АКАДЕМІЯ УКРАЇНСЬКОЇ ПРЕСИ
ОКСАНА ПОЧАПСЬКА

(НЕ)БЕЗПЕКА В ЦИФРОВОМУ СВІТІ

НАВЧАЛЬНИЙ ПОСІБНИК З ЦИФРОВОЇ ГРАМОТНОСТІ ТА БЕЗПЕКИ

АКАДЕМІЯ УКРАЇНСЬКОЇ ПРЕСИ
Бібліотека масової комунікації та медіаграмотності Академії української преси

АКАДЕМІЯ УКРАЇНСЬКОЇ ПРЕСИ

Оксана Почапська

(НЕ)БЕЗПЕКА В ЦИФРОВОМУ СВІТІ

Навчальний посібник з цифрової грамотності та безпеки

АКАДЕМІЯ УКРАЇНСЬКОЇ ПРЕСИ

Бібліотека масової комунікації та медіаграмотності Академії української преси

УДК : 070:004.7:343.346(075.8)

Почапська О. І. (Не)безпека в цифровому світі. Навчальний посібник / Київ: Академія української преси, Центр вільної преси, 2024. 59 с.

Автор **Оксана Почапська**, доцент кафедри журналістики Кам'янець-Подільського національного університету імені Івана Огієнка (Україна), ад'юнкт Інституту філософії і соціології Польської академії наук (Польща)

Рекомендовано до друку
на засіданні кафедри журналістики
Кам'янець-Подільського національного університету імені Івана Огієнка
(протокол від 23 січня 2024 р. №1).

«(Не)безпека в цифровому світі» — це навчальний посібник, який допоможе зрозуміти цифрові виклики, загрози, з якими стикаються користувачі в Інтернеті, та основні навички безпечної роботи, збереження й передавання інформації, користування соціальними мережами.

Матеріал розділено за тематичними модулями, кожен з яких містить теоретичну інформацію, інструкції (алгоритми) до налаштування облікових записів, захисту персональних даних у соціальних мережах і под., завдання для самостійного виконання, а також списки джерел, які допоможуть глибше зрозуміти сутність описаної теми.

Загалом, «(Не)безпека в цифровому світі» є корисним джерелом інформації для всіх, хто хоче зберегти свою безпеку та конфіденційність у мережі.

АКАДЕМІЯ
УКРАЇНСЬКОЇ
ПРЕСИ

ISBN 978-617-7370-66-5

ЗМІСТ

ЦИФРОВА БЕЗПЕКА ЯК КЛЮЧОВА НАВИЧКА 4

МОДУЛЬ 1. ЦИФРОВІ ЗАГРОЗИ Й ВИКЛИКИ: ЯК ПОЧУВАТИСЯ БЕЗПЕЧНО 6

Технічні загрози й виклики 6

Психологічні загрози й виклики 11

Завдання 13

Джерела для поглибленого вивчення теми 14

МОДУЛЬ 2. ЕЛЕКТРОННА ПОШТА Й НАЛАШТУВАННЯ ОБЛІКОВИХ ЗАПИСІВ 16

Завдання 22

Джерела для поглибленого вивчення теми 22

МОДУЛЬ 3. СОЦІАЛЬНІ МЕРЕЖІ Й МЕСЕНДЖЕРИ: СПІЛКУЙСЯ БЕЗПЕЧНО 23

Завдання 28

Джерела для поглибленого вивчення теми 29

МОДУЛЬ 4. АНОНІМНІСТЬ У МЕРЕЖІ: ЯК НЕ ВЛЯПАТИСЬ У ЦИФРОВУ ІСТОРІЮ 30

Завдання 39

Джерела для поглибленого вивчення теми 40

МОДУЛЬ 5. ЯК ЗБЕРІГАТИ Й ПЕРЕДАВАТИ ІНФОРМАЦІЮ 41

Завдання 47

Джерела для поглибленого вивчення теми 47

МОДУЛЬ 6. ШТУЧНИЙ ІНТЕЛЕКТ І ОСОБЛИВОСТІ РОБОТИ З СЕРВІСАМИ, СТВОРЕНИМИ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ 48

Завдання 54

Джерела для поглибленого вивчення теми 54

ГЛОСАРІЙ 55

ПІСЛЯМОВА 58

ЦИФРОВА БЕЗПЕКА ЯК КЛЮЧОВА НАВИЧКА

Сучасний світ — це світ стрімкого розвитку інформаційних технологій і їхнього проникнення в усі сфери життя людини.

Цифрова грамотність — це одна з важливих навичок XXI століття. Сьогодні вона межує з життєво необхідними навичками і є запорукою безпечного життя людини не лише у віртуальному, але й у цілком реальному світі (поза усіма технічними засобами й мережами).

У швидкозмінному світі, де інформація поширюється з непередбачуваною швидкістю через різноманітні канали, розуміння специфіки функціонування мережі Інтернет, уміння аналізувати, вчасно виявляти й усувати потенційні небезпеки й ризики, що приходять до людей із цифрового простору, — це базові навички всіх і кожного.

Уявлення про те, що кіберзлочинці полюють виключно на «багатих і знаменитих» сьогодні спростовується чи не щодня. Злодіїв цікавить не тільки корпоративна інформація, вони зазіхають не лише на фінансові активи великих компаній і їхніх власників чи на пікантні фото знаменитостей, — дедалі частіше жертвами цифрових злочинів стають звичайні користувачі: шахраї отримують доступ до персональних даних (номери банківських рахунків і кредитних карток, паролі та ін.), отримують повний або частковий доступ до пристроїв, якими послуговуються пересічні люди.

Один із методів, яким активно користується ворог в інформаційній війні проти України та всього цивілізованого світу, — кібератаки на підприємства, ресурси, цифрову критичну інфраструктуру для дестабілізації ситуації та досягнення злочинних цілей. Страждають від цього, насамперед, звичайні громадяни, користувачі інформаційно-комунікаційними засобами, тому сьогодні надзвичайно важливо володіти базовими навичками та знаннями про те, як влаштований цифровий світ і як реагувати на його виклики.

Цифрова грамотність охоплює спектр навичок і знань. У її основі лежить здатність критично оцінювати цифрові джерела, аналізувати та виявляти потенційні ризики й небезпеки, здатність безпечно збирати, зберігати, опрацьовувати й передавати інформацію. З появою соціальних мереж та спрощених вимог до створення контенту, кожна людина повинна орієнтуватися в розгалуженому цифровому просторі, де інформація може швидко поширюватися.

Посібник «(Не)безпека в цифровому світі» складається з п'яти модулів і охоплює інформацію про цифрові виклики й загрози, правила безпечного використання облікових записів і електронної пошти, соціальних мереж і месенджерів. Окрім того, проаналізовані основні правила зберігання та передавання інформації, створення й збереження надійних паролів, специфіка використання VPN та програм-шифрувальників.

Цей посібник стане провідником у цифровій павутині, допоможе напрацювати звичку безпечного користування мережею Інтернет і цифровими пристроями. Він є гідним продовженням Бібліотеки масової комунікації та медіаграмотності Академії української преси. АУП видала

вже понад 140 підручників, посібників, навчальних програм тощо, які стали в нагоді сотням тисяч користувачів. Тільки у 2023 році нашими ресурсами скористалося більш ніж 140 тисяч унікальних користувачів. Певні, що цей посібник стане добрим порадником юзерам різного віку та досвіду.

Оксана Почапська,
доцент кафедри журналістики Кам'янець-Подільського національного університету імені Івана Огієнка, ад'юнкт Інституту філософії і соціології Польської академії наук

Валерій Іванов,
президент Академії української преси

Максим Запорожченко,
менеджер медіаосвітніх програм Академії української преси, завідувач центру цифрової освіти та медіакультури Миколаївського ОІППО

Модуль 1

ЦИФРОВІ ЗАГРОЗИ Й ВИКЛИКИ: ЯК ПОЧУВАТИСЯ БЕЗПЕЧНО

У цьому модулі поговоримо про те, які цифрові виклики й загрози сьогодні постають перед журналістами та що таке цифрова гігієна; чому важливо періодично аналізувати й виявляти потенційні загрози й небезпеки, а також про те, що цифровий світ несе не лише загрози технічні, але й психологічні.

ТЕХНІЧНІ ЗАГРОЗИ Й ВИКЛИКИ

З розвитком цифрових технологій ми дедалі частіше маємо справу не лише з перевагами цифрових мереж, але й із загрозами, які вони несуть кожному конкретному індивіду зокрема й стабільній діяльності компаній, підприємств, відомств і усій державі загалом.

Коли говоримо про загрози й виклики, ми повинні розуміти, що **загроза** — це всього лише потенційна небезпека, яка за певних обставин може призвести до негативних (небажаних) наслідків. Якщо користувач чи його комп'ютерна система є **вразливими,** то ймовірність реалізації загрози значно підвищується. Чим більш вразливим є користувач (чи його комп'ютерна система), тим більшим є **ризик** реалізації загрози.

Серед найпоширеніших небезпек визначають найперше ті, що пов'язані з втратою (скиданням) паролей, доступом до персональних даних, а також втратою інформації через різноманітні вірусні програми чи програми-шпигуни.

Найпоширенішими загрозами є:

Фішинг — один з популярних методів соціальної інженерії або просто звичайне шахрайство (скам) у інтернеті. Найчастіше користувачі стикаються саме з комерційними фішингами, мета яких — дізнатися дані для входу в акаунти, як правило, заради доступу до певних фінансових можливостей користувача (тут від отримання інформації, яка має певну цінність, і аж до онлайн-банкінгу). Журналісти, які працюють із соціально гострими чи політичними темами, нерідко стають жертвами таргетованих атак. Вони добре продумані й націлені на певну людину або групу людей. Жертву вивчають упродовж тривалого періоду часу, вивчають її звички, дізнаються про її очікування та прагнення, якими сервісами користується, з якими організаціями чи особами комунікує в мережі Інтернет та поза нею. Як правило, для цього використовуються відкриті джерела, чи які-небудь зливи, які вже були до того.

Цільовим атакам протистояти найважче, оскільки зловмисники вже добре підготувалися й подають саме ту інформацію, на яку очікує користувач. До прикладу, людина надіслала запит на якусь інформацію до державної установи. Природньо, що вона очікує на відповідь. Саме тому, коли ця відповідь приходить, часто на відмінності в кількох елементах електронної поштової скриньки, насправді, мало хто звертає увагу. У подібному листі може міститися програмне забезпечення, яке може надати зловмисникам віддалений доступ до комп'ютера чи

телефону користувача. Окрім програмного забезпечення, у подібних листах може бути покликання на фішингові сайти.

Подібні атаки називають фішинговими.

Серед методів фішингових атак сьогодні виокремлюють такі:

1. **Спрямований фішинг.** Злочинці зацікавлені в конкретній людині. Перш ніж розпочати, вони намагаються дізнатися персональну інформацію та вивчити все навколишнє середовище жертви. Найбільш поширеними цілями атаки є працівники, які мають право авторизувати платежі. Їм надсилають електронний лист начебто від керівництва компанії з проханням надіслати платіж, який потім перенаправляється злочинцям на підроблений сайт.
2. **Фішинг-клонування.** Зловмисники дублюють реальне повідомлення, отримане жертвою, у якому є посилання або вкладені файли. Вони замінюють вкладення та надсилають повідомлення жертві. Натиснувши на покликання та перейшовши на вебсайт або відкривши файл, користувач надає злочинцям доступ до свого комп'ютера. Далі вони шукають конфіденційну інформацію та викрадають її.
3. **Нігерійські листи або «обман 419».** Користувач отримує листа від якої-небудь високопоставленої (як правило, ім'я цієї особи нічого не скаже користувачеві, проте її посада завжди привертає увагу) особи, у якому докладно описується важка ситуація, у яку він або вона потрапила. Далі йде прохання вказати банківські реквізити нібито для переказу великої суми грошей для порятунку. Або ж, що частіше зустрічається останнім часом, у листі від особи, яка начебто займає високу посаду і/або хоче пожертвувати значну суму коштів саме цьому користувачеві. Поряд з цією заманливою пропозицією додається прохання надіслати банківські реквізити, аби цей доброчинець (ця доброчиниця) могла переказати кошти.
4. **Вішинг (голосовий фішинг).** Зловмисники дзвонять жертві та видають себе за співробітника банку. Вони намагаються використати погрози, щоб отримати особисту інформацію або змусити жертву зробити грошовий переказ на вказаний рахунок. Часто вдаються до історій про те, що картка користувача в якомусь із банків заблокована, і щоб відновити доступ до рахунку, потрібно повідомити номер картки, тризначний номер зі звороту картки (CV-код), а тоді ще й прислати код-підтвердження, який прийде на номер телефону користувача.
5. **SMS-фішинг (смішинг).** У цій схемі часто використовуються шкідливі посилання, які ведуть жертву до шахрайського ресурсу. Цей метод поступово зникає, оскільки певні фахівці можуть відстежувати фішингові повідомлення шахраїв та повідомляти про порушення.
6. **Фішингові атаки засновані на оплаті банківськими картками.** Усе більшого поширення набувають операції з використанням банківських карток та інших платіжних систем, наприклад, PayPal, без участі власника. Для доступу до них використовують:
   a. фейкові інтернет-магазини;
   b. перенаправлення на підроблені сайти відомих порталів, коли людина замовляє на них послугу, а оплата йде шахраям;
   c. зараження електронного обладнання шкідливим вірусом.
7. **Spear-фішинг (Списфішинг).** Spear-фішинг націлений на певну особу чи підприємство, а не на випадкових користувачів. Це більш поглиблена версія фішингу, яка вимагає спеціальних знань про організацію, включаючи її структуру.

Кейс 1.1.

Проаналізуйте особливості фішингової атаки. Спробуйте визначити, до якого різновиду фішингу її можна віднести. Яких заходів слід вжити після того, як з'ясувалось, що лист був підробкою?

У компанії «А» стався витік інформації. Зловмисники отримали доступ до бази даних співробітників (імена, прізвища, посади). Відтак, керівникові відділу проєктів і проєктної документації надходить лист начебто від керівника маркетингового відділу, у якому подано посилання (коротке — виконане за допомогою одного із сервісів, що використовуються для скорочення URL) на оновлену базу бланків, що необхідно використовувати в розробці проєктної документації. У листі вказано такі параметри: ім'я, прізвище та посада відправника, дотримано офіційно-ділового стилю, використано логотип компанії. Разом з тим, у стрічці, де зазначається адреса відправника, при натисканні кнопкою мишки випадає адреса електронної скриньки із доменним ім'ям gmail.com*, але не доменне ім'я сайту компанії «А».*

У результаті переходу за цим покликанням керівник відділу проєктів і проєктної документації надає зловмисникові доступ до власного облікового запису.

Як визначити, чи сайт є фішинговим? Основні ознаки фішингового сайту (чи сайту-клону) зображені на Малюнку 1.1.

Сервіс **Whois (див. Малюнок 1.2.)** дає можливість перевірити дату створення вебадреси, а також власника (приватної особи) доменного імені.

Перейти на сайт можна, перейшовши за покликанням (https://www.whois.com/whois/) або відсканувавши QR-код:

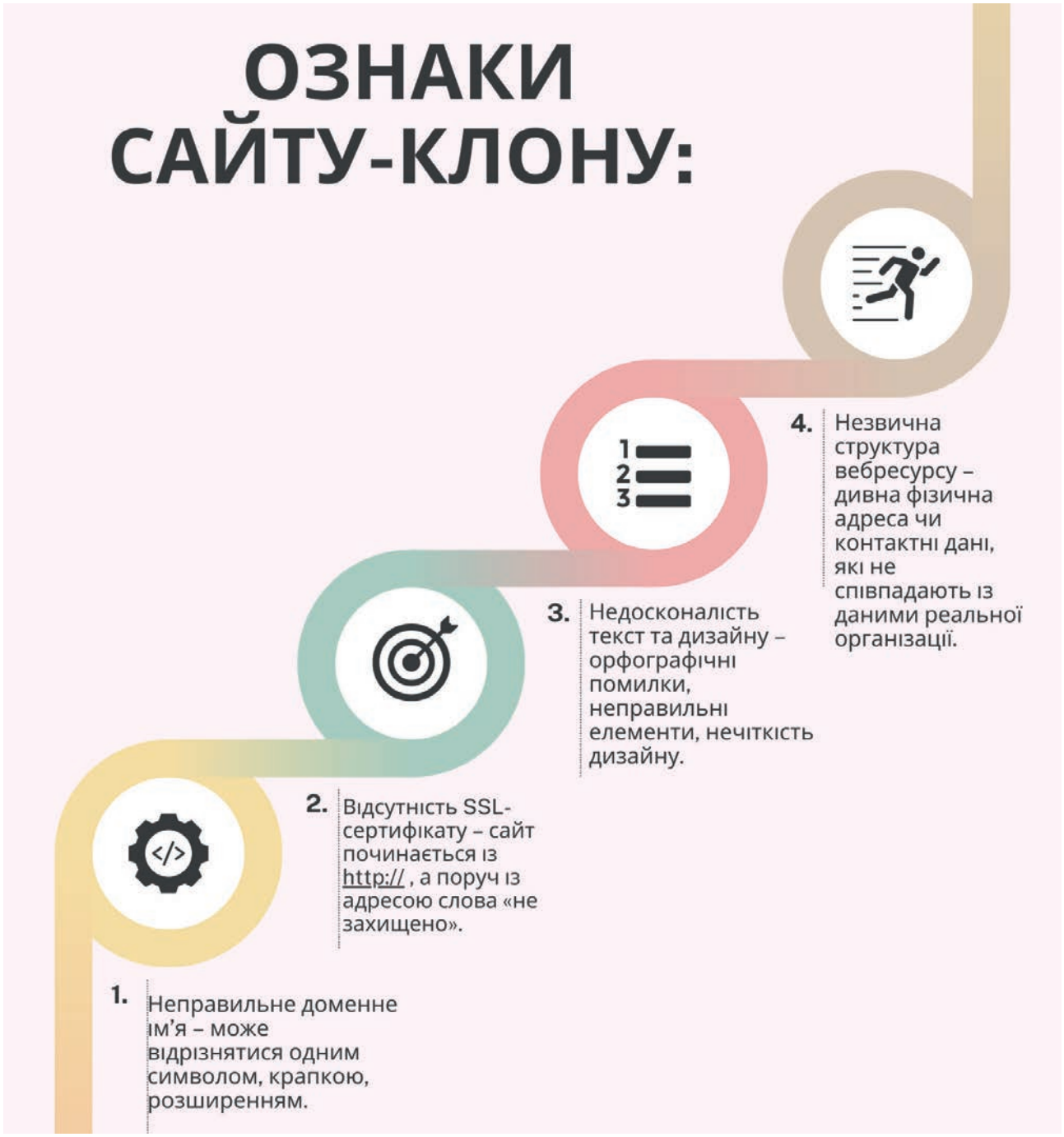
Скидання паролю через електронну поштову скриньку чи номер телефону. Це ще одна небезпека, з якою стикаються сьогодні користувачі мережі Інтернет. Людський мозок здатен забувати. У тому числі й паролі. І саме тому більшість сервісів дають можливість відновлювати паролі через телефон чи електронну поштову скриньку.

Якщо до основної пошти стало звично встановлювати унікальний пароль та двофакторну автентифікацію, то про резервну або забувають, або навіть не знають, що вона підключена до акаунту. Резервна пошта використовується для того, щоб отримати доступ до облікового запису, якщо користувач втратив доступ до основної пошти.

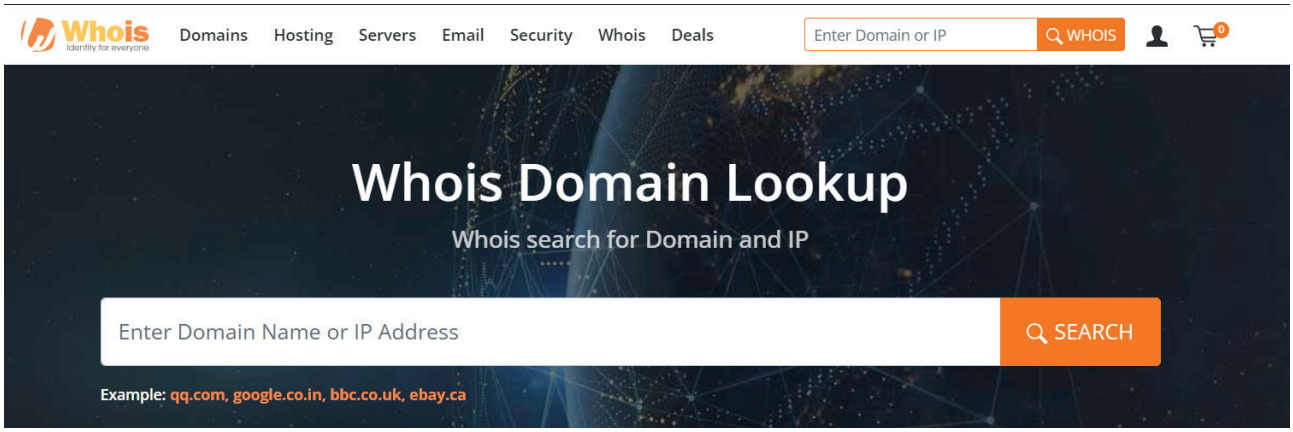
Повторне використання паролів. Проблема паролів стоїть досить гостро, оскільки це дуже пов'язано з особливостями функціонування людського мозку, який, аби запам'ятати більшу кількість інформації, намагається цю інформацію впорядкувати, систематизувати та спростити. А тому досить часто користувачі створюють паролі, які з чимось асоціюються чи містять пряму назву (ім'я, прізвище, дата народження та под.), а також один і той же пароль використовуються для різних облікових записів і застосунків. Причому це характерно не лише для новачків, але й для досвідчених і просунутих користувачів мережі Інтернет. Відтак, якщо зловмисники зламають (чи скинуть) пароль до одного з облікових записів, автоматично отримають доступ до всіх застосунків, у яких користувач зареєстрований.

Перехоплення, скидання і злам паролів найчастіше відбуваються під час підключення користувача до Wi-Fi без використання VPN. Основні небезпеки використання публічного Wi-Fi описані на малюнку 1.3.

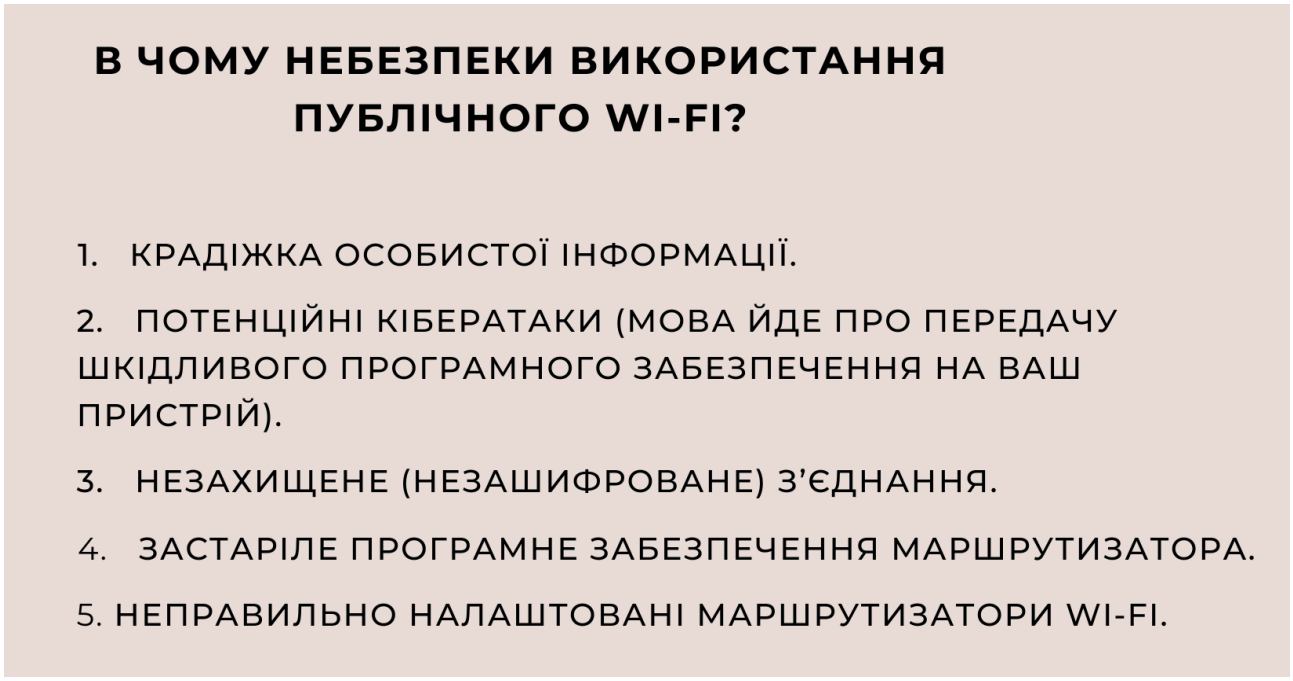
Перехоплення SMS. Цим способом часто користуються зловмисники, аби отримати доступ до месенджерів, оскільки більшість з них мають прив'язку до номеру телефону. До речі, перехоплення SMS і відкриття віртуальної Sim-карти з дублем номеру телефону користувача



Малюнок 1.1. Ознаки сайту-клону



Малюнок 1.2. Інтерфейс сервісу **Whois**



Малюнок 1.3. Небезпеки використання публічного Wi-Fi

дає можливість, до прикладу, оформити мікропозику на користувача, за умови, що в нього є обліковий запис у такій фінансовій установі з підвантаженими документами (як правило, ідеться про паспорт та ідентифікаційний код).

Блокування акаунтів. З 2014 року через російську війну користувачі інтернету (особливо користувачі соціальних мереж) почали багато інформації публікувати про російські воєнні злочини, передавати власний досвід, публікувати чутливі фото, використовувати мову ворожнечі. І на цьому тлі зіткнулися з масовим блокуванням акаунтів у соціальних мережах. Інколи це критично, особливо, якщо комунікація ведеться виключно через соціальні мережі. Якщо обліковий запис (акаунт) блокується через надмірну активність на сторінці, а користувач забув пароль, і немає можливості відновити його жодним з доступних способів (втрачено доступ до номеру телефону, неактивний e-mail і под.), відновити доступ можна за допомогою паспортних даних (за умови, що користувач під час реєстрації вказав реальне ім'я та прізвище, а також використовує власне фото).

Як оцінити ризики?

Для оцінки ризиків користувач повинен проаналізувати початковий (стартовий) рівень безпеки та потенційні ризики. Для цього потрібно дати відповіді на такі запитання:

1. Яка інформація є критично важливою?
2. Де зберігається ця інформація (на яких сервісах та/чи пристроях вона розміщена — смартфон, планшет, лептоп, робочий комп'ютер, персональний комп'ютер, зовнішній жорсткий диск, флешки та ін.)?
3. Кому ця інформація може бути потенційно цікавою?
4. До кого можна звернутися, якщо настане безпековий інцидент?

На другому (більш детальному) етапі аналізу потрібно звернути увагу на те, як використовуються пристрої, як і де зберігається важлива інформація, на скільки захищені робочі й персональні пристрої від проникнення шкідливого програмного забезпечення і под. (структурована інформація в Таблиці 1.1.).

Таблиця 1.1. Виявлення потенційних ризиків і небезпек

Персональний комп'ютер / ноутбук	***Розмежовую домашній і робочий комп'ютер***	***Постійно оновлюю програмне забезпечення***	***Користуюсь ліцензійним програмним забезпеченням***	***Маю ліцензійну програму виявлення блокування шкідливого програмного забезпечення***	
	Так / ні	Так / ні	Так / ні	Так / ні	
Соціальні мережі	***Користуюсь двофакторною автентифі-кацією***	***Перевіряю активність***	***Розмежовую персональний і робочий обліковий запис (акаунт)***	***Приховую персональну інформа-цію***	***Використовую актуальний номер телефону і e-mail для відновлення облікового запису в соціальних мережах***
	Так / ні	Так / ні	Так / ні	Так / ні	Так / ні
E-mail / обліковий запис	***Розмежовую персональний і робочий e-mail / обліковий запис***	***Використовую двофакторну автенти-фікацію***	***Використовую актуальний номер телефону і e-mail для відновлення облікового запису***	***Використовую синхроні-зацію***	***Розмежовую персональ-ний і фінансовий e-mail***
	Так / ні	Так / ні	Так / ні	Так / ні	Так / ні
Зберігання та передавання інформації	***Використовую хмарні сховища***	***Використовую програмне шифрування***	***Використовую VPN, коли використовую публічний Wi-Fi***		
	Так / ні	Так / ні	Так / ні		

Кейс 1.2.

Ви — журналіст газети. Ви працюєте в невеликій редакції, яка не має змоги купити вам робочий комп'ютер. Саме тому ви користуєтесь власним лептопом і вдома, і на роботі. До вашої персональної поштової скриньки прив'язано онлайн-банкінг, а також ця ж сама скринька слугує логіном і паролем для входу на сайт видання для його наповнення. Проаналізуйте потенційні небезпеки. Поміркуйте, як уникнути ризиків.

ПСИХОЛОГІЧНІ ЗАГРОЗИ Й ВИКЛИКИ

Тролінг — це одна з тих психологічних загроз, з якими користувачі мережі Інтернет (а особливо соціальних мереж) сьогодні зустрічаються мало не щодня. **Тролінг** — це такий різновид комунікативної взаємодії, основна мета якого — спровокувати емоцію та витягнути більшу аудиторію на конфлікт. Тобто, основною метою інтернет-троля є нагнітання конфліктів.

Тролінг може бути «тонким» і «грубим». При «грубому» тролінгу ідеться про застосування хамства, лайливих висловлювань і відкриту провокацію на конфлікт. «Тонкий» тролінг потребує глибокого знання психології маніпулювання людьми. Тут ідеться про зміщення акцентів, переформатування питання, формулювання провокативних питань, на соціально чутливі теми, на які немає чіткої єдиної правильної відповіді, і под.

Від тролінгу найчастіше потерпають особи публічні, які є лідерами думок для значного кола користувачів соціальних мереж. Інколи тролінг використовують недоброчесні користувачі для «накручування» кількості підписників і відвідувачів сторінки.

Різновидів цькування користувачів у мережі Інтернет є кілька десятків. Загальна назва для них — кібербулінг. **Кібербулінг —** це психологічне цькування користувачів у мережі Інтернет

та соціальних мережах, що інколи переростає у фізичне переслідування в реальному житті. Прийнято виокремлювати такі різновиди кібербулінгу:

1. **Суперечки**, або **флеймінг** (від англ. *flaming* — пекучий, гарячий, полум'яний). Тут ідеться про взаємний обмін невеликими, але, як правило, досить гнівними й провокативними повідомленням між двома чи більше учасниками такої комунікативної ситуації. Як правило, флеймінг передбачає наявність публічного простору для дискусії, оскільки основна мета — це дискредитація користувача на очах у значної аудиторії. Такі суперечки часто перетворюються на затяжні «війни» у мережі Інтернет.

2. **Нападки**, постійні виснажливі **атаки** (англ. *harassment*). У цьому випадку зазвичай ідеться про систематичне пересилання образливих повідомлень жертві. Тут ідеться не лише про соціальні мережі. Часто для таких виснажливих атак використовується телефон: спам із SMS-повідомлень, постійні дзвінки з невідомих номерів телефону. Основна мета — перевантаження персональних каналів комунікації і психологічний тиск на користувача. Такі речі часто використовують колекторські компанії, котрі перевантажують робочу телефонну лінію та персональні канали комунікації не лише конкретному користувачеві, але і його родичам, знайомим.

3. **Обмовлення**, **зведення наклепів** (англ. *denigration*). Цей різновид базується на широкому розповсюдженні принизливої і образливої неправдивої інформації. Щоправда, з цією метою використовуються комп'ютерні технології.

4. **Дісінг** (англ. Dissing). Якщо на меті псування репутації користувача та псування його відносин з іншими людьми, використовується дісінг — публікація компроментуючої інформації про користувача онлайн (на форумах, сайтах, у соціальних мережах і под.).

5. **Хепіслепінг** (англ. *happy slappying*). У цьому випадку ідеться про досить поширений «тренд» з просторів YouTube, TikTok та інших соціальних мереж — знімання та поширення відео про те, як агресори (як правило, ті, хто знімають цей ролик) б'ють чи знущаються з когось. Найчастіше жертвами таких «любителів трендів» стають безхатьки, оскільки вони, здебільшого, не звертаються до правоохоронних органів. Рідше сюжетна лінія вибудовується на знущанні групи осіб над однією особою, яка не здатна чинити опір.

6. **Фрейпінг** (англ. *fraping*). З цим різновидом фішингу найчастіше зустрічаються користувачі соціальних мереж, оскільки ідеться про злам облікових записів з подальшим розміщенням сумнівного контенту або на сторінці користувача, обліковий запис якого було зламано, або ж у спілкування від його імені з його контактами (здебільшого, ідуть прохання позичити певну суму коштів чи поповнити рахунок його номеру телефону).

7. **Кетфішінг** (англ. *catfishing*). Цьому виду булінгу, як правило, піддаються публічні особи чи громадські активісти. Він полягає в тому, що зловмисники крадуть інформацію з основного профілю користувача та створюють профіль-двійник. Мета створення такого профілю може бути різною: від просування власного контенту за рахунок імені та контактів особи аж до виманювання грошей.

8. **Кіберпереслідування** (**кіберсталкінг**) — це ті самі дії, які часто виходять за межі мережі Інтернет, оскільки ідеться не лише про переслідування в соціальних мережах, відстежування активності користувача, але й про стеження за ним у реальному житті з метою вчинення злочинних дій: від пограбування до зґвалтування, побиття і навіть убивства. Як правило, необережні користувачі самі дають усю необхідну інформацію про свої дії та пересування: позначка геолокації, публікація фото з різних місць у реальному часі і под.

9. **Doxing (**сленгове від *docs* (документи)) — дії зловмисника, внаслідок яких особиста інформація користувача (найчастіше, адреса та номер телефону) виставляється в

публічний простір, частіше із закликом телефонувати цьому користувачеві, стежити за ним, погрожувати та под. Тобто, подібна інформація використовується з метою залякувань і переслідувань.

У сучасному світі, насиченому технологіями та інтернетом, цифрові загрози стають невід'ємною частиною нашого цифрового життя. Ці загрози та виклики мають різноманітні форми та можуть впливати на різні аспекти суспільства, від особистої безпеки до національної безпеки.

Поширення зловмисного програмного забезпечення (malware) є однією з основних цифрових загроз — віруси, троянці, шпигунське програмне забезпечення та інші шкідливі програми, які можуть завдати шкоди комп'ютерам та іншим пристроям, викрадати конфіденційну інформацію або навіть блокувати доступ до системи до викупу (ransomware).

Соціальна інженерія є іншою серйозною загрозою, яка полягає в маніпуляції людьми з метою отримання конфіденційної інформації або здійснення шахрайства. Це може включати в себе фішингові атаки, у яких зловмисники намагаються отримати конфіденційні дані, такі як паролі або номери кредитних карт, шляхом відправлення підроблених повідомлень електронної пошти або повідомлень через соціальні мережі.

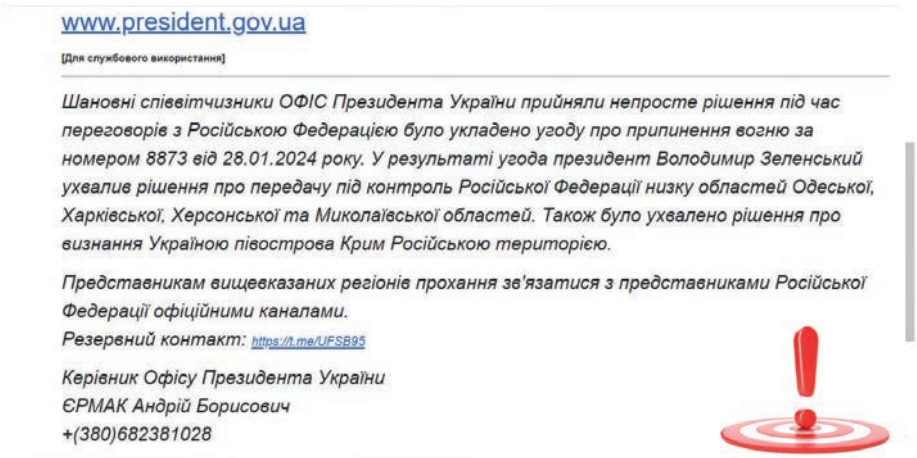
Кібератаки на критичну інфраструктуру, таку як електроенергетичні системи, фінансові установи чи мережі телекомунікацій, також є серйозним викликом для суспільства. Атаки цієї природи можуть призвести до серйозних розладів у роботі суспільства та навіть загрози національній безпеці.

Безпека персональних даних та приватності в інтернеті також є значущим викликом. Збільшення обсягів зберігання та обробки особистих даних у сучасному світі призводить до зростання загроз неправильного їх використання, включаючи можливість витоку даних або порушення конфіденційності.

Усі ці цифрові загрози й виклики підкреслюють важливість впровадження ефективних заходів безпеки та захисту в інтернеті. Це охоплює не лише технічні заходи, такі як використання антивірусного програмного забезпечення чи захищених паролів, а й освіту та навчання користувачів щодо безпечних практик в інтернеті. Тільки шляхом спільних зусиль ми можемо ефективно протистояти цифровим загрозам і забезпечити безпеку та захищеність у цифровому світі.

ЗАВДАННЯ

Завдання 1. Проаналізуйте текст електронного листа. Поясніть, чому інформація в листі є фейковою? Що вказує на фейковість інформації? Чи можна вважати такий лист фішинговим?


www.president.gov.ua

[Для службового використання]

Шановні співвітчизники ОФІС Президента України прийняли непросте рішення під час переговорів з Російською Федерацією було укладено угоду про припинення вогню за номером 8873 від 28.01.2024 року. У результаті угода президент Володимир Зеленський ухвалив рішення про передачу під контроль Російської Федерації низку областей Одеської, Харківської, Херсонської та Миколаївської областей. Також було ухвалено рішення про визнання Україною півострова Крим Російською територією.

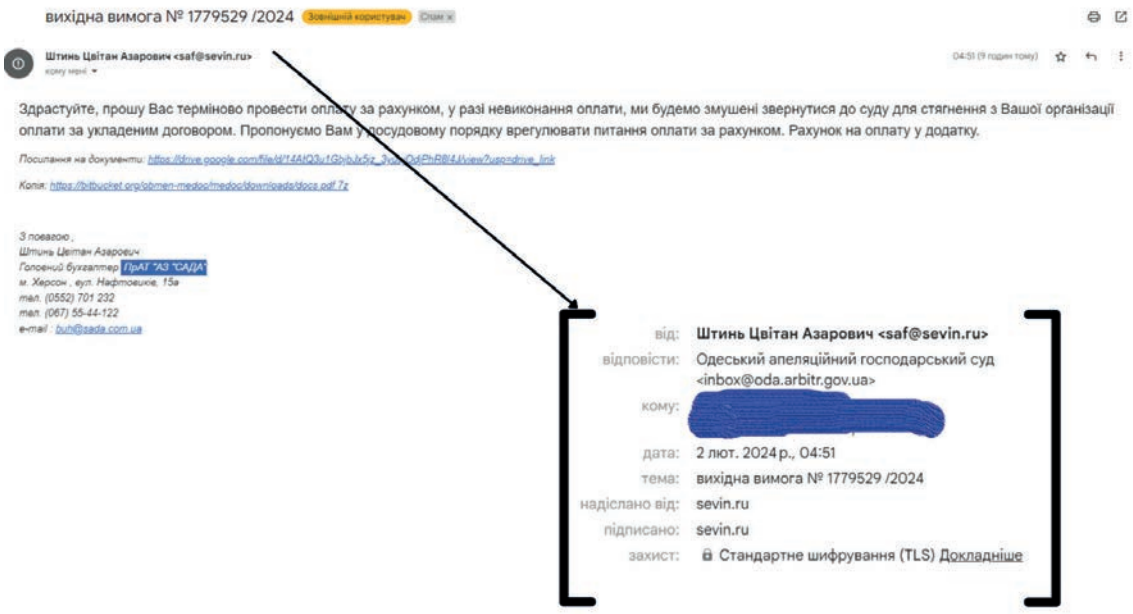
Представникам вищевказаних регіонів прохання зв'язатися з представниками Російської Федерації офіційними каналами.
Резервний контакт: https://t.me/UFSB95

Керівник Офісу Президента України
ЄРМАК Андрій Борисович
+(380)682381028

Завдання 2. Пройдіть тест від Інституту масової інформації «Чи захищені ваші акаунти під час тролінгу в соцмережах» (https://imi.org.ua/advices/test-chy-zahyshheni-vashi-akaunty-pid-chas-trolingu-v-sotsmerezhah-i43130), скориставшись QR-кодом.

Завдання 3. Користуючись табличкою (Таблиця 1.1.), проаналізуйте потенційні загрози й ризики, які несе для вас сучасний цифровий світ. Подумайте, як можна уникнути ризиків, або хоча б потенційно їх зменшити? При цьому потрібно усвідомлювати, що ваша безпека — це не разова дія, це процес, який передбачає людський і технологічний фактори. Якщо людський фактор забезпечується вами і вашим усвідомленням необхідності захисту, то технологічний фактор — це встановлення паролю, двофакторна автентифікація і под., про що ми будемо говорити в наступних розділах.

Завдання 4. Уважно перегляньте лист. З'ясуйте, чи є цей лист фішинговим? Обґрунтуйте відповідь, аналізуючи складові листа.



ДЖЕРЕЛА ДЛЯ ПОГЛИБЛЕНОГО ВИВЧЕННЯ ТЕМИ

1. *Автостопом по цифрових правах.* Дія. Освіта. URL: https://osvita.diia.gov.ua/courses/hitchhiking-on-digital-rights
2. *Афери з подарунковими сертифікатами: як не «подарувати» шахраям свої гроші.* URL: https://www.eset.com/ua/about/newsroom/blog/data-protection/afery-s-podarochnymi-sertifikatami-kak-ne-podarit-moshennikam-svoi-dengi/
3. *Базові цифрові навички. Сезон 1. Навчіться користуватися смартфоном, комп'ютером і планшетом без проблем.* Дія. Освіта. URL: https://osvita.diia.gov.ua/courses/bazovij-serial-1-sezon
4. *Базові цифрові навички. Сезон 2. Навчіться нових навичок у другому сезоні: як користуватися Google і Facebook та полагодити комп'ютер, який завис.* Дія. Освіта. URL: https://osvita.diia.gov.ua/courses/bazovij-serial-iz-cifrovoi-gramotnosti-2-sezon
5. *Базові цифрові навички. Сезон 3. Більше секретів пошуку в Google. Дізнавайтеся, як створити особистий бренд у Facebook та що таке авторське право. Фінальний сезон.*

Дія. Освіта. URL: https://osvita.diia.gov.ua/courses/bazovij-serial-iz-cifrovoi-gramotnosti-3-sezon

6. *Блокування та обмеження. Як журналістам захистити себе від кіберцькування.* Інститут Масової Інформації. URL: https://imi.org.ua/advices/blokuvannya-ta-obmezhennya-yak-zhurnalistam-zahystyty-sebe-vid-kibertskuvannya-i42427
7. *Кетфішинг. Як розпізнати кетфішера?* Інститут Масової Інформації. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/ketfishing/
8. Мороз О. *Нація овочів? Як інформація змінює мислення і поведінку українців.* Київ : Якабу Паблішинг, 2020. 286 с.
9. *Навіщо медійникам оцінювати ризики у сфері цифрової безпеки та як це правильно зробити.* Інститут масової інформації. URL: https://imi.org.ua/advices/navishho-medijnykam-otsinyuvaty-ryzyky-u-sferi-tsyfrovoyi-bezpeky-ta-yak-tse-pravylno-zrobyty-i42620
10. *Основи кібергігієни. Як держслужбовцям захиститися від хакерських атак.* Дія. Освіта. URL: https://osvita.diia.gov.ua/courses/cyber-hygiene
11. *Основи кіберпростору, кібербезпеки та кіберзахисту* : навч. посіб. / Володимир Михайлович Богуш, Володимир Володимирович Богуш, Володимир Дмитрович Бровко, Володимир Петрович Настрадін; під ред. Володимир Михайлович Богуш.Київ : Ліра-К, 2020. 553 с.
12. *Персональна кібергігієна.* Дія. Освіта. URL: https://osvita.diia.gov.ua/courses/personal-cyberhygiene
13. *Регіональна цифрова трансформаці.* Дія. Освіта. URL: https://osvita.diia.gov.ua/courses/regional-digital-transformation
14. Скіннер К. *Людина цифрова : четверта революція в історії людства, яка торкнеться кожного* : пер. з англ. /Кріс Скіннер; пер. Ганна Якубовська. Харків : Фабула, Ранок, 2020. 270,[1] с.
15. *Смартфон для батьків. Як користуватися смартфоном: інтернет, дзвінки, обліковий запис Google, мобільні додатки, безпека, налаштування «під себе» та користь у побуті.* Дія. Освіта. URL: https://osvita.diia.gov.ua/courses/gostiovy-kurs-smartfon-dlia-batkiv
16. *Цифрова грамотність держслужбовців на базі Google:* частина 1. Дія. Освіта. URL: https://osvita.diia.gov.ua/courses/civil-servants
17. *Цифрова грамотність під час війни. Навчайтеся на оновленій платформі Дія. Цифрова освіта.* Міністерство Цифрової Трансформації України. URL: https://thedigital.gov.ua/news/tsifrova-gramotnist-pid-chas-viyni-navchaytesya-na-onovleniy-platformi-diyatsifrova-osvita
18. *Цифрова журналістика.* Дія. Освіта. URL: https://osvita.diia.gov.ua/courses/digital-journalism
19. *Doxxing як вид булінгу. Що робити медійникам.* Інститут Масової Інформації. URL: https://imi.org.ua/advices/doxxing-yak-vyd-bulingu-shho-robyty-medijnykam-i42978

Модуль 2

ЕЛЕКТРОННА ПОШТА Й НАЛАШТУВАННЯ ОБЛІКОВИХ ЗАПИСІВ

У цьому модулі ми поговоримо про те, чому електронна пошта є важливою, як її захистити, а також спробуємо покроково налаштувати двофакторну автентифікацію для вашого Google-акаунту та зрозуміємо, що ж таке надійні паролі й де краще їх зберігати.

Електронна пошта — це один з наших найголовніших цифрових активів. Усе дуже просто. Під електронну пошту підв'язується онлайн-банкінг, Google-акаунт, з яким синхронізується інформація на смартфоні. Через електронну поштову скриньку створюються профілі в соціальних мережах. Окрім того, вона використовується як логін для входу на сайт і навіть як варіант для відновлення корпоративної електронної скриньки. Відтак, можемо говорити про важливість електронної скриньки для підтримки безпечного цифрового середовища. Саме тому електронна поштова скринька повинна бути максимально захищеною, що дасть можливість користувачеві убезпечити себе та свої дані від витоку й використання в різноманітних шахрайських схемах.

Історична довідка:

Винахідником електронної пошти називають Рея Томлінсона, який у 1971 році працював у ARPANET (проєкті, що був фінансований американським урядом і став прототипом сучасного інтернету). У цьому проєкті була можливість залишати повідомлення лише в межах одного комп'ютера для користувачів, які ним користуються. Рей Томлінсон знайшов спосіб передавати повідомлення на інші комп'ютери, підключені до однієї мережі. Ми й досі користуємось символом, який розробив Рей Томлінсон, — @.

Рей Томлінсон

Типи загроз для електронної пошти (саме на них акцентує увагу компанія **Microsoft**):

Ексфільтрація даних. Ексфільтрація даних — це несанкціоноване передавання даних за межі організації вручну або за допомогою шкідливого програмного забезпечення (вірусів). Шлюзи електронної пошти допомагають компаніям уникнути надсилання чутливих (персональних) даних без авторизації, що може призвести до їхнього витоку. Наслідки такого витоку можуть бути непередбачуваними.

Підробка. Підробка виникає, коли кіберзлочинці маскуються під надійну особу або організацію, щоб виманювати гроші або дані за допомогою електронної пошти. Один з таких прикладів — порушення безпеки корпоративної електронної пошти, коли шахрай видає себе за працівника, щоб викрасти щось у компанії або її клієнтів і партнерів.

Фішинг (цей різновид ми вже розглядали в попередньому модулі).

Шкідливе програмне забезпечення («віруси»). Шкідливе програмне забезпечення має на меті зашкодити комп'ютерам і комп'ютерним системам. До найпоширеніших типів шкідливого програмного забезпечення належать віруси, хробаки, зловмисні програми з вимогою викупу, а також

шпигунське ПЗ. Останнє може надсилатися, у тому числі, і через **QR-код** — штрих-код, призначений для миттєвого зчитування й відображення інформації сучасним девайсом. Один код може зберігати до 4296 символів у вигляді букв та цифр, хоча, як правило, їх використовується менше. Це дозволяє легко розшифровувати QR-коди за допомогою камери смартфона, на якому встановлений сканер для QR-коду.

QR-код може містити різноманітну інформацію. Після зчитування коду, програма робить запит на перехід за посиланням (по суті, ідеться про відкриття коду). Відтак, коди використовуються для переходу на вебсайти, завантаження файлу, додавання контакту, підключення до мережі Wi-Fi, а також навіть і для здійснення платежів.

QR-код можна видозмінювати, у тому числі й через додавання логотипу компанії. Більше того, розробники вказують на те, що в динамічних версіях кодів є можливість змінити їхній вміст або дію в будь-який час, що роблять їх максимально мобільними й небезпечними.

Види шахрайства з використанням QR-коду:

- перенаправлення на шкідливий сайт для викрадення конфіденційних даних;
- завантаження шкідливого файлу на пристрій;
- запуск небезпечних дій на пристрої користувача;
- переадресування платежу або запит на отримання коштів;
- викрадення особистих даних або отримання доступу до програми.

Спам. Спам — це небажані повідомлення, що надсилаються у великій кількості користувачам без їхньої на те згоди. Компанії використовують небажані повідомлення електронної пошти з комерційною метою. Натомість шахраї використовують спам, щоб розповсюджувати шкідливе програмне забезпечення, виманювати в одержувачів чутливу (персональну) інформацію або вимагати від них гроші.

Перша кампанія поширення небажаних електронних повідомлень через електронну пошту була зафіксована в 1978 році, під час якої розсилку отримали майже 400 (або 15% від усіх) користувачів, підключених до попередника мережі Інтернет — ARPANET. Кампанія рекламувала презентацію продукту компанії, але після отримання великої кількості негативних відгуків ця форма маркетингу деякий час не використовувалась.

Як визначити, що ідеться саме про спам? Більшість повідомлень цього типу характеризуються, серед іншого, такими ознаками:

- відсутність персоналізації — усі отримувачі отримують повідомлення з однаковим змістом;
- масовість — надсилається одночасно тисячам одержувачів;
- часто незаконна діяльність — дані користувача отримуються без його згоди, часто метою спамера є також спроба заразити систему з метою виманювання приватних даних, таких як номер банківського рахунку та пароль для доступу до нього;
- введення одержувача в оману — «реклама» предметів розкоші за непристойно низькою ціною, виділення пропозиції більш жирним шрифтом, опускання так званого дрібного шрифту.

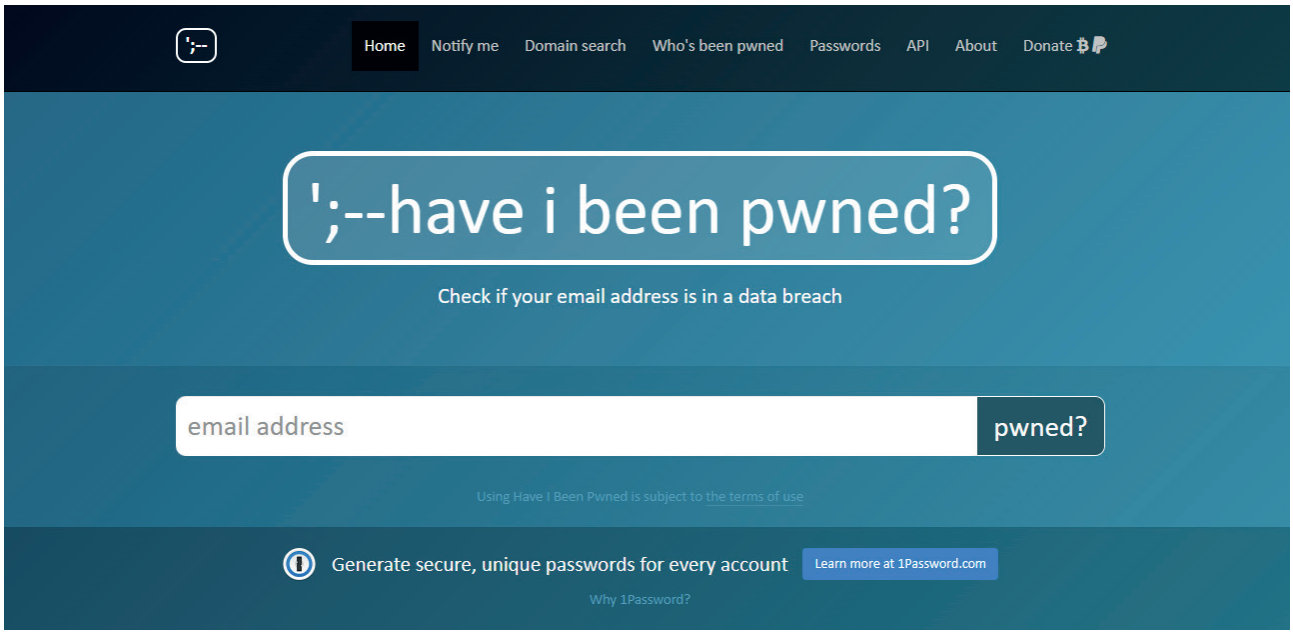
Сучасні електронні поштові скриньки обладнані захистом від спаму, і листи такого типу одразу потрапляють у папку «Спам». Інколи в цю папку втрапляють листи випадково, оскільки мають ознаки масової розсилки. Саме тому система не видаляє спам автоматично.

Підвищена кількість спаму, необґрунтована активність можуть свідчити про те, що обліковий запис зламано. Окрім цих характеристик, індикаторами зламу електронної поштової скриньки є:

- невідомі листи у відправлених повідомленнях;
- змінений пароль, який блокує користувачеві доступ;
- сповіщення про вхід в акаунт з незнайомих IP-адрес.

Також підозри можуть виникнути в разі отримання кількох запитів на зміну пароля від інших сайтів або програм, та спам-повідомлення зі скриньки користувача його контактам (знову ж таки, як правило, з проханням позичити певну суму коштів).

Перевірити, чи було зламано електронну поштову скриньку можна за допомогою безкоштовних застосунків. До прикладу, можна використати сайт HaveIBeenPwned.com (https://haveibeenpwned.com/) (див. Малюнок 2.1.), який має базу даних викрадених облікових записів та мобільних телефонів.



Малюнок 2.1. Інтерфейс сервісу **HaveIBeenPwned**

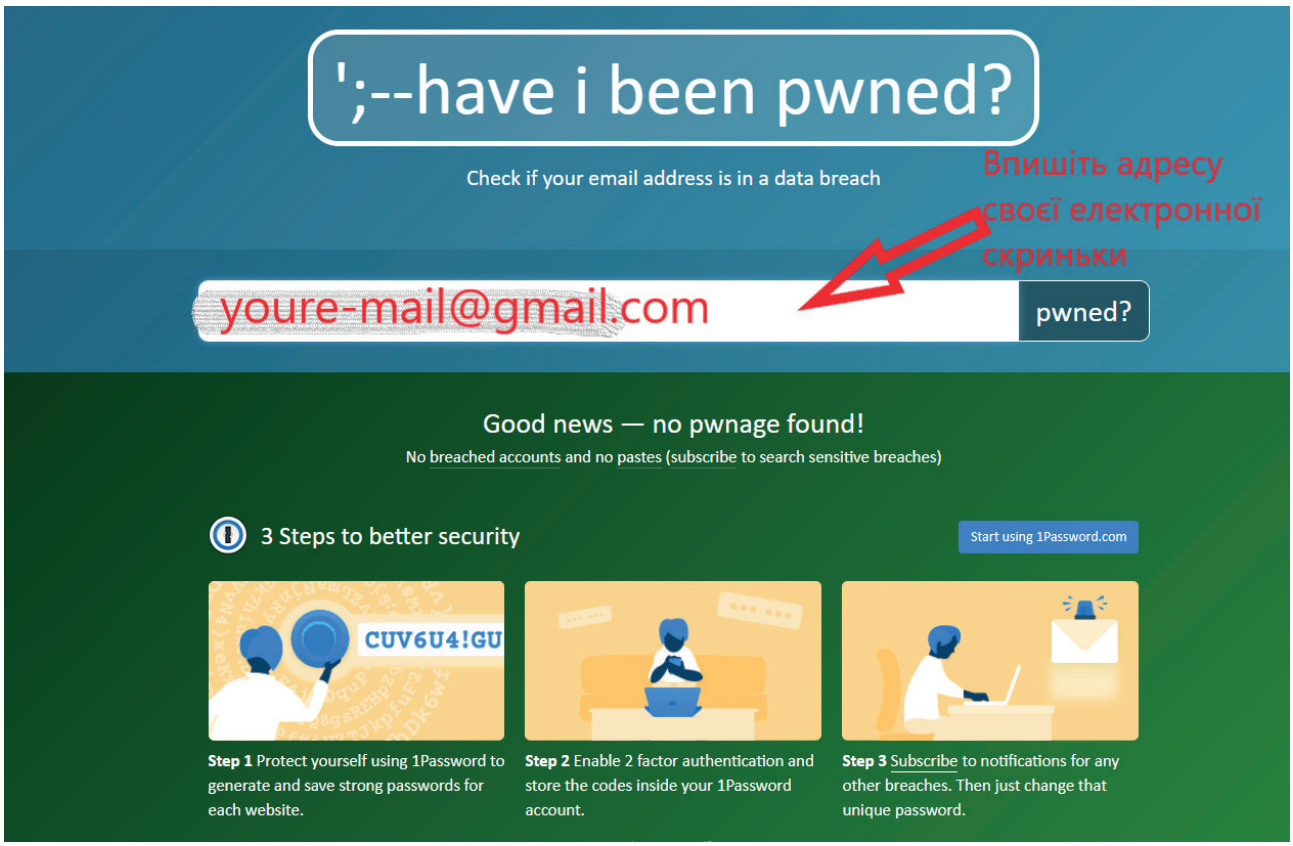
Після введення адреси електронної скриньки користувача, потрібно натиснути кнопку «**pwned?» (див. Малюнок 2.2.)** і за кілька секунд отримати результат щодо того, чи було зламану електронну скриньку чи ні.

Крім цього, Google дає змогу переглядати останні дії в акаунті та виконувати «Перевірку безпеки», яка містить дані про нещодавню активність, наприклад, новий вхід. Інші сервіси також мають подібні параметри та інструкції щодо відновлення зламаного акаунту Gmail, Yahoo Mail та Outlook.com.

Як убезпечити електронну скриньку та власний обліковий запис?

Необхідно звертати увагу на такі речі:

1. **Пароль.** Для того, щоб вважатися надійним, пароль повинен відповідати таким параметрам:
   - мінімальна довжина надійного паролю — 12–14 символів;
   - використання комбінації букв верхнього і нижнього регістрів, цифр, а також спеціальних символів;



Малюнок 2.2. Алгоритм роботи із сервісом **HaveIBeenPwned**

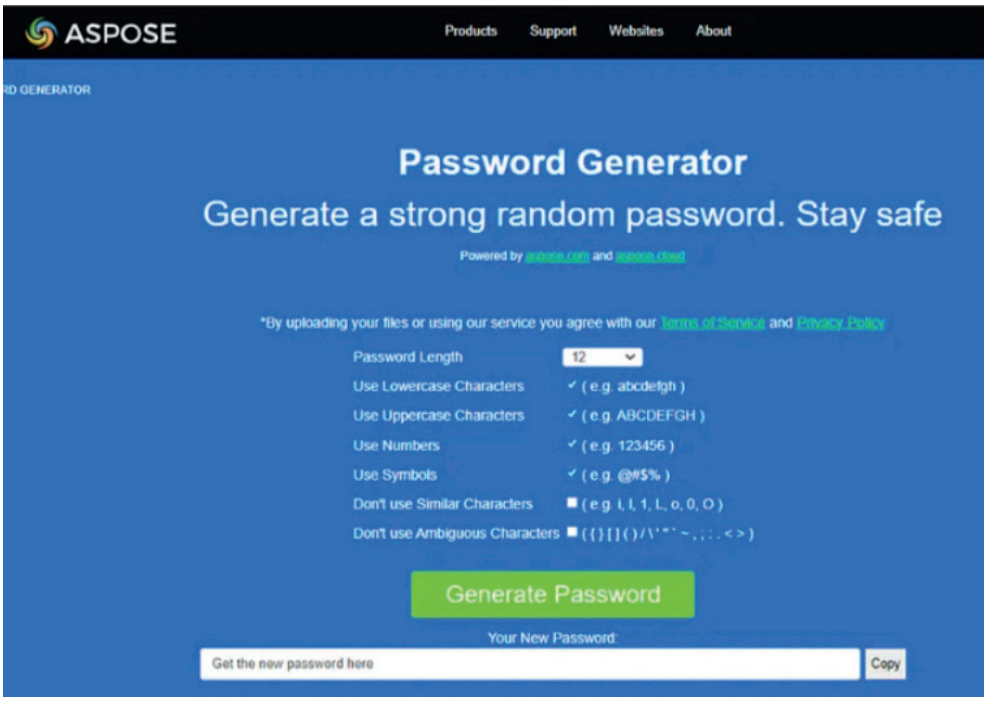
– це не повинно бути слово, яке можна знайти в словнику, і тим більше пароль не повинен мати жодної асоціації з користувачем (не варто використовувати імен, прізвищ своїх чи родичів і под.).

На сьогодні існує близько десятка сервісів, що допомагають згенерувати надійний пароль: від менеджерів, які не лише створюють, але й зберігають паролі (як от: Dashlane, Keeper, RoboForm, LastPass і под.) і аж до онлайн-генераторів надійних паролів, які, по суті, працюють за одним і тим самим принципом.

Малюнок 2.3. Інтерфейс сервісу ESET

До прикладу, онлайн-генератор від ESET (див. Малюнок 2.3.), який дає можливість згенерувати пароль з дотриманням усіх рекомендацій до створення надійних паролів:

Ще один генератор паролів від компанії Aspose.PDF (Aspose Ltd. Pty) (див. Малюнок 1.4.), який можна вільно використовувати:



Малюнок 2.4. Інтерфейс сервісу генерації паролів від Aspose.PDF

Як вберегти свої паролі від витоку?

1. Не варто передавати пароль стороннім особам.
2. Не варто надсилати пароль електронною поштою, у миттєвому повідомленні або за допомогою інших засобів зв'язку, які не гарантують надійного захисту.
3. Рекомендовано використовувати унікальний пароль для кожного вебсайту.
4. Аби не запам'ятовувати декілька паролів, можна скористатися диспетчером паролів. Найкращі з них будуть автоматично оновлювати збережені паролі, зберігати їх у зашифрованому вигляді та вимагати багатофакторну автентифікацію для отримання доступу.
5. Якщо виникає підозра, що до паролю мала доступ стороння особа, рекомендовано негайно його змінити.
6. Рекомендовано ввімкнути багатофакторну автентифікацію (за наявності). Для входу до облікового запису можна користуватися кількома типами облікових даних (до прикладу, введення паролю та ще додаткового коду, створеного програмою). Це додає ще один рівень безпеки на випадок, якщо хтось інший отримає несанкціонований доступ до паролю користувача.

2. Двофакторна автентифікація. Таке налаштування допомагає захистити обліковий запис, якщо пароль стає відомим зловмисникові. Якщо двофакторна (багатофакторна) автентифікація увімкнена, то сервіс, окрім пароля, попросить користувача іншим способом підтвердити своє право на цей акаунт. Це може бути код смс, код зі спеціального додатка, push-сповіщення, використання спеціального токена або одноразового коду доступу.

Розгляньмо на прикладі Google-акаунта, як встановити двофакторну автентифікацію (див. інфографіку «Як налаштувати двофакторну автентифікацію на прикладі Google-акаунту).

Для посилення захисту облікового запису Google радить використовувати push-сповіщення, оскільки вони допомагають захиститися від заміни SIM-карти й інших атак через номер телефону. Ці push-сповіщення будуть надходити на:

- телефони **Android**, на яких користувач увійшов в обліковий запис **Google;**
- пристрої **iPhone** з додатками **Smart Lock**, **Gmail**, **Google Фото**, **YouTube** або **Google**, у яких користувач увійшов в обліковий запис Google.

Залежно від інформації про пристрій і місцезнаходження в сповіщенні користувач має можливість:

- дозволити вхід, натиснувши **Так**;
- заблокувати вхід, торкнувшись опції **Ні**.

Задля підвищення безпеки Google може попросити ввести PIN-код або скористатися іншим способом підтвердження.

Якщо пристрій надійний, другий етап можна пропустити, просто поставивши прапорець біля опції «Не запитувати на цьому комп'ютері» або «Не запитувати на цьому пристрої».

Важливо. Цю опцію варто обирати лише для пристроїв, доступу до яких не мають інші особи, окрім користувача.

3. Способи відновлення акаунту та переадресація повідомлень на інші електронні скриньки. Якщо в способах відновлення вказана неактуальна електронна пошта (часто йдеться про ті електронні скриньки, які створювалися на російських сервісах до 2017 року та про які успішно забули) або номер телефону, це підвищує ризик легкого доступу до облікового запису користувача. Така ж ситуація із переадресаціями, якщо налаштована переадресація на неактуальні електронні скриньки.

4. Контроль активних сесій. Активні сесії — це список пристроїв, з яких здійснювався вхід в обліковий запис. Незвична активність в акаунті — це перше, на що варто звернути увагу. У цьому налаштуванні можна завершити сеанс на пристроях, яких користувач не знає, або на пристроях, які він передав іншим людям чи загубив. Але важливо пам'ятати, що, якщо використовується VPN, то в активностях буде відображатися та країна, яку обрав у налаштуваннях користувач.

5. Вхід на інші сайти з обліковим записом Google. Ідеться про перелік тих сервісів, аплікацій та ін., куди користувач заходив за допомогою кнопки «Увійти через Google». Тут варто звертати увагу на те, до яких саме даних користувач надає право застосунку, у якому реєструється. Автоматично після входу через таку кнопку сервісам стають доступні ім'я, електронна адреса та зображення профілю.

ЗАВДАННЯ

Завдання 1. Спираючись на інформацію з розділу, налаштуйте двофакторну автентифікацію для свого облікового запису Google.

Завдання 2. Перейдіть за покликанням https://haveibeenpwned.com/. Використовуючи підказки сайту, перевірте, чи була зламана ваша електронна скринька.

Завдання 3. Пройдіть тест від Інституту масової інформації «Чи надійно захищені мої персональні дані?» (https://imi.org.ua/advices/test-chy-nadijno-zahyshheni-moyi-oblikovi-zapysy-i42975).

Завдання 4. Проведіть дослідження. Для цього проаналізуйте ступінь захищеності власної електронної пошти (пароль, двофакторна автентифікація, шифрування і под.). На основі цього аналізу розробіть план безпеки для використання електронної пошти. Проведіть невелике тестування на практиці, до прикладу, через створення і надсилання фішингових листів. Підготуйте презентацію з результатами дослідження.

ДЖЕРЕЛА ДЛЯ ПОГЛИБЛЕНОГО ВИВЧЕННЯ ТЕМИ

1. *Налаштування облікового запису електронної пошти в Пошті за допомогою невізуального екрана*. URL: http://surl.li/pyxxt
2. *Не поспішай сканувати: як хакери можуть використовувати QR-коди для шахрайства.* URL: https://www.eset.com/ua/about/newsroom/blog/data-protection/ne-speshi-skanirovat-kak-khakery-mogut-ispolzovat-qr-kody-dlya-moshennichestva/
3. *Як хакери можуть зламати вашу пошту та що робити для її захисту*. URL: https://www.eset.com/ua/about/newsroom/blog/data-protection/kak-khakery-mogut-vzlomat-vashu-pochtu-i-chto-delat-dlya-zashchity/
4. Pochapska O. *Password generators in Ensuring cybersecurity.* URL: https://medium.com/asposepdf/password-generators-in-ensuring-cybersecurity-1b5dae2f6e70

Модуль 3

СОЦІАЛЬНІ МЕРЕЖІ Й МЕСЕНДЖЕРИ: СПІЛКУЙСЯ БЕЗПЕЧНО

У цьому модулі поговоримо про те, як безпечно користуватися соціальними мережами, чому двофакторна ідентифікація тут є не менш важливою, а також подумаємо над тим, чи існують які-небудь справді безпечні месенджери.

Соціальні мережі сьогодні — це не лише розвага, але й часто робота. Саме тому на профілі в соціальних мережах і через них здійснюються хакерські атаки, направлені на збір персональних даних, доступ до профілів з метою реалізації певних шахрайських схем і под.

У попередніх модулях уже згадувалось поняття «персональні дані». У цьому модулі спробуємо розібратися детальніше, що це таке, і яке змістове наповнення має цей термін, які персональні дані й навіщо отримують соціальні мережі під час реєстрації облікового запису користувачем. Коли користувач реєструє обліковий запис у Google, він вказує своє ім'я, вік, стать, місце проживання. Більше того, обов'язково аналізуються пошукові записи, і в цьому контексті формується певний набір даних про нього і його вподобання. Система запам'ятовує навіть ті гаджети, через які користувач заходить в обліковий запис.

Так само працює Facebook (та власне й будь-яка соціальна мережа): ім'я, номер телефону, електронну адресу, місце знаходження, країни чи місця, до яких подорожує особа із зареєстрованим обліковим записом. І, найголовніше, цю інформацію користувачі добровільно надають соціальним мережам.

Поняття «персональні дані» і його визначення подається у восьмому абзаці статті 2 Закону України (ЗУ) «Про захист персональних даних», де вказується на те, що персональними даними є відомості чи сукупність відомостей про фізичну особу, за допомогою яких цю особу можна ідентифікувати або вже ідентифіковано.

Разом з тим, ЗУ не надає чіткого переліку відомостей (персональних даних) про фізичну особу, проте такий перелік визначається для кожного конкретного випадку.

Відповідно до законодавства більшості європейських країн визначаються персональні дані загального характеру й «чутливі» (вразливі) особисті дані.

До загальних особових даних відносять:

- ідентифікаційні дані (прізвище, ім'я, по батькові, адресу, номер телефону тощо);
- паспортні дані;
- особисті відомості (вік, стать, сімейний стан тощо);
- склад сім'ї;
- інформацію про освіту;

- професію;
- житлові умови;
- спосіб життя;
- життєві інтереси та захоплення;
- споживчі звички;
- фінансову інформацію.

До «чутливих» особових даних відносять:

- інформацію про расове, етнічне походження, національність;
- відомості, що стосуються політичних, світоглядних і релігійних переконань;
- відомості про членство в політичних партіях, профспілках, релігійних або громадських організаціях;
- відомості про стан здоров'я та статеве життя;
- генетичні й біометричні дані;
- місце знаходження та шляхи пересування особи;
- інформацію про застосування до особи заходів у межах трудового слідства;
- інформацію про вчинення щодо особи різних видів насильства.

Припустимо, користувач встановив новий додаток на свій смартфон. На екрані з'являється угода про використання персональних даних. Зазвичай, ця інформація залишається поза увагою та приймається автоматично натисканням кнопки *«Приймаю»* чи *«Погоджуюсь»*. Натомість застосунок цілком може отримати доступ до всіх файлів, які завантажуються через смартфон. Тобто всі сторінки, які власник смартфону відвідує зі свого мобільного телефону, геолокацію та іншу особисту інформацію, — до усього цього інформація надається користувачем добровільно шляхом натискання однієї кнопки.

Профіль у **Facebook** так само має певну екосистему, що складається з особистої сторінки, фейсбук-месенджера, де відбувається листування, та опціонально, публічних сторінок, до яких користувач має доступ або які він створював. Також там можуть бути групи або рекламні кабінети. Захищеність цих інструментів залежить від захищеності користувацького профілю.

Щоб подивитися на безпекові налаштування, необхідно натиснути на значок облікового запису в правому верхньому кутку та вибрати **«Налаштування та конфіденційність»**. Далі — **«Налаштування»**. У меню ліворуч потрібно обрати функцію **«Безпека та авторизація»**. У цьому розділі можна налаштувати сповіщення про підозрілу активність. Facebook пропонує надсилати сповіщення в додаток і на електронну поштову скриньку, якщо хтось намагатиметься зайти в обліковий запис із нового пристрою або браузера. Корисна функція, щоб оперативно дізнатися про підозрілу активність у профілі. Рекомендовано увімкнути сповіщення як у додаток, так і в пошту, оскільки котрась із опцій може не спрацювати.

Також можна налаштувати функцію надсилання сповіщень на електронну поштову скриньку користувача про будь-які дії, які відбуваються на його сторінці чи якось пов'язані з ним.

Якщо користувач є власником публічної сторінки у Facebook, необхідно звернути увагу на ролі на сторінці. Кожна роль має свій ступінь доступу до контенту. Подивитися ролі на сторінці можна в пункті «**Налаштування**» — «**Ролі на сторінці**».

Дві ключові ролі, що мають значний вплив на сторінку, це роль «**Власника**» та «**Адміністратора**». Власник сторінки може її видалити, призначити адміністраторами інших користувачів

або передати право власності на сторінку іншій людині. Тому акаунт власника варто додатково захистити, аби зменшити ризик втрати сторінки через злам.

Варто почати з перевірки пароля — чи відповідає він критеріям надійного, чи не фігурував у витоках даних. Наступний крок — налаштування двофакторної автентифікації.

Ще одне налаштування, на яке варто звернути увагу — прив'язані групи до публічної сторінки. Це налаштування є в розділі «**Групи**». Якщо в списку є старі або неактуальні групи, їх можна вимкнути в налаштуваннях. Також якщо сторінка підключена до групи, усі адміністратори, модератори й редактори сторінки можуть керувати групою. Про це важливо пам'ятати.

Чи існує можливість захистити персональні дані в соціальних мережах загалом і соціальній мережі Facebook зокрема? Можна принаймні максимально убезпечити свій обліковий запис від витоку персональних даних.

Двофакторна автентифікація у Facebook

Довідковий центр Facebook пропонує низку порад з налаштування двофакторної автентифікації. Загальні правила та принципи не відрізняються від налаштування двофакторної автентифікації будь-якого облікового запису. Разом з тим, варто детальніше ознайомитися з цими порадами (https://uk-ua.facebook.com/help/148233965247823) (див. Малюнок 3.1.):

Окрім того, медійникам (як публічним особам, на сторінках яких фіксується підвищена активність) рекомендують використовувати Facebook Protect — розширену програму безпеки в соціальних мережах Facebook та Instagram, створену для додаткового захисту акаунтів високоризикованих користувачів. Детальніше про програму й особливості її підключення можна почитати за покликанням (https://www.facebook.com/help/1052552578831700) на сторінці довідкового центру Facebook. Як правило, облікові записи користувачів із великою кількістю підписників і відвідувачів автоматично підключаються до Facebook Protect.

Налаштування конфіденційності в Telegram

Зайдіть у налаштування розділу **«Приватність та безпека»** і виконайте такі дії:

- Номер телефону. — Хто може бачити мій номер? — Мої контакти/Ніхто.
- Відвідини та стан у мережі. — Хто може бачити мої відвідини? — Мої контакти/Ніхто.
- Фото й відео профілю. — Хто може бачити мої фото та відео профілю? — Мої контакти.
- Пересилання повідомлень. — Хто може пересилати мої повідомлення разом із покликанням на мій акаунт? — Мої контакти/Ніхто.
- Виклики. — Хто мені може телефонувати? — Мої контакти/Ніхто.
- Групи й канали. — Хто може додавати мене до групових чатів? — Мої контакти.

У кожному з цих пунктів можна скористатися функцією «Додати винятки».

Перед тим, як надавати права Вашим користувачам на перегляд даних, важливо перевірити та відфільтрувати телефонну книгу.

Більше про особливості налаштування **Telegram** можна почитати, перейшовши за покликанням (https://telegram.org/)

Малюнок 3.1.Налаштування двофакторної автентифікації у соціальній мережі Facebook

Безпека у Viber

Для додаткового захисту в налаштуваннях у пункті «Конфіденційність» рекомендовано вимкнути статуси «У мережі» та «Переглянуто». Існує також функція «Приховані чати», доступ до яких можна обмежити, увівши PIN-код. Є змога також налаштувати та обмежити коло людей, які можуть додавати Вас у групи («Мої контакти»).

Анонсовано, що скоро у Viber має з'явитися двоетапна перевірка для додаткової безпеки. Користувачі зможуть захистити свої акаунти за допомогою додаткового PIN-коду та електронної пошти.

Детальніше про налаштування облікового запису у Viber можна почитати, перейшовши за покликанням (https://help.viber.com/hc/uk):

Налаштування захисту в Instagram

Для захисту аканту Instagram пропонує такі шляхи:

- Встановлення додатку для автентифікації.
- Надсилання коду у WhatsApp.
- Надсилання коду для входу на номер телефону.
- Використання резервних кодів.

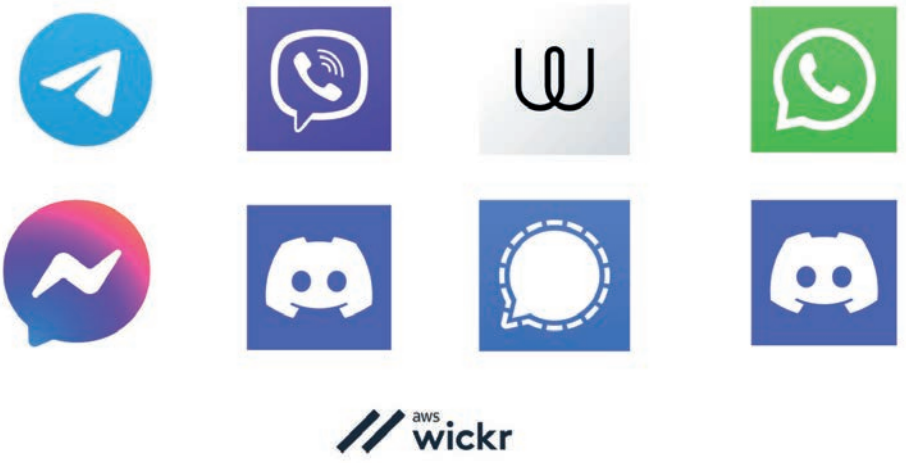
Більш детальну інформацію про особливості налаштування облікового запису й дотримання всіх правил безпеки можна почитати, перейшовши за покликанням на сторінку довідкового центру (https://help.instagram.com/?hl=uk).

Для дотримання правил безпеки в тому числі й у соціальних мережах, а також з етичних міркувань, Комісія журналістської етики радить розмежовувати приватні й робочі сторінки:

Поряд з соціальними мережами сьогодні активно використовуються й месенджери — канали обміну повідомленнями: від текстових і голосових аж до фото- і відеоповідомлень. Чи є месенджери безпечними? І які з них є хоча б відносно захищеними? Нині існує низка досліджень з цього приводу. Різноманітні IT-компанії робили власні рейтинги безпечних месенджерів. Аналіз досліджень дає можливість сформувати таку умовну градацію від найбільш безпечних і захищених месенджерів (див. Малюнок 3.2) до найменш безпечних.

Найбільш безпечними й захищеними месенджерами вважають **Threema, Wickr, Signal і Wire.** Говорячи про їхню захищеність, компанії-дослідники мають на увазі високу надійність криптографічних протоколів та алгоритмів. Ні **Threema,** ні **Wickr** не збирають і не надсилають контактну інформацію за умови анонімного використання. Тоді як **Signal** збирає номери користувачів (в обов'язковому порядку), а **Wire** зберігає та передає дані для Google Analytics, а також зберігає незашифровані локальні дані в Desktop-версії.

> «Журналісти мають усвідомлювати, що аудиторія не може розрізнити, які висловлювання представника медіа відбивають його журналістську позицію, а які є думкою приватної особи. Аудиторія журналіста в соціальних мережах не бачить різниці між професійною поведінкою та особистими уподобаннями журналіста. З точки зору читачів або глядачів ви є журналістом завжди, незалежно від того, перебуваєте на роботі чи відпочиваєте вдома».
>
> **КЖЕ (Комісія з журналістської етики)**



Малюнок 3.2. Найпопулярніші месенджери

Найбільш популярні месенджери — **Telegram, Viber, WhatsApp, Facebook Messenger, Discord** — IT-компанії, що проводили дослідження, називають більш небезпечними месенджерами, не зважаючи на історії про протоколи шифрування, а також про відсутність угоди про передачу персональних даних спецслужбам.

До прикладу, **Telegram** збирає номери телефонів, а також ID і передає спецслужбам на їхній запит (Privacy policy, п. 8.1). Проте жодного такого випадку жодна з компаній навести не може. **WhatsApp, Facebook Messenger, Discord** також зберігають дані без шифрування й, відповідно, до політики приватності передають інформацію на вимогу спецслужбам. Із закордонними правоохоронними органами можуть ділитися інформацією також **Wickr** і **Signal**.

Разом з тим, **Telegram, WhatsApp, Facebook Messenger** мають обов'язкову прив'язку до номера телефону, а також закритий програмний код сервера. У **Telegram** відкритий код лише для застосунків. Знову ж таки, у **Telegram** поза секретними чатами цілковито відсутнє наскрізне шифрування. Так само немає наскрізного шифрування в групових чатах і **Facebook Messenger.**

Відтак, важко говорити про те, що якийсь з месенджерів є абсолютно безпечним. Разом з тим, є месенджери, що забезпечують певну конфіденційність даних, а які такої конфіденційності не забезпечують.

ЗАВДАННЯ

Завдання 1. Проаналізуйте свою сторінку у Facebook на наявність потенційних небезпек та ризиків. Налаштуйте двофакторну автентифікацію облікового запису.

Завдання 2. Проаналізуйте свої облікові записи в інших соціальних мережах. Оцініть потенційні небезпеки та ризики. Налаштуйте двофакторну автентифікацію своїх облікових записів.

Завдання 3. Оберіть одну соціальну мережу. Проведіть невелике дослідження щодо їхньої популярності, функцій та особливостей. Проаналізуйте персональні потенційні ризики, пов'язані з використанням обраної соціальної мережі, включаючи проблеми приватності (кібербулінг, виток особистих даних і под.). Розробіть план заходів безпеки, який можна використати для мінімізації ризиків (до прикладу, налаштування приватності, обмеження контактів і под.). Підготуйте презентацію з результатами своїх досліджень.

ДЖЕРЕЛА ДЛЯ ПОГЛИБЛЕНОГО ВИВЧЕННЯ ТЕМИ

1. *Безпека дітей в інтернеті для батьків. Як убезпечити дітей від шкідливого контенту, цькування, суїцидальних інтернет-спілок та сексуальної експлуатації в інтернеті.* Дія. Освіта. URL: https://osvita.diia.gov.ua/courses/serial-dlya-batkiv-onlayn-bezpeka-ditey
2. *Обережно! Кібершахраї.* Дія. Освіта. URL: https://osvita.diia.gov.ua/courses/attention-cyber-fraudsters
3. *Одвічне питання медійників: чи слідкує за мною мій смартфон?* URL: https://imi.org.ua/advices/odvichne-pytannya-medijnykiv-chy-slidkuye-za-mnoyu-mij-smartfon-i42182
4. *Про кібербулінг для підлітків. Як протистояти булінгу в інтернеті.* Дія. Освіта. URL: https://osvita.diia.gov.ua/courses/cyberbullying
5. Сінґер, П. В. *Війна лайків. Зброя в руках соціальних мереж : пер. з англ.* / П. В. Сінґер, Емерсон Т. Брукінґ; пер.Ярослав Лебеденко; відп. за вип. А. В. Альошичева.Харків : Книжковий Клуб «Клуб Сімейного Дозвілля», 2019. 319 с.
6. *Що про медійників знає їхній мобільний оператор.* URL: https://imi.org.ua/advices/shho-pro-medijnykiv-znaye-yih-mobilnyj-operator-i42864
7. *Поняття про віруси.* Step-by-step. URL: https://step.org.ua/konspekt/antivir/tema2
8. *Як медійникам захистити їхні соціальні мережі в часи особливої інформаційної активності.* URL: https://imi.org.ua/advices/yak-medijnykam-zahystyty-yihni-sotsialni-merezhi-v-chasy-osoblyvoyi-informatsijnoyi-aktyvnosti-i42830
9. *Як стати YouTube-блогером. Як створити свій YouTube-канал, просунути і монетизувати його, впоратися з алгоритмами, слідкувати за авторським правом та шукати ідеї для відео.* Дія. Освіта. URL: https://osvita.diia.gov.ua/courses/youtube
10. *Як функціонують та завойовують аудиторію неінституціоналізовані новинні телеграм-канали* / Д. Дуцик, А. Плис, А. Сичова, О. Почапська, О. Юркова. 2023. URL: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/e6c3edc6–37a6–4a21-a194–7fdac553d328/content
11. *TikTok, Instagram, Facebook: як залишатись в тренді.* Дія. Освіта. URL: https://osvita.diia.gov.ua/courses/tiktok-instagram-facebook

Модуль 4

АНОНІМНІСТЬ У МЕРЕЖІ: ЯК НЕ ВЛЯПАТИСЬ У ЦИФРОВУ ІСТОРІЮ

У цьому модулі ми поговоримо про те, як зробити свій цифровий слід максимально непомітним, що таке робота в режимі «інкогніто», як очистити кеш, що таке Cookies і як працювати з віртуальними приватними мережами (VPN).

Коли ми говоримо про цифровий слід, то маємо на увазі всі ті цифрові дані, які користувач залишає в мережі Інтернет: від адреси електронної пошти до коментарів у соціальних мережах, від історії запитів у Google і аж до наповнення кошика в будь-якому інтернет-магазині.

Узагалі, якщо говорити про цифровий слід, то, в першу чергу, необхідно відкинути паніку. Зовсім не залишити цифрового сліду в сучасному світі, швидше за все, не вийде, оскільки тоді важко буде оптимально користуватися інтернетом. Разом з тим, ділитися власними даними потрібно обережно (див. Малюнок 4.1). Відтак, користуючись сервісами мережі Інтернет, необхідно пам'ятати, що, по-перше, **цифровий слід видалити непросто.** Тобто, якщо користувач, до прикладу, опублікував свої фото в соціальній мережі, контролювати їх поширення буде неможливо. Навіть якщо всі ці фото пізніше будуть видалені, хтось з інших користувачів може зробити скриншоти чи попередньо завантажити ці фото на власні ресурси, а потім опублікувати ці фото у вигляді ілюстрацій до якої інформації чи под. По-друге, **кожна дія користувача доповнює характеристики його цифрової ідентичності.** До прикладу, інтернет-майданчики зберігають і оновлюють профайли користувачів, аби можна було розсилати персоналізовану рекламу. По-третє , **цифровий слід досить складно зробити конфіденційним.** До прикладу, інформація навіть із закритих облікових записів або особистого

Мал. 4.1. Помилки користувачів

листування може стати публічною через витоки даних чи скріншоти. Ну, і по-четверте, **цифровий слід користувача можуть використовувати злочинці,** до прикладу, для фішингу чи для доступу до облікових записів.

Залежно від усвідомленості дій, цифровий слід може бути **активним** і **пасивним.**

Активний цифровий слід говорить про те, що користувач залишає про себе інформацію навмисне (до прикладу: коментар в соціальній мережі, заповнений профіль, дописи і под.). Чим більше такої інформації залишає користувач, тим більш помітним стає його цифровий слід.

Пасивний цифровий слід — це та інформація, яка збирається про користувача за допомогою різноманітних інструментів (до прикладу: рекламні трекери, файли Cookies, фінгерпринти под.).

Фінгерпринт — це цифровий відбиток пальця користувача, інструмент, який робить людину помітною та унікальною на основі налаштувань браузера та пристроїв. Насамперед фінгерпринт потрібен, щоб сайти відображалися правильно. Передаються дані про роздільну здатність екрана, операційну систему, місцезнаходження та налаштування мови. Усі ці деталі формують унікальний зліпок, який формує пасивний цифровий слід користувача.

Розглянемо, яку інформацію ми залишаємо про себе у вигляді цифрового сліду на різноманітних сайтах і платформах в мережі Інтернет (див. Малюнок 4.2).

Чи можна дізнатися, яку саме інформацію про користувача збирають сайти?

Так, це можна дізнатися за допомогою низки спеціальних програм:

- **Cover Your Track** — ця програма аналізує онлайн-відстеження та унікальність фінгерпринту користувача. Тест імітує завантаження кількох трекерів активності й визначає рівень захисту від відстеження.

Щоб спробувати цей застосунок, можна перейти за покликанням, скориставшись QR-кодом:

- **Whoer —** цей сервіс дає можливість перевірити інформацію, яку браузер передає до мережі Інтернет. По суті, програма дає можливість з'ясувати, наскільки користувач залишається анонімним у мережі Інтернет. Цей сервіс підходить для перевірки proxy і socks серверів, надасть інформацію про VPN користувача, перевірить IP-адресу, визначить, чи перебуває вона в чорних списках, підкаже, чи включені Flash, Java, Cookies на комп'ютері, які його мовні й системні налаштування, яка операційна система використовується, визначить DNS та ін.

Рекламні трекери — це спеціальні інструменти, які збирають та ідентифікують інформацію про користувачів для аналітики та персоналізованої реклами. З їхньою допомогою маркетологи дізнаються, як люди взаємодіють з контентом в інтернеті. Найчастіше їх вбудовують у сайти за згодою власників. Але трапляються й шахрайські трекери, які передають інформацію третім особам.

Cookies: що це? Чи можуть вони бути небезпечними?

Cookies — це ще один інструмент, який дозволяє збирати інформацію про користувача. Як правило, коли відвідуєш який-небудь сайт, з'являється випадне вікно з пропозицією прийняти **Cookies** (усі, тільки необхідні чи взагалі відхилити). У більшості випадків користувачі швиденько погоджуються прийняти всі необхідні **Cookies,** аби віконечко, яке закриває більшу частину інформації, нарешті зникло.

Сервіс	Номер телефону	e-mail	Платіжна інформація	Ім'я / нікнейм	Історія дій	Дані про пристрій	Фото / Аватар
Месенджери	✓	✓		✓	✓	✓	✓
Соцмережі	✓	✓		✓	✓	✓	✓
Пошукова мережа					✓	✓	
Форуми		✓		✓	✓	✓	✓
Маркетплейси	✓	✓	✓	✓	✓	✓	✓
Таксі (застосунки)	✓	✓	✓	✓	✓	✓	✓

Малюнок 4.2. Цифровий слід, який залишає користувач

Малюнок 4.3. Інтерфейс застосунку Cover Your Track

Головна функція Cookies — підлаштувати сайт під конкретного користувача.

Ми не можемо говорити про те, що **Cookies** є чимось небезпечним. Це всього лише фрагменти даних, що надсилаються з вебсерверу й зберігаються на комп'ютері користувача. За допомогою цих даних сайт запам'ятовує, у який спосіб користувачі залогінились на сайті, які сторінки вони переглядали, які товари додавали в кошик. Це значно спрощує процедуру наступного відвідування.

Cookies бувають двох видів:

Постійні. Вони зберігають інформацію протягом кількох тижнів чи місяців і не видаляються після закриття сайту.

Тимчасові. Вони існують лише тоді, коли користувач перебуває на сайті, а після закриття сторінки видаляються.

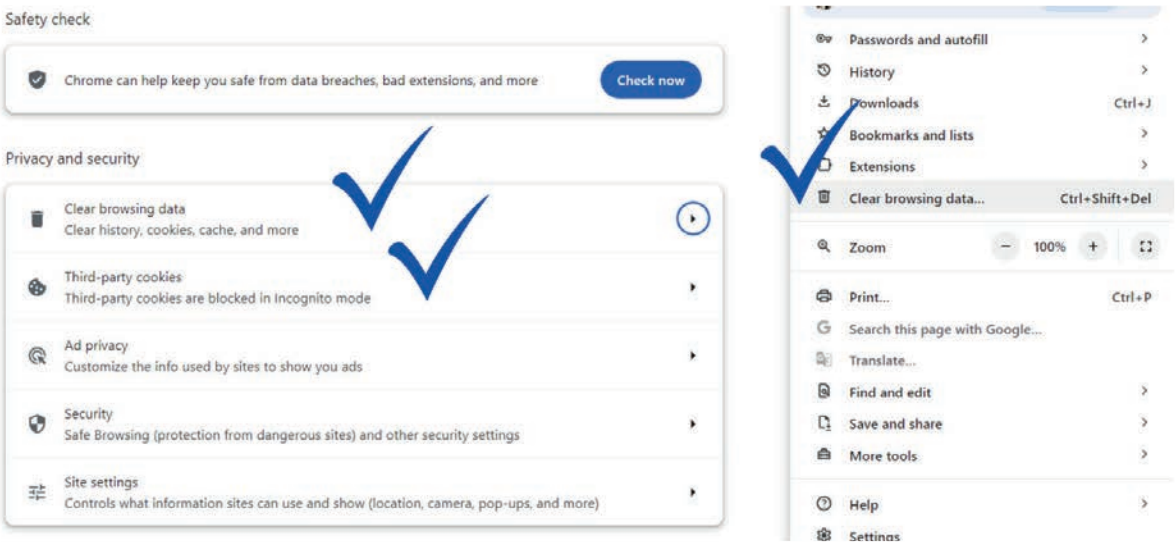
Чи потрібно чистити Cookie? Чи можна вимкнути Cookie? Ці питання виникають періодично в кожного користувача. Підтримки Cookie вимагає більшість сайтів: медіа, соціальні мережі, інтернет-магазини. Звісно, можна їх не приймати. У гіршому випадку користувач не зможе зайти в особистий кабінет — доведеться повторити процедуру реєстрації.

Рекомендують Cookie час від часу чистити. Краще це робити з тими сайтами, на які користувач заходить рідко або на які більше не збирається заходити взагалі. Якщо анонімність у користувача в пріоритеті, тоді можливо краще Cookie чистити.

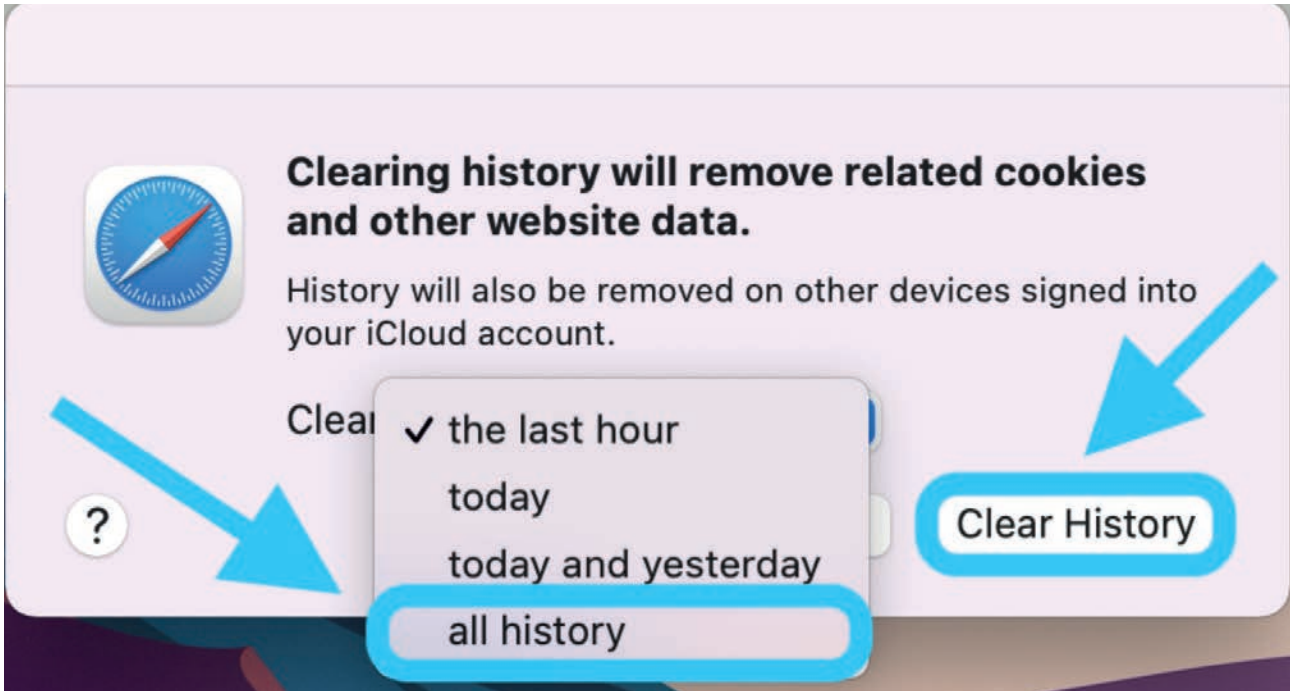
Принципи й способи чищення Cookie залежать від браузера.

Google Chrome. Потрібно зайти в «Інструменти» → «Історія», натиснути «Очистити історію», відзначивши «Файли cookie та інші дані сайтів». Також у розділі «Файли Cookie та інші дані сайтів» можна налаштувати винятки — обрати сайти, які завжди можуть використовувати Cookie (Див. Малюнок 4.3.).

Детальніше про те, як налаштувати обліковий запис і систему безпеки Google, можна подивитися на сторінці довідкового центру Google за покликанням:



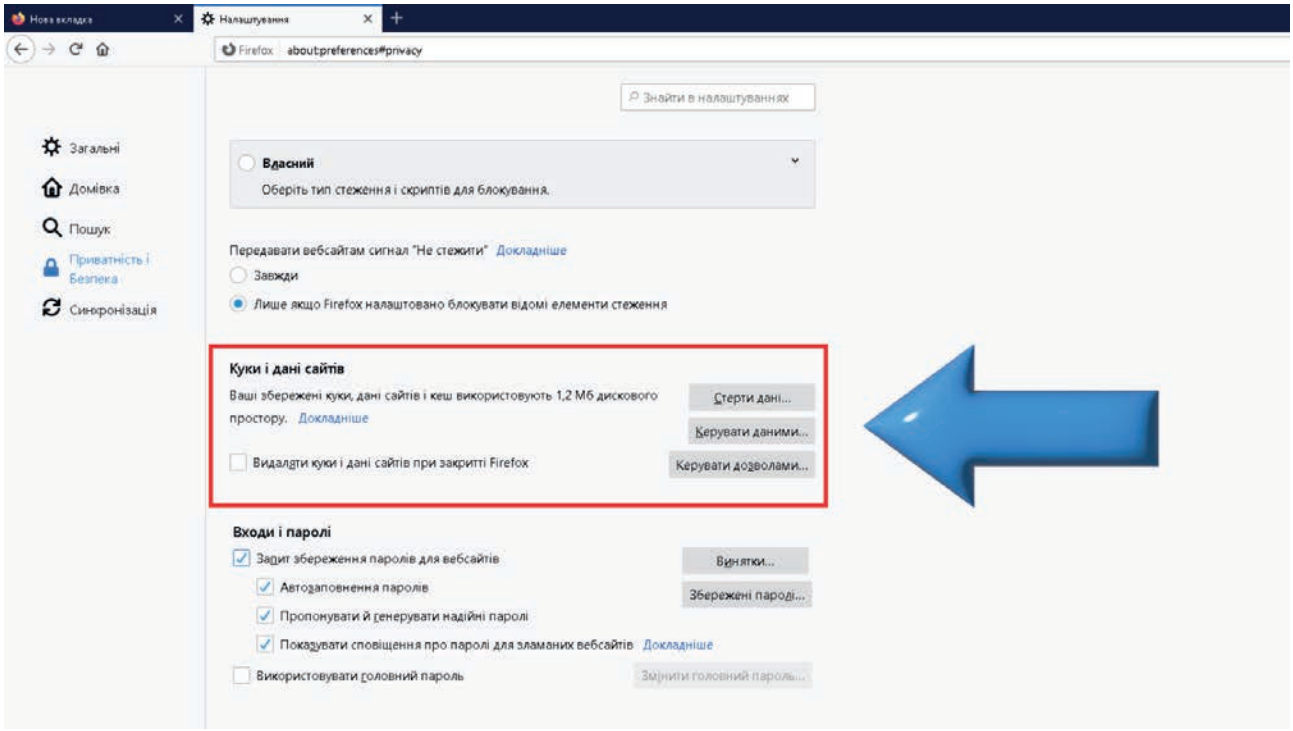
Малюнок 4.3. Налаштування Cookie у **Google Chrom**



Малюнок 4.4. Налаштування Cookie у **Safari**

Safari (див. Малюнок 4.4.). У «Налаштуваннях» необхідно обрати розділ «Конфіденційність», а потім — «Керування даними на вебсайті». Можна почистити всі Cookie або вибірково.

Firefox. Користувачеві необхідно зайти до розділу «Бібліотека», вибрати пункт «Історія» та натиснути «Видалити історію», позначивши галочкою пункти «Cookie» та «Кеш» (див. Малюнок 4.5.).



Малюнок 4.5. Налаштування Cookie у **Firefox**

Як зробити свій браузер максимально анонімним? (див. Малюнок 4.6.)

Малюнок 4.6. Як зробити свій цифровий слід менш помітним?

Є низка програм, яка допомагає анонімізувати браузер. За їх допомогою можна приховати цифровий слід або зробити його менш помітним.

1. Розширення, що може змінити ідентифікацію браузера. До прикладу, **Privacy Possum, Random User-Agent, Chameleon WebExtension, 30 Seconds of Knowledge, Browser Plugs Fingerprint Privacy Firewall, Man in the Middle, User-Agent Switcher.**
2. Можна встановити плагін, що блокує рекламні трекери чи інші маячки. Такими плагінами, до прикладу, можуть бути **Adguard, Adblock Plus, Adblock Pro, NoScript, uBlock.**
3. За допомогою спеціальних сервісів можна підмінити фінгерпринт. Таким сервісом, до прикладу, може бути **AQUM, Multiloginapp**.
4. Можна скористатися **виділеним сервером.** За його допомогою можна зберігати дані на окремій фізичній машині.

Окрім того, користувач може зробити свій цифровий слід більш анонімним, якщо змінить налаштування мови, часового поясу, роздільної здатності екрану, масштабу вебсторінки, підключення Flash, JavaScript, WebGl. Щоправда, усе це робить користування мережею Інтернет вкрай незручним, а тому до таких дій слід вдаватися вже за крайньої потреби.

Є можливість зменшити свій цифровий слід і через використання смартфону. Уже в iOS 14.5 є функція **App Tracking Transparency**. Вона дає можливість заборонити відстеження даних на рівні системи.

Якщо смартфон користувача базується на системі Android, то слід пам'ятати, що з 2013 року на телефонах є спеціальний рекламний ідентифікатор. Його задають сервіси Google Play, щоб відстежувати звички та захоплення користувачів. Цей ідентифікатор можна скинути через «Налаштування». Необхідно увійти до «**Налаштування**» → **Google** → «**Реклама**» → «**Скинути рекламний ідентифікатор» / «Видалити рекламний ідентифікатор».** Якщо користувач обирає перший варіант, то з'явиться новий ідентифікатор; якщо ж –другий, то додатки не зможуть використовувати рекламний ідентифікатор для персоналізації рекламних повідомлень.

ПРАВО НА ЗАБУТТЯ як форма зменшення цифрового сліду

Право на забуття — це право користувача на вилучення із загального доступу інформації, яка може йому зашкодити. До такої інформації належить:

- недостовірні чи неактуальні відомості;
- інформація, яка поширюється з порушенням закону;
- дані, які можуть зашкодити людині.

Не можна видалити інформацію про кримінальні злочини, незняту чи непогашену судимість.

Щоб **скористатися правом на забуття**, необхідно виконати такі дії:

- зібрати покликання на ті матеріали, які користувачеві необхідно видалити;
- написати заяву на видалення інформації (тут обов'язково потрібно вказати причини видалення, перелік покликань на інформацію, яку потрібно видалити, паспортні дані, контактну інформацію, а також згоду на обробку персональних даних);
- надіслати заяву до пошукової системи за допомогою спеціальної форми (до прикладу, як у Google).

Після того, як сервіс розгляне заявку та ухвалить рішення, можливі два шляхи розвитку подій: якщо рішення позитивне, інформація буде видалена упродовж 10 днів; якщо рішення негативне, користувач отримає мотивовану відмову.

Якщо рішення про відмову у видаленні інформації не задовільнило користувача, він має право звернутися до суду.

VPN: різновиди й особливості використання

VPN або Virtual Private Network — це технологія, яка забезпечує анонімне підключення до мережі Інтернет. Основне її завдання — захистити користувачів від витоку персональної інформації. Ця технологія захищає логін і пароль від перехоплення навіть за умови, що користувач підключається до мережі Інтернет через публічний Wi-Fi.

Технологія Віртуальної приватної мережі (**VPN)** дає можливість:

- забезпечити роботу додатку, використовуючи IP (ідентифікатор мережевого рівня) зі зміненою адресою;
- анонімізувати роботу в мережі Інтернет;
- приховати реальне місце знаходження комп'ютера, на якому працює користувач;
- забезпечити безпечне приєднання до загальної (публічної) мережі;
- отримати високу швидкість інтернет-з'єднання;
- уникнути збоїв підключення до мережі Інтернет, а також можливих збоїв при передачі інформації;
- створити анонімний канал, захищений від атак хакерів;
- підтримувати безпеку корпоративних мереж.

Є декілька різновидів мереж VPN. Найбільш розповсюдженими є VPN — це PPTP VPN, Site-to-Site VPN, L2TP VPN, IPsec, SSL, MPLS VPN, та Hybrid VPN.

Розглянемо кожен з цих різновидів окремо, щоб зрозуміти переваги й недоліки кожного.

1. **PPTP (**Point-to-Point Tunneling Protocol**) VPN**. Ця мережа працює із застосуванням протоколу тунелювання «точка-точка». PPTP VPN створює тунель і фіксує дані. PPTP VPN-адреси ідеально підходять для приватного користування та бізнесу, оскільки вони не вимагають придбання та встановлення додаткового обладнання й функцій, які зазвичай пропонуються як недороге додаткове програмне забезпечення. PPTP VPN-адресами найчастіше користуються також завдяки їхній сумісності з системами Windows, Mac та Linux. **Недоліком** PPTP VPN є те, що мережа не забезпечує шифрування, що зазвичай, і є причиною звернення за послугою до мережі VPN.
2. **Site-to-Site VPN** також називають Router-to-Router (маршрутизатор-маршрутизатор) VPN і використовують переважно в корпоративних операціях. Якщо сказати просто, Site-to-Site VPN створює віртуальний міст, який об'єднує мережі в різних місцях, для підключення їх до Інтернету та підтримки безпечного й приватного зв'язку між цими мережами. Як і PPTP VPN, Site-to-Site VPN створює безпечну мережу. Проте не існує спеціальної лінії, яка дозволяє використовувати різні вебсайти в межах компанії, як ми вже згадували, для підключення до форми VPN. Також, на відміну від PPTP, маршрутизація, шифрування та дешифрування виконуються апаратним або програмним забезпеченням на обох кінцях.
3. **L2TP** (**Layer to Tunneling**) розроблена Microsoft та Cisco. L2TP VPN — це VPN мережі, які, як правило, поєднуються з іншим протоколом VPN безпеки для встановлення

більш безпечного VPN-з'єднання. L2TP VPN утворює тунель між двома пунктами підключення L2TP, а інший VPN, такий як протокол IPsec, шифрує дані та фокусується на забезпеченні зв'язку між тунелями.

4. **IPsec** (Internet Protocol Security) — це протокол VPN, який використовується для забезпечення інтернет-зв'язку в IP-мережі. Тунель, налаштований на віддаленому сайті, дозволяє отримати доступ до вашого центрального сайту. Існує два режими, у яких працює IPsec VPN. Це режим транспортування та тунелювання. Обидва режими створені для захисту передачі даних між двома різними мережами. Суттєвим **недоліком** використання цього протоколу є те, що сам процес фінансово й часозатратний.
5. **SSL TLS VPN. SSL** (**Secure Sockets Layer**) та **TLS** (**Transport Layer Security)** працюють як один протокол. Обидва використовуються для встановлення VPN-з'єднання. Це з'єднання VPN, де веббраузер виконує роль клієнта, і користувацький доступ обмежується лише певними програмами, а не цілою мережею.
6. **MPLS VPN** (**Multi-Protocol Label Switching**) найкраще використовувати для типу з'єднання Site-to-Site. Це, у першу чергу, пов'язано з тим, що MPLS — найбільш гнучкий та легкий для адаптування варіант. MPLS — це стандартний ресурс, який використовується для прискорення розподілу мережевих пакетів за допомогою декількох протоколів.

Сьогодні існує багато різноманітних **VPN.** За різними версіями, до першої десятки входять:

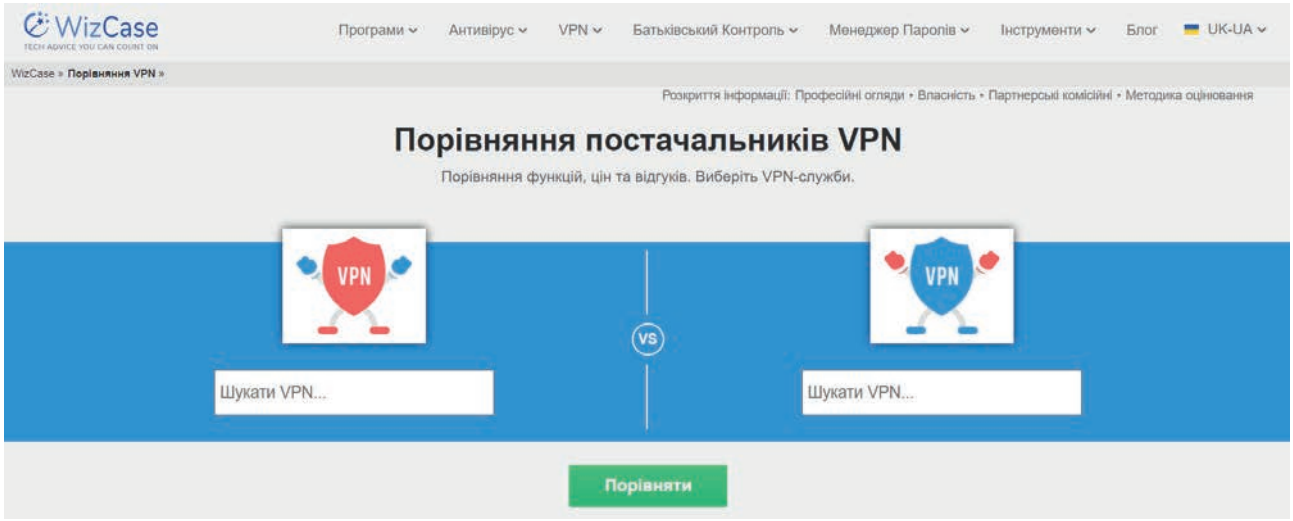
- SurfShark — https://surfshark.com/
- NordVPN — https://nordvpn.com/
- ExpressVPN — https://www.expressvpn.com/
- Proton VPN — https://protonvpn.com/
- Cyber Ghost — https://www.cyberghostvpn.com/
- Privat Internet Access — https://www.privateinternetaccess.com/
- IPVanish — https://www.ipvanish.com/
- VyprVPN — https://www.vyprvpn.com/
- PrivateVPN — https://privatevpn.com/
- Atlas VPN — https://atlasvpn.com/

Для того, аби визначитись, який VPN підходить найбільше, можна скористатися сервісом, який допомагає порівнювати характеристики VPN (https://uk.wizcase.com/vpn-comparison/) (див. Малюнок 4.7.).

Соціальні мережі стали неодмінною складовою сучасного світу, забезпечуючи користувачів можливістю спілкуватися, обмінюватися інформацією та взаємодіяти з іншими. Проте, поряд з цими перевагами, робота користувачів у соціальних мережах також пов'язана з ризиками та небезпеками.

Першою серйозною загрозою є приватність та безпека даних. Багато користувачів не усвідомлюють, що інформація, якою вони діляться в соціальних мережах, може бути доступною для широкого кола людей, включаючи зловмисників. Недбале використання налаштувань приватності може призвести до витоку особистих даних, що може використовуватися для шахрайства, крадіжки особистої ідентичності або інших злочинів.

Другим ризиком є негативний вплив на психічне здоров'я. Спостереження за ідеальним життям інших користувачів у соціальних мережах може призвести до почуття неповноцінності,



Малюнок 4.7. Інтерфейс застосунку Wizcase

ревнощів та депресії. Багато людей порівнюють своє життя з ідеалізованими зображеннями, що представлені в соціальних мережах, і це може викликати стрес та низьку самооцінку.

Третій ризик полягає в залученні до онлайн-шахрайств та кібербулінгу. Соціальні мережі можуть стати платформою для кібербулінгу, дискримінації та цифрового насильства. Крім того, зловмисники можуть послуговуватися соціальними мережами для спілкування з потенційними жертвами шахрайства, використовуючи підроблені профілі або маніпулюючи даними користувачів.

Нарешті, четвертим ризиком є вплив соціальних мереж на реальні відносини. Велика кількість часу, витраченого в соціальних мережах, може призвести до відчуження від реального світу та справжніх соціальних зв'язків. Люди можуть відвернутися від особистого спілкування в реальному житті на користь віртуального спілкування, що може призвести до втрати глибини та значущості відносин.

Отже, робота користувачів у соціальних мережах має свої ризики та небезпеки, які важливо усвідомлювати. При цьому необхідно дотримуватися засад безпечного користування, включаючи налаштування приватності, обмеження часу, витраченого в соціальних мережах, та постійну обережність у взаємодії з іншими користувачами. Тільки так можна забезпечити позитивний та безпечний досвід використання соціальних мереж.

ЗАВДАННЯ

Завдання 1. Використовуючи підказки, з'ясуйте власний цифровий слід. Спробуйте визначити, чи інформація, яку мережа Інтернет знає про вас, не становить для вас потенційної небезпеки.

Завдання 2. Опираючись на інформацію з розділу, спробуйте очистити Cookies у власному браузері.

Завдання 3. Оберіть для себе VPN. Спробуйте налаштувати його.

ДЖЕРЕЛА ДЛЯ ПОГЛИБЛЕНОГО ВИВЧЕННЯ ТЕМИ

1. Буга В.В., Турбін Д.О. *Право на забуття в системі захисту персональних даних*. Правовий часопис Донбасу. 2020, №1 (70). С. 46–53. URL: https://ljd.dnuvs.ukr.education/wp-content/uploads/2022/01/6-buga-turbin.pdf
2. *Вебсерфінг. Безпечна робота в браузері*. Інститут Масової Інформації. URL: https://imi.org.ua/advices/vebserfing-bezpechna-robota-v-brauzeri-i32148
3. Використання месенджерів як елементів цифрової розвідки: проблематика та шляхи вирішення. URL: https://intelmag.com/digitalization/17454-vykorystannya-mesendzheriv-yak-elementiv-czyfrovoyi-rozvidky-problematyka-ta-shlyahy-vyrishennya/
4. Що таке VPN? Посібник для обережних користувачів. URL: https://7vpn.com/ua/blog/shho-take-vpn-posibnik-dlya-kiber-oberezhnih-koristuvachiv/
5. *Інтернет знає все. Як журналістам обмежити збір даних про них у мережі*. Інститут Масової Інформації. URL: https://imi.org.ua/advices/internet-znaye-vse-yak-zhurnalistam-obmezhyty-zbir-danyh-pro-nyh-u-merezhi-i38397
6. *Контрацепція в мережі. Як убезпечитися під час роботи в браузері*. Інститут Масової Інформації. URL: https://imi.org.ua/advices/kontratseptsiya-v-merezhi-yak-ubezpechytysya-pid-chas-roboty-v-brauzeri-i31595
7. Матюшко Д. *10 Кращих Безкоштовних VPN у 2024* . URL: https://uk.vpnmentor.com/
8. *Як убезпечитися від зараження комп'ютерним вірусом? Поради*. . Інститут Масової Інформації. URL: https://imi.org.ua/advices/yak-ubezpechytysya-vid-zarazhennya-komp-yuternym-virusom-porady-i31434

Модуль 5

ЯК ЗБЕРІГАТИ Й ПЕРЕДАВАТИ ІНФОРМАЦІЮ

У цьому модулі ми поговоримо про те, як і де краще зберігати інформацію, щоб уникнути її витоку, які бувають програми для шифрування інформації, що передається, що таке хмарні сервіси і як ними користуватися.

Чим більш важливу інформацію ми маємо, тим важче її зберігати, впорядковувати й передавати. Окрім смислового групування інформації по папках і дисках, необхідно також передбачати резервне її копіювання і зберігання поза конкретним пристроєм, але зі збереженням конфіденційного доступу.

Для зберігання інформації на власному ПК (ноутбуці, планшеті і т.п.) рекомендовано дотримуватися таких правил:

1. Будь-який комп'ютер повинен містити, як мінімум, два логічних диски (традиційно «C» і «D»). Зазвичай, на першому розміщується операційна система, яку потрібно періодично оновлювати, перевстановлювати, а на диску «D» найкраще зберігати іншу важливу інформацію.
2. Бажано не зберігати даних на робочому столі (див. п.1.), оскільки робочий стіл — це та ж папка, яка розташована на диску «C».
3. Для забезпечення збереження даних необхідно робити резервні копії важливої інформації. Головне правило: резервна копія повинна зберігатися на іншому носії інформації, відмінному від того пристрою, на якому її було створено.

Де зберігати резервні копії?

Існує декілька варіантів збереження резервних копій інформації:

- **CD/DVD-диски**: так, цей застарілий варіант був популярним у 2000–2010 роках; сьогодні він не є ефективним (хоча подекуди все ще використовується), оскільки, по-перше, сучасні ноутбуки практично не обладнані дисководами, а по-друге, на ці пристрої вміщається невеликий обсяг інформації;
- **USB-флеш-накопичувач** («флешка»): на цьому накопичувачі можна зберігати великий обсяг інформації; усі комп'ютери сприймають USB-флеш-накопичувачі як окремий диск, тому не потрібне встановлення додаткового програмного обладнання; разом з тим, цей спосіб збереження резервної інформації важко назвати надійним;
- **зовнішній жорсткі диски (SSD та HDD):** зовнішні жорсткі диски — це портативні прилади, які не вбудовані в комп'ютери чи ноутбуки, а можуть бути підключені до будь-якого пристрою, який має можливість зчитування, обробки та зберігання даних; ці пристрої дають змогу зберігати великі обсяги інформації. Якщо залишити поза увагою технічні особливості побудови обох типів жорсткого диску (SSD/HDD), для користувача важливими характеристиками залишаються місткість (обидва різновиди можуть

містити навіть терабайт інформації, але мають значні відмінності в ціні), зношуваність (HDD мають багато рухомих елементів, а тому швидше зношуються, аніж SSD), швидкість видачі та зберігання інформації (оскільки SSD не мають рухомих частин, а працюють за принципом флеш-накопичувача, цей тип зовнішніх дисків мають більшу швидкість видачі та зберігання інформації).

- **«хмарні» сховища**: у цьому випадку інформація зберігається на віртуальному диску, і користувач може мати до нього доступ з будь-кого пристрою — достатньо мати логін і пароль доступу.

«Хмарні» сховища сьогодні користуються попитом. Розглянемо детальніше особливості їхнього функціонування.

«Хмарне» сховище — це модель збереження даних, відповідно до якої цифрові дані накопичуються в логічні об'єкти, а їхнє фізичне зберігання охоплює декілька серверів. Тобто — і це важливо! — дані не зберігаються на робочому пристрої користувача, а передаються на сервер (віддалене фізичне середовище) компанії-хоста, а користувач має доступ у вигляді облікового запису з власним логіном і паролем.

Як правило, компанії такий простір для зберігання даних на віддалених серверах надають у безкоштовне користування з певними обмеженнями — у часі та/або просторі для зберігання (наприклад, DropBox, OneDrive, GoogleDrive та ін.). Для розширення можливостей (збільшення місця для зберігання інформації, збільшення часу зберігання інформації і под.) необхідно купувати пакети послуг.

Розглянемо ці сервіси детальніше.

Google Drive — один з найбільш популярних сервісів для резервного копіювання та зберігання даних. Це хмарне сховище було створене ще у 2012 році. Цей ресурс є продуктом компанії Google, а тому він легко інтегрується з іншими сервісами, що досить зручно для роботи: Google Documents, Google Photo та ін.

Особливості **Google Drive:**

- до 15 Гб безкоштовного простору для збереження даних;
- максимальний розмір одного файлу, який можна завантажити на **Google Drive, — 10 Гб;**
- доступ до різних пристроїв з різними операційними системами (Android, iOS, MacOS, Windows);
- можливість керування доступом до файлів, спільною роботою в документі, редагуванням у режимі реального часу;
- відстеження історії внесення змін;
- HTTPS шифрування та алгоритм PFS;
- можливість скасування внесених змін і повернення документа до початкової версії;
- створення архівів для завантаження;
- робота з понад трьома десятками типами даних (фото, відео, документи, презентації і под.).

OneDrive — це хмарний сервіс від компанії Microsoft, що був створений у 2007 році. Цей сервіс є частиною пакетного рішення Microsoft365, що включає різні програми типу Excel, Word, PowerPoint та ін. Такий підхід (аналогічний до підходу компанії Google), що робить цей сервіс досить

зручним та функціональним. Здебільшого сервісом користуються корпорації, а також звичайні користувачі, які використовують пакет за підпискою.

Особливості **OneDrive:**

- до 5 Гб безкоштовного простору для збереження даних;
- максимальний розмір одного завантаженого файлу — 2Гб;
- доступ до різних пристроїв з різними операційними системами (Android, iOS, MacOS, Windows);
- можливість керування доступом до файлів, спільною роботою в документі, редагуванням у режимі реального часу;
- вбудований пошук та Skype;
- сейф з додатковим рівнем захисту;
- віддалений доступ до ПК, де виконаний вхід в обліковий запис Microsoft;
- покликання на файли з обмеженим терміном дії (термін встановлює власник даних);
- автозавантаження файлів з підключених пристроїв.

Dropbox — це хмарний сервіс, який функціонує з 2007 року. Особливість його полягає у відсутності прив'язки до будь-якого продукту, а тому не продається пакетно (як, до прикладу, у ситуації із Google Drive чи OneDrive), що дає можливість обрати виключно ту послугу, яка потрібна тут і зараз. Цей сервіс працює за принципом синхронізації даних. Це дає можливість дозавантажувати файли, вносити зміни у файлах, видаляти їх — і все це з різних пристроїв на конкретний обліковий запис (акаунт).

Особливості **Dropbox:**

- до 2 Гб безкоштовного простору для збереження даних (+2 ГБ для робочої хмари, +3 ГБ після увімкнення автозавантаження, +250 МБ за проходження курсу, +500 МБ за кожного запрошеного користувача та до +48 ГБ для власників останніх моделей Samsung);
- максимальний розмір одного файлу для завантаження — 250 Гб (за платною підпискою);
- відновлення видалених файлів;
- доступ до різних пристроїв з різними операційними системами (Android, iOS, MacOS, Windows);
- можливість керування доступом до файлів, спільною роботою в документі, редагуванням у режимі реального часу;
- відображення історії змін файлів, а також функція повідомлення про внесені зміни;
- можливість редагування PDF-файлів;
- вбудований пошук.

Mega — це хмарне сховище, яке було розроблене у 2013 році (новозеландським підприємцем). **Mega** поєднує функціонал хмарного сховища і файлообмінника. Цей сервіс пропонує наразі найбільший обсяг для безкоштовного зберігання інформації. Більше того, цей ресурс виконує шифрування в браузері, що дає можливість забезпечити високий рівень надійності збереження даних.

Особливості **Mega:**

- до 20Гб місця безкоштовно;
- не встановлено обмеження на максимальний розмір завантаженого файлу;
- доступ до різних пристроїв з різними операційними системами (Android, iOS, MacOS, Windows);
- можливість керування доступом до файлів, спільною роботою в документі, редагуванням у режимі реального часу;
- робота з файлами будь-якого типу;
- до 100 версій файлу для його захисту;
- автоматичне резервне копіювання;
- чати з можливістю обміну повідомленнями, онлайн-зустрічами та дзвінками;
- можливість використання двофакторної автентифікації.

Звісно, хмарні сховища — це не набір суттєвих переваг. Є також недоліки, котрі потрібно враховувати, обираючи найнадійніший ресурс для захисту. Порівняємо переваги та недоліки хмарних сховищ (див. Таблиця 5.1.).

Таблиця 5.1. Переваги та недоліки хмарних сховищ

Переваги	Недоліки
▸ захист даних; ▸ віддалений доступ; ▸ швидкий обмін даними; ▸ економія місця; ▸ спільний доступ та робота; ▸ відновлення та резервне копіювання.	▸ ризик хакерських атак та зливу інформації в мережу Інтернет; ▸ ризик перегляду файлів нечесними співробітниками компанії, на серверах якої знаходиться сховище; ▸ залежність від роботи сервера та наявності підключення до мережі Інтернет.

Для спрощення роботи з хмарними сервісами, особливо, коли йдеться про необхідність копіювати кілька десятків чи навіть сотень файлів одномоментно та зберігати їх у віддаленому сховищі, існують спеціальні програми, що забезпечують автоматичне копіювання й зберігання документів (різних форматів) у віддалених сервісах.

Таких програм на сьогодні нараховують кілька десятків. Кожна має свої переваги, технічні вимоги й специфіку роботи. Поговоримо лише про деякі з них, що є найбільш популярними (за різними версіями й рейтингами) серед користувачів через їхню доступність, універсальність і функціонал.

- **Cobian Backup**. Ця програма дає можливість регулярно створювати копії важливих файлів (за розкладом), стискати їх, шифрувати й переносити на віддалений сервер. Користувач сам встановлює зручний час, коли програма буде запускатися самостійно й працювати у фоновому режимі. Автоматизація процесу дозволяє зберегти час. Окрім того, програма може самостійно скопіювати великий обсяг інформації і самостійно вимкнути пристрій після завершення роботи.
- **Allways Sync .** Ця програма дозволяє синхронізувати файли й каталоги між персональним комп'ютером, ноутбуком, флешками й под. Також може самостійно створювати резервні копії даних.
- **Free Backup.** Це безкоштовна програма, яка дає можливість створення резервних копій інформації, працює в Microsoft Windows.

- **FreeFileSync**. Ця програма є безкоштовним синхронізатором для GNU/ Linux і Microsoft Windows.
- **Time Machine**. Ця програма дає можливість резервного копіювання від Apple. Вона вже включена в операційну систему MacOS версій 10.5 і вище.
- **Unison File Synchronizer.** Це програма є синхронізатором для Microsoft Windows, Mac OS і GNU / Linux.

Інформація, яка видалилась з пристрою через некоректну роботу програм, випадково (через дії користувача) чи через інші обставини, може бути відновлена (за умови, що така інформація не була видалена за допомогою програм надійного очищення типу Eraser або спеціальної опції в CCleaner).

Ідеально — звернутися до фахівця, який може допомогти користувачеві відновити втрачену інформацію.

Разом з тим, є низка програм, що дають можливість відновити втрачену інформацію:

- **Recuva** — програма, яка допомагає користувачам відновлювати видалену інформацію не тільки на комп'ютері, а й на флешках, CD-дисках, і картах пам'яті;
- **Diskdigger** — програма для відновлення стертих файлів для користувачів Windows і Linux;
- **TestDisk** і **PhotoRec** — програми для відновлення даних для користувачів MacOS;
- **R-Linux** — програма для відновлення даних для користувачів Linux.

Для більш надійного збереження інформації можна використовувати **програми для шифрування інформації.**

Шифрування — це процес, у результаті якого дані кодуються з метою приховування інформації. Вони змінюються таким чином, що особа, яка не має спеціального «ключа», побачить лише набір цифр або просто пошкоджений файл.

Для шифрування програм існує низка програм, що мають інтуїтивний інтерфейс і дають можливість сформувати надійний шифр для будь-якого документу. Фахівці **Центру національного спротиву** радять використовувати програми, наведені нижче, оскільки вони забезпечують автоматичне шифрування інформації, яка зберігається на ваших пристроях:

VeraCrypt — програмне забезпечення для шифрування як файлів, так і дисків. Зручна програма з можливістю обирати алгоритм шифрування обраного елементу.

PGP Desktop — програма, яка вміє шифрувати файли й каталоги, захищати поштові повідомлення, локальну мережу та створювати зариштовані образи дисків.

Folder Lock — програма має можливості приховувати папки та шифрувати файли на переносних носіях, зберігати паролі та інформацію в захищеному сховищі. Повністю стирає документи й вільне місце на дисках.

Dekart Private Disk — програма для створення виключно образів дисків, що можна налаштовувати з автозапуском програм при монтуванні.

Поряд з цими програмами значну популярність серед користувачів мають і такі:

PicaSafe — це віртуальний сейф, який надає можливість безпечного збереження та перегляду фотографій. Програма призначена для робочого столу Windows і вимагає активації, після якої користувач зможе використовувати зазначені функції в повному обсязі абсолютно безкоштовно.

AxCrypt — це утиліта з відкритим вихідним кодом, призначена для захисту користувацьких даних методом шифрування. Програма поширюється на безкоштовній основі з дещо обмеженим функціоналом. Ця утиліта об'єднує кодувальник і менеджер зашифрованих файлів. Робота першого ґрунтується на використанні криптографічного алгоритму AES-128 (AES-256 доступний у версії Premium). Усе, що потрібно користувачеві для захисту власних документів, це увійти до облікового запису AxCrypt і вказати бажаний пароль.

TrueCrypt — безкоштовна програма для шифрування даних «на льоту». Одна з основних особливостей програми TrueCrypt — відсутність у заголовку створеного «диска» специфічної сигнатури, характерної для інших подібних програм, що робить неможливим ідентифікувати його, оскільки жодна з частин віртуального диска не відрізняється від випадкових даних.

Отже, збереження та передавання інформації в мережі Інтернет з використанням хмарних технологій стає все більш важливою складовою сучасного цифрового світу. Хмарні технології дозволяють користувачам зберігати, обробляти та передавати дані через Інтернет, забезпечуючи зручний доступ до них з будь-якого пристрою та місця. Проте, цей підхід також має свої особливості та виклики, що важливо враховувати.

Однією з головних переваг хмарних технологій є можливість зберігання даних на віддалених серверах. Це дозволяє користувачам уникнути проблем з обмеженою пам'яттю на пристроях та забезпечити резервне копіювання інформації. Крім того, хмарні рішення забезпечують високу доступність та швидкий доступ до даних, що дозволяє працювати з ними ефективно навіть з великих відстаней.

Однак зберігання даних у хмарі також вносить ризики з точки зору безпеки та конфіденційності. Хоча провайдери хмарних послуг зазвичай використовують різноманітні заходи захисту, такі як шифрування та аутентифікація, вони все ще можуть стикатися з інцидентами безпеки, такими як витік інформації або несанкціонований доступ. Тому користувачам важливо обирати надійних провайдерів хмарних послуг та дотримуватися найвищих стандартів безпеки, зберігаючи та передаючи конфіденційну інформацію.

Ще одним важливим аспектом є проблеми з приватністю. Зберігання даних у хмарі може вимагати передачі особистої інформації третім сторонам, що може породжувати питання щодо контролю над власною інформацією. Тому важливо обирати провайдерів, які гарантують конфіденційність даних та дотримання вимог законодавства з приватності.

Відтак, користувачам важливо бути свідомими цих аспектів та вживати відповідних заходів безпеки й конфіденційності, використовуючи хмарні послуги.

ЗАВДАННЯ

Завдання 1. Пройдіть тест «Цифрова безпека журналістів». Для цього перейдіть за покликанням: https://imi.org.ua/advices/test-tsyfrova-bezpeka-zhurnalistiv-i38677

Завдання 2. Проаналізуйте власний досвід роботи з інформацією (як ви зберігаєте та передаєте інформацію). З'ясуйте, які небезпеки трапляються та як ви на них реагуєте. Опираючись на наведений вище матеріал, розробіть стратегії для кращого захисту важливої для вас інформації (може включати, але не обмежуватися встановленням паролів, використанням VPN, використанням програм для шифрування інформації і под.). Проведіть тестування запропонованих стратегій збереження та передавання інформації. Результати дослідження подайте у формі презентації.

ДЖЕРЕЛА ДЛЯ ПОГЛИБЛЕНОГО ВИВЧЕННЯ ТЕМИ

1. *Безпечна хмара. Правила зберігання інформації для медійників*. Інститут масової інформації. Інститут Масової Інформації. URL: https://imi.org.ua/advices/bezpechna-hmara-pravyla-zberigannya-informatsiyi-dlya-medijnykiv-i39936
2. *Дім як цифрова фортеця: що варто знати журналістам про цифрову безпеку в дистанційній роботі*. Інститут Масової Інформації. URL: https://imi.org.ua/advices/dim-yak-tsyfrova-fortetsya-shho-varto-znaty-zhurnalistam-pro-tsyfrovu-bezpeku-v-dystantsijnij-roboti-i33010
3. *Кіберняні. Цифрова безпека для початківців: як попередити кібератаку та захищати дані в інтернеті.* Дія. Освіта. URL: https://osvita.diia.gov.ua/courses/cybernanny
4. Снопченко Д. *Як правильно зберігати інформацію, щоб уникнути втрати даних.* Посібник з інформаційної безпеки. URL: https://yug.com.ua/uk/blog-ua/posibnik-z-informatsijnoji-bezpeki/jak-pravilno-zberigati-informatsiju-schob-uniknuti-vtrati-danih.html
5. *Топ7 хмарних сховищ.* Gigacloud. URL: https://gigacloud.ua/blog/navchannja/top-7-hmarnih-shovisch
6. *Шифрування даних*. Центр національного спротиву. URL: https://sprotyv.mod.gov.ua/shyfruvannya-danyh/
7. *Що таке віртуальний маршрутизатор і навіщо він потрібен.* Gigacloud. URL: https://gigacloud.ua/blog/navchannja/scho-take-virtualnij-marshrutizator-i-navischo-vin-potriben
8. *Що таке приватна хмара та в чому її відмінність відпублічної?* Gigacloud. URL: https://gigacloud.ua/blog/navchannja/scho-take-privatna-hmara-ta-v-chomu-ii-vidminnist-vid-publichnoi
9. *7 трендів хмарних технологій у 2024 році.* Gigacloud. URL: https://gigacloud.ua/blog/navchannja/7-trendiv-hmarnih-tehnologij-u-2024-roci

Модуль 6

ШТУЧНИЙ ІНТЕЛЕКТ І ОСОБЛИВОСТІ РОБОТИ З СЕРВІСАМИ, СТВОРЕНИМИ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

У цьому модулі ми поговоримо про те, що таке штучний інтелект, як працюють сервіси, розроблені на основі ШІ, про їхні переваги та недоліки, а також про те, чому ChatGPT — це гарний помічник, але не замінник живого творчого мислення.

Штучний інтелект сьогодні перестав бути витвором уяви письменників, які працюють у жанрі наукової фантастики, а поступово втілюється в життя через різноманітні застосунки й програми, що імітують поведінку людини в процесі вирішення різноманітних завдань. Що ж таке штучний інтелект (ШІ) і як він працює?

Історична довідка

Спроби створити штучний інтелект були ще у 50-х роках XX століття. Одним з перших, хто спробував працювати в цьому напрямку, і, власне, вважається сьогодні батьком штучного інтелекту, був Джон Маккарті із Массачусетського технологічного інституту (за свою роботу (винайшов мову LISP) у 1971 році він був удостоєний Премії Тьюрінга). Першою програмою, яка зробила прорив у розробці ШІ, була програма «Logic Therorist», створена Джоном Маккарті, Марвіном Мінскі та ще групою вчених MIT. Ця програма могла доводити математичні теореми.

Джон Маккарті

Штучний інтелект — це штучна симуляція людського мислення. Найпопулярнішими мовами програмування, з якими працюють розробники штучного інтелекту, є Python, R, Java, C++, Scala, Julia, Rust, Lisp, Prolog. Про що це нам говорить? Як тим, хто може користуватися лише готовим продуктом, не бажаючи розуміти весь процес створення цього продукту, це говорить виключно про те, що розробка ШІ — це комплексне вирішення цілого спектру завдань. Відтак, ШІ складається з двох основних блоків (підмножин) — машинного (Machine Learning — ML) і глибинного (Deep Learning — DL) навчання, — та залученням нейронних мереж (мереж, що імітують нейрони або клітини людського мозку).

На сьогодні ШІ виконує досить широкий спектр функцій, що постійно розширюється. До прикладу, ШІ розпізнає зображення та розуміє мову, робить прогнози, розпізнає небезпечні ситуації і шахрайські дії, допомагає діагностувати хвороби та розробляти нові лікарські засоби, прогнозувати рух транспорту й уникати аварій, керувати транспортними засобами, автоматизувати процеси в бізнесі й оптимізувати роботу підприємств.

ШІ активно використовується в таких галузях: медицина, фінанси, транспорт, виробництво, бізнес, освіта, інтернет-сервіси й розробка окремих програмних продуктів.

Нині практично кожна компанія, яка позиціонує себе на ринку IT-послуг, намагається залишатися в тренді й пропонує власний застосунок чи програму (залежно від цільової аудиторії), що працює на основі ШІ. Серед тих, які сьогодні можуть застосовуватися журналістами й освітянами, можна сформувати такі функціональні групи:

- робота з текстом (генерування, опрацювання, формування короткого змісту, створення кількох варіантів текстів на одну й ту ж тему для різних платформ і аудиторій і под.);
- робота з фото та ілюстраціями (генерування фотографій, картинок на основі запиту й ключових слів, створення логотипів і под.);
- робота з відео (генерування відео, коригування відео, створення відео для різних платформ, створення навчального відео і под.);
- робота з форматами документів (до прикладу, робота з форматом PDF чи PPT і под.);
- планування часу й завдань;
- нотатники для зустрічей і інтерв'ю і под.

Здебільшого, демоверсії усіх цих програм є безкоштовними, але якщо є необхідність в ширшому функціоналі, доведеться користатися одним з безлічі запропонованих тарифних планів: від покупки одного готового продукту (наприклад, згенерованого логотипу) аж до річної підписки чи покупки ліцензії (останнє, здебільшого стосується користувачів, які займаються розробкою IT-продуктів).

Таблиця 6.1. Робота з текстом (програми й застосунки на основі ШІ)

jenni	**Jenny AI** (https://jenni.ai/) — застосунок, який допомагає працювати з текстами. Особливо ефективний, коли йдеться про аналітичні чи освітні матеріали. Jenny AI має можливість автоматично доповнити текст, перевірити його на плагіат, перефразувати окремі конструкції на більш влучні чи більш відповідні. Наразі цей застосунок підтримує англійську, французьку, німецьку, японську, китайську та інші мови.	
	ChatGPT (https://chat.openai.com/) — один з найбільш поширених застосунків, який дає можливість генерувати тексти відповідно до створених запитів, добирає заголовки, формує тексти для різних платформ і в різних стилях. Цей застосунок добре працює з текстами на тих мовах, що в основі мають латинку й зберігають чіткий порядок слів у реченні. З флективними мовами (як, до прикладу, українська, польська і под.) потрібно додатково перевіряти текст, оскільки трапляються смислові помилки, що виникають при неправильному використанні закінчень і структуруванні речень. Але цей недолік поступово усувається.	
WS	**Writesonic** (https://writesonic.com/) — це цікавий інструмент для копірайтерів. За допомогою цього застосунку можна створити маркетинговий контент для будь-якого бізнесу: від рекламних оголошень аж до описів продуктів для різних платформ. Специфіка роботи сервісу полягає в тому, що користувач задає ключові слова, робить запит на різновид матеріалу. Після того ШІ генерує спершу кілька структур текстів, серед яких потрібно обрати найбільш доцільну. Після виконання цієї опції іде генерація самого тексту.	
	Copysmith (https://copysmith.ai/) — це застосунок, який можна використовувати не лише для генерування текстів (описів товарів, послуг або ж навіть публікацій для блогів), але й для запуску й відстеження рекламних кампаній, а також для SEO-текстів з метою збільшення органічного трафіку.	

DeepL	**DeepL** (https://www.deepl.com/translator) — це застосунок, який позиціонують як один з найточніших перекладачів текстів. У його арсеналі є і українська мова. Фахівці стверджують, що за якістю перекладу він значно випереджає Google Translate і Microsoft, які нині користуються значною популярністю серед широкої аудиторії.	

Інші сервіси для генерації текстів: Hypotenuse, Rytr, Peppertype, HyperWrite, Wordtune, Copy.ai, Jasper, ClosersCopy, AI-Writer, Rytr, ContentBot.ai, Bertha.ai, INK, Headlime.

Таблиця 6.2. Робота з фотографіями, ілюстраціями й відео

	Deep Dream Generator (https://deepdreamgenerator.com/) — це один з найбільш відомих сервісів для генерації зображень на основі ШІ. Здебільшого його використовують для генерування зображень для сайтів та ілюстрацій для текстових матеріалів. Генерувати зображення можна кількома способами: завантажити картинку, на основі якої буде створено нове оригінальне зображення, або ж дати словесний опис бажаної ілюстрації. Окрім того, цей сервіс також дає можливість генерувати короткі (від 1 до 10 секунд) відео.	
Loopsie	**Loopsie** — це застосунок, розроблений для перетворення вже існуючих фото на оригінальні ілюстрації в різноманітних стилях. До прикладу, дуже добре працює в стилі аніме. Можна завантажити власне фото, і за кілька хвилин сервіс його опрацює та перетворить на ілюстрацію в заданому стилі. Застосунок однаково добре використовується і для Android, і для MacOS.	
	Gencraft AI Image and Video Generator (https://gencraft.com/) — застосунок на основі ШІ, який дає можливість генерувати фото й короткі відео як за попередньо завантаженими картинками чи фото, так і на основі опису й ключових слів.	

Інші сервіси для генерування зображень: DALL-E 2, GLIDE, Latent Diffusion, Dezgo, Image Creator by Microsoft Designer, ImageFX by Google, Dream Studio by Stability AI, Dream by WOMBO, Craiyon, Midjourney, Generative AI by Getting Images.

Таблиця 6.3. Генерація ідей і контенту

	SAGA (https://saga.so/ai) — застосунок, розроблений на основі штучного інтелекту, за допомогою якого можна згенерувати ідеї, до прикладу, для проведення бренсторму, підготувати e-mail, перекласти текст різними мовами (важливо, що в цьому застосунку підтримується українська мова), перевірити текст на помилки. Перевагою цього застосунку є наявність вбудованого пошуковика, що дає можливість вводити запити на пошук (до прикладу, знайти ТОП найкрасивіших місць в Україні) і отримувати відповідь у вигляді добірки матеріалів, з якими можна далі працювати.	

Таблиця 6.4. Планування часу й зустрічей

	Motion (https://www.usemotion.com/) — це застосунок, що дозволяє ефективно планувати день користувача. ШІ визначає пріоритетність ваших завдань, перепланує будь-яку незавершену роботу, розставляє пріоритети, перепланує та об'єднує зустріч, а також формує маршрути користувача, щоб мінімізувати збої в графіку роботи.	

taskade	**Taskade** (https://www.taskade.com/) — застосунок, який дає можливість планувати не лише завдання користувача та їхню пріоритетність, але й пропонує різні режими перегляду цих завдань (календарі, діаграми, дошки, динамічні списки справ, блок-схеми і под.). Чатбот, який створений на основі ШІ, сканує документи, оптимізує завдання, а також надає поради користувачам щодо оптимального розподілу часу на робочий день.	

Інші сервіси для планування і оптимізації праці користувача: TimeHero, MayDay, Clockwise, Smarty, ClickUp, Clara, Infinity, Reclaim AI, Trevor AI та ін.

Таблиця 6.5. Застосунки й програми для генерування голосу

LOVO	Lovo.ai (https://lovo.ai/?lmref=aQMezw) — це застосунок, призначений для синтезування голосу шляхом перетворення завантаженого тексту на звук. Застосунок здатен генерувати голоси максимально наближені до голосів людей (мінімізується роботизація тексту). На сьогодні застосунок надає доступ до 500+ голосів з емоціями (відтворюється трохи більше двох десятків емоцій) на 150 мовах світу. Окрім того, цей застосунок надає можливість редагування відео з одночасним синтезуванням чи редагуванням синтезованого голосу за кадром.	
MURF.AI	Murf.ai (https://murf.ai/) — цей застосунок дає можливість генерувати голос з тексту (закадровий голос, голос диктора і под.). В арсеналі застосунку є 110 голосів і 15 мов (станом на 2024 рік). Стилі мовлення можуть бути експресивними, емоційними. Є можливість налаштування тону голосу.	
SYNTHESYS	**Synthesys** (https://synthesys.io/) — це застосунок, який має здатність перетворювати текст на голос, а також текст на відео. Має бібліотеку професійних голосів (жіночих і чоловічих), дає можливість створювати та продавати власні голоси, додавати й коригувати паузи, розставляти акценти. Також має режим попереднього перегляду, що цінно, оскільки завжди хочеться побачити готовий продукт ще на етапі редагування, а не після його завантаження та перегляду/прослуховування.	
Speechify	**Speechify** (https://studio.speechify.com/) — застосунок, який дає можливість перетворювати текст з різних форматів (PDF, e-mail, документів та под.) на живе мовлення. Надає до використання більше 200 голосів на більше, ніж 20 мовах з використанням різних емоцій, тонів, акцентів і под. Можна керувати тоном, швидкістю, висотою. Надає права на комерційне використання.	

Інші сервіси для генерування (синтезування) голосу: Лабораторії WellSaid, ElevenLab, Fliki, Altered Studio, Play.ht, Resemble.io.

Отже, голосові генератори штучного інтелекту надають реалістичні голосові виходи, роблять контент більш доступним та охоплюють глобальну аудиторію. Вони є передовою аудіотехнологією, яка поєднує простоту використання з результатами професійного рівня, підходячи як для окремих творчих особистостей, так і для великих підприємств.

Таблиця 6.6. Робота з презентаціями

	**Gamma AI (**https://gamma.app/?lng=en**) —** застосунок, який дає можливість генерувати презентації, окремі документи чи одразу вебсторінки, що значно полегшує роботу та дає можливість створення багатогранної і живої презентації, яку можна одразу вбудувати у власний сайт. Застосунок містить готові шаблони презентацій, документів, вебсторінок за тематичними блоками, які дають можливість одразу зорієнтуватися в кінцевому результаті роботи застосунку.	

Звісно, це далеко не повний перелік застосунків, які працюють на основі штучного інтелекту, оскільки цей перелік постійно розширюється та доповнюється.

Нижче в таблиці 6.7 подано підбірку програм на основі штучного інтелекту, що можуть значно спростити роботу журналістів і викладачів журналістики.

Таблиця 6.7. Підбірка програм на основі штучного інтелекту

ЗАВДАННЯ	ПРОГРАМИ / ЗАСТОСУНКИ		
Написати текст	CHATGPT	BARD	COPILOT
Намалювати зображення	MIDJOURNEY	STABLE DIFFUSION	ADOBE FIRELY
Створити відео	RUNWAY	PIKA	GOOGLE VIDEOPOET
Створити озвучування	SPEECHIFY	LANDR	DESPRIT
Створити аватар	HEYGEN	SYNTHESIA	D-ID
Зробити субтитри	CAPTIONS	VEED.IO	VIDYO.AI
Знайти в інтернеті	PERPLEXITY	POE	KOMO
Допомогти в роботі (спланувати день / завдання на день)	NOTION	JASPER	ZAPIER
Допомогти в навчанні	GRAMMARLY	SOCRATIC	CONSENSUS

Але чи можна вважати ці застосунки абсолютно безпечними? Мабуть, ні. Зважаючи на певну вразливість Інтернет-мереж і систем персонального захисту робочих машин, з якими працюють користувачі, навіть застосунки, що працюють на основі штучного інтелекту, мають певні ризики. Якщо технічні ризики більше стосуються розробників програм і застосунків, оскільки вони не є повністю дослідженими (фахівці, до прикладу, вказують на такі: «отруєння ШІ» через використання помилкових чи маніпулятивних даних; використання вірусів для атак на програми, побудовані на основі штучного інтелекту; використання шкідливих команд і запитів; сповільнення роботи чи пошкодження системи роботи ШІ через використання великої кількості суперечливих даних і запитів; викрадення персональних даних і под.). Детальніше про це можна почитати, до прикладу, у публікаціях Давида Розенталя (David Rosenthal)[1].

А от щодо інших загроз, якими не варто легковажити і які треба обов'язково враховувати, формуючи систему комунікації, слід пам'ятати про те, що, **по-перше**, нейромережа, яка постійно навчається (у тому числі й на тій інформації, яку отримує від користувача), здатна чітко формувати профіль користувача й видавати його на запити від інших користувачів. Профіль цей формується відповідно до системи запитів і команд, які користувач відправляє в аналітичний простір програми, розробленої на основі ШІ.

По-друге, даючи вказівку ШІ прибрати, до прикладу, з тексту чутливі дані, тим самим ми даємо ШІ інформацію про те, що ці дані є чутливими. Вони, звісно, будуть прибрані з конкретного тексту, але залишаться в пам'яті ШІ, що абсолютно не гарантує безпеки цих чутливих даних.

1 Rosenthal, David. Part 6: The flip side of the coin: Where we need to protect AI from attackers. URL: Part 6: The flip side of the coin: Where we need to protect AI from attackers — 20 February 2024 — VISCHER

По-третє, нейромережа, на основі аналізу соціальних мереж, здатна створювати контент, який може формувати порядок денний, а, отже, і систему переконань у таргетованих груп користувачів (algorithmic bias) і тим самим впливати, до прикладу, на результати виборів і под.

По-четверте, і ця небезпека є вже відомою, і з нею користувачі (особливо, українські користувачі в умовах російсько-української війни) зустрічаються майже регулярно, — **глибинні фейки (Deep Fakes).**

Глибинні фейкти (Deep Fakes) — це методика синтезу зображення людини, яка базується на штучному інтелекті. Використовують для поєднання та накладання одних зображень і відео на інші зображення й відео. Основна мета — ввести в оману користувачів, знищити (зіпсувати) репутацію якоїсь конкретної особи, сформувати думку щодо конкретного явища, посіяти паніку і под.

Окрім того, є можливість виникнення систем з штучним інтелектом, які діють неочікувано чи неправильно. Навіть найбільш ретельно розроблені програми можуть виявити недоліки або вразливості, які можуть призвести до непередбачуваних наслідків. Наприклад, автономні автомобілі, оснащені ШІ, можуть призвести до аварій через неправильне розпізнавання об'єктів на дорозі або через збої в програмному забезпеченні.

Ще однією серйозною небезпекою є можливість використання штучного інтелекту для зловживання або злочинних дій. Це може включати в себе створення шкідливих програм, що атакують системи, або навіть розробку систем масового шпигунства, які порушують приватність людей.

Також важливо враховувати можливість соціальних та етичних проблем, пов'язаних із застосуванням ШІ. Наприклад, може виникнути проблема безробіття через автоматизацію багатьох видів робіт, або можуть виникнути проблеми з приватністю через великий обсяг персональних даних, що збираються і аналізуються програмами на основі штучного інтелекту.

Отже, хоча штучний інтелект відкриває безліч можливостей для технологічного прогресу, важливо ретельно вивчити його небезпеки та вживати заходів для запобігання можливим негативним наслідкам. Це вимагає не лише технічної експертизи, але й врахування соціальних, етичних і правових аспектів використання ШІ.

Безпечне користування програмами, розробленими на основі штучного інтелекту (ШІ), важливе для збереження приватності користувачів. ШІ стає все більш поширеним у різних галузях життя: від особистих асистентів до систем автоматизації великих підприємств. Правильне їхнє використання може допомогти уникнути потенційних ризиків.

Перш за все, важливо звернути увагу на джерело програм, з якими користувач планує працювати. Варто використовувати лише програми, розроблені відомими й надійними компаніями або розробниками, які дотримуються стандартів безпеки та конфіденційності. Важливо перевірити рейтинг програми, читати відгуки користувачів і звертатися до офіційних джерел (сайтів компаній-розробників) завантаження програм.

Другим важливим аспектом є оновлення програмного забезпечення. Багато вразливостей і помилок у програмах на основі ШІ виправляються через випуск патчів і оновлень. Тому важливо регулярно перевіряти наявність оновлень для програм і вчасно їх встановлювати.

Третім кроком є уважне вивчення умов використання та політики конфіденційності кожної програми. Важливо зрозуміти, які дані збираються програмою, як вони використовуються та чи має користувач можливість контролювати цей процес. Необхідно з обережністю використовувати програми, які збирають більше даних, ніж необхідно для їхньої нормальної роботи, а також з програмами, які передають ці дані третім сторонам без згоди користувача.

Крім того, важливо ретельно перевіряти дозволи, які користувач надає програмі. Варто надавати лише необхідні дозволи, що дозволять програмі виконувати свої основні функції.

Загалом, безпечне користування програмами на основі ШІ вимагає обережності, усвідомленості й виваженості. Слід дотримуватися вищезазначених кроків і завжди залишатися свідомими щодо потенційних ризиків та заходів безпеки, використовуючи ці програми.

ЗАВДАННЯ

Завдання 1. Відштовхуючись від ваших зацікавлень чи ваших робочих завдань, створіть для себе підбірку застосунків чи програм, розроблених на основі штучного інтелекту (ШІ). Обґрунтуйте, чим саме й чому вони можуть бути корисними. Зверніть увагу на недоліки цих застосунків.

Завдання 2. Ознайомтеся з матеріалом Зої Захарової «Алгоритми YouTube забанили канал про шахи через расизм» (https://news.online.ua/algoritmi-youtube-zabanili-kanal-pro-shahi-cherez-rasizm-830279/). З'ясуйте, чому така ситуація мала місце. Спробуйте віднайти інформацію, чи траплялися подібні ситуації в соціальних мережах. Знайдіть закономірності в роботі алгоритмів.

Завдання 3. Оберіть одну з програм (бажано ту, досвід використання якої у вас є), розроблену на основі штучного інтелекту, яка працює з текстами. Визначте можливі загрози і ризики, пов'язані з її використанням. Розробіть інструкцію з безпеки для потенційних користувачів цієї програми. Підготуйте буклет-інструкцію з власними рекомендаціями, використовуючи одну з програм, розроблену на основі штучного інтелекту.

ДЖЕРЕЛА ДЛЯ ПОГЛИБЛЕНОГО ВИВЧЕННЯ ТЕМИ

1. Вишня, Георгій. *Штучний інтелект і людина: загрози і можливості*. Радіо Свобода. Суспільство. URL: https://www.radiosvoboda.org/a/shtuchnyi-intelekt-zagrozy-i-mozhlyvisti/31145992.html
2. Смінк, Вероніка. *Три стадії штучного інтелекту: чи може він знищити людство?* BBC News Україна. URL: https://www.bbc.com/ukrainian/features-65728291
3. *Що таке штучний інтелект: історія, види та складові*. Gigacloud. URL: https://gigacloud.ua/blog/navchannja/scho-take-shtuchnij-intelekt-istorija-vidi-ta-skladovi
4. *11 програм штучного інтелекту для написання текстів*. URL: https://ailaboratory.wixsite.com/shi-ua/post/11-prohram-shtuchnoho-intelektu-dlia-napysannia-tekstiv
5. *12 найкращих програм для щоденного планування зі штучним інтелектом*. URL: http://surl.li/qwoql
6. Rosenthal, David. *Part 6: The flip side of the coin: Where we need to protect AI from attackers*. URL: Part 6: The flip side of the coin: Where we need to protect AI from attackers — 20 February 2024 — VISCHER
7. *The Best AI Image Generators to try Right Now*. URL: https://www.zdnet.com/article/best-ai-image-generator/

ГЛОСАРІЙ

Адміністратор — основний обліковий запис з максимальним доступом до платформ.

Активна сесія — проміжок часу, коли користувач взаємодіяв з додатком.

Антивірус — спеціальна програма для пошуку та ідентифікації шкідливого й небажаного програмного забезпечення.

Атака повним перебором — злам пароля шляхом перебору всіх можливих комбінацій.

Аудит цифрової безпеки — оцінювання захищеності організації від визначених цифрових ризиків. Аудит проводять фахівці з цифрової безпеки поза межами організації.

Безпековий інцидент — ситуація, за якої сталося щось негативне з цифровим активом.

Витоки даних — неправомірний доступ до інформації. Витік може бути через фізичні недосконалості або через вразливості програмного забезпечення.

Вразливість — стан, при якому загроза може реалізуватися.

Двофакторна автентифікація — додатковий спосіб підтвердження особи при авторизації на сайті. Для соцмереж частіше за все це код із додатку, код із смс, push-сповіщення або використання спеціального токену. Для месенджерів — пін-код, або пароль.

Дісінг (англ. **Dissing**) — передача або публікація компрометуючої інформації про жертву онлайн.

Домен (домене ім'я) — це ім'я, пов'язане із фізичною IP-адресою в інтернеті; унікальне ім'я, яке з'являється після знака @ в адресах електронної пошти та після www у вебадресах.

Ексфільтрація даних — це несанкціоноване передавання даних за межі організації вручну або за допомогою зловмисного програмного забезпечення.

Загроза — це будь-що, що може призвести до небажаних наслідків (втрати інформації, недоступності ресурсу, витоку даних).

Зменшення, **уникнення, передача, прийняття ризиків** — дії, які можна прийняти, щоб керувати ймовірністю настання небажаних ситуацій.

Контроль активних сесій — список девайсів, з яких виконано вхід в обліковий запис.

Легальне програмне забезпечення — програмне забезпечення, яке завантажене з офіційних джерел розповсюдження. Необов'язково є платним, але обов'язково не є піратським.

Модератор — це користувач інформаційних ресурсів (форумів, чатів і т.п.), який має особливі права, порівняно з іншими користувачами.

Оцінка ризиків — інструмент для визначення та аналізу власних цифрових активів; аналіз, чи є в активів загрози та наскільки можливим є те, що вони реалізуються.

Парольна фраза — пароль, який складається з речення або комбінації слів. Частіше за все ускладнюється додатково цифрами та спецсимволами. Допомагає створити довгий складний пароль, який легко ввести та просто запам'ятати, ніж звичайний набір символів.

Парольний менеджер — сервіс або програмне забезпечення, яке допомагає зберігати, генерувати та вводити паролі з зашифрованої бази даних. Доступ до нього отримується через майстер-пароль. Допомагає зберігати велику кількість паролів в одному місці без потреби їх запам'ятовувати.

Переадресація пошти — налаштування, через яке ваші листи відправляються на іншу поштову скриньку.

Плагін — додаток, що підключається до основної програми, призначений для розширення або використання її можливостей.

Політика цифрової безпеки — це документ з описом технологій та посадових обов'язків і практик, які організація використовує, щоб зменшити цифрові ризики.

Програми з відкритим кодом — програми, початковий код яких знаходиться у вільному доступі. Залежно від типу ліцензії код таких програм можна вільно переглядати, змінювати, використовувати для нових програм.

Резервні коди — список одноразових кодів, які необхідно зберегти за межами пристроїв на випадок їх втрати.

Резервне копіювання — процес створення копії даних з пристрою на іншому носії або у хмарному сховищі.

Рекламні трекери — це спеціальні інструменти, які збирають та ідентифікують інформацію про користувачів для аналітики та персоналізованої реклами.

Ризик — це ймовірність реалізації загрози з огляду на існуючі вразливості.

Сервер — комп'ютер у локальній чи глобальній мережі, який надає користувачам свої обчислювальні і дискові ресурси, а також доступ до встановлених сервісів.

Соціальна інженерія — 1) наука, що вивчає поведінку людей та фактори, що на неї впливають; 2) це спосіб атаки, який використовує не технічні вразливості системи, а особливості людської психіки; одним з найпопулярніших методів небезпечної соціальної інженерії є фішинг.

Спам — це небажані повідомлення, що надсилаються у великій кількості користувачам, які не давали на це своєї згоди.

Способи відновлення акаунту — варіанти, за допомогою яких ви можете відновити доступ до акаунта.

Тролінг — це вид взаємодії в онлайн-дискусіях, скерований на провокування читачів на емоційну відповідь, образи, тривалі емоційні дискусії, нагнітання конфліктів для досягнення мети інтернет-троля.

Фізичний ключ безпеки — це апаратний ключ, який можна налаштувати як другий фактор для входу.

Фішинг — вид соціальної інженерії, направлений на отримання від користувача важливої інформації. Зазвичай йдеться про дані для входу в облікові записи (Credentials).

Флеймінг (суперечки) (від англ. flaming — пекучий, гарячий, полум'яний) — обмін короткими гнівними й запальними репліками між двома чи більше учасниками, використовуючи комунікаційні технології.

Хепіслепінг (англ. Happy slappying) — зйомка роликів, у яких агресори б'ють жертву або знущаються над нею, щоб розмістити відео в Інтернеті.

Хмарні сервіси — сервіси, пов'язані з наданням користувачам постійного доступу до віддалених інтернет-ресурсів (серверів, додатків, сховищ тощо).

Хостинг — це послуга надання дискового простору для розміщення сайтів та баз даних, які перебувають онлайн.

Цифрова безпека — стан захищеності систем обробки та зберігання даних, коли забезпечені конфіденційність, доступність та захищеність інформації. Це також комплекс заходів, спрямованих на захист від несанкціонованого доступу, використання, оприлюднення, руйнування, редагування, ознайомлення, запису чи знищення інформації особи, суспільства та держави.

Цифрові активи організації — будь-які електронні ресурси, що мають цінність для організації.

Шифрування — це процес, у результаті якого дані кодуються з метою приховування інформації. Вони змінюються таким чином, що особа, яка не має спеціального «ключа», побачить лише набір цифр або просто пошкоджений файл.

Шифрування пристроїв — технічний процес, за допомогою якого дані на пристрої перетворюються в певний секретний код, що маскує оригінальну інформацію.

Шкідливе програмне забезпечення (віруси) — програми, які за умови запуску на пристрої, можуть завдати шкоди системі, інформації або «залізу». Існують різні типи ШПЗ, у кожного з них — свої завдання та алгоритми роботи.

Штучний інтелект (ШІ) — це галузь інформатики, яка займається розробкою інтелектуальних машин, здатних виконувати завдання, що зазвичай потребують людського інтелекту. Це метод, особливістю якого є змусити комп'ютер чи програмне забезпечення «мислити» як людський мозок.

Credentials — дані, необхідні для входу в акаунт (логін і пароль).

DDoS-атака (розподілена атака на відмову в обслуговуванні) — напад на вебресурс з метою зробити його недоступним користувачам, яким він був призначений.

TechSoup — неприбуткова міжнародна мережа неурядових організацій, яка надає технічну підтримку та технологічні інструменти для інших неприбуткових організацій.

VPN (virtual private network) — узагальнена назва технологій, які допомагають зашифрувати та захистити трафік, що генерується користувачем в інтернеті.

ПІСЛЯМОВА

Цифрова безпека — це не лише набір технічних заходів, але й важлива складова сучасного життя, яка вимагає уваги та обережності від кожного з нас. Посібник, який ви мали можливість вивчити, має на меті познайомити вас з основними аспектами безпеки в цифровому середовищі та надати необхідні інструменти та знання для захисту ваших даних та конфіденційності в Інтернеті.

Пам'ятайте, що цифрова безпека — це постійний процес, який вимагає уважності, самодисципліни та постійного оновлення знань. Не соромтеся вдосконалювати свої навички й ділитися знаннями з тими, хто вас оточує. Лише спільними зусиллями ми можемо зробити цифровий світ безпечнішим для всіх.

Зверніть увагу на важливість захисту своїх даних та збереження конфіденційності в Інтернеті, дотримуючись передових стандартів безпеки та використовуючи навички, які ви отримали в цьому посібнику. Нехай ваша подорож в цифровому світі буде захищеною та безпечною!

Бажаємо вам успіху та безпеки в усіх ваших онлайн-пригодах!

Навчально-методичний посібник

(НЕ)БЕЗПЕКА В ЦИФРОВОМУ СВІТІ

Навчальний посібник з цифрової грамотності та безпеки

Відповідальність за підбір ілюстративного матеріалу несуть автори.

Редактор: Наталія Пономаренко

Макетування: Андрій Чернявський

Академія української преси тел. 067–372–27–33,
e-mail: info@aup.com.ua
Сайт: http://aup.com.ua/
Портал «Медіаосвіта та медіаграмотність»: http://www.medialiteracy.org.ua/
Сторінка на Facebook: https://www.facebook.com/aupfoundation
Telegram-канал: https://t.me/aup_info