навчання на основі графів, яка використовує методи, засновані на вмісті та структурі, для виявлення атак Sybil. Він заснований на напівконтрольованому алгоритмі, який використовує інформацію графа взаємодії вузла, де позначена інформація

вузлів протікає через непомічені вузли. Він збирає інформацію про мережу та її користувачів і використовує цю інформацію для виявлення зловмисників. Ця система стійка до різних стратегічних атак, таких як цілеспрямовані або випадкові атаки. Він розроблений для роботи в будь-яких умовах і застосовний до всіх існуючих соціальних мереж незалежно від рівня довіри до них [3].

- Виявлення спаму.

Запропоновано структуру під назвою SpamSpotter для вирішення проблеми спам-атаки на Facebook. Вона заснований на інтелектуальній системі підтримки прийняття рішень (IDSS). Збирає всю відповідну інформацію з профілю користувача за допомогою процесу прийняття рішень в IDSS, а потім аналізує її, зіставляючи дані користувача з класифікацією профілю користувача як спамера або законного. Це вирішує деякі проблеми та проблеми. Вирішує проблему неадекватного набору функцій, які існують у більшості систем виявлення спамерів. Це вирішує проблему невизначеності щодо критично важливих частин інформації Facebook і публічної недоступності. Використання системи IDSS вирішує проблему низької точності та високого часу відгуку. Використання класифікаторів машинного навчання в IDSS забезпечує швидкий час відповіді, що дуже важливо для виявлення спаму у Facebook.

- Шкідливе програмне забезпечення.

Фагані та Саіді виявили, що поведінка відвідувачів соціальної мережі впливає на розповсюдження хробаків XSS. Хробак поширюється повільніше, коли учасники здебільшого відвідують друзів, а не незнайомців. Його також може уповільнити кластерний характер соціальних мереж. Це тому, що заражені профілі на ранніх стадіях розповсюдження хробака XSS призводять до швидшого розповсюдження хробака.Розроблено підхід до виявлення хробаків, який використовує властивості онлайн-соціальної мережі та характеристик розповсюдження

хробаків OSN. Спочатку він створює мережу спостереження на основі властивостей соціального графа для збору доказів проти підозрілого розповсюдження хробаків. Він відстежує лише невелику частину облікових записів користувачів, щоб максимізувати охоплення спостереження. Щоб забезпечити відсутність шуму в мережі спостереження, пропонується схема. Таблиця 3 представляє ймовірність зустрічі різних типів загроз на різних платформах, розглянутих у розділі «Вступ». Це показує, що платформи, які використовуються для соціальних зв’язків, є найбільш вразливими серед усіх платформ.

2.1.2 З боку власників облікових записів

Ось 6 найкращих порад для зменшення ризиків соціальних мереж для акаунту:

- Увімкнути двохфакторну автентифікацію (2FA).

Двофакторна автентифікація — додатковий захист, що поєднується із стандартним рівнем у вигляді ПІН-коду чи пароля. Полягає захист у отриманні додаткового цифрового коду, який підтверджує користувача. Для отримання коду можуть використовуватись програми для автентифікації, push-сповіщення, програмні маркери.

- Реалізація строгої політики паролів.

Комбінація імені користувача та пароля стала вразливою, оскільки більшість не дотримуються належної гігієни паролів. Застосувавши надійну політику паролів, ви можете захистити свої облікові записи користувачів і внутрішню мережу від більшості типів паролів і спроб злому.

- Перевіряйте свої підписки.

Чим більше підписок, тим більша загроза від шахрайських або скомпрометованих атак. Не кожен у соціальних мережах є вашим потенційним другом. У темних куточках соціальних мереж блукає чимало загроз.

Навіть якщо дбаєте про безпеку, не всі у вашій особистій мережі можуть бути настільки пильними чи технічними. Хтось у онлайн-мережі може несвідомо поділитися зловмисним посиланням, створюючи небезпеку для облікового запису чи мережі. Тому потрібно бути обережними щодо того, з ким зв'язуєтеся та взаємодієте в Інтернеті.

- Контроль поширеної інформації.

Інформацію, яку розміщують на цих платформах, можуть позбирати зловмисники для створення цільових фішингових електронних листів для викрадення облікових записів і шкоди репутації або отримати доступ до внутрішніх мереж.

Тому, щоб захистити свій акунт, потрібно мати чітку політику щодо соціальних мереж. Ці політики повинні регулювати, якою інформацією можна, а що не можна ділитися, використання ділових і особистих облікових записів і активів, як реагувати на неприйнятний або делікатний вміст і як керувати ризиками прямого чи непрямого збитку репутації.

- Ознайомлюйтесь із можливими загрозами.

Атаки в соціальних мережах становлять реальну небезпеку для акаунта. Регулярні програми підвищення обізнаності та навчання можуть допомогти розпізнавати атаки в соціальних мережах і захистити акаунт від фішингових атак у соціальних мережах.

2.2 Роль штучного інтелекту (ШІ) у просуванні та потенційній боротьбі з дезінформацією

Програмісти, які розробляють алгоритми ранжування мемів у соціальних мережах, припускають, що «мудрість натовпу» швидко визначить високоякісні елементи; вони використовують популярність як проксі для якості. Разом з тим, дослідження 2015 року проаналізувало емпіричні дані про «емоційне зараження» в Twitter і виявило, що люди, які

надмірно стикаються з негативним контентом, як правило, діляться негативними публікаціями, тоді як ті, хто надмірно стикається з позитивним контентом, як правило, діляться більше. позитивні пости. Оскільки негативний контент поширюється швидше, ніж позитивний, емоціями легко маніпулювати, створюючи розповіді, які викликають негативні реакції, такі як страх і тривога.

Якість інформації ще більше погіршується соціальними ботами, які можуть використовувати всі наші когнітивні лазівки. В роботі показали, що під час референдуму про незалежність Каталонії в Іспанії в 2017 році соціальні боти використовувалися для ретвітів насильницьких і провокаційних історій, загострюючи соціальний конфлікт.

Ботів легко створити. Платформи соціальних медіа надають так звані інтерфейси прикладного програмування, завдяки яким одному учаснику досить легко налаштовувати й контролювати тисячі ботів. Але посилення повідомлення, навіть за допомогою лише кількох ранніх голосувань ботів на платформах соціальних мереж, таких як Reddit, може мати величезний вплив на подальшу популярність публікації.

Наразі існує декілька алгоритмів машинного навчання для виявлення соціальних ботів. Один із них, Botometer, є загальнодоступним інструментом, який витягує 1200 характеристик із заданого облікового запису Twitter, щоб охарактеризувати його профіль, друзів, структуру соціальної мережі, часові моделі активності, мову та інші особливості. Програма порівнює ці характеристики з характеристиками десятків тисяч раніше ідентифікованих ботів, щоб оцінити обліковий запис Twitter за ймовірне використання автоматизації.

У 2017 році було підраховано, що до 15% активних облікових записів Twitter були ботами — і що вони зіграли ключову роль у поширенні дезінформації під час виборів у США 2016 року. За кілька секунд після публікації фейкової новинної статті, як-от статті, у якій стверджувалося, що

передвиборча кампанія Клінтон була залучена до окультних ритуалів, багато ботів опублікували її в Твіттері, а люди, введені в оману очевидною популярністю вмісту, ретвітнули її.

Боти також впливають на людей, вдаючи, що представляють людей із їхньої групи. Щоб швидко проникнути в онлайн-спільноту, боту потрібно лише слідкувати за кимось із онлайн-спільноти, ставити лайки та ретвітувати її. Відома модель, де деякі з агентів є ботами, які проникають у соціальну мережу та діляться оманливо привабливим вмістом низької якості. Моделювання показує, що ці боти можуть ефективно пригнічувати якість інформації всієї екосистеми, проникаючи лише в невелику частину мережі.

РОЗДІЛ 3. РЕКОМЕНДАЦІЇ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Правила безпеки для користувачів соціальних мереж

Використовуйте надійний пароль: для забезпечення безпеки облікових записів користувачі повинні вибрати надійний пароль. Він не повинен бути занадто коротким, оскільки короткі паролі можна легко вгадати. Він має бути достатньо довгим і містити буквено-цифрові значення з деякими спеціальними символами [3]. Користувачі не повинні використовувати той самий пароль, який вони використовують для інших облікових записів, оскільки якщо зловмисник якимось чином дізнається цей пароль, він може скомпрометувати всі облікові записи цього користувача. Отже, вибір надійного пароля може допомогти користувачеві захистити свій обліковий запис і профіль від несанкціонованого доступу.

Обмежте передачу даних про місцезнаходження: сьогодні передача інформації про місцезнаходження стала трендом. Багато сайтів соціальних мереж також запровадили функцію геотегування, яка автоматично позначає географічне розташування користувача, коли користувач завантажує будь-який мультимедійний файл у соціальні мережі . Користувач має перемкнути його в ручний режим, щоб він не позначав місце розташування автоматично. Повідомлення про місцезнаходження в Інтернеті робить користувача вразливим до таких злочинів у реальному житті, як пограбування. Отже, щоб зменшити цей ризик, користувач може опублікувати своє місцезнаходження пізніше після завершення візиту . Користувачі повинні дуже обережно завантажувати свій мультимедійний вміст онлайн, оскільки він може містити конфіденційні метадані, тому рекомендується перемкнути геотеги в ручний режим на всіх своїх мобільних пристроях і облікових записах. Також пропонується

використовувати програмне забезпечення, яке видаляє такі метадані із зображень перед завантаженням.

Будьте вибірковими щодо запитів друзів: видно, що багато користувачів приймають запити друзів, не аналізуючи повний профіль особи, яка запитує. Зазвичай люди приймають запити про дружбу на основі спільних друзів. Якщо у запитувача є спільні друзі, вони приймають його [3]. Іноді зловмисники навмисно роблять свій профіль привабливим або можуть видавати себе за обліковий запис. Отже, якщо особа, яка надсилає запит про дружбу, невідома, слід ігнорувати цей запит. Це може бути підроблений обліковий запис, який намагається викрасти конфіденційну інформацію.

Будьте обережні з тим, що ви публікуєте: користувачі повинні бути обережними зі своїми публікаціями, оскільки це може розкрити їх особисту інформацію, а іноді й інших. Багато організацій дотримуються суворих правил і норм для обміну інформацією та мультимедійним вмістом. Є багато повідомлень про те, що людей звільняють з роботи через незаконне поширення інформації. Цієї ситуації можна уникнути, якщо співробітники добре поінформовані про протоколи організації, в якій вони працюють, щодо зображень, відео та повідомлень, які вони публікують в Інтернеті. Нелегітимний обмін інформацією може завдати шкоди репутації організації на ринку, а також її даним та інтелектуальній власності.

Будьте уважні до посилань і сторонніх програм: нелегітимні користувачі можуть отримати доступ до чийогось облікового запису та отримати конфіденційну інформацію, поділившись шкідливим посиланням. Сьогодні скорочені URL-адреси стають дуже популярними на різних платформах соціальних мереж. Ці скорочені URL-адреси можуть бути захищені зловмисним кодом або сценарієм. Ці сценарії намагаються зібрати особисту та конфіденційну інформацію користувача, яка може порушити конфіденційність цього користувача. Крім того, хакери можуть

скористатися вразливістю стороннього додатку, який інтегрований у багато популярних соціальних мереж [3]. Прикладом такої сторонньої програми є ігри, які можна грати в онлайн-соціальних мережах, які запитують загальнодоступну інформацію користувача для використання їхніх послуг. Ця зібрана інформація може бути надана стороннім особам або третім особам. Щоб уникнути цього ризику, користувач повинен бути обережним, встановлюючи сторонні програми у своєму профілі.

Встановіть програмне забезпечення безпеки в Інтернеті: деякі загрози, шаблон яких відомий, можна легко виявити за допомогою антивірусів. Такі загрози, як кібергрумінг, кібербулінг, можна певною мірою виявити за допомогою антивірусного програмного забезпечення. Наші друзі можуть несвідомо поширювати багато шкідливих посилань, що перенаправляє користувача на якийсь фішинговий веб-сайт. Антивірусне програмне забезпечення слід регулярно оновлювати через наявність багатьох вірусів, створених хакерами щодня. Деякі сайти соціальних мереж також мають власні засоби безпеки, які користувачі можуть використовувати для захисту від кібератак.

3.2 Автоматизовані інструменти для користувачів соціальних мереж

3.2.1 Додатки для виявлення дезінформації

Існує ряд інструментів, які допомагають людям зрозуміти власні вразливі місця, а також слабкі місця платформ соціальних мереж. Одним з них є мобільний додаток під назвою Fakey , який допомагає користувачам навчитися виявляти дезінформацію. Гра імітує стрічку новин соціальних мереж, показуючи фактичні статті з джерел з низькою та високою довірою. Користувачі повинні вирішити, що вони можуть, а що не повинні ділитися, а що перевірити. Аналіз даних Fakey підтверджує поширеність соціального

стадування в Інтернеті: користувачі частіше діляться статтями з низькою довірою, якщо вважають, що ними поділилися багато інших людей.

Інша загальнодоступна програма під назвою Ноаху показує, як будь-який існуючий мем поширюється через Twitter. У цій візуалізації вузли представляють фактичні облікові записи Twitter, а посилання зображують, як ретвіти, цитати, згадки та відповіді поширюють мем від облікового запису до облікового запису. Кожен вузол має колір, що відображає його оцінку від Botometer, що дозволяє користувачам бачити масштаб, у якому боти посилюють дезінформацію. Журналісти-розслідувачі використовували ці інструменти, щоб виявити коріння кампаній з дезінформації, як-от змова «pizzagate» у США. Вони також допомогли виявити спроби придушення виборців, керовані ботами під час проміжних виборів у США в 2018 році. Однак маніпуляції стає все важче помітити, оскільки алгоритми машинного навчання стають кращими для імітації людської поведінки.

3.2.2 Додатки для виявлення ботів та об’єктів, які є популярними

Окрім поширення фейкових новин, кампанії дезінформації також можуть відвернути увагу від інших, більш серйозних проблем. Для боротьби з такими маніпуляціями є програмний інструмент під назвою BotSlayer. Він витягує хештеги, посилання, облікові записи та інші функції, які одночасно зустрічаються в твітах про теми, які користувач хоче вивчити. Для кожного об’єкта BotSlayer відстежує твіти, облікові записи, які їх публікують, і оцінки їхніх ботів, щоб позначати об’єкти, які є популярними та, ймовірно, посилюються ботами чи скоординованими обліковими записами. Мета полягає в тому, щоб дати можливість репортерам, організаціям громадянського суспільства та політичним кандидатам виявляти та відстежувати неавтентичні кампанії впливу в режимі реального часу.

3.3 Рекомендації щодо інституційних змін в організаціях та країнах

Ці програмні інструменти є важливою допомогою, але інституційні зміни також необхідні для стримування розповсюдження фейкових новин. Навчання може допомогти, хоча воно навряд чи охопить усі теми, щодо яких людей вводять в оману. Деякі уряди та платформи соціальних медіа також намагаються боротися з онлайн-маніпуляціями та фейковими новинами. Але хто вирішує, що є фейком чи маніпуляцією, а що ні? Інформація може супроводжуватися попереджувальними мітками, такими як Facebook і Twitter, але чи можна довіряти людям, які ставлять ці мітки? Ризик того, що такі заходи можуть навмисно чи ненавмисно пригнічувати свободу слова, яка життєво важлива для надійних демократій, реальний. Домінування платформ соціальних мереж із глобальним охопленням і тісними зв’язками з урядами ще більше ускладнює можливості.

Однією з найкращих ідей може бути ускладнення створення та поширення неякісної інформації. Це може спричинити додаткове тертя, змусивши людей платити за обмін або отримання інформації. Оплата може здійснюватися у вигляді часу, розумової роботи, як-от розгадування головоломок, або мікроскопічної плати за підписку чи використання. Автоматичне розміщення слід розглядати як рекламу. Twitter обмежив автоматичні публікації. Ці зусилля можна розширити, щоб поступово перемістити стимули для обміну в Інтернеті на інформацію, яка є цінною для споживачів.

РОЗДІЛ 4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Кваліфікаційна робота магістра присвячена аналізу технології впливу соціальних мереж на інформаційну безпеку. Враховуючи що користувачі використовують для соц. мереж не лише телефони, але й комп'ютери, то важливим є дотримання вимог з охорони праці і техніки безпеки при роботі з комп'ютером.

Основні принципи правильної роботи за комп’ютером:

- у робочому приміщенні (кімнаті), де встановлені комп’ютери, щодня потрібно виконувати вологе прибирання;
- приміщення, у якому знаходяться комп’ютери, потрібно провітрювати щогодини;
- після кожної години роботи рекомендується робити десяти хвилинну перерву, яку зручно суміщати з провітрюванням. За будь-яких умов безперервна робота за комп’ютером для дорослої людини не повинна перевищувати двох годин. Під час перерви не варто читати або дивитися телевізор. Перерва, яку проводиться за комп’ютером (наприклад, граючись або шукаючи матеріали в Інтернеті), просто не має сенсу;
- необхідно постійно слідкувати за станом екрану монітора: він має бути чистим, без плям та пилу. Крім того, обов’язково слідкуйте за чистотою окулярів – комп’ютерних чи звичайних;
- слідкуйте за поставою: ноги твердо стоять на підлозі чи на спеціальній підставці; стегна розташовані під прямим кутом до тулуба, а гомілки – під прямим кутом до стегон; сидіти потрібно прямо або злегка нахилившись вперед; пальці рук знаходяться на рівні зап’ястків або трохи нижче – у такому положенні вони найбільш рухливі; плечі мають бути розслаблені та вільно опущені, що сприяє розслабленню рук; відстань від

очей до екрану монітора – не менше 55-60 см; центр екрану має знаходитися на рівні очей чи трохи нижче; рекомендується хоча б раз на день виконувати гімнастику для очей;

- щоб попередити „синдром сухого ока”, моргайте кожні 3-5 секунд;
- як не дивно, але й у наш час є люди, які замість монітору використовують звичайний телевізор. Так чинити категорично не рекомендується: випромінювання від телевізора практично у сто разів перевищує випромінювання монітора. Це зумовлено тим, що телевізор призначений для перегляду на значній відстані;
- у процесі роботи за комп’ютером обов’язково звертайте увагу на дихання: воно має бути рівномірним, без затримок;
- при роботі з текстом рекомендується, щоб колір шрифту був темним, а колір фону – світлим (ідеальний варіант – чорний шрифт на білому фоні);
- якщо шрифт занадто мілкий, то потрібно збільшити масштаб документу (наприклад, до 150% чи більше);
- при наборі текстів з паперів чи книг рекомендується помістити джерело якомога ближче до монітору. Це дозволить уникнути частих рухів головою та очима;
- якщо є можливість, міняйте вид діяльності, якою займаєтеся протягом дня;
- у процесі роботи рекомендується періодично (приблизно раз на 20-30 хвилин) переводити погляд з екрану на найбільш віддалений предмет у кімнаті, а ще краще – на віддалений об’єкт за вікном;
- якщо з’явилося відчуття втоми, напруження, сонливості, тяжкості в очах, потрібно припинити роботу та хоча б трохи відпочити.

Рекомендовані умови для роботи за персональним комп'ютером:

- Сидіть глибоко на твердому стільці з високою спинкою, що має вигин для попереку, - це вирівняє спину і дасть підтримку шиї. Край стільця не повинен тиснути на судини під колінами.
- Відстань до монітора повинна бути 50-70см.
- Використовуйте мишку відповідних розмірів, зручної форми.
- Робіть перерву в сидячій роботі, вставайте і ходіть 15-20 хвилин кожні 1-2 години.
- Правильно організуйте освітлення робочого місця. При слабкому світлі очі напружуються і болять. Стримайте яскравість екрану. Літери і цифри на екрані це маленькі світлові промені, які йдуть прямо в очі. Потрібно відрегулювати їх контрастність, щоб світло не був дуже яскравим.
- Закривайте очі для відпочинку. Час від часу відводите очі вбік, щоб дати відпочити своєму зору.
- Переміщайте погляд по всій площі екрану, намагайтеся не дивитися напружено в одну точку. Нехай поперемінно працюють всі м'язи очей, а не окремі групи, на які в цьому випадку буде падати максимальне навантаження.
- Використовуйте спеціальний очний гель (Визин, Видисик), який запобігає «обсушування» рогівки ока. Запобігти захворювання можуть окуляри для роботи за комп'ютером, які має особливе покриття.

Наслідки неправильної роботи за пк:

- Неправильна постава - це призводить до подальшого розвитку викривлення хребта сколіозу, лордозу, кіфозу, а як результат головні болі, болі в області шиї і всього хребта, болі в області таза. Неправильно положення ніг може привести до артриту (запалення суглобів), артрозу (деформації).

- Тунельний синдром - найвідоміше захворювання людей працюють за комп'ютером. Воно ж синдром зап'ястного каналу. Тунельний синдром проявляється після кількох годин напруженої роботи за комп'ютером. Синдроми - почуття «бігають мурашки" на кисті, біль пронизує кисть, оніміння кисті, важкість у руці, знесилення кисті.

Тунельний синдром надає собою травму зап'ястя. Через зап'ястний канал між кістками (тунель) проходять серединний нерв і 9 сухожиль м'язів кисті. Серединний нерв забезпечує чутливість пальців, а також управляє м'язами, що забезпечують руху великого, вказівного і середнього пальців. Сам тунельний канал дуже вузький. В і стискається, защемляється серединний нерв. Під час частих, повторюваних рухів кистей рук в незручному положенні сухожилля труться об кістки зап'ястя і зв'язки. Постійно повторювані дрібні рухи пальцями призводять до внутрішніх мікротравм. Накопичуючись, вони і дають про себе знати в початковій стадії хвороби тремтінням, сверблячкою набряком і поколювання в пальцях.

- Розвиток короткозорості - через те, що екран монітора за контрастом вище, ніж навколишні об'єкти розвивається короткозорість.
- Порушення фокусування - наслідком напруженої роботи за монітором є порушення фокусування, яка може бути викликана перенапруженням очних м'язів.
- Сухість очей - через рефлексу, заснованого на тому, що при погляді на джерело світла очей починає менше моргати виникає «обсушування» рогівки ока яке призводить до очних болів.

4.2 Фактори, що впливають на функціональний стан користувачів комп’ютерів

Трудова діяльність користувачів комп'ютерів (ВДТ) відбувається у певному виробничому середовищі, яке впливає на їх функціональний стан. Найбільш значимі — фізичні фактори виробничого середовища, до яких належать електромагнітні хвилі різних частотних діапазонів, електростатичні поля, шум, параметри мікроклімату та ціла низка світлотехнічних показників. Вплив хімічних та, особливо, біологічних факторів виробничого середовища на користувачів комп'ютерів — значно менший. Трудовий процес суттєво впливає на психофізіологічні можливості користувачів комп'ютерів, оскільки їх діяльність характеризується значними статичними фізичними навантаженнями; недостатньою руховою активністю; напруженнями сенсорного апарату, вищих нервових центрів, які забезпечують функції уваги, мислення, регуляції рухів. Окрім того, трудовий процес користувачів комп'ютерів відзначається значними інформаційними навантаженнями. Професійні якості та виробничий досвід, які визначають внутрішні засоби діяльності, обумовлюють надійну та безпомилкову діяльність користувачів комп'ютерів, дозволяють знаходити безпечні методи розв'язання виробничих завдань навіть у нестандартних ситуаціях. Зовнішні засоби діяльності, які в основному визначаються ергономічними показниками щодо організації робочого місця, форми та параметрів його елементів, просторового розташування основного і допоміжного устаткування, можуть суттєво знизити фізичні та психофізіологічні навантаження, що діють на користувачів комп'ютерів.

У професійних операторів частіше зустрічаються порушення органів зору, опорно-рухового апарату, центральної нервової, серцево-судинної, імунної та статевої систем, захворювання шкіри. Зафіксована значна

кількість скарг операторського персоналу на загальне недомагання, передчасне стомлювання, головний біль, порушення функцій органів зору, які здійснювали несприятливий психофізіологічний вплив на самопочуття та працездатність операторів. Сучасна професія користувача ВДТ належить до розумової праці, яка характеризується: високою напруженістю зорових функцій; одноманітною позою; великою кількістю стереотипних висококоординованих рухів, що виконуються лише м'язами кистей рук на фоні малої загальної рухової активності; значним нервово-емоційним компонентом, особливо в умовах дефіциту часу; роботою з великими масивами інформації, що викликає активізацію уваги та інших вищих психічних функцій. Крім того, при роботі з дисплеями на електронно-променевих трубках виникає вплив на користувача цілої низки факторів фізичної природи — електростатичні поля, радіочастотне та рентгенівське випромінювання тощо. Діяльність професіоналів можна поділити на три групи: 1. Діяльність, яка пов'язана з виконанням нескладних багаторазово повторюваних операцій, що не вимагають великого розумового напруження. Наприклад, робота операторів комп'ютерного набору, працівників довідкових служб. 2. Діяльність, яка пов'язана із здійсненням логічних операцій, що постійно повторюються. Це робота інженера-економіста, інженера-проектувальника, оператора автоматизованого виробництва. 3. Діяльність, коли в процесі роботи необхідно приймати рішення за відсутності заздалегідь відомого алгоритму. Наприклад, робота інженера-програміста, диспетчерів руху залізничного транспорту, аеропортів тощо. У користувачів, які інтенсивно використовують комп'ютер в умовах значних розумових напружень досить часто (40—70%) виникають психологічні та поведінкові порушення (нервозність, роздратування, тривога, нерішучість, замкнутість тощо). Серед користувачів ВДТ в США і Європі значного поширення набуло специфічне захворювання, яке отримало назву синдром комп'ютерного стресу (СКС).

СКС супроводжується головним болем, запаленням очей, алергією, роздратованістю, млявістю і депресією. Інформаційне перевантаження користувачів ВДТ супроводжується низкою специфічних захворювань, які називають інформаційними. Першим симптомом їх є головний біль. Дослідження, проведені в США, Німеччині, Швейцарії та інших країнах, показали, що робота з обслуговування ВДТ супроводжується підвищеним напруженням зору, інтенсивністю і монотонністю праці, збільшенням статичних навантажень, нервово-психічним напруженням, впливом різного виду випромінювань та ін. Внаслідок цього серед операторів ВДТ, як зазначають фахівці Всесвітньої організації охорони здоров'я, частіше, ніж в інших групах працюючих, трапляються такі професійні захворювання, як передчасна стомлюваність, погіршення зору, м'язові і головні болі, психічні й нервові розлади, хвороби серцево-судинної системи, онкологічні захворювання та ін. Вважається, що стан організму операторів ВДТ визначається комплексним впливом факторів трудового процесу і середовища, значення яких є неоднаковим. На операторів з малим стажем роботи на ВДТ домінуючий вплив чинять фактори середовища, а на операторів зі стажем понад 5 років - фактори трудового процесу.

ВИСНОВКИ

В ході виконання роботи було проведено аналіз соціальних мереж . За результатами аналізу був зроблений висновок, що соц. мережі мають великий вплив на інформаційну безпеку не тільки користувачів, але й організацій та країн в цілому . Тому було проведено визначення загроз, які є характерними для даних мереж та методів боротьби з ними.

Наведено основні правила користування соціальним мережами для користувачів. Проаналізовано методи боротьби кожної мережі із загрозами та надано рекомендації для змін в організаціях та країнах.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Загрози інформаційної безпеки [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B8_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8 (дата звернення 05.10.2022).

2. ДЕЗИНФОРМАЦИЯ В СОЦИАЛЬНЫХ СЕТЯХ: КАК РАСПОЗНАТЬ И КАК БОРОТЬСЯ? [Електронний ресурс]. URL: https://marketer.ua/ru/disinformation-in-social-networks-how-to-recognize-it/ (дата звернення: 07.10.2022).

3. Віддалені мережеві атаки[Електронний ресурс]. URL: https://ru.wikipedia.org/wiki/%D0%A3%D0%B4%D0%B0%D0%BB%D1%91%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D1%8B%D0%B5_%D0%B0%D1%82%D0%B0%D0%BA%D0%B8 (дата звернення: 06.10.2022)

4. ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА: СОЦІОТЕХНІЧНИЙ АСПЕКТ. URL: http://ippi.org.ua/sites/default/files/dovsmib_46_2_2015_0.pdf (дата звернення 10.10.2022).

5. СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ВПЛИВУ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ[Електронний ресурс]. URL: http://ippi.org.ua/sites/default/files/dovsmib_46_2_2015_0.pdf (дата звернення 10.10.2022).

6. Забезпечення інформаційної безпеки у соціальних мережах[Електронний ресурс]. URL:http://dspace.kntu.kr.ua/jspui/bitstream/123456789/4999/1/AUConferenceCyberSecurity_November2016_p204.pdf (дата звернення 12.10.2022).

7. Дезинформация в социальных сетях: состояние и перспективы психологических исследований[Електронний ресурс]. URL:

https://psyjournals.ru/files/93632/sps_2018_n2_Miheeva_Nestik.pdf(дата звернення 20.10.2022).

8. Рапорт компанії Norton[Електронний ресурс]. URL: https://www.yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf (дата звернення 12.09.2022).

9. Щорічний рапорт Cisco[Електронний ресурс]. URL: http://expo.jspargo.com/exhibitor/web/Cisco2016AnnualSecurityReport.pdf (дата звернення 15.09.2022).

10. Один із п'яти бізнесів інфікований зловмисним програмним забезпеченням через соцмережі[Електронний ресурс]. URL: http://www.pandasecurity.com/mediacenter/social-media/uh-oh-one-out-of-five-businesses-are-infected-by-malware-through-social-media/ (дата звернення 19.09.2022).

11. Війна в соцмережа між Росією та США[Електронний ресурс]. URL: https://time.com/4783932/inside-russia-social-media-war-america/ (дата звернення 23.09.2022).

12. Press releases[Електронний ресурс]. URL: https://www.symantec.com/about/newsroom/press-releases/2011/symantec_0721_01 (дата звернення 27.09.2022).

13. Telegram[Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/Telegram (дата звернення 27.09.2022).

14. Криптосистема RSA[Електронний ресурс]. URL : https://de.wikipedia.org/wiki/RSA-Kryptosystem (дата звернення 30.09.2022).

15. Протокол Ди́ффи — Хе́ллмана[Електронний ресурс]. URL: https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%94%D0%B8%D1%84%D1%84%D0%B8_%E2%80%94_%D0%A5%D0%B5%D0%BB%D0%BB%D0%BC%D0%B0%D0%BD%D0%B0 (дата звернення 30.09.2022).

16. SHA-1[Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/SHA-1 (дата звернення 30.09.2022).

17. Битва за біженців. Як проросійські телеграм-канали на (ново)окупованих територіях намагаються утримати людей від евакуації[Електронний ресурс]. URL: https://texty.org.ua/articles/107294/bytva-za-bizhenciv-yak-prorosijski-telehram-kanaly-na-novookupovanyh-terytoriyah-namahayutsya-utrymaty-lyudej-vid-evakuaciyi/ (дата звернення 08.10.2022).

18. "Зґвалтуємо матір та сестру". Як українським військовим погрожують в інтернеті[Електронний ресурс]. URL: https://www.bbc.com/ukrainian/features-63493253 (дата звернення 15.10.2022).

19. Facebook[Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/Facebook (дата звернення 18.10.2022).

20. How the Facebook Algorithm Works in 2023 and How to Make it Work for You[Електронний ресурс]. URL: https://blog.hootsuite.com/facebook-algorithm/ (дата звернення 22.10.2022).

21. Twitter[Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/%D0%A2%D0%B2%D1%96%D1%82%D1%82%D0%B5%D1%80 (дата звернення 28.10.2022).

22. The Twitter Rules[Електронний ресурс]. URL: https://help.twitter.com/en/rules-and-policies/twitter-rules (дата звернення 28.10.2022).

23. How The Twitter Algorithm Works[Електронний ресурс]. URL: https://www.searchenginejournal.com/twitter-algorithm/467459/ (дата звернення 28.10.2022).

24. Role of Social Networks in E-government: Risks and Security Threats[Електронний ресурс]. URL: https://www.researchgate.net/publication/328896849_Role_of_Social_Networks_in_E-government_Risks_and_Security_Threats (дата звернення 01.11.2022).

25. Social Media Security Risks To Businesses And Best Practices[Електронний ресурс]. URL: https://www.itjones.com/blogs/2020/9/1/social-media-security-risks-to-businesses-and-best-practices (дата звернення 07.11.2022).

ДОДАТОК А – АПРОБАЦІЯ НАУКОВОЇ РОБОТИ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

X НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

7–8 грудня 2022 року

ТЕРНОПІЛЬ
2022

УДК 004.056
М. Турчиняк
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ТЕХНОЛОГІЇ ВПЛИВУ СОЦІАЛЬНИХ МЕРЕЖ НА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

UDC 004.056
M. Turchyniak

TECHNOLOGIES OF THE INFLUENCE OF SOCIAL NETWORKS ON ENSURING INFORMATION SECURITY

Науково-технічна революція початку XXI сторіччя спричинила в усьому світі глибокі системні перетворення. Передусім завдяки поєднанню досягнень у сфері новітніх інформаційно-комунікаційних технологій (ІКТ)[1] із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем (ІТС), сформувалися принципово нові глобальні субстанції – інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу.

Разом з тим, феномен «соціальних медіа» пов'язаний більше з культурним позиціонуванням, ніж з технологічними можливостями. Соціальні мережі швидко набули популярності і стали одним із найкращих способів проведення вільного часу та залучення клієнтів. Вони дозволяють людям підтримувати зв'язок з друзями та родиною, надають можливості пошуку кар'єрних можливостей, обміну власними думками, почуттями та ідеями в Інтернеті. Однак, використання соціальних медіа також може мати негативний вплив на особисте життя людини.

Із зростанням репутації LinkedIn, Facebook, Telegram зростають і ризики їх використання. Вільне спілкування не є безкоштовним. Зменшивши вартість інформації, втрачається її цінність і збільшується ймовірність її фальсифікації. Щоб відновити здоров'я інформаційної екосистеми, необхідно зрозуміти вразливі місця перевантаженого розуму та те, як можна використати економіку інформації, щоб захистити людей від введення в оману.

Згідно матеріалів The New York Post щодня лише у Facebook зламують 160 000 облікових записів, а дослідники Університету Фенікса що близько 66% облікових записів громадян США було хоч раз зламано (це означає, що якщо ви знаєте ім'я собаки свого менеджера соціальних мереж, ви на півдорозі до брут форсінгу облікового запису вашої організації). На відміну від інших активів, служби безпеки не можуть відключити зламаний обліковий запис у соціальних мережах, тобто зловмисник може зберігати контроль протягом годин, якщо не днів. Вартість? Кожна секунда, коли ви не контролюєте свій обліковий запис, спричиняє каскад вірусної інформації, що призводить до шкоди стосункам із брендом і клієнтом, втрати бізнесу, кошмарів зі зв'язків із громадськістю та витрат на підтримку клієнтів.

В доповіді наведено детальний аналіз[2] найбільш відомих атак на соціальні мережі. Надано пропозиції щодо забезпечення інформаційної безпеки в інтернет середовищі. До найбільш відомих атак належать:

- фішинг,
- викрадення особистих даних,
- розповсюдження зловмисного програмного забезпечення,
- соціальна інженерія та
- компрометація облікових даних банківського або системного входу.

Зокрема зазначено, що багато нападників координують свої зусилля серед білого дня. Відомо, що атаки розподіленої відмови в обслуговуванні (DDoS) використовують певний хештег Twitter для координації атаки. Зловмисники, особливо хактивісти, краудсорсингують учасників атак через кампанії з хештегами та керують DDoS-атакою в Twitter, публікуючи IP-адреси,

домени, інструменти атаки, час атаки та бажану ціль. Оскільки атаки використовують громадські місця для участі, команди безпеки можуть підготувати стратегію захисту, наприклад, ховати вхідні запити або координувати дії з мережевими командами, професійними службами та постачальниками послуг Інтернету (ISP). Команди безпеки також можуть стежити за розмовами учасників загрози, щоб виявити, чи згадується їх організація. Це одні з найчистіших, найдешевших, найактивніших і доступних у реальному часі даних про загрози. Дивно, але така публічна балаканина досить поширена. Аналізуючи, хто говорить і контекст ключової фрази, служби безпеки можуть отримати вирішальну систему раннього попередження проти атак. Зловмисники часто афішують або хваляться своїми успіхами в соціальних мережах. Вони також рекламують викрадені дані, які можуть продавати. Подібно до того, як соціальні медіа є основною рушійною силою діяльності легального ринку, ними також користуються продавці на чорному ринку. Організації можуть інтегрувати конфіденційну інформацію, виявлену на сайтах соціальних мереж, у фреймворки DLP, щоб швидше визначати, коли стався злом, і ефективніше починати дії з усунення. Витоку або викрадених даних частіше торгують у відкритому доступі, ніж усвідомлюють. Якщо облікові дані співробітників або конфіденційні файли виявлені в соціальних мережах або цифрових каналах, наприклад на сайтах вставлення, служби безпеки можуть оновити тренінги компанії, скинути облікові дані співробітників або відстежити, де заходи запобігання потенційній втраті даних (DLP) не змогли запобігти конфіденційним файлам, таким як медичні записи, інтелектуальну власність або інформацію облікового запису від виходу з мережі.

Для шахрая соціальні медіа є новим потужним інструментом для використання дуже специфічної масової групи користувачів, наприклад підписників певного бренду. Соціальні мережі [3] дозволяють шахраям націлюватися на цих користувачів, оскільки списки підписників бренду та залучення користувачів до фірмового хештегу є загальнодоступними. Таким чином, шахрай має безпрецедентну можливість отримати список жертв і розпочати цілеспрямовану атаку. Шахрайство, орієнтоване на клієнтів, зазвичай обіцяючи винагороду за певну вартість участі та використовує фальшиві логотипи бренду або історії успіху з інших облікових записів маріонеткових учасників, які вказують на те, що шахрайство є «законним». Ці шахрайства процвітають у соціальних мережах, тому що їх дуже легко створити та поширювати серед цільової аудиторії у великих масштабах. Навіть нетехнічний шахрай може створити групу фальшивих облікових записів, створених для коментування один одного та надання довіри, маючи лише підключення до Інтернету з будь-якої точки світу.

Соціальні медіа є неминучою константою для ведення бізнесу в сучасному світі. Оскільки маркетологи, рекрутери, продавці та рекламодавці постійно розширюють свою присутність, групи безпеки повинні працювати разом з ними, щоб гарантувати, що це робиться безпечно та надійно. Щоб усунути ризики соціальних мереж, служби безпеки повинні тісно співпрацювати з кількома іншими відділами. Усі інші департаменти стикаються з ризиками в соціальних мережах, і тепер командам безпеки доручено усунути ризики, одночасно забезпечуючи безпечне використання каналів соціальних мереж. Найголовніше, що команди безпеки повинні очолити цю ініціативу. Ризики в соціальних мережах залишаються.

Для зменшення ризиків[3] необхідно реєструватися не у всіх соцмережах, а лише у тих, які викликають довіру та пропонують надійні механізми аутентифікації і розмежування доступу до особистої інформації користувача, особливу увагу слід приділяти посиланням, які надходять від інших користувачів – вони можуть бути частиною фішингової чи фармінгової атаки.

Література

1. Інформаційна та кібербезпека: соціотехнічний аспект. URL: http://ippi.org.ua/sites/default/files/dovsmib_46_2_2015_0.pdf (дата звернення: 10.09.2022).
2. Рапорт компанії Norton. URL: https://www.yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf (дата звернення: 12.09.2022).
3. Забезпечення інформаційної безпеки у соціальних мережах. URL: http://dspace.kntu.kr.ua/jspui/ bitstream/123456789/4999/1/AUConferenceCyberSecurity_November2016_p204.pdf (дата звернення: 20.09.2022).