МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації

На рецензію	До захисту
Завідувач кафедри УІКБ	Завідувач кафедри УІКБ
доктор економічних наук, доцент	доктор економічних наук, доцент
_____ С.В. Легомінова	_____ С.В. Легомінова
«___»_____20__ р.	«___»_____20__ р.

ДИПЛОМНА РОБОТА

на тему:

АНАЛІЗ ВИМОГ І МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СОЦІАЛЬНИХ МЕРЕЖАХ

СТУДЕНТ: Подорожний Данило Денисович _____
(підпис)

КЕРІВНИК: к.держ.упр. Мужанова Тетяна Михайлівна _____
(підпис)

НОРМОКОНТРОЛЕР: к.в.н., доц. Якименко Юрій Михайлович _____
(підпис)

Київ – 2021

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В. Легомінова
«_____»_____ 2021 р.

ЗАВДАННЯ

на дипломну роботу

студенту Подорожному Данилу Денисовичу

Тема роботи: «АНАЛІЗ ВИМОГ І МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СОЦІАЛЬНИХ МЕРЕЖАХ», затверджена наказом по університету № 230 від «13» жовтня 2020 р.

1. **Термін здачі** студентом оформленої роботи «___» _____ 20___ р.
2. **Об'єкт дослідження:** забезпечення захисту персональних даних.
3. **Предмет дослідження:** вимоги і методи забезпечення захисту персональних даних у соціальних мережах.
4. **Мета дослідження** полягає в аналізі вимог і методів забезпечення захисту персональних даних у соціальних мережах.
5. **Перелік питань, які мають бути розроблені:**

5.1 Вивчити основні положення нормативно-правової бази з питань безпеки персональних даних.

5.2 Встановити види загроз і методи атак на персональні дані користувачів соціальних мереж.

5.3 Проаналізувати методи забезпечення безпеки персональних даних в соціальних мережах.

6. **Дата видачі завдання «**16» вересня 2020 р.

Науковий керівник _____ Т.М. Мужанова
підпис

Завдання прийнято до виконання _____ Д.Д. Подорожний
підпис

Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою

КАЛЕНДАРНИЙ ПЛАН
виконання дипломної роботи
студентом ПОДОРОЖНИМ Данилом Денисовичем

Дата видачі завдання: «16» вересня 2020 р.

№ з/п	Етапи дипломної роботи	Термін виконання етапів	Примітка
	Визначення об'єкта, предмета, мети та завдань дослідження.	16.09.2020	
	Збір та аналіз літератури.	28.09.2020	
	Вивчення основних положень нормативно-правової бази з питань безпеки персональних даних.	12.10.2020	
	Встановлення видів загроз і методів атак на персональні дані користувачів соціальних мереж.	26.10.2020	
	Аналіз методів забезпечення безпеки персональних даних в соціальних мережах.	09.11.2020	
	Формулювання висновків за результатами проведеного дослідження.	23.11.2020	
	Оформлення роботи.	07.12.2020	
	Оформлення презентації.	14.12.2020	
	Отримання рецензії на роботу.	25.12.2020	
	Захист у ДЕК.	__.01.2021	

Студент Д.Д. Подорожний
(підпис)

Науковий керівник Т.М. Мужанова
(підпис)

РЕФЕРАТ

Дипломна робота присвячена дослідженню вимог і методів забезпечення захисту персональних даних у соціальних мережах. Робота складається зі вступу, трьох розділів, що містять 9 рисунків, висновків та списку використаних джерел з 42 найменувань. Загальний обсяг роботи становить 89 аркушів, з яких 4 аркуші займає список використаних джерел.

Об'єктом дослідження є забезпечення захисту персональних даних.

Предмет дослідження - вимоги і методи забезпечення захисту персональних даних у соціальних мережах.

Метою роботи є аналіз вимог і методів забезпечення захисту персональних даних у соціальних мережах.

Для цього у роботі використані методи аналізу, порівняння та систематизації, насамперед нормативно-правових документів, класифікації загроз інформаційній безпеці та соціальної інженерії.

Як результат у роботі вивчено основні положення нормативно-правової бази з питань безпеки персональних даних; встановлено види загроз і методи атак на персональні дані користувачів соціальних мереж; проаналізовано методи забезпечення безпеки персональних даних в соціальних мережах.

Галузь застосування. Розроблені підходи можуть бути використані для навчання та підвищення обізнаності користувачів мережі Інтернет та соціальних мереж щодо вимог і методів забезпечення захисту персональних даних та іншої конфіденційної інформації у процесі користування сервісами онлайн-комунікації, що в подальшому сприятиме зростанню культури інформаційної безпеки суспільства.

Ключові слова: ПЕРСОНАЛЬНІ ДАНІ, ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ, СОЦІАЛЬНІ МЕРЕЖІ, ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У СОЦМЕРЕЖАХ.

ЗМІСТ

ВСТУП

Актуальність теми. В умовах швидкого розвитку Інтернет-технологій відносини між людьми все більше переходять на віртуальний рівень: популярним середовищем комунікації стали соціальні мережі. Про це свідчать дані звіту Digital 2020 від We Are Social і Hootsuite, відповідно до якого у липні 2020 року світова аудиторія соціальних мереж досягла 3,96 млрд осіб, тобто понад 50% всього населення планети.

Водночас, у зв'язку з тим, що процес розвитку соціальних відносин у новому глобальному інформаційному середовищі не достатньо законодавчо регламентований, слабо контролюється онлайн-платформами, які надають комунікаційні сервіси, а також не внормований на культурному й поведінковому рівнях, зростає кількість випадків незаконного отримання й використання інформації, зокрема й конфіденційних даних особи. 64% користувачів всесвітньої мережі усвідолюють наявність таких проблем і виражають стурбованість щодо використання їхньої особистої інформації.

Для подолання проблеми зловживання конфіденційною інформацією необхідним є об'єднання зусиль усіх зацікавлених сторін: міжнародних організацій, урядів держав, компаній-надавачів онлайн-сервісів та користувачів. Тому аналіз вимог і методів забезпечення захисту персональних даних у соціальних мережах як важливої проблеми забезпечення інформаційної безпеки є актуальним науковим завданням.

Мета і завдання дослідження. **Мета роботи** полягає в аналізі вимог і методів забезпечення захисту персональних даних у соціальних мережах.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Вивчити основні положення нормативно-правової бази з питань безпеки персональних даних.

2. Встановити види загроз і методи атак на персональні дані користувачів соціальних мереж.

3. Проаналізувати методи забезпечення безпеки персональних даних в соціальних мережах.

Об’єкт дослідження - забезпечення захисту персональних даних.

Предмет дослідження - вимоги і методи забезпечення захисту персональних даних у соціальних мережах.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу, порівняння та систематизації, насамперед нормативно-правових документів, класифікації загроз інформаційній безпеці та соціальної інженерії.

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані для навчання та підвищення обізнаності користувачів мережі Інтернет та соціальних мереж щодо вимог і методів забезпечення захисту персональних даних та іншої конфіденційної інформації у процесі користування сервісами онлайн-комунікації, що в подальшому сприятиме зростанню культури інформаційної безпеки суспільства.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу здійснити обґрунтований вибір методів і засобів забезпечення безпеки персональних даних та іншої конфіденційної інформації при користуванні соціальними мережами та іншими Інтернет-сервісами.

РОЗДІЛ 1.
НОРМАТИВНО-ПРАВОВА БАЗА З ПИТАНЬ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ

Право на захист персональних даних та конфіденційність є старим основоположним правом людини, яке отримало нову та особливу актуальність з поширенням і розвитком інформаційних технологій.

Суть проблеми полягає в тому, що при використанні Інтернету або мобільних телефонів значні обсяги персональних даних часто обробляються і передаються без чіткої згоди чи навіть інформування про їх обробку.

Багато різної особистої інформації: від дати народження, місця роботи до планів на вихідні та відпустку, щодня розміщується в соціальних мережах. Люди діляться з Інтернетом відомостями про майже всі аспекти свого життя. Однак, немає впевненості в тому, що персональні дані в мережі Інтернет належним чином захищені.

Поки немає механізмів вирішення проблем захисту персональних даних глобального охоплення, їх намагаються вирішити на рівні національних законодавств. На рівні Європейського Союзу питання захисту персональних даних регламентуються у Загальному регламенті захисту персональних даних (GDPR – General Data Protection Regulation).

1.1. Положення Загального регламенту захисту даних (GDPR)

Загальний регламент захисту персональних даних - постанова Європейського Союзу, за допомогою якого Європейський парламент, Рада ЄС та Європейська Комісія підсилюють і уніфікують захист персональних даних всіх осіб в Європейському Союзі (ЄС). Постанову, також направлено на експорт даних з ЄС. GDPR спрямований перш за все на те, щоб дати громадянам контроль над власними персональними даними, і на спрощення нормативної бази для

міжнародних економічних відносин шляхом уніфікації регулювання в рамках ЄС [1].

Ключові принципи GDPR:

Законність, справедливість і прозорість - повинні бути легальні підстави в рамках GDPR для збору і використання даних, не дорущення порушення будь-яких законів, відкритість, чесність від початку і до кінця при використанні персональних даних;

Обмеження за метою - обробка повинна зводитися до того, що було заявлено суб'єкту даних. Всі конкретні завдання повинні бути закріплені в політиці конфіденційності і чітко дотримуватися;

Мінімізація даних - використання мінімально необхідного об’єму даних для досягнення поставлених цілей;

Точність - персональні дані повинні бути точні і не повинні вводити в оману; помилкові дані підлягають корегуванню;

Обмеження збереження даних - не зберігати дані довше, ніж потрібно, періодично проводити аудит даних та видаляти невикористані;

Цілісність та конфіденційність/безпека – зберігати дані в безпечному місці та приділяти достатню увагу збереженню даних;

Підзвітність – відповідальність за обробку персональних даних і виконання всіх інших принципів GDPR, включаючи записи про конфіденційність, захист, використання, перевірку даних; призначення посадової особи по захисту даних (англ. DPO, data protection officer).

Об’єкти захисту персональних даних відповідно до GDPR

Положення GDPR застосовуються до даних, які збираються, обробляються і / або зберігаються в Європі незалежно від того, де зібрані дані. Якщо, наприклад, у фізичної особи є Інтернет-магазин в Україні з інформаційної розсилкою і хоча б один потенційний клієнт з Європейського Союзу підписався на неї, тоді на такий Інтернет-магазин поширюються правила GDPR.

Важливою умовою GDPR є те, що з моменту вступу в силу даного Закону заборонена передача даних за межі Європейського Союзу в будь-яку країну, яку

ЄС не вважає такою, що відповідає вимогам законодавства про захист персональних даних. Якщо дані передаються особисто за межі ЄС для обробки або зберігання, то необхідно отримати явну згоду на це від користувача, якому належать дані.

Варто звернути увагу на те, що багаторівневий характер юрисдикцій всесвітньої мережі Інтернет і такі технології, як CDN, призведуть до того, що в певний момент, дані, які збираються і зберігаються особою, будуть передаватися за межі Європейського Союзу і схвалених країн. Тому незалежно від того, які інші дозволи запитуються у своїх користувачів, бажано завжди отримувати дозвіл на зберігання даних за межами ЄС і дані повинні бути захищені.

Визначення персональних даних відповідно до GDPR є достатньо широким і передбачає що персональні дані – це не лише інформація, яка прямо ідентифікує особу, а таакож інформація, яка в сукупності з іншими даними може бути використана для ідентифікації особи. Так, відповідно до офіційного визначення Європейської комісії, персональні дані - це будь-яка інформація щодо фізичної особи, незалежно від того, чи вона стосується його/її особистого, професійного чи суспільного життя. Це може бути що завгодно, зокрема: ім’я, домашня адреса, світлина, адреса електронної пошти, банківські реквізити, повідомлення на сайтах соціальних мереж, медична інформація або IP-адреса комп’ютера [2].

GDPR розрізняє два основних типи даних, які повинні бути захищені: особисті і делікатні.

Особисті дані - це будь-які дані, що ідентифікують людину. Ім'я, адреса електронної пошти, місце розташування, біометричні дані, логін (інші онлайн-ідентифікатори) - все це особисті дані.

Делікатні дані - це те, що, на думку ЄС, більш особисте, ніж ім'я. Етнічне походження, релігійні переконання, сексуальні вподобання, політичні погляди, кримінальна історія - все це можна віднести до делікатних даних. Нові правила покликані приділяти більше уваги захисту делікатних даних.

Також GDPR встановлюють вимоги до даних, які можуть збиратися з різних джерел. Найкраща поведінка, в такому випадку, полягає в тому, щоб ніколи не

запитувати більше даних, ніж необхідно - чим менше даних зберігається, тим менше ризику їх втратити.

Права користувачів згідно з правилами GDPR

GDPR визначають наступні офіційні права, якими володіють власники даних: право доступу, право на об'єкт, право бути поінформованими, право на виправлення, право на перенесення даних, право на видалення даних, право не піддаватися автоматичному прийняттю рішень, право обмеження обробки даних.

Однак особи, що зберігають дані, також мають права. Наприклад, якщо користувач підписався на розсилку, а згодом, він вирішує, що більше не хоче отримувати розсилку і відписується. У такому випадку, джерело розсилки зобов'язане назавжди стерти адресу електронної пошти даного користувача. У той же час, коли користувач підписується на розсилку, відправник повинен знати призначену для користувача IP-адресу, щоб забезпечити отримання розсилки (відповідно до взятих зобов'язань), адже відправник має право зберегти ці дані, щоб підтвердити виконання своїм сайтом правил GDPR.

Вплив GDRP на український інформаційний та законодавчий простір

Проблеми регулювання процесу збору персональних даних, забезпення інформаційної безпеки та інші супутні питання, пов'язані з роботою з персональними даними в Україні, зараз є відносно вирішеною.

Очевидно, що законодавство не зовсім досконале і потребує поліпшення, проте основні положення регулюються Законом України «Про захист персональних даних» від 1 червня 2010 № 2297-VI. Так, відповідно до ст. 12 зазначеного Закону збір персональних даних є складовою процесу їх обробки, який передбачає дії з підбору чи впорядкування відомостей про фізичну особу [3].

Суб'єкту персональних даних повідомляється про власника персональних даних, склад та зміст зібраних персональних даних, його права, визначені Законом, мету збору персональних даних та осіб, яким передаються його персональні дані: в момент збору персональних даних, якщо вони збираються в суб'єкта персональних даних, і в інших випадках - протягом тридцяти робочих днів з дня збору персональних даних.

Окрім вищенаведеного Закону, юридичні та фізичні особи мають можливість вирішувати питання, пов'язані з власною інформаційною безпекою, використовуючи положення Цивільного кодексу України, Закону України «Про інформацію» та інші акти законодавства України.

Менш дослідженим і цікавішим питанням з точки зору кроків в майбутнє і євроінтеграційних амбіцій України є ознайомлення, вивчення і аналіз засад регулювання захисту персональних даних, зокрема їх збору в країнах Європейського Союзу. Найбільш актуальною зараз і такою, що активно розвивається, є проблематика захисту персональних даних та інформаційної безпеки в Інтернеті.

Так, 25 травня 2018 року вступили в силу правила нового Регламенту про захист персональних даних GDPR (The General Data Protection Regulation), який також регулює питання захисту персональних даних в Інтернеті для користувачів, що знаходяться на території Європейської економічної зони (ЄЕЗ). Тут необхідно розуміти, що ЄЕЗ охоплюються не тільки країни власне Європейського Союзу, а й країни Європейської асоціації вільної торгівлі (ЄАВТ), крім Швейцарії.

Загальний регламент поширюється на всіх учасників всесвітньої мережі Інтернет, які беруть участь в зборі, зберіганні або обробці персональних даних. Хоча зазначений нормативний акт прийнятий для захисту європейських даних, глобальний характер Інтернету означає, що GDPR встановлює стандарт конфіденційності даних у всьому світі. Практично всі найбільші Інтернет-компанії, включаючи Facebook, Twitter і Google, підпадають під регулювання вимог GDPR.

Важливо вказати, що GDPR - це давно назрілий набір сучасних методів забезпечення та дотримання конфіденційності в бізнесі і особливо в Інтернеті, який є надважливим в нових умовах розвитку глобальної економіки. Він покликаний навчити людей ставитися до даних користувачів з такою ж ретельністю і повагою, з якою всі відносяться до власних даних.

Штрафи за недотримання правил істотні: до 20 млн євро або 4% від загального обороту за порушення. Крім того, GDPR забезпечує користувачам

можливість компенсації будь-якого матеріального і / або нематеріального порушення GDPR.

Перспективи адаптації нормативних умов GDRP в Україні

У сучасному цифровому світі, особливо з розвитком Big Data, інформація стає одним із головних ресурсів, а її обсяги, що зберігаються компаніями - просто колосальні. Так, практично кожен користується послугами доставки їжі, таксі, авіаперевезеннями або будь-якими іншими сервісами, де, для зручності онлайн оплати, повністю вказується інформація банківської картки, особисті дані, номер та інше.

Саме тому, і з огляду на гучні скандали з витоками даних (наприклад Uber, Cambridge Analytica і Facebook) захист інформації і його контроль з боку держави стрімко рухається до пріоритетних завдань. І Україна не є винятком: з одного боку, це необхідно для стабільного розвитку країни, з іншого - ЄС є головним партнером України не тільки в експорті / імпорті, але і в стратегічних цілях, і впровадження норм GDPR значно спростить процеси, пов'язані з даними (зберігання, обмін, обробку і т.д.) і послабить існуючі бар'єри.

Так, український бізнес буде повністю відповідати вимогам безпеки даних ЄС, тобто не потрібно буде додатково підтверджувати, що рівень захисту даних в компанії знаходиться на належному рівні при співробітництві. Це, наприклад, спростить роботу з європейськими банками - значно зменшить обсяг документів і підтверджень, які вимагаються зараз.

У той же час, імплементація GDPR і отримання статусу країни, що надає належний рівень захисту персональних даних, істотно полегшить і залучення інвестицій і ведення бізнесу з країнами ЄС.

Етапи досягнення відповідності вітчизняного законодавства про персональні дані та їх захист нормам GDPR включають: регулювання відносин з контрагентами та користувачами, досягнення внутрішньої відповідності, ініціювання відповідності, аудит відповідно до GDPR [4] (Рис.1.1.).

Рис. 1.1. Етапи досягнення відповідності GDPR.

Так, згідно зі статтею 45 Регламенту, особисті дані можна передати в країни з адекватним рівнем захисту персональної інформації без додаткових дозволів і погоджень з контролюючими органами. У той же час, стаття 13 GDPR вимагає повідомляти своїх клієнтів про передачу даних поза ЄС. При цьому, зараз можна отримати не дуже привабливе повідомлення: «дані будуть передані на обробку в Україну - країну, яка не має належного рівня захисту персональних даних». А якщо до цього всього додати передбачені Регламентом штрафи в розмірі десятків мільйонів євро, то шансів на співпрацю залишається досить мало.

Наразі, якщо компанія працює з даними громадян ЄС, вона автоматично підпадає під дію Регламенту і змушена трансформувати свої процеси, щоб відповідати європейським вимогам.

1.2. Огляд законодавства України у сфері безпеки персональних даних

У червні 2010 року в Україні був прийнятий Закон України № 2297-VI «Про захист персональних даних». Через місяць, в липні 2010 року, Україна ратифікувала Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних шляхом прийняття Закону України № 2438-VI «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних [5] та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних».

Обидва закони вступили в силу з 01 січня 2011 року.

Прийняття Закону України «Про захист персональних даних» та ратифікація Конвенції наблизили українське суспільство до європейських стандартів захисту інформації, а саме, персональних даних, гармонізувавши українське законодавство і привівши його у відповідність з такими нормативно-правовими актами, як:

Конвенція про захист осіб в зв’язку с автоматизованою обробкою даних особистого характеру, підписана 28 січня 1981 року в м. Страсбурзі,

Директива 95/46/ЕС Європарламенту та Ради ЄС від 24 жовтня 1995 року про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних [6],

Закон України «Про захист персональних даних», який регулює правові відносини, пов'язані із захистом і обробкою персональних даних і спрямований на захист основних прав людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних.

Відповідно до Закону України:

- персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

- база персональних даних - іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних;

- володілець персональних даних - фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом;

- обробка персональних даних - будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем.

Даний Закон розповсюджується на:

- діяльність по обробці персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів;

- обробку персональних даних, що містяться в картотеці або підлягають внесенню до картотеки, із застосуванням неавтоматизованих засобів.

Згода на обробку персональних даних може надаватися як в письмовому, так і в електронному вигляді.

При складанні згоди, суб'єкт персональних даних надає про себе наступну інформацію: ПІБ, рік народження, серію і номер паспорта, дані про орган, яким виданий паспорт, а також адресу реєстрації.

Відповідно до Закону про захист персональних даних суб'єктами відносин, пов'язаних із персональними даними, є:

- суб’єкт персональних даних;
- володілець персональних даних;
- розпорядник персональних даних;
- третя особа;
- Уповноважений Верховної Ради України з прав людини.

Володільцями чи розпорядниками персональних даних можуть бути підприємства, установи і організації усіх форм власності, органи державної влади

або органи місцевого самоврядування, фізичні особи - підприємці, які обробляють персональні дані відповідно до закону.

Безпосередньо, об'єктами захисту є персональні дані.

Персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою. Не є конфіденційною інформацією про персональні дані, що стосуються особи, якаа займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень.

Загальні вимоги до обробки персональних даних

Обробка персональних даних здійснюється відкрито і прозоро із застосуванням засобів та у спосіб, що відповідає визначеним цілям такої обробки.

У разі зміни визначеної мети обробки персональних даних на нову мету, що несумісна з попередньою, для подальшої обробки даних володілець персональних даних повинен отримати згоду суб’єкта персональних даних на обробку даних відповідно до зміненої мети:

1) персональні дані повинні бути точними, достовірними і оновлюватися в міру необхідності, визначеної метою їх обробки;

2) склад і зміст персональних даних мають бути відповідними, адекватними і не зневажливими щодо певної мети їх обробки;

3) первинними джерелами відомостей про фізичну особу є: видані на її ім'я документи; підписані нею документи; відомості, які особа надає про себе;

4) обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних або у випадках, передбачених законами України, у порядку, встановленому законодавством;

5) не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини;

6) якщо обробка персональних даних необхідна для захисту життєво важливих інтересів суб'єкта персональних даних, обробляти персональні дані без його згоди можна до часу, коли отримання згоди стане можливим;

7) персональні дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це необхідно для законних цілей, в яких вони збиралися або в подальшому оброблялися. Подальша обробка персональних даних в історичних, статистичних чи наукових цілях може здійснюватися за умови забезпечення їх належного захисту;

8) типовий порядок обробки персональних даних затверджується Уповноваженим Верховної Ради України з прав людини.

Права суб'єкта персональних даних

Особисті немайнові права на персональні дані, які має кожна фізична особа, є невід'ємними і непорушними.

Відповідно до Закону України «Про захист персональних даних» суб'єкт персональних даних наділений такими правами:

- знати про джерела збору, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;

- отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані; та на доступ до своїх персональних даних;

- отримувати не пізніше, ніж за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, що обробляються його персональні дані, а також отримувати зміст таких персональних даних;

- пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних;

- пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем і розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;

- на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи; звертатися зі скаргами на обробку своїх персональних даних до Уповноваженого або до суду;

- застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;

- вносити застереження про обмеження права на обробку своїх персональних даних при наданні згоди;

- відкликати згоду на обробку персональних даних;

- знати механізм автоматичної обробки персональних даних; на захист від автоматизованого рішення, яке має для нього правові наслідки [7].

1.3. Регулювання питань безпеки персональних даних в угодах про користування послугами соціальних мереж Facebook і Twitter

Умови використовування, вимоги надання послуг (англ. Terms of service/use) - це правила, з якими потрібно погодитись перед використанням будь-якої послуги, частіше всього в Інтернеті. Також умови використання містять відмову від відповідальності.

Як правило, вимоги використання є на сайтах компаній, які надають програмне забезпечення або Інтернет-сервіси. Наприклад, до таких сервісів можна віднести веб-браузери, сервіси електронної комерції, пошукові системи, соціальні мережі й додатки. Головне визначення умов використання - юридичне.

Умови використання мають юридичну силу і можуть бути змінені. Компанії можуть посилатися на умови використання для відмови від надання послуг. Клієнти можуть подати позов, якщо вони постраждали від порушення умов використання. При цьому під час злиття компаній і під час інших юридичних угод існує ризик неправильного зберігання даних користувачів [8].

В умовах використання можуть міститися такі розділи:

- визначення ключових слів і фраз;
- права та обов’язки користувача;
- правильне та неправильне використання сервісу;
- відповідальність за дії, вчинені користувачем;
- політика конфіденційності та обробки персональних даних;
- платні послуги (членство чи підписка);
- правила відмови від підписки та видалення акаунту;
- врегулювання конфліктів у судовому порядку;
- відмова від відповідальності або її обмеження;
- можливість зміни умов використання (способи повідомлення користувачів про зміни).

Важливо також відзначити, що практично всі соціальні мережі не несуть відповідальність за дані користувачів і в своїх публічних юридичних документах стверджують, що розміщені дані є публічними і доступні будь-яким користувачам Інтернету.

На Рисунку 1.2. червоним відзначені заборонені способи використання даних з соціальних мереж і відкритих Інтернет-ресурсів, а зеленим – дозволені [9].

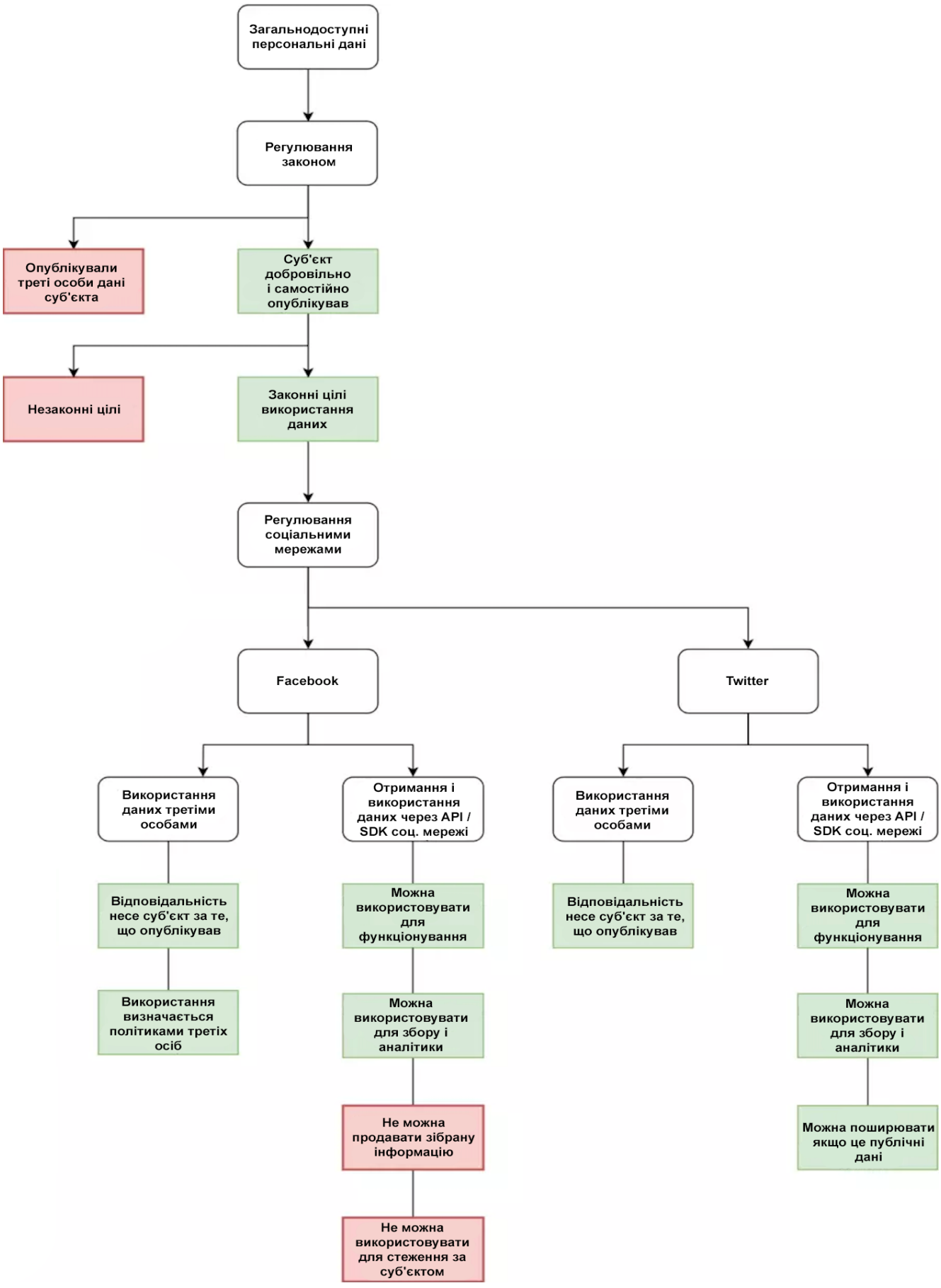

Рис. 1.2. Дозволені й заборонені дії щодо персональних даних у соцмережах.

Аналіз документів і угод соціальної мережі Facebook

Важливо відзначити, що розгляд угод буде стосуватися не тільки соціальної мережі Facebook, але і всіх продуктів, які належать Facebook Inc. і Facebook Ireland Limited (Facebook, Instagram, Messenger). Правовий статус визначається наступними документами і додатками, які також є публічними офертами:

- Політика використання даних;
- Угода користувача;
- Положення довідкового центру;
- Політика платформи Facebook.

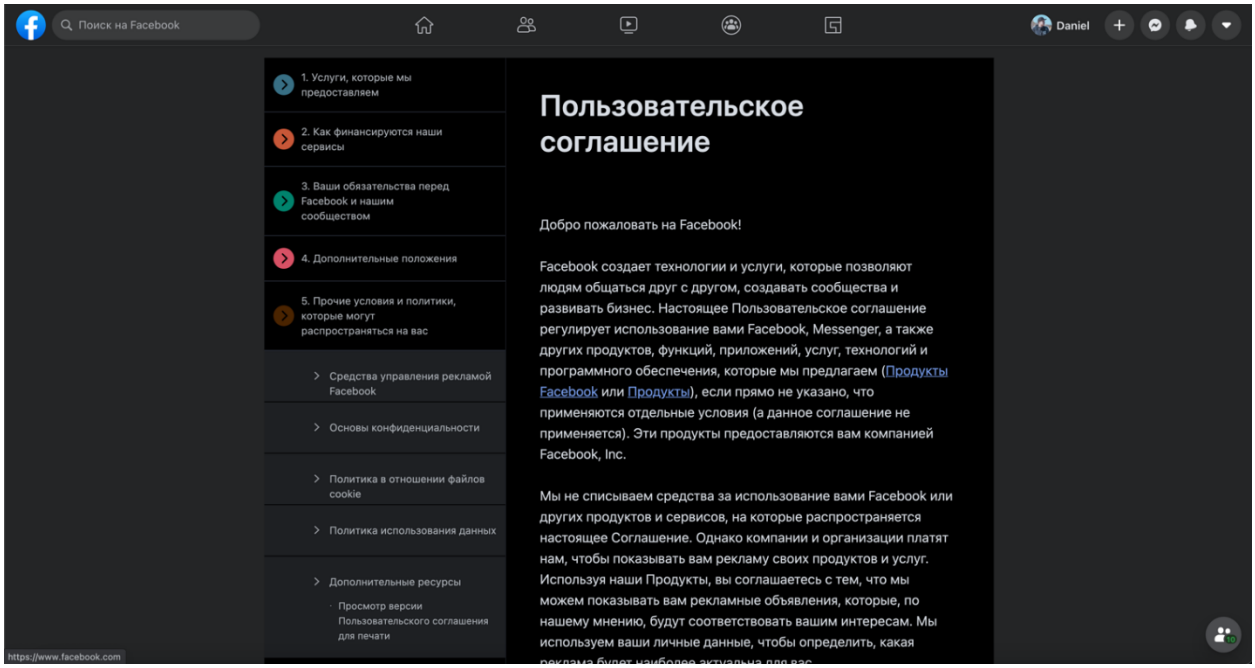

Рис. 1.3. Головна сторінка користувацької угоди Facebook

У Політиці використання даних відразу визначено, що Facebook обробляє контент, повідомлення та іншу інформацію, які користувачі надають при використанні продуктів мережі, в тому числі при реєстрації акаунта, створенні контенту або розповсюдженні інформації, відправленні повідомлень або взаємодії з іншими людьми. Це може бути інформація з наданого користувачами контенту або про нього (така як метадані), наприклад, місце, де було зроблено фото або дата створення файлу. Крім того, Facebook може збирати дані про те, що бачать користувачі, за допомогою наданих компанією функцій, таких як камера, наприклад, щоб пропонувати маски і фільтри або поради по використанню

форматів камери. Системи соціальної мережі автоматично обробляють контент і повідомлення, що надаються користувачами, для аналізу їх контексту і змісту. Можна схематично зобразити рух даних від користувача так:

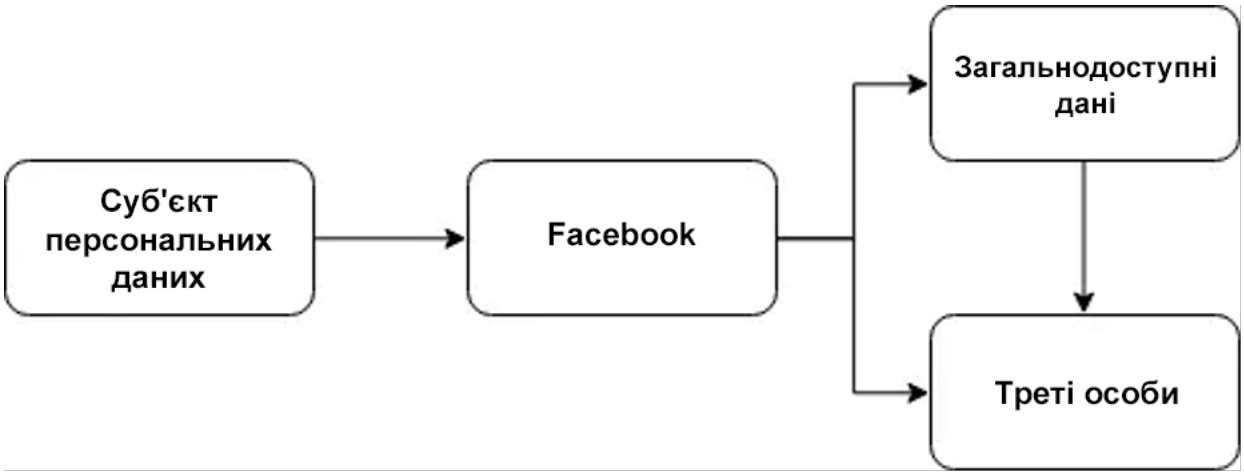

Рис. 1.4. Схема руху даних від користувача

Facebook у своїх публічних документах досить однозначно визначає, що відноситься до загальнодоступних даних в Політиці використання даних.

Загальнодоступну інформацію видно кожному користувачеві в Продуктах Facebook і поза ними - в тому числі при відсутності акаунту. Це ім'я користувача Instagram; будь-яка інформація, якою користувач ділиться з усіма людьми; інформація в загальнодоступному профілі на Facebook; і контент, яким користувач ділиться на сторінці Facebook, в загальнодоступному акаунті Instagram або на будь-якій інший загальнодоступній платформі, такій як Facebook Marketplace.

Усі користувачі Facebook і Instagram, включаючи сам Facebook можуть надавати доступ або відправляти загальнодоступну інформацію будь-яким особам в Продуктах Facebook і поза ними, в тому числі в Продуктах інших компаній Facebook, в результатах пошуку або за допомогою інструментів і API. Можливі також перегляд, репост, скачування загальнодоступної інформації та доступ до неї через сторонні сервіси, такі як пошукові системи, API і звичайні ЗМІ, наприклад, ТВ, а також виконання цих дій додатками, сайтами та іншими сервісами, інтегрованими з Продуктами компанії [10].

Положення довідкового центру додатково конкретизують і розкривають, що є загальнодоступною інформації:

- Інформація, що публікується користувачами завжди доступна для всіх. Частина інформації, яку користувач повідомляє Facebook, коли заповнює профіль, є загальнодоступною, наприклад віковий діапазон, мова і країна. Facebook також використовує частину призначеного для користувача профілю, так званий публічний профіль, щоб користувачеві було простіше зв'язатися зі своїми друзями і родичами. Публічний профіль включає ім'я особи, стать, ім'я користувача і його ідентифікатор (номер акаунту), фото профілю, фото обкладинки і спільноти. Ця інформація також є загальнодоступною.

- Інформація, яка доступна для всіх. Якщо розміщується загальнодоступна публікація (наприклад, вибирається «Доступно всім» в інструменті вибору аудиторій), така інформація вважається загальнодоступною. Якщо користувач ділиться чимось і не бачить поруч інструменту вибору аудиторії або інші налаштування конфіденційності, ця інформація також є загальнодоступною.

- Матеріали, якими діляться інші люди. Інші люди можуть зробити загальнодоступною навіть ту призначену для користувача інформацію, якою інший користувач з ним поділився, не роблячи її доступною для всіх. Крім того, коли коментуються загальнодоступні публікації інших людей, кожен коментар також буде доступний всім.

- Публікації на Сторінках Facebook або в публічних групах. Сторінки Facebook і публічні групи - це загальнодоступні місця. Будь-яка людина, яка може переглядати сторінку або групу, може побачити особисту публікацію або коментар. Загалом, коли користувач розміщує публікацію або коментар на сторінці, в суспільній групі або стрічці новин, а також в інших місцях на Facebook і поза ним, може з'явитися новина про це.

До загальнодоступних даних Facebook юридично додає також всі дії користувача в соціальній мережі (такі як лайки, репости та ін.), а також в Політиці використання даних попереджає, що до загальнодоступних даних про користувачів також відносяться:

- будь-які дії користувача у Facebook з іншими користувачами і контентом (наприклад, коментування) - це можуть бачити всі, навіть ті, хто не є обраною аудиторією;

- фактом цієї дії можуть поділитися інші користувачі;

- при листуванні через особисті повідомлення інший користувач може зробити скріншот або репост повідомлення, що стане загальнодоступною інформацією;

- користувача можуть відзначити в контенті, на світлинах - тоді дані про користувача теж стають загальнодоступними.

При створенні IT-продуктів з використанням API / SDK Facebook, розробники повинні дотримуватися вимог, що встановляються в Політиці платформи Facebook, де визначено, що не можна робити з отриманими даними, яким умовам повинні відповідати положення і дії розробників. Наприклад:

- дані користувачів, отримані від Facebook, не повинні передаватися компаніям, які торгують інформацією, або продаватися, навіть якщо користувач не попереджає про це в своїй політиці конфіденційності;

- розробник повинен опублікувати і дотримуватися своєї політики;

- розробник повинен отримати згоду людей, перш ніж використовувати їх дані в будь-якій рекламі;

- розробнику заборонено продавати і передавати за ліцензією, або купувати дані, отримані від Facebook;

- заборонено використовувати дані, отримані від Facebook, для прийняття рішень про відповідність будь-яким вимогам, в тому числі для схвалення або відхилення заявки або визначення процентної ставки за кредитом.

У свою чергу, для користувачів положення Політики використання даних визначають наступне:

- Коли користувач вирішить використати сторонні додатки, сайти або інші сервіси, які використовують продукти Facebook або інтегровані в них, вони можуть отримувати інформацію про те, що публікує користувач або чим він (вона) ділиться.

- Крім того, коли користувач завантажує або використовує такі сторонні сервіси, вони можуть здійснювати доступ до загальнодоступного профілю на Facebook і будь-якої інформації, якою користувач ділиться з ними.

- Інформація, яку збирають такі сторонні сервіси, регулюється їхніми власними умовами і політиками.

Facebook також дозволяє використовувати загальнодоступні дані для аналітики: системи автоматично обробляють контент і повідомлення, що надаються користувачем і іншими людьми, для аналізу їх контексту і змісту в цілях, описаних у Політиці використання даних.

І в цій же Політиці використання даних визначено, хто може отримувати доступ до аналітичних звітів і збирати дані користувачів:

- Дослідники і вчені.

Для чого: інформація і контент партнерам з досліджень і вченим для проведення досліджень, які сприяють розвитку науки та інновацій, корисні для спільної діяльності або місії, а також відкриття нових розробок в області загального соціального забезпечення, технічного прогресу, громадських інтересів, охорони здоров'я та благополуччя.

- Партнери, що використовують сервіси аналітики.

Для чого: узагальнена статистика, яка допомагає людям і компаніям аналізувати взаємодію людей з контентом в продуктах Facebook і поза ними. Наприклад, інформація про кількість людей або акаунтів, які переглянули, прокоментували їх публікації або відреагували на них, а також узагальнена демографічна та інша інформація, яка допомагає їм аналізувати взаємодії з їх сторінкою або акаунтом.

- Інші особи.

Для чого: в цілях досліджень і інновацій для суспільного блага використовується наявна інформація (в тому числі отримана від партнерів з досліджень) для проведення і підтримки досліджень та інновацій на теми загального соціального забезпечення, технічного прогресу, громадських інтересів,

охорони здоров'я і благополуччя. Наприклад, аналітика інформації про шляхи міграції під час криз з метою надання гуманітарної допомоги.

Позиція Facebook щодо даних користувачів більш гнучка, ніж у інших соціальних мереж, але загальний тренд про те, які дані соціальна мережа надає третім особам за додатковою угодою - аналогічний. При цьому, Facebook більш однозначно і чітко закріплює правове становище користувача, його даних, а також визначає які дані про користувачів, підстави і методи збирання даних.

Аналіз документів та угод соціальної мережі Twitter

У не менш популярній соціальній мережі Twitter також розроблено велику кількість нормативних документів, що регламентують правовий статус користувача та інформації і прописують всі питання досить детально, серед них:

- Правовий статус публікування і використання загальнодоступних даних користувачів визначається наступними документами:
- Політика конфіденційності Twitter;
- Про конфіденційну інформацію в Twitter;
- Умови надання сервісів;
- API-інтерфейси Twitter;
- Угода з розробниками (Developer agreement);
- Політика конфіденційності для розробників (Developer policy);
- Умови для розробників: Детальніше про обмеження використання API Twitter (Developer terms: More about restricted uses of the Twitter APIs).

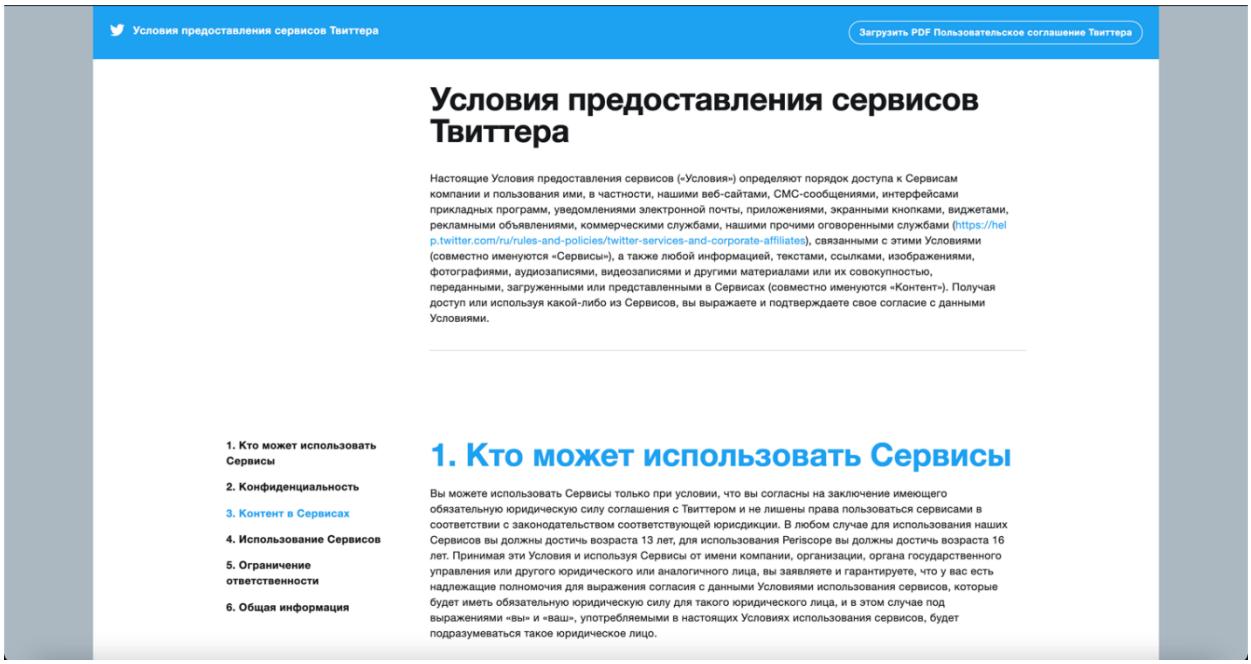

Рис. 1.5. Головна сторінка вимог надання сервісів Twitter

Політика конфіденційності Twitter в першу чергу декларує, що соціальна мережа є загальнодоступною, а твіти відразу доступні для перегляду та пошуку у всьому світі [11].

У цьому вся основна суть політики Twitter у відношенні до даних користувачів контенту, який вони створюють - максимальна публічність та прозорість процесів. Ця позиція Twitter закріплена в пункті 1.2. Політики конфіденційності й визначає, що в відкритому доступі знаходиться вся інформація:

- часовий пояс і мова спілкування, час створення облікового запису, твіти та певна інформація про них (дата, час, додаток і версії Twitter, за допомогою якої ретвітнули твіт);
- місцезнаходження в твітах та в обліковому записі в Twitter (якщо користувач це опублікував і надав доступ);
- створені списки, людей, на яких підписаний користувач, і які підписані на користувача;
- твіти, які відзначили як такі, що сподобалися, або ретвітнули;
- трансляції в Periscope, які створені, на які клікнув користувач або з якими пов’язаний тим чи іншим чином в Periscope або Twitter;

- залишені користувачами серця (Hearts), коментарі, кількість отриманих сердець, облікові записи;

- ті трансляції, які користувач дивився у прямому ефірі або в режимі відтворення;

- будь-які матеріали, коментарі або інший контент, який користувач публікує в ефірі іншого облікового запису;

- інформація про користувача, що розміщена іншими особами, використовуючи сервіси Twitter, також може буде загальнодоступною.

Окрім представлення публічної інформації безпосередньо на Twitter, більшість користувачів також використовує такі технології, як інтерфейси API та впроваджує їх для того, щоб зробити цю інформацію доступною для веб-сайтів, додатків та іншої мети їх використовування, наприклад, відображення твітів на новинному веб-сайті або аналіз інформації, що розміщується людьми в Twitter.

Зазвичай користувачі надають цей контент в обмеженій кількості безкоштовно і стягують плату за ліцензування для великомасштабного доступу. Є також стандарті умови, які визначають порядок використання цих даних, а також програма нормативно-правової відповідності для забезпечення виконання цих умов. Але ці особи і компанії не пов’язані з Twitter, а їх пропозиції можуть не відображати оновлення, які користувачі роблять в Twitter.

Таким чином, усі дії користувача в соціальній мережі Twitter є публічними, окрім особистих повідомлень, які Twitter, на відміну від Facebook, не аналізує.

Twitter передає зміст особистих повідомлень особам, яким користувачі їх відправили. Також компанія не використовує зміст призначених для користувача особистих повідомлень для підбору реклами. При взаємодії з публічним контентом Twitter в особистому повідомленні, наприклад, при відмітці твіта як «такого, що сподобався», переданого в особистому повідомленні, ця дія буде доступна загальнодоступній публіці.

У частині правових документів, що стосуються конфіденційної інформації в Twitter, зазначено пряму заборону оприлюднювати чужі особисті та конфіденційні дані, якщо інше не було відомо публічно раніше або не є просто

посиланням на таку інформацію, тоді це дозволено. При цьому, якщо є сумнів в тому, що подібна інформація розміщена правомірно, Twitter має право заблокувати пост і направити запит особі, щоб дізнатися про її згоду.

Для розробників компанія Twitter створила ряд угод і політик, яких слід дотримуватися при роботі з Twitter і даними, доступними через нього: API-інтерфейси Twitter, Угода з розробниками (Developer agreement), Політика конфіденційності для розробників (Developer policy), Умови для розробників: докладніше про обмеження використання API Twitter (Developer terms: More about restricted uses of the Twitter APIs). Центральна ідея цих документів полягає в тому, що Twitter забороняє використання даних Twitter і API інтерфейсів Twitter будь-якою організацією з метою стеження або будь-яких інших видів діяльності, які не відповідають розумним очікуванням користувачів соціальної мережі щодо конфіденційності.

Узагальнюючи правові положення розробників, можна виділені такі дозволені дії розробників:

- використовувати всі доступні дані, окрім даних із особистих повідомлень користувачів;

- самостійно організовувати захист отриманих даних користувачів, і нести особисту відповідальність за їх збереження та їх відповідність законодавству при їх обробці;

- узагальнювати контент і дані Twitter, що не містять особистих даних (наприклад, ідентифікаторів користувачів, імен користувачів та інших ідентифікаторів), за умови, що аналіз також відповідає чинному законодавству і правовим нормам.

До заборонених дій при використанні API і даних Twitter відносяться (але не обмежуються ними):

- вивчення або стеження за «чутливими» групами користувачів, що представляють громадські інтереси, таких як профспілки або групи активістів;

- вивчення поведінки окремих осіб, перевірка біографічних даних або будь-який інший збір інформації про конкретну особу;

- аналіз кредитного або страхового ризику;
- вивчення конкретної особистості та створення її психологічного портрету;
- розпізнавання осіб.

Таким чином, політика Twitter, як і всі інші правові документи, містить багато ідеологічних позицій про те, що все, зроблене з використанням Twitter - це публічна інформація і той обсяг даних, що збирається є основною перевагою соціальної мережі. І тому Twitter покладає повну відповідальність за дотримання законодавства та забезпечення безпеки використання загальнодоступних даних на тих, хто здійснює дію - користувачів, читачів, розробників.

Висновки до першого розділу

Вивчення положень Загального регламенту захисту персональних даних ЄС показав, що нормативний акт визначає персональні дані досить широко, відносячи до особистих даних не лише інформацію, яка прямо ідентифікує особу, але й інформацію, яка в сукупності з іншими даними може бути використана для ідентифікації особи. Регламент встановлює основні принципи безпечного використання й обробки персональних даних, зокрема принципи мінімізації даних, обмеження часу їх зберігання, забезпечення цілісності і конфіденційності, підзвітності й відповідальності за обробку персональних даних.

У результаті аналізу нормативно-правової бази щодо забезпечення безпеки та обробки персональних даних в Україні встановлено, що вітчизняна система захисту персональних даних, в тому числі питання збору, обробки та забезпечення їх безпеки, потребують розвитку. При чому вектор цього розвитку має бути спрямований на вивчення й адаптування найбільш прогресивних норм західних нормативних документів, в тому числі Загального регламенту захисту даних ЄС. Оскільки країни Європейського Союзу вже пройшли цей шлях, поступово вибудовували системи, усували слабкі місця і адаптувалися до нових умов.

Розгляд положень угод про користування соціальними мережами Facebook і Twitter показав, що кожен користувач несе особисту відповідальність за контент і персональні дані, що публікуються, і повинен усвідомлювати наявність загроз і відповідати за свої дії в соцмережі. Також, використовуючи загальнодоступні дані в персональних цілях, користувач має дотримуватися законних прав та інтересів тих осіб, дані яких використовує. При створенні облікового запису або додаванні контенту, користувач вносить цю інформацію в базу даних, яка належить правовласнику соціальної мережі, відповідно, надає йому виключне право на право використання цих даних.

РОЗДІЛ 2.
ВИДИ ЗАГРОЗ І МЕТОДИ АТАК НА ПЕРСОНАЛЬНІ ДАНІ КОРИСТУВАЧІВ СОЦІАЛЬНИХ МЕРЕЖ

Соціальні мережі сьогодні надзвичайно популярні, що неминуче приваблює зловмисників, що використовують безпечність користувачів і прогалини в системі захисту для організації атак і крадіжки персональних даних.

Великі соціальні мережі стали надзвичайно популярними завдяки стрімкому розвитку мережевих і мобільних технологій, однак ця популярність неминуче тягне за собою використання значної користувацької аудиторії для поширення шкідливих програм і крадіжки персональних даних. Допомагаючи підтримувати зв'язок з близькими, друзями і колегами, соціальні мережі одночасно створюють ризики безпеці. Деякі соціальні мережі, наприклад, Facebook і Twitter, вимагають, щоб користувачі вказували про себе реальні відомості, і можуть зберігати великий обсяг персональної інформації, в тому числі дані по кредитних картах.

Далі буде розглянуто категорії загроз інформаційній безпеці користувачів соціальних мереж, а також різні види і класифікації атак на дані користувача.

2.1. Інформаційно-технологічні й інформаційно-психологічні загрози інформаційній безпеці користувачів соціальних мереж

Загалом усі загрози інформаційній безпеці користувачів соціальних мереж можна умовно поділити на інформаційно-технологічні й інформаційно-психологічні.

Інформаційно-технологічні загрози

Соціальні мережі є вразливими до практично всіх основних загроз інформаційній безпеці, характерних для таких сервісів як веб-сайти, електронна пошта і системи миттєвого обміну повідомленнями.

Найбільш очевидною загрозою інформаційній безпеці користувачів соціальних мереж є несанкціонований вхід в акаунт. При реалізації даної загрози зловмисник може використовувати підбір або перехоплення облікових даних користувача, помилкове відновлення його пароля з використанням секретного питання й інші способи.

Соціальні мережі ускладнюють такі атаки, застосовуючи схеми двофакторної аутентифікації, блокування облікового запису при спробі підбору пароля й інші схеми захисту.

Наслідки успішної атаки для власника облікового запису можуть бути найрізноманітнішими, а саме:

- крадіжка особистих даних власника, включаючи особисту переписку, світлини тощо;
- використання профілю в шахрайських цілях шляхом експлуатації довіри друзів атакованого користувача;
- дискредитація власника профілю;
- деанонімізація власника профілю.

Інші поширені проблеми, такі як «кроссайтовий скриптинг» і поширення вірусів і «черв'яків», реалізуються за допомогою засобів інформаційного обміну в соціальних мережах, а саме: публікацій на особистих сторінках і на сторінках груп, особистих повідомлень. Успіх «кроссайтового скриптинга» в соціальних мережах може призвести до виконання різних дій від імені користувача, підміни посилань, виконання інших дій на користувача [12].

Значну загрозу користувачам соціальних мереж має фішинг, який може реалізовуватися всередині платформи (через особисті повідомлення і публікації в профілях) або за її межами (електронна пошта, миттєві повідомлення). При підготовці до атаки можуть використовуватися дані з відкритих джерел. Так пошук клієнтів певного банку може бути реалізований, наприклад, через збір підписників сторінки банку в соціальній мережі. Серед знайдених підписників можуть бути обрані найбільш вразливі особи, які мають низький рівень технічної грамотності в силу вікових та освітніх особливостей. Фішингові повідомлення

можуть містити звернення на ім'я та певну особисту інформацію, що автоматично підвищує шанси зловмисника на успіх.

Для захисту користувачів соціальних мереж від «традиційних» загроз інформаційній безпеці використовують традиційні заходи: стійкі паролі, антивірусне програмне забезпечення, перевірку дійсності SSL-сертифікатів при доступі до сторінки мережі тощо.

Окрім перерахованих загроз, користувач може стикнутися зі специфічною проблемою безпеки особистих даних, а саме «наявною втратою контролю над особистою інформацією». Вище згадувалося непряме отримання відомостей про користувача шляхом аналізу особистих даних його друзів.

Іншим прикладом непрямого вилучення відомостей є отримання інформації про переміщення або улюблені місця користувача через аналіз метаданих його світлин. Деякі соціальні мережі надають функцію пошуку світлин, зроблених в області із вказаними координатами, що дозволяє, наприклад, виявляти облікові записи користувачів, які проживають або працюють за заданою адресою.

Інший шлях втрати контролю за особистими відомостями, а саме «вічне» зберігання даних, характерне для багатьох «глобальних» інформаційних сервісів. У користувача соціальної мережі немає ніякої можливості упевнитися в реальності видалення соціальною мережею даних, що видаляються користувачем. Так, наприклад, політика використання даних Facebook говорить, що компанія зберігає дані стільки часу, скільки це необхідно, щоб забезпечити функціонування продуктів і послуг, в тому числі описаних вище, для власника даних і інших користувачів. Інформація, пов'язана з особистим обліковим записом, буде зберігатися до його видалення або ж до того моменту, коли Facebook більше не будуть потрібні ці дані для надання продуктів і сервісів [13].

Активні користувачі соціальних мереж нерідко стикаються з небажаним розголошенням інформації третіми особами. Наприклад, користувач може бути згаданий в публікації іншого користувача, може бути відзначений на світлині, опублікованій ним. Негативні наслідки подібного можуть бути різноманітними - проблеми на роботі або в сім'ї через розкриття фактів, які приховувалися.

Інформаційно-психологічні загрози

Соціальні мережі відмінно підходять для маніпулювання циркулюючою в них інформації для здійснення різних впливів на свідомість користувачів соціальних мереж. Загрози інформаційно-психологічній безпеці користувачів соціальних мереж (далі - УІПБ) різні і можуть реалізовуватися із застосуванням спеціальних програмних засобів.

Прикладом найпростішої УІПБ може служити соціальна інженерія. Метою такої атаки на користувача соціальної мережі часто є отримання відомостей, що дозволяють виконати деяку традиційну атаку (наприклад, отримання відповіді на «секретне питання»). Атака може виконуватися з будь-облікового запису соціальної мережі [14].

В основі більшості УІПБ в соціальних мережах лежить неможливість достовірно ідентифікувати користувача соціальної мережі. Навіть якщо користувач особисто знайомий з власником профілю, він не може бути впевнений в тому, що профіль не зламаний і не перебуває під контролем зловмисника. Ця особливість є основою для соціальної інженерії з використанням зламаних облікових записів. При такій атаці зловмисник використовує довіру «друзів» користувача зламаного облікового запису. Найбільш широко використовувана схема такої маніпуляції включає:

- злом облікового запису користувача соціальної мережі;
- масова розсилка друзям повідомлень з проханням про переведення грошових коштів;
- короткий діалог із загальних фраз, що завершується передачею номера анонімної банківської карти зловмисника;
- видалення діалогів для приховування факту злому облікового запису.

Злам облікових записів найбільш популярних соціальних мереж стає досить складним завданням, тому зловмисники нерідко застосовують соціальну інженерію з використанням неправдивих особистостей. Така атака вимагає завчасного створення зловмисником несправжньої (фейкової) особистості - копії облікового запису деякого користувача соціальної мережі, і, найчастіше,

додавання в «друзі» друзів копійованого користувача. Поява дубліката зазвичай мотивується тим, що доступ до колишнього облікового запису втрачено з тієї чи іншої причини [15].

Для наповнення профілю фейкової особистості коректними відомостями можуть використовуватися дані, витягнуті з облікового запису користувача соціальної мережі, в якій створюється підробна особистість, або його облікових записів в інших соцмережах. Користувач, присутній не у всіх соціальних мережах, популярних серед його друзів, більш вразливий до загрози копіювання його облікового запису в іншу соціальну мережу.

Метою створення фейкових особистостей і їх інфільтрації в довірену мережу користувача, що атакується, може бути збір даних обмеженого доступу за допомогою неправдивих особистостей, а саме прихованих атрибутів профілю користувача – жертви атаки, його публікацій, доступних тільки для друзів тощо.

Хибна особистість може бути повністю штучним об'єктом, керованим зловмисником, може не мати прототипу, і використовуватися для збору даних обмеженого доступу з закритих груп соціальних мереж.

Прикладом УІПБ, в реалізації якої можуть використовуватися великі колективи неправдивих особистостей, які не мають явного прототипу - це інформаційно-психологічний вплив на користувачів соціальних мереж шляхом імітації масовості. Як засіб здійснення впливу можуть виступати: голосування, масова публікація коментарів, що виражають одну і ту ж думку, встановлення позначки «мені подобається» тощо. Результатом впливу може стати прийняття користувачем соціальної мережі рішень, шкідливих для нього, прийняття точки зору, яка не має під собою об'єктивного обґрунтування. Під впливом ефекту масовості користувач може змінити своє ставлення до значущих питань його особистого, економічного, політичного життя, до чого особливо схильна молодь.

Фейкові особистості можуть застосовуватися для реалізації загроз з метою дезінформування користувачів мережі. Для соціальних мереж, на відміну від традиційних засобів масового поширення інформації (друкована преса, радіо, телебачення) характерна децентралізованість джерел інформаційних повідомлень.

Це тягне за собою, зокрема, й неможливість упевнитися в тому, що розповсюдження повідомлень відповідає реальності. Використання хибних особистостей, крім, власне, поширення неправдивого повідомлення, дозволяє імітувати інтерес до публікації, підтверджувати дані, представлені в ній, і одночасно приховати першоджерело [16].

Фейкові особистості можуть застосовуватися для посилення ефекту поляризації і радикалізації думок користувачів соціальної мережі, що представляє УІПБ як для окремих користувачів мережі, так і, в ряді випадків, для держави загалом.

Ефект пов'язаний з тим, що соціальні мережі до неперевершеного раніше рівня спростили пошук однодумців. Носій будь-якої, навіть найбільш екзотичної ідеї, в соціальній мережі може знайти інших носіїв цієї ідеї. Корекція радикальних думок і обмін аргументами між ідейними опонентами, природні для соціуму, що не залучений в соціальну мережу, не відбувається, замість чого підвищується переконаність носія ідеї у власній правоті. Даний ефект може бути істотно посилений правильним застосуванням неправдивих особистостей.

Схильність користувачів до перерахованих УІПБ у поєднанні з постійним зростанням аудиторії соціальної мережі створюють можливості залучити до реалізації даних загроз різні категорії організацій, зацікавлених в інформаційно-психологічному впливі на маси - великих компаній, які постачають продукти та послуги фізичним особам, рекламних агентств, політичних партій, іноземних розвідок.

Загальна класифікація загроз персональним даним в соціальних мережах

Сьогодні персональні дані - це джерело багатства для багатьох зловмисників. Уподобання користувача, його улюблені місця, близькі люди або будь-які інші подробиці про нього є цінною інформацією. Раніше ці дані були б миттєво використані для скоєння крадіжки особистості, але сьогодні зловмисникам вигідніше їх продати. Підозрілі організації та сервіси використовують таку інформацію, щоб налаштовувати цільову рекламу, запускати кампанії соціальної

інженерії або впливати на користувачів за допомогою інших маніпулятивних прийомів. Крім цього, з'являються все нові способи фінансового шахрайства.

Злочинці вміють обманом змусити користувачів соціальних мереж передавати конфіденційну інформацію, красти особисті дані і отримувати доступ до облікових записів, які вони вважають конфіденційними. Нижче перераховані популярні загрози в соціальних мережах [17].

Майнинг даних

Кожен залишає в Інтернеті інформаційний слід. Щоразу, коли особа створює новий обліковий запис в соціальних мережах, вона надає особисту інформацію, яка може включати ім'я, дату народження, географічне розташування й особисті інтереси. Крім того, компанії збирають дані про поведінку користувачів: коли, де і як вони взаємодіють з їх платформою. Всі ці дані зберігаються і використовуються компаніями для більш цілеспрямованої реклами для своїх користувачів. Іноді компанії діляться даними користувачів зі сторонніми організаціями, часто без відома або згоди користувачів.

Спроба фішингу

Фішінг - один з найбільш поширених способів, за допомогою якого злочинці намагаються отримати доступ до конфіденційної особистої інформації. Здійснена у формі електронного листа, текстового повідомлення або телефонного дзвінка фішингова атака представляється як повідомлення від законної організації. Ці повідомлення обманом заманюють людей з метою обміну конфіденційними даними, включаючи паролі, банківську інформацію або дані кредитних карток.

Фішингові атаки часто реалізовуються у соціальних мережах. У серпні 2019 року масштабна фішингова кампанія була націлена на користувачів Instagram, видаючи себе за двофакторну систему аутентифікації і пропонуючи користувачам увійти на помилкову сторінку Instagram.

Використання шкідливого ПЗ

Шкідливі програми призначені для отримання доступу до комп'ютерів і даних, що в них містяться. Після проникнення шкідливих програм на комп'ютер користувача вони можуть бути використані для крадіжки конфіденційної

інформації (шпигунські програми), вимагання грошей (програми-вимагачі) або отримання прибутку від примусової реклами (рекламні програми).

Платформи соціальних мереж є ідеальною системою доставки для розповсюджувачів шкідливих програм. Після злому облікового запису (часто шляхом отримання паролів через фішингову атаку) кіберзлочинці можуть взяти цей обліковий запис на себе для поширення шкідливих програм серед усіх друзів або контактів користувача.

Ботнет-атаки

Боти соціальних мереж - це автоматичні облікові записи, які створюють повідомлення або автоматично стежать за новими людьми, коли згадується певний термін. Велика група ботів може утворювати мережу, відому як бот-мережу. Боти і бот-мережі широко поширені в соціальних мережах і використовуються для крадіжки даних, розсилки спаму і запуску розподілених атак типу «відмова в обслуговуванні» (DDoS), які допомагають кіберзлочинцям отримати доступ до пристроїв і мереж людей [18].

2.2. Методи атак на дані користувачів та шахрайства у соціальних мережах

Як показує практика, більшість користувачів соціальних мереж вразливі до діяльності шахраїв: злочинці, користуючись низькою комп'ютерною грамотністю або довірливістю людей, придумують все нові способи вчинення подібних злочинів. Далі буде розглянуто схеми шахрайських дій, які найчастіше зустрічаються в соціальних мережах.

Найпростіший і найпоширеніший спосіб полягає в тому, що злочинець зламує профіль користувача соціальної мережі і починає масову розсилку повідомлень його «друзям» з проханням позичити йому певну суму грошей, перерахувавши кошти на номер мобільного телефону, банківську карту, або рахунок в тій чи іншій платіжній системі. При цьому суми зазвичай невеликі, так

злочинцеві простіше отримати гроші від якомога більшої кількості обманутих «друзів» користувача [19].

Наступним досить поширеним способом скоєння злочинів в соціальних мережах є шахрайство, яке пов'язане з неправомірним отриманням даних банківської карти потерпілого. В даному випадку злочинець, неправомірно отримавши доступ до «профілю» користувача, починає від його імені розсилку повідомлень його «друзям», в яких повідомляє, що його картка заблокована, а йому треба перевести грошові кошти. Потім шахрай просить надати йому дані банківської картки потенційної жертви, а потім і захисний код. Після того як потерпілий виконує прохання злочинця, з його рахунку списується сума грошей, а злочинець перестає виходити на зв'язок.

Окремо слід відзначити такий спосіб розкрадання грошових коштів з банківської карти як свідомо фіктивний продаж або купівля товарів, а також надання різних послуг. У цьому випадку злочинцеві достатньо створити кілька підроблених «профілів», за допомогою яких він буде здійснювати шахрайства. Злочинець розміщує в соціальній мережі оголошення про продаж товарів або надання послуг, після того як жертва відгукується на оголошення, їй пропонується перерахувати кошти за товар або послугу в якості передоплати або повної оплати. Після перерахування потерпілим грошових коштів, злочинець видаляє «профіль» або не виходить на зв'язок.

За іншою схемою шахрай сам відгукується на розміщене в соціальній мережі оголошення, пропонує оплатити товар і просить продавця передати йому дані своєї банківської картки, а потім і цифри коду, що прийшли в смс-повідомленні. Після чого з карти потерпілого знімаються кошти, а злочинець, як і в першому випадку, видаляє «профіль» або перестає виходити на зв'язок [20].

Окрім розглянутих методів, також можна виділити такі популярні схеми шахрайства.

Опитування, тести і конкурси для збору даних

У цьому методі шахраї закликають користувача пройти платне опитування, за результатми якого потрібно лише залишити дані банківської картки, щоб

оплатити невелику комісію за отримання винагороди. Бувають випадки, коли подібні пропозиції з'являються в соціальних мережах за допомогою таргетованої реклами, оскільки реклама помилково проходить модерацію адміністраторів соціальних мереж.

У численних фейкових тестах також можуть використовуватися прийоми, що змушують учасників поділитися певною інформацією. Користувачам може здаватися, що це гра, і вони можуть вважати свої персональні дані, такі як дата народження або місце проживання, неважливими. Насправді, таким чином зловмисники виманюють у користувачів інформацію про них і їхніх друзів для подальших атак.

Клікбейт

Зловмисники витрачають багато сил на створення яскравих заголовків, за якими користувачам хочеться перейти. Заголовки повинні бути такими, щоб встояти було складно: привабливими і неймовірними, але при цьому правдоподібними. Чим більше у зловмисників призначених для користувача даних, тим простіше їм створити клікбейтний заголовок, який приверне увагу користувача. І якщо користувач на нього натисне, то його може перенаправити на будь-який невідомий або ненадійний веб-сайт.

Це може бути сторінкою входу на сайт через акаунт на Facebook або Twitter. Користувача може не збентежити той факт, що потрібно заново виконати вхід, і він може виконати вхід машинально. Ввівши свої дані для входу в соціальну мережу, особа дозволить зловмисникам заволодіти своїм профілем користувача в соціальній мережі і використовувати його для своїх неправомірних цілей [21].

Скорочені URL-адреси

Скорочені URL-адреси виглядають короткими і зовні приємними для деяких користувачів, починаючи, наприклад, з bit.ly (популярний сервіс для скорочення посилань), але зловмисники використовують їх для приховування підозрілих сайтів, поширюючи подібні посилання в соціальних мережах і мотивуючи перейти по ним. Однак подібні скорочені URL-адреси можуть маскуватися під

офіційні сайти, коли насправді перейшовши за посиланням можна, навіть не усвідомлюючи, встановити шкідливі програми на свій пристрій.

Запити від людей, які вже були в списку друзів

Даний спосіб полягає в тому, що шахраї створюють і дублюють існуючий профіль знайомого жертви, щоб потрапити до нього в «друзі». Цей прийом соціальної інженерії, розрахований на те, що користувач додасть шахрая в список контактів, вважаючи, що на іншому кінці - його або її знайомий.

Повідомлення про надзвичайні ситуації

Це «термінові» попередження від імені «друзів» або будь-якого сервісу, що містять нібито термінову і важливу інформацію про обліковий запис користувача. Наприклад, користувач може отримати лист від банку, в якому говориться, що карта заблокована через підозрілі операції, і для верифікації необхідно ввести його дані (або перейти за посиланням на підробну Інтернет-сторінку банку й увійти в свій акаунт).

За допомогою прийомів соціальної інженерії зловмисники вводять жертву в стан паніки і тривоги, щоб він (вона) необачно ввели якусь інформацію і надали дозвіл, перебуваючи у стані психологічної напруги [22].

Накрутка схвалень

Атака Likejacking, або накрутка схвалень - це прийом кіберзлочинців, в якому такі функції соціальної мережі Facebook, як обмін інформацією між користувачами і вираження схвалення, використовуються для значного збільшення масштабів шахрайства. Користувачам зазвичай надходять різні пропозиції, наприклад взяти участь у розіграші призів. Якщо користувач клацає посилання у відповідь на таку пропозицію, він, сам не знаючи того, натискає кнопку схвалення («подобається») на деякий об'єкт в іншому профілі соціальної мережі [23].

Шахрайство з використанням копіювання / вставки

У цьому виді шахрайства для поширення матеріалів використовуються можливості облікового запису користувача соціальної мережі. Кіберзлочинці використовують різні способи для того, щоб змусити користувача запустити

сценарій автоматичного поширення спам-публікацій в облікових записах інших користувачів. Автоматично поширені публікації в свою чергу намагаються поширитися далі цим же методом.

Для активації такого виду шахрайства необхідно, щоб користувач вручну скопіював і вставив сценарій, тому можливості його поширення дещо обмежені.

Шахрайство із заходами

При такому виді шахрайства в соціальній мережі Facebook створюється сторінка заходу з метою перенаправлення користувачів на шкідливі веб-сайти, збору особистої інформації користувачів, а також отримання доступу до їхніх профілів у Facebook. Кіберзлочинець, як правило, намагається запросити на сторінку заходу велике число користувачів, щоб збільшити число потенційних жертв.

Підроблений модуль

При цьому виді шахрайства користувачеві соціальної мережі обманом пропонують встановити модуль для браузера, який є шкідливим. Для цього шахраї можуть поширювати в соціальних мережах різні відеоролики з інтригуючими заголовками. Коли користувач клацає таке відео, йому пропонується встановити шкідливий модуль для перегляду даного відео.

Фальшиві пропозиції

У публікаціях в соціальних мережах з'являються підроблені пропозиції, що пропонують користувачам можливість виграти призи. Однак злочинці не виконують свою обіцянку, замість цього вони перенаправляють користувачів на шкідливі сайти або сайти з анкетами, переконують користувачів поширити далі цю пропозицію або передати їм особисту інформацію.

Накрутка коментарів

У цьому виді шахрайства, також відомого як Commentjacking, користувача соціальної мережі спонукають відправити коментар до публікації, в результаті чого вона відображається в його стрічці подій. Кіберзлочинці використовують заголовки, що привертають увагу, щоб змусити користувача вибрати посилання на відео. Після клацання посилання користувачеві відображається фальшивий тест CAPTCHA. Коли користувач проходить цей фальшивий тест, він, сам не

знаючи того, відправляє коментар до якоїсь публікації в Facebook. Прокоментована користувачем публікація відображається в стрічці новин його друзів, таким чином шахрайство поширюється далі.

Запити дозволів

Для роботи цього виду шахрайства необхідна установка шкідливих додатків для соціальних мереж, які отримують доступ до облікового запису користувача. Кіберзлочинці спонукають користувача встановити шкідливий додаток, який запитує різні дозволи, що дозволяють зловмисникові діяти і створювати публікації від імені користувача.

Самостійне розповсюдження матеріалу користувачем

При цьому виді шахрайства користувача обманом спонукають самостійно натиснути кнопку «поділитися», щоб переглянути якийсь відеоматеріал. Для цього кіберзлочинці використовують публікації про шокуючі, непристойні, сексуальні або просто смішні події і пропонують посилання на відповідне відео. Коли користувач намагається переглянути це відео, його просять поділитися цією публікацією або натиснути кнопку «поділитися», що відображається на іншій мові. Після того як користувач поділився з друзями публікацією, його можуть попросити заповнити анкету, підписатися на послугу або завантажити шкідливе розширення для браузера або шкідливий додаток [24].

Перенаправлення в підробні додатки

У цьому виді шахрайства здійснюється перенаправлення користувача з веб-сайту соціальної мережі на зовнішній веб-сайт. З зовнішнього веб-сайту користувач може бути перенаправлений назад у додаток на сайті соціальної мережі, на якому він до цього перебував. Додаток, в який здійснюється перенаправлення, може вимагати від користувача дозволу, що дасть можливість шахраям діяти від імені користувача.

Facebook-боти

Facebook-бот - це програма, яка створює фальшиві профілі для відсилання повідомлень в чаті і поширення публікацій із шкідливими посиланнями. Боти поширюються шляхом розсилки пропозицій дружби з користувачами Facebook.

Шахрайство в Twitter

Кіберзлочинці використовують твіти для шахрайства або поширення спам-матеріалів. У результаті таких дій користувач може бути перенаправлений на шкідливі сайти, де його обліковий запис може бути скомпрометований, особиста інформація користувача може бути вкрадена, або користувача можуть обманом змусити відправити гроші шахраям, а також встановити шкідливе ПЗ на його комп'ютер [25].

Романтичні афери.

Як правило, такі шахраї відправляють романтичні повідомлення незнайомим людям і прикидаються, що розлучені, перебувають у невдалому шлюбі або овдовіли. Вони починають онлайн-стосунки з жертвою, а потім заявляють, що їм потрібні гроші, щоб заплатити за авіаквитки або отримати візу. Їх мета - увійти в довіру, тому листування може тривати тижнями, перш ніж шахрай попросить у жертви грошей [26].

Лотерейне шахрайство.

Лотерейне шахрайство зазвичай здійснюється з акаунтів або сторінок людей, які видають себе за знайомих жертви або будь-якої організації (наприклад, державна установа або Facebook). У повідомленнях від таких акаунтів може бути сказано, що користувач виграв в лотерею і може отримати гроші за невеликий аванс. Шахраї можуть попросити надати особисті дані, наприклад реальну адресу проживання або банківську інформацію.

Кредитне шахрайство.

Такі шахраї відправляють повідомлення або розміщують публікації, пропонуючи кредити за низькою відсотковою ставкою за невеликий аванс.

Крадіжка маркера доступу.

Жертва отримує посилання, яке вимагає доступ до його/її акаунту або сторінки у Facebook. Посилання може виглядати зовсім безневинно, але таким чином шахраї здатні отримати доступ до призначеного для користувача акаунту для розсилки спаму.

Шахрайство, пов'язане з пошуком роботи.

За такою схемою шахраї розміщують фальшиві вакансії, щоб отримати особисту інформацію або гроші користувачів. Натискаючи посилання в публікації з вакансією, і після чого потрапляючи на невідомий сайт, користувача можуть запитувати особисту інформацію (наприклад, дані офіційного посвідчення особи), а також іншу конфіденційну інформацію [27].

Загалом найбільш поширені методи атак на дані користувачів і шахрайські дії у соціальних мережах можна представити у вигляді схеми (Рис. 2.1).

Рис. 2.1. Найбільш поширені методи атак на дані користувачів і шахрайські дії у соцмережах

2.3. Приклади атак на персональні дані в соціальних мережах

Історія з Cambridge Analytica і Facebook

Британська компанія Cambridge Analytica, створена в 2013 році, зібрала особисті дані 50 мільйонів користувачів Facebook. Потім вона змоделювала поведінку десятків мільйонів американців для того, щоб показувати їм релевантну політичну рекламу. Вважається, що вона внесла вагомий вклад в перемогу Дональда Трампа на виборах президента США. Завдяки розслідуванням The New York Times і The Guardian стало відомо, як саме працювала Cambridge Analytica [28].

Cambridge Analytica, як вказано на сайті компанії, займається впливом на поведінку користувачів в соціальних мережах. По суті, Cambridge Analytica займається рекламою, а великі обсяги даних про користувачів використовує, щоб доносити ту чи іншу інформацію від політика або комерційної компанії максимально ефективно. Серед інших послуг Cambridge Analytica - маркетингові дослідження та аналіз цільової аудиторії.

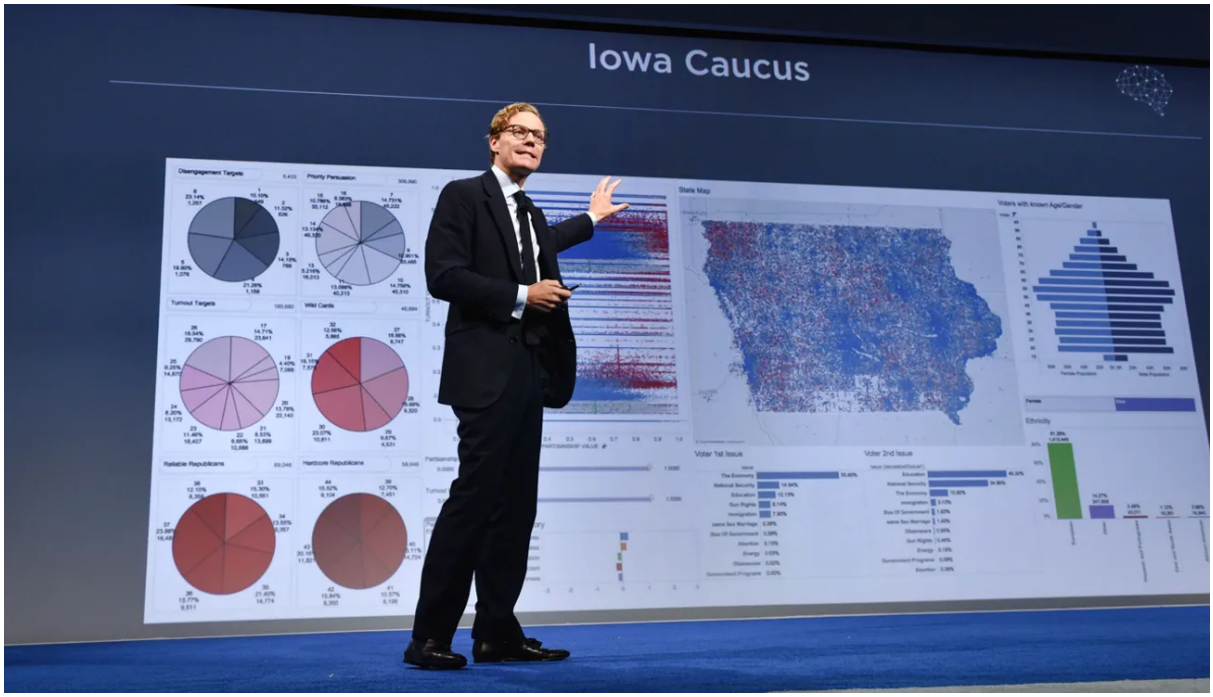

Рис. 2.2. Керівник Cambridge Analytica Олександр Нікс, вересень 2016 р.

Cambridge Analytica називає себе лідером індустрії з 25-річним досвідом. Насправді компанія створена в 2013 році за участю сім'ї Мерсер, головних

донорів передвиборного штабу Д.Трампа. Віце-президент компанії - Стівен Беннон, колишній керівник популярного серед ультраправих консервативного сайту Breitbart і колишній радник Д.Трампа. В Cambridge Analytica працювали кілька людей з Кембриджського університету; у компанії є офіси в США і Великобританії.

Для збору даних про користувачів соціальних мереж Cambridge Analytica зв'язалася з професором психології з російським корінням Олександром Коганом. За даними The Guardian, він працює в Кембриджському університеті, а також викладає в Санкт-Петербурзькому державному університеті.

О.Коган створив спеціальний психологічний тест; за його проходження користувачам платили гроші. При цьому програма запитувала інформацію про профілі користувачів і їхніх друзів (в той час Facebook дозволяв стороннім додаткам такий збір даних). О.Коган стверджував, що його тест збирає дані виключно в академічних цілях. Насправді, він їх продавав без відома користувачів.

На збирання даних О.Коган витратив 800 тис. доларів, які йому компенсувала Cambridge Analytica. У розпорядженні дослідника виявилися дані про 87 мільйонів користувачів Facebook, хоча сам тест пройшли тільки 270 тисяч осіб.

Всі ці дані дозволили не просто скласти уявлення про особистості користувачів, але і створити їх повноцінний профіль, в якому вказані переконання, особливості характеру, уподобання, інтереси і багато іншого. Колишній співробітник Cambridge Analytica Крістофер Уайлі, докладно розповів журналістам про схему роботи компанії, і стверджував, що він сам придумав схему роботи «психологічної зброї Стівена Беннона» - так він називає систему аналізу особистостей користувачів.

Перед тим, як почати працювати на Cambridge Analytica, Уайлі вивчав методику пророкувань трендів в індустрії моди, а до цього здобув освіту в області права в Лондонській школі економіки. К.Уайлі ще в підлітковому віці почав працювати з політиками в рідній Канаді - він був волонтером в місцевому парламенті, а в Лондоні працював з Ліберально-демократичною партією. К.Уайлі

знав про дослідження в Кембриджі, які дозволяли складати докладні профілі користувачів на основі вірусних тестів в Facebook.

Такі тести дозволяли виявляти в тому числі і політичні уподобання: люди з певними характеристиками зазвичай голосують схожим чином. Наприклад, прихильники ліберальних поглядів - найчастіше люди відкриті, але не схильні до акуратності. Найбільше про користувачів говорили їхні «лайки» - по набору з декількох десятків, на перший погляд, дрібниць, вдавалося вибудовувати досить точні моделі поведінки. Про все це йшлося в дослідженнях центру психометрії Кембриджського університету, де до сих пір працює О.Коган. Один із співробітників центру зазначає, що дослідження «лайків» іноді приносило абсолютно несподівані результати: наприклад, виявлялося, що люди, які лайкають Nike і KitKat, схильні негативно ставитися до Ізраїлю.

Як з'ясувала The New York Times, з Cambridge Analytica тісно співпрацював штаб кандидата у Президенти США Д.Трампа. Спроможність штабу Д.Трампа ефективно працювати з виборцями в Інтернеті, особливо в Facebook, не раз називали однією головних причин його перемоги на виборах [28].

10 квітня засновник Facebook Марк Цукерберг дав свідчення в сенаті США, 11 квітня - в палаті представників (верхня і нижня палати конгресу США). На цих сесіях засновник Facebook нарешті визнав витік даних 87 мільйонів користувачів (за словами Цукерберга, він і сам був серед цих користувачів), але запевнив, що Facebook все одно абсолютно безпечний, заявивши, що він сам, його родина і всі близькі люди постійно користуються цією соцмережею.

Через три тижні після виступу Цукерберга перед конгресменами, 2 травня, Cambridge Analytica заявила, що починає процедуру банкрутства в Великобританії і незабаром почне її в США [29].

Twitter-шахрайство з біткоїнами

15 липня 2020 року, між 20:00 і 22:00 UTC, в результаті кібератаки було зламано кілька топ-акаунтів на Twitter, кожен з яких мав мільйони передплатників, з метою спровокувати шахрайство з біткоїнами. Шахраї від імені власників облікових записів запропонували відправляти біткоїни на певний

криптовалютний гаманець з обіцянкою, що відправлені гроші будуть подвоєні і повернуті. За відомостями джерел в Vice і TechCrunch, зловмисники отримали доступ до адміністративних інструментів Twitter, і змогли змінювати облікові записи і публікувати твіти безпосередньо, причому доступ був отриманий за рахунок оплати співробітникам Twitter за використання інструменту або зі скомпрометованого аккаунта працівника, що мав прямий доступ до інструменту [30].

На 16 липня 2020 року шахраям вдалося виманити понад 12 біткоїнів, що за курсом на той момент становило більш 110 тисяч доларів США. Через кілька хвилин після публікації твітів на одному з опублікованих гаманців вже сталося понад 320 транзакцій.

Д.Альперович, співзасновник компанії з кібербезпеки CrowdStrike, назвав цей інцидент «найгіршим зломом великої платформи соціальних мереж на той момент». Дослідники в галузі безпеки висловили стурбованість тим, що соціальна інженерія, яка могла бути використана для злому, може вплинути на використання соціальних мереж в важливих онлайн-дискусіях, включаючи підготовку до президентських виборів в США у 2020 році.

Публікація 117 мільйонів облікових даних LinkedIn

У 2016 році невідомий хакер рекламував продаж більше 100 млн. логінів і паролів користувачів мережі LinkedIn. Як повідомляється, логіни були вкрадені в 2012 році під час злому соціальної мережі. Тоді вважалося, що було вкрадено значно менше паролів. Після того, як це сталося, представники компанії заявили, що всі зламані облікові записи були переустановлені [31].

Мережа LinkedIn використовується багатьма для пошуку роботи і відправки повідомлень, що стосуються роботи, тому очевидно, що користувачі хочуть зберігати анонімність листування. Злочинці могли скористатися конфіденційною інформацією або простежити, чи не використовуються ті ж логіни і паролі в інших місцях.

Подробиці продажу, вкраденої з сайту LinkedIn інформації, вперше з'явилися на сайті Motherboard. За їхніми даними, деталі продажу рекламувалися принаймні

на двох сайтах, якими користуються хакери. Голова компанії LinkedIn Рід Гарретт Хоффман, в свою чергу, не повідомив, чи були порушені запобіжні заходи всередині компанії.

Злом акаунтів в Instagram

У 2018 році понад 200 користувачів соціальної мережі Instagram повідомили про те, що вони отримали повідомлення про зміну адреси електронної пошти, пов'язаної з їхнім акаунтом [32]. Кіберзлочинці зуміли отримати доступ до акаунтів користувачів, змінили в них адреси електронної пошти та імена, а також отримали повний контроль над профілями, в результаті чого реальні власники акаунтів не змогли скинути свої паролі. Також були скомпрометовані й акаунти, в яких були налаштовані процеси двофакторної авторизації.

Через кілька днів після першого публічного обурення, все більше і більше людей стали повідомляти про те, що за останні кілька місяців вони втратили доступ до своїх акаунтів в Instagram. Дане порушення безпеки стає ще більш цікавим в силу того, що навіть якщо хакери мали доступ до різних профілів, то вони, як правило, не завдавали шкоди.

У більшості випадків, коли хакери отримують несанкціонований доступ до акаунтів в соціальних мережах, вони видаляють зображення, розміщують небажані коментарі або просто псують профіль. У даному випадку жоден з постраждалих акаунтів не був істотно «спотворений», не було оприлюднено жодних політичних гасел. Очевидно, хакери могли просто показати новий спосіб злому акаунтів в Instagram.

Витік у відкритий доступ даних 235 млн профілів користувачів Instagram, TikTok і YouTube

Фахівці компанії Comparitech виявили в мережі Інтернет незахищену базу даних, що містила близько 235 млн. профілів користувачів сервісів Instagram, TikTok і YouTube. На сьогоднішній день інцидент є одним з наймасштабніших випадків витоку даних [33].

Масив даних був виявлений дослідником Бобом Дьяченко 1 серпня нинішнього року. Він містив витягнуті з публічних профілів відомості,

включаючи логіни, повні імена користувачів, контактну інформацію, зображення, статистику про кількість підписників, дані про вік, стать тощо. Більш 192 млн. записів були пов'язані з користувачами Instagram, 42 млн. стосувалися користувачів TikTok і майже 4 млн. - користувачів YouTube. Хоча вся інформація є публічно доступною, правила всіх трьох сервісів забороняють отримувати дані з профілів.

Проаналізувавши витік, експерти прийшли до висновку, що провина лежить на компанії Deep Social, яку в 2018 році заблокували на майданчику Facebook. Причина блокування була проста - Deep Social не зовсім сумлінно збирала дані профілів користувачів.

Висновки до другого розділу

Встановлено, що для соціальних мереж характерні як інформаційно-технічні, так і інформаційно-психологічні загрози безпеки даних користувачів. Наслідки успішної атаки на персональні дані власника облікового запису можуть включати: крадіжку особистих даних власника, зокрема особисту переписку, світлини; використання профілю в шахрайських цілях шляхом експлуатації довіри друзів атакованого користувача; дискредитацію або деанонімізацію власника профілю.

Для захисту від інформаційно-технічних загроз використовують традиційні засоби (стійкі паролі, антивірусне ПЗ та ін.). Різні сервіси надають різні способи вирішення цих проблем.

Як показало дослідження, соціальні мережі є ідеальним середовищем для маніпулювання циркулюючою в них інформацією і здійснення різних впливів на свідомість користувачів. Найбільш поширеними прикладами інформаційно-психологічних загроз можуть служити методи соціальної інженерії. Питання захисту користувачів соціальних мереж від інформаційно-психологічних загроз сьогодні опрацьовано недостатньо, і безпека даних користувачів в більшості залежить від їх правильної поведінки, знання і виконання вимог інформаційної безпеки.

Вивчення методів атак на персональні дані і пов'язаних з ними шахрайських дій дозволило виділити такі основні види зазначених протиправних дій в соцмережах: опитування, тести і конкурси для збору даних, скорочені URL-адреси, повідомлення про надзвичайні ситуації, підроблені Plug-in, запити дозволів, підробні додатки, крадіжки маркерів доступу.

Масштаби і різноманітність злочинів, спрямованих на оприлюднення і незаконне використання персональних даних в соціальних мережах, зростають з кожним днем, і про це свідчать випадки масового злому акаунтів користувачів соцмереж, витоків даних багатьох мільйонів їхніх користувачів, незаконного збору особистої інформації власників акаунтів в соцмережах часто з метою подальшого маніпулювання їх свідомістю або фінансового шахрайства.

РОЗДІЛ 3.
МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ В СОЦІАЛЬНИХ МЕРЕЖАХ

Заходи, за допомогою яких забезпечується безпека персональних даних в соціальній мережі, можна розділити на дві групи: ті, що надаються веб-сайтом, і ті, що не залежать від нього.

Основним інструментом першої групи є розмежування доступу. Це механізм безпеки, що надається багатьма соціальними мережами, який дозволяє тільки певній категорії учасників вчиняти ті чи інші дії щодо інформації на сторінці користувача. Наприклад, при завантаженні світлин можна обмежувати доступ стороннім таким чином, щоб переглядати їх могли тільки друзі.

До другої групи можна віднести наступні заходи. По-перше, скорочення кількості наданих персональних даних. Це досить ефективний захід у разі, якщо користувач недавно зареєструвався у соціальній мережі і ще не встиг внести багато особистих даних.

По-друге, створення окремого e-mail для реєстрації в соціальній мережі і його приховування з використанням налаштувань приватності. Необхідність такого захисту пояснюється тим, що в адресі електронної пошти у відкритому доступі існує ризик потрапити в базу даних спам-відправників і щодня отримувати масу непотрібних листів, в тому числі шкідливих.

Третім засобом варто розглядати ігнорування підозрілих повідомлень. Однак якщо все-таки відбувся перехід за шкідливим посиланням, то захистити свої персональні дані можна за допомогою антивірусних програм і їх своєчасного оновлення.

Останній варіант для забезпечення безпеки персональних даних - використання псевдоніму. Але це не завжди можливо, тому що багато сайтів дотримуються «політики справжніх імен».

Далі будуть докладніше розглянуті технічні можливості популярних соціальних мереж щодо забезпечення безпеки облікового запису та

конфіденційності персональних даних, а також загальні рекомендації щодо забезпечення безпеки при використанні соціальних мереж.

3.1. Рекомендації щодо забезпечення конфіденційності даних і безпеки акаунта у соцмережі Facebook

Можливості забезпечення безпеки облікового запису Facebook

Facebook вказує, що система безпеки вбудована в кожен продукт Facebook, і пропонує кілька функцій безпеки, таких як попередження про вхід і двофакторна аутентифікація, щоб допомогти забезпечити додатковий захист акаунтів користувачів соціальної мережі. Також, користувачі можуть в будь-який час перевірити і оновити свої налаштування конфіденційності.

Функції безпеки та поради щодо її забезпечення:

- Захист власного пароля

Важливо використовувати пароль тільки для Facebook і ніколи не повідомляти його іншим людям. Далі, щоб пароль було складно вгадати зловмисникам, не варто використовувати в ньому власне ім'я або поширені слова.

- Захист особистих даних для входу

Шахраї можуть створити фальшивий сайт, схожий на Facebook, і попросити користувача увійти на нього з електронною адресою та паролем. Перш ніж вводити дані для входу, обов'язково потрібно перевірити URL-адресу сайту. Якщо виникли сумніви, рекомендується ввести www.facebook.com в адресний рядок браузера, щоб з упевненістю потрапити на Facebook. Не слід пересилати іншим людям листи від Facebook, оскільки в них може міститися конфіденційна інформація про обліковий запис користувача.

- Не рекомендується приймати запити на додавання в друзі від незнайомих людей

Шахраї можуть створювати фальшиві акаунти для додавання людей в друзі. Додаючи шахраїв у друзі, користувачі дають їм можливість публікувати спам в їх хроніці, відзначати їх у публікаціях і відправляти шкідливі повідомлення.

- Захист від шкідливого ПЗ

Шкідливе ПЗ може пошкодити комп'ютер, сервер і комп'ютерну мережу. Необхідно регулярно оновлювати браузер і видаляти підозрілі програми та розширення. Не рекомендується переходити за підозрілими посиланнями, навіть якщо здається, що їх відправив друг або знайома компанія.

Це також стосується посилань, розміщених на Facebook (наприклад, в публікаціях) або надісланих електронною поштою. Facebook ніколи не запитує пароль по електронній пошті.

- Використання додаткових функцій безпеки

Користувачі також можуть отримувати повідомлення про непізнані спроби входу і налаштувати двофакторну аутентифікацію. Якщо користувачі увійшли на Facebook з комп'ютера, то вони можуть перевірити свої налаштування безпеки за допомогою інструменту «перевірка безпеки».

Перевірка безпеки на Facebook

Перевірку безпеки можна використовувати для перевірки облікового запису і підвищення рівня його безпеки. Перевірка безпеки допоможе:

- отримувати повідомлення про спроби входу в обліковий запис з невідомого комп'ютера або мобільного пристрою;

- дізнатися способи захисту свого пароля;

- включити двофакторну аутентифікацію як додаткову можливість підвищити рівень безпеки облікового запису Facebook. Ця функція буде доступна у разі входу на Facebook з комп'ютера або буде використовувати останню версію програми Facebook для Android або iOS.

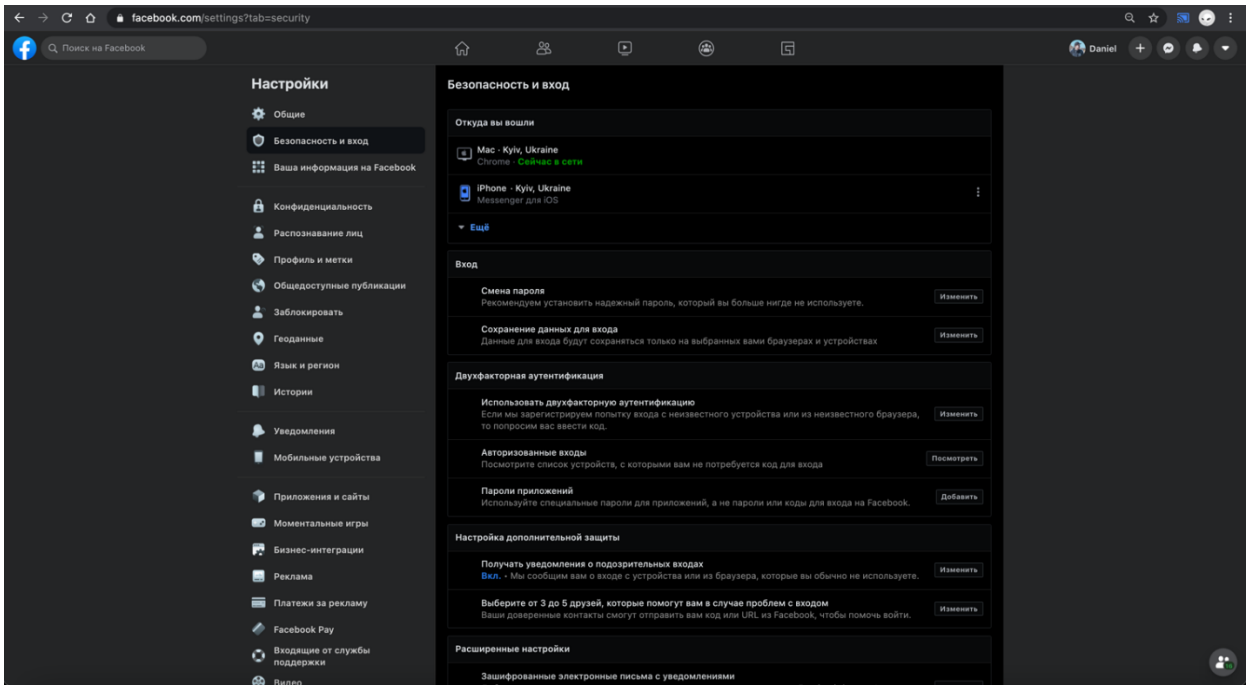

Рис.3.1. Екран налаштувань безпеки акаунта на Facebook

Захищений перегляд в Facebook

Функція захищеного перегляду (протокол HTTPS) автоматично шифрує підключення до Facebook. Вона необхідна для захисту облікового запису, тому що ускладнює доступ до інформації на Facebook без дозволу користувачів. Підключення до Facebook можливо тільки з використанням захищеного перегляду. Цю функцію не можна вимкнути.

Одноразовий пароль

Користувач може увійти в свій акаунт Facebook за допомогою одноразового пароля, якщо не хоче вказувати справжній пароль (наприклад, в бібліотеці або Інтернет-кафе). Одноразовий пароль є тимчасовим, і його не можна використовувати повторно. А також, одноразові паролі недоступні, якщо включена функція двофакторної аутентифікації.

Вихід з акаунта Facebook на іншому пристрої

У налаштуваннях безпеки і входу можна контролювати, на яких пристроях виконаний вхід в акаунт Facebook. У розділі «Звідки ви увійшли» вказані пристрої, на яких зараз виконаний вхід до системи. У кожному записі наведена дата, час, місце розташування і тип пристрою.

Визначення місця розташування

Якщо користувач не дізнається місце розташування, спочатку необхідно перевірити, чи не пов'язане воно з мобільним пристроєм. Часто при вході з мобільного пристрою користувачі підключаються через IP-адресу, яка не відображає поточне місце розташування.

Якщо місце розташування незнайоме і не пов'язане зі входом з мобільного пристрою, причина може бути в наступному:

- Facebook володіє неточною інформацією. Іноді Facebook може тільки приблизно визначити місце розташування користувача. Ці дані можуть не збігатися з реальним поточним місцезнаходженням.

- Користувач забув вийти зі свого облікового запису. Можливо, видно місце розташування мобільного пристрою, на якому не вийшли з Facebook. Якщо користувач вважає, що не вийшов з власного облікового запису на мобільному пристрої іншої людини, то може вийти з системи з іншого пристрою.

- У іншої людини є доступ до призначеного для користувача аккаунту Facebook. Якщо користувач вважає, що в аккаунт увійшла стороння людина, важливо спочатку вийти з системи, а потім захистити аккаунт, змінивши пароль [35].

Двофакторна аутентифікація Facebook

Двофакторна аутентифікація - це міра безпеки, яка допомагає захищати акаунт Facebook і доповнює захист паролем. Якщо налаштувати двохфакторну аутентифікацію, то потрібно буде вводити спеціальний код для входу або підтверджувати вхід кожного разу, коли хтось спробує отримати доступ до акаунту Facebook з невпізнаного браузера або мобільного пристрою. Користувачі також можуть отримувати повідомлення про невпізнані входи.

Якщо користувач ще не зберіг браузер або мобільний пристрій, яким користується, то буде запропоновано зробити це після включення двофакторної аутентифікації. Тоді не потрібно буде вводити код безпеки при наступному вході.

Facebook важливо запам'ятати дані комп'ютера і браузера користувача, щоб розпізнавати їх при наступному вході. Деякі функції браузерів блокують таку

можливість. Якщо користувач увімкнув безпечний режим роботи або поставив у налаштуваннях браузера видалення історії при кожному закритті, можливо, буде потрібно вводити код при кожному вході на сайт.

Для двофакторної аутентифікації можна використовувати новий або вже доданий в акаунт номер мобільного телефону.

Повідомлення про підозрілі спроби входу на Facebook

Користувачі можуть підвищити безпеку акаунта Facebook, включивши повідомлення про спроби увійти в обліковий запис з невпізнаного пристрою або браузера. Такі повідомлення містять інформацію про те, з якого пристрою і з якого місця відбувалася спроба входу.

Також можливо додати пристрій або браузер в список довірених браузерів або упізнаних пристроїв. Тоді користувачам не обов'язково буде отримувати повідомлення про вхід з комп'ютера або мобільного пристрою, які зазвичай використовуються для входу на Facebook.

Генератор кодів

Генератор кодів - це функція безпеки в додатку Facebook, яка використовується для двофакторної аутентифікації. Якщо включити цю функцію, телефон буде генерувати спеціальний код безпеки, який можна використовувати для підтвердження особи при вході з нового пристрою або браузера.

Генератор кодів працює на мобільному пристрої, навіть якщо немає доступу до SMS-повідомлень або Інтернет-підключення. Функцію також можна використовувати, якщо необхідно скинути пароль. Коди безпеки з генератора кодів, які використовуються для двофакторної аутентифікації, завжди складаються з шести цифр і діють 30 або 60 секунд в залежності від використовуваного мобільного пристрою.

Сторонній додаток для двофакторної аутентифікації

Щоб включити двофакторну аутентифікацію, потрібно вибрати основний спосіб отримання кодів безпеки: SMS або сторонній додаток для аутентифікації. Сторонні додатки для аутентифікації (наприклад, Google Authenticator or LastPass)

генерують коди для входу, які дозволяють переконатися, що це власник акаунта входить в систему з нового пристрою.

Ключ безпеки

Ключі безпеки - це частина процедури двофакторної аутентифікації. Щоб використовувати двофакторну аутентифікацію на Facebook, потрібно вибрати спосіб отримання кодів перевірки для свого облікового запису: в SMS або за допомогою стороннього додатка для аутентифікації.

Після цього можна налаштувати ключ безпеки. Якщо є сумісний ключ безпеки стандарту Universal 2nd Factor (U2F) (наприклад, спеціальний пристрій USB з підтримкою U2F) і якщо додати його в якості способу аутентифікації, то можна користуватися цим ключем при вході в акаунт Facebook з невідомого комп'ютера або мобільного пристрою.

За принципом роботи ключ безпеки схожий на дверний ключ. Після введення пароля, замість того щоб вводити код, користувачі можуть просто натиснути кнопку на фізичному ключі безпеки. Ключі безпеки сумісні не з усіма браузерами та мобільними пристроями, тому буде потрібно ще один спосіб аутентифікації, наприклад, мобільний телефон або сторонній додаток для аутентифікації.

Коди для входу і відновлення акаунта Facebook.

Якщо включена двофакторна аутентифікація, користувачі можуть отримати 10 кодів для входу і відновлення акаунта, які можна використовувати, коли при них немає телефону. 10 кодів, що з'явилися можна роздрукувати або записати. Кожен код можна використовувати тільки один раз. Якщо коди закінчилися або їх втратили, можна зробити запит для отримання нових [36].

Можливості забезпечення конфіденційності на Facebook

Вибір аудиторії публікації на Facebook

Коли користувачі діляться контентом на Facebook, наприклад, публікаціями, фото або інформацією в своєму профілі, можна побачити інструмент вибору аудиторії. Інструмент вибору аудиторії також видно біля публікації, якою користувач вже поділився. Завдяки цьому буде зрозуміло, кому доступний певний контент. Аудиторію розміщеної публікації можна змінити.

Перегляд перепостів опублікованих матеріалів

Якщо хтось натискає «поділитися» під публікацією, то у третіх осіб не буде можливості поділитися фото, відео або оновленнями статусу через Facebook з людьми, які не входили в аудиторію, яку користувач спочатку встановив. Публікації, під якими хтось натиснув «поділитися», доступні для перегляду тільки тим людям, які могли бачити їх відразу після публікації користувачем.

В інструменті вибору аудиторії можна налаштувати, хто буде бачити публікації. Якщо «друг» ділиться опублікованим користувачем посиланням, він може поділитися ним з більш широкою аудиторією в порівнянні з тією, з якої спочатку поділився користувач. Важливо пам'ятати, що текст, доданий користувачем до публікації, не буде опублікований.

Видимість публікацій при використанні хештегів

Коли користувачі додають хештег до публікації, люди, з якими вони нею поділилися, також побачать її в стрічці цього хештега. Наприклад, якщо користувачі діляться публікацією з хештегом з друзями, вони зможуть також побачити її в стрічці хештега. Якщо користувачі використовують хештег в публікації з аудиторією «Доступно всім» і дозволяють людям підписуватися на них, публікація з'явиться в загальнодоступному профілі і в стрічці хештегу.

Налаштування аудиторії, якій доступна хроніка і профіль Facebook

Будь-яка людина може бачити відкриту інформацію про користувачів, в тому числі ім'я, світлини профілю й обкладинки, стать, ім'я та ID користувача (номер акаунта) і спільноти.

Залишати публікації в хроніці можуть тільки самі власники акаунтів і друзі користувачів. При опублікуванні матеріалів можна вказати, кому вони будуть показані, за допомогою інструменту вибору аудиторії. Щоб вибрати, хто бачитиме публікації інших користувачів в хроніці, необхідно використовувати налаштування «хто може бачити, що публікують інші в хроніці». При редагуванні можна вказати, хто буде бачити інформацію про користувача, за допомогою інструменту вибору аудиторії.

Перш ніж фото, публікації і дії в додатках, в яких користувач відзначений, з'являться в хроніці, можна схвалити або відхилити їх. Для цього треба включити перевірку хроніки. При цьому, все одно інші користувачі можуть відзначити на фото або в публікації і поділитися цим контентом, так що його можна буде побачити в інших місцях на Facebook (наприклад, у стрічці новин або в результатах пошуку).

Користувачі можуть вибрати, хто буде бачити в хроніці публікації, в яких він чи вона відзначені.

Видимість електронної адреси в профілі на Facebook

У електронної адреси є налаштування конфіденційності (з ким користувач нею ділиться) і налаштування видимості (чи він показується у профілі Facebook). Наприклад, користувачі можуть показувати електронну адресу в профілі, але встановити для нього параметр конфіденційності «Друзі». У цьому випадку для користувача електронну адресу в профілі і в інших місцях на Facebook будуть бачити тільки друзі. Навіть якщо приховати електронну адресу в профілі, люди, у яких є до нього доступ, все одно будуть бачити його в інших місцях на Facebook (наприклад, у результатах пошуку).

Відображення списку друзів в профілі на Facebook

За замовчуванням, розділ «Друзі» в профілі загальнодоступний, тобто бачити список друзів можуть всі. При цьому, користувачі можуть налаштувати доступ тільки до власного списку друзів. Друзі теж можуть управляти доступом до своїх списків друзів. Наприклад, якщо користувач вибере варіант «Тільки я», то бачити повний список друзів у профілі буде тільки користувач.

Однак, якщо один друг користувача зробив список загальнодоступним, то інші люди будуть бачити користувача в профілі друга. Якщо ж один друг зробив свій список загальнодоступним, то інформація про дружбу може з'являтися в стрічці новин, результатах пошуку та інших місцях на Facebook.

Управління особистими публікаціями

Журнал подій дозволяє перевіряти ті матеріали, якими користувачі поділилися на Facebook, і управляти ними. За замовчуванням в журналі подій відображаються дії за поточний рік, починаючи з нового.

Важливо пам'ятати, що доступ до журналу подій є тільки у власника акаунта, але відображені новини можуть з'являтися в інших місцях на Facebook, наприклад, в особистій хроніці, результатах пошуку або стрічці новин у друзів.

Відображення профілю в результатах пошуку

Знайти профіль і натиснути на нього можуть всі люди, яких користувач не заблокував, проте інформація, яка показується в результатах пошуку, залежить від налаштувань конфіденційності.

У результатах пошуку враховуються налаштування конфіденційності для всього контенту: і для опублікованої інформації, і для публікацій інших людей, в яких зазначили користувача. Всі користувачі можуть управляти інформацією, яку інші люди бачать в їх профілі і хроніці, а також вибирати аудиторію опублікованого контенту.

Людям, яким користувач надасть доступ до контенту (наприклад, оновлень статусу, фото або позначок «Подобається»), можуть бачити цей текст в результатах пошуку. Наприклад, загальнодоступний контент буде видно в результатах пошуку всім людям, а контент, яким користувач ділиться з друзями, буде видно в результатах пошуку тільки друзям і так далі. Якщо в публікації користувач поділиться своїм номером телефону або електронною адресою, можливо, люди зможуть використовувати ці дані, щоб знайти цю публікацію.

Якщо користувачі не хочуть, щоб посилання на профіль Facebook з'являлися в результатах пошуку в сторонніх пошукових системах, слід змінити відповідний параметр в налаштуваннях конфіденційності. При цьому, якщо вимкнути цей параметр, посилання на профіль не буде з'являтися в результатах пошуку в пошукових системах. Однак певний контент профілю (наприклад, загальнодоступна інформація) може і далі показуватися в результатах пошуку, навіть якщо вибрати протилежний варіант [37].

Налаштування конфіденційності для відкритого пошуку дозволяє приховати з пошукових систем тільки власний профіль і хроніку на Facebook. Це налаштування не поширюється на відкриті обговорення на Facebook, в тому числі на коментарі, які користувач залишив в групах або на сторінках, доступних всім. Можна видалити особисті коментарі, якщо немає бажання, щоб коментарі індексувалися пошуковими системами. Після видалення цей контент все ще може з'являтися в результатах пошуку, але посилання буде вже недійсним.

Facebook не може контролювати контент, який вже був індексований і збережений в кеші пошукових систем. Щоб запросити повне видалення інформації користувача з результатів пошуку, потрібно звернутися в службу підтримки відповідної пошукової системи. Однак Facebook не може відправити запит від імені одного зі своїх користувачів.

3.2. Рекомендації мережі Twitter щодо методів забезпечення безпеки облікового запису користувача

Безпека облікового запису в Twitter.

Наступні практичні рекомендації допоможуть захистити обліковий запис:

- наявність надійного пароля, який не використовується на інших веб-сайтах;

- використання двофакторної аутентифікації. Для запиту посилання або коду для зміни пароля буде потрібна адреса електронної пошти або номер телефону;

- обережність щодо підозрілих посиланнь і перед введенням облікових даних - необхідно завжди перевіряти, чи дійсно людина перебуває на сайті twitter.com;

- користувач не повинен повідомляти власне ім'я та пароль стороннім особам, особливо якщо ці особи обіцяють збільшити число читачів, пропонують заробити або підтвердити справжність облікового запису;

- слідкувати за тим, щоб на комп'ютері було встановлено останню версію програмного забезпечення, в тому числі браузера, з усіма необхідними виправленнями, оновленнями і антивірусними засобами.

Рекомендації Twitter зі створення пароля

Рекомендується придумати для власного облікового запису в Twitter надійний унікальний пароль. Слід поставити надійний унікальний пароль для адреси електронної пошти, пов'язаної з власним обліковим записом в Twitter.

Рекомендується також:

- створити пароль, що складається як мінімум з 10 символів і поєднує заголовні й малі букви, цифри і символи;

- використовувати різні паролі на різних відвідуваних веб-сайтах;

- зберігати пароль у безпечному місці. Рекомендується використовувати програмне забезпечення для управління паролями, за допомогою якого можна безпечно зберігати всі облікові дані.

При цьому категорично не рекомендується використовувати:

- особисті відомості, такі як номери телефонів, дні народження та іншу персональну інформацію в якості паролів;

- загальновживані слова зі словника, наприклад «пароль», «любов» і т. ін.;

- алфавітні і цифрові послідовності, наприклад «abcd1234», або послідовності клавіш на клавіатурі, наприклад «qwerty»;

- використовувати один і той же пароль на декількох веб-сайтах. Пароль облікового запису в Twitter повинен призначатися тільки для соціальної мережі Twitter.

Крім того, можна вибрати пункт «Запитувати особисту інформацію для зміни пароля» в розділі налаштувань «Обліковий запис». Якщо встановити цей прапорець, для зміни забутого пароля буде потрібно ввести або адресу електронної пошти, або номер телефону, або спочатку адресу електронної пошти, а потім номер телефону, якщо вони обидва були прив'язані до облікового запису на випадок втрати пароля, щоб користувачі могли отримати посилання або код підтвердження на пошту або на телефон.

Рис.3.2. Екран налаштувань безпеки акаунта в Twitter

Використання двофакторної аутентифікації

Двофакторна аутентифікація - це додатковий рівень безпеки облікового запису в Twitter і по суті є другим рівнем захисту, який з високою часткою ймовірності гарантує, що сторонні особи не отримають доступ до облікового запису в Twitter. Увійти в обліковий запис зможуть тільки ті люди, які мають доступ і до паролю, і до мобільного телефону (або ключа безпеки).

Перевірка місця знаходження користувача безпосередньо на twitter.com

Фішинг - це спроба обманним шляхом дізнатися ім'я користувача в Twitter, адресу електронної пошти або номер телефону і пароль, як правило, з метою розсилки спаму від чужого імені. Найчастіше шахраї намагаються обдурити користувачів, пропонуючи посилання, що веде на підроблену сторінку входу. Побачивши запит на введення пароля від облікового запису в Twitter, слід перевірити URL-адресу в адресному рядку браузера і переконатися, що користувач соціальної мережі знаходиться на сайті twitter.com. Крім того, якщо прийшло приватне повідомлення (навіть від друга) з підозрілою URL-адресою, рекомендується не переходити за таким посиланням.

Фішингові веб-сайти, як правило, схожі на сторінку входу в Twitter, але не мають до Twitter ніякого відношення. Домени Twitter завжди містять базовий домен https://twitter.com/. Нижче наведені деякі приклади сторінок входу в Twitte:

- https://twitter.com
- https://twitter.com/login

Якщо у користувачів немає впевненості в тому, що вони знаходяться на цій сторінці, можна відкрити сайт twitter.com і ввести облікові дані на ньому. Якщо вони вважають, що стали жертвами фішингу, рекомендується якомога швидше змінити пароль і ознайомитися з додатковими інструкціями.

Twitter не просить користувачів надати пароль

Twitter ніколи не просить надіслати пароль електронною поштою, в особистому повідомленні або у відповіді. Twitter ніколи не просить завантажити будь-що зі сторінки, яка не належить до соціальної мережі, або виконати вхід на подібну сторінку. Ніколи не варто відкривати вкладення і встановлювати будь-які програмні забезпечення, які прийшли в повідомленні електронної пошти, у відправниках якого вказано Twitter.

Якщо Twitter запідозрить, що обліковий запис піддався фішингу або був зламаний, то може змінити пароль даного користувача, щоб хакер не зміг використовувати обліковий запис в незаконних цілях. У цьому випадку Twitter відправить користувачеві електронного листа з посиланням на сайт twitter.com для зміни пароля.

Повідомлення про вхід в обліковий запис з невідомого або підозрілого пристрою

У разі, якщо буде виявлено вхід в обліковий запис в Twitter з підозрілого або нового пристрою, Twitter відправить push-повідомлення через власний додаток або електронною поштою для додаткового захисту користувацького облікового запису. Повідомлення про вхід в обліковий запис відправляються тільки, якщо користувач увійшов за допомогою програми «Twitter для iOS» або «Twitter для Android», через сайт twitter.com або мобільну версію сайту.

Такі повідомлення дозволяють упевнитися, що з нового пристрою зайшли дійсно власники акаунтів. Якщо користувачі не заходили в Twitter з вказаного пристрою, слід виконати дії, описані в повідомленні, щоб захистити обліковий запис. Для початку рекомендується негайно змінити пароль в Twitter. Також, важливо звернути увагу, що місце розташування в повідомленні зазначено лише приблизно на основі IP-адреси, з якого здійснювався вхід в Twitter, і може не збігатися з фактичним місцезнаходженням.

Перевірка посилань в Twitter

Багато користувачів Twitter використовують сервіси по скороченню посилань, наприклад bit.ly або TinyURL, для створення унікальних коротких посилань, якими простіше ділитися в твітах. Однак сервіси по скороченню посилань дозволяють приховати кінцевий домен, тому зрозуміти, куди веде посилання, дуже складно. Для деяких браузерів, наприклад, Chrome і Firefox, розроблені безкоштовні модулі, які показують повні URL-адреси без необхідності переходу за посиланнями.

Завжди рекомендується дотримуватися обережності при переході за посиланнями. Якщо користувачі натиснули посилання і несподівано виявилися на сторінці, яка схожа на сторінку входу в Twitter, не слід вводити ім'я користувача і пароль. Замість цього рекомендується відкрити сайт twitter.com і ввійти на головну сторінку Twitter.

Установка оновлень і захист від вірусів на комп'ютері і в браузері

Важливо оновлювати браузер і операційну систему з використанням найновіших версій і виправлень, які власне випускаються для усунення встановлених раніше загроз безпеки. Тому слід регулярно перевіряти комп'ютер на наявність вірусів, а також шпигунського і рекламного ПЗ. При використанні загальнодоступного комп'ютера обов'язково необхідно виходити з Twitter перед завершенням роботи.

Ретельний вибір сторонніх додатків

Незалежні розробники створили на платформі Twitter безліч сторонніх додатків, які можна використовувати з обліковими записами в Twitter. Однак слід з обережністю надавати стороннім додаткам доступ до облікового запису.

Якщо користувачі хочуть надати сторонньому додатку доступ до облікового запису, рекомендується використовувати метод перевірки автентичності Twitter - OAuth. Це безпечний спосіб підключення, при якому не потрібно повідомляти ім'я користувача і пароль в Twitter третім особам.

Необхідно проявляти особливу обережність, якщо просять повідомити ім'я користувача і пароль в додатку або на веб-сайті, оскільки стороннім додаткам не потрібні ім'я користувача і пароль для доступу до облікового запису з використанням методу OAuth. Якщо користувачі нададуть іншій людині ім'я користувача і пароль, то у третіх осіб з'явиться повний доступ до облікового запису з можливістю блокування дій або здійснення від чужого імені дій, які призведуть до призупинення користувацького облікового запису [38].

Також, рекомендується час від часу перевіряти, яким стороннім додаткам надано доступ до облікового запису. Відкликати доступ у незнайомих додатків або додатків, які твітять від імені користувача, можна на вкладці «Додатки» в налаштуваннях облікового запису.

Можливості забезпечення безпеки і конфіденційності в Twitter

Налагодження та використання PIN-коду для SMS

Якщо користувач турбується, що хтось може отримати доступ до облікового запису обманним шляхом, можна задати короткий PIN-код (personal identification number, особистий ідентифікаційний номер), який потрібно буде вказувати перед мобільними оновленнями і командами. Для забезпечення безпеки нікому не варто повідомляти PIN-код.

Якщо для облікового запису включене введення PIN-коду, його потрібно додавати перед текстом твіту або SMS-командою, яку користувач відправляє на короткий номер Twitter. Якщо користувач забуде ввести PIN-код перед текстом повідомлення, то прийде повідомлення «Введено невірний PIN-код». Якщо

користувачеві прийшло таке повідомлення, необхідно відправити SMS ще раз, вказавши PIN-код на його початку.

Використання двофакторної аутентифікації

Як зазначалося, двофакторна аутентифікація – це додатковий рівень безпеки облікового запису в Twitter, яка передбачає введення коду або секретного ключа для входу в обліковий запис. Цей додатковий крок гарантує, що ніхто інший не зможе зайти в обліковий запис. Після включення даної функції для входу в обліковий запис буде необхідний пароль, а також додаткові методи захисту: код, підтвердження входу через додаток чи фізичний ключ безпеки.

Вхід в обліковий запис за допомогою аутентифікації через додаток

Користувачам можуть запронувати підключити додаток аутентифікації до облікового запису в Twitter за допомогою QR-кода. Якщо додаток не встановлено на пристрої, його необхідно скачати. Можна використати будь-який додаток для створення одноразових паролей для захищеної аутентифікації, як наприклад Google Authenticator, Authy, Duo Mobile, 1Password тощо. Таким чином користувачі зможуть бачити і використовувати коди для входу в обліковий запис у Twitter.

Вхід в обліковий запис за допомогою секретного ключа

Щоб почати налаштування, необхідно включити функцію двофакторної аутентифікації за допомогою текстового повідомлення чи додатку аутентифікації. Рекомендовано натиснути на «Секретний ключ», потім прочитати загальні інструкції, а потім натиснути «Почати». Після чого, можна вставити фізичний ключ безпеки в USB-порт комп’ютера. Необхідно дотримуватися наведених на екрані інструкцій, щоб завершити налаштування. Щоб додати секретний ключ або увійти з його допомогою в обліковий запис, необхідно використовувати нову версію браузера Chrome, Edge, Firefox, Opera або Safari.

Тимчасові паролі

Після включення двофакторної аутентифікації на сайті twitter.com необхідно використовувати тимчасовий пароль для входу в Twitter на інших пристроях і в додатках, що вимагають введення пароля облікового запису в Twitter. Увійти в

обліковий запис за допомогою звичайного імені користувача і пароля не можна. Якщо буде потрібно тимчасовий пароль, Twitter надішле його в SMS-повідомленні на телефон користувача. Також згенерувати тимчасовий пароль можна самостійно.

Відкриті і захищені твіти

Різниця між відкритими і захищеними твітами полягає в тому, що при реєстрації облікового запису в Twitter твіти нового користувача за замовчуванням відкриті. Це означає, що будь-який інший користувач може переглядати їх і взаємодіяти з ними. При бажанні можна включити захист твітів, змінивши відповідні налаштування облікового запису.

Якщо твіти захищені, користувачі отримують запити на читання від інших користувачів, які хочуть читати їхні повідомлення, і можуть відхиляти або приймати ці запити. Ті користувачі, які почали читати записи іншого користувача, до того, як користувач включив захист твітів, як і раніше можуть переглядати власні захищені твіти та взаємодіяти з ними, якщо тільки користувач не внесе їх в чорний список.

Хто може бачити твіти

Відкриті твіти (налаштування за замовчуванням) видно всім користувачам, в тому числі тим, що не мають облікового запису в Twitter. Захищені твіти видно тільки читачам користувача в Twitter. Важливо пам'ятати, що читачі користувачів можуть робити скріншоти твітів і ділитися ними. Якщо надати доступ до власного облікового запису сторонньому додатку, цей додаток отримає доступ і до захищених твітів. Якщо користувачі діляться будь-якими матеріалами чи інформацією з іншими користувачами Twitter, вони можуть завантажити такі матеріали або інформацію на свій комп'ютер і поділитися ними з іншими читачами.

Налаштування видимості профілю

Нижче наведена інформація про налаштування видимості профілю та про те, як Twitter використовує інформацію про дату народження користувача, якщо вона додана в профіль.

Параметри видимості

Переважна частина інформації профілю завжди є відкритою. Це, наприклад, відомості про особу, місцезнаходження, веб-сайт і фотографії. Для деяких полів інформації в профілі Twitter пропонує налаштування видимості, за допомогою яких всі користувачі можуть вибрати, які інші користувачі Twitter зможуть побачити цю інформацію в профілі. Якщо користувачі не знайшли налаштувань видимості для тієї чи іншої інформації в профілі, це означає, що інформація є відкритою.

У налаштуваннях також можна вибрати, які користувачі Twitter зможуть побачити рік народження, а також точну дату (день і місяць) народження в профілі. Варто звернути увагу, що вказати потрібно день народження особи, яка управляє обліковим записом. У категорії аудиторій для обмеження доступу входять:

- Усі. Дана інформація буде загальнодоступною, іншими словами, будь-яка людина зможе її побачити.
- Читачі користувача. Дану інформацію в профілі зможуть побачити тільки читачі користувача.
- Інші користувачі, які читають повідомлення даного користувача. Дану інформацію в профілі зможуть побачити тільки ті користувачі, яких читає людина.
- Взаємне читання один одного. Дану інформацію в профілі зможуть побачити тільки ті користувачі, яких людина читає і які читають її.
- Тільки власник акаунта. Дану інформацію зможе побачити тільки власник облікового запису в Twitter. Якщо користувачу менше 18 років, для року народження буде застосовано дане налаштування. Після того, як користувачу виповниться 18 років, з'явиться можливість змінити це налаштування, вибравши будь-яке інше.

Можливість знайти людину за адресою електронної пошти та номером телефону

Адреса електронної пошти и номер телефону

Як правило, найчастіше користувачі спілкуються в Twitter з людьми, яких уже знають. Щоб було простіше почати спілкування з цими людьми, Twitter

використовує призначену для користувача адресу електронної пошти і номер телефону. За допомогою налаштувань конфіденційності «Можливість знаходити людину» можна дозволити або заборонити іншим користувачам знаходити користувача в Twitter за адресою електронної пошти або номером телефону. Якщо користувач заборонить іншим користувачам знаходити акаунт за адресою електронної пошти або номером телефону, Twitter також не використовуватиме контакти з призначеної для користувача адресної книги (якщо їх завантажили), щоб пропонувати цей обліковий запис іншим користувачам.

Якщо адреса електронної пошти або номер телефону даного користувача є у списку контактів будь-якого іншого користувача, той, у свою чергу, може знайти акаунт даної людини, завантаживши особисті контакти в Twitter. Якщо адреса електронної пошти або номер телефону вказаний у контактах, завантажених іншим користувачем, обліковий запис може з'явитися у списку рекомендацій цього користувача.

Користувацькі адресу електронної пошти і номер телефону не відображаються публічно в Twitter, навіть якщо користувачі включили налаштування, що дозволяє іншим користувачам знаходити користувача за адресою електронної пошти або номером телефону [39].

Небезпечні посилання

Коли в Twitter відображається попередження про небезпечне посилання, це означає, що його URL-адресу виявлено в базі даних потенційно шкідливих URL-адрес, а одже відповідні сторінки можуть становити небезпеку, пов'язану з фішингом, шкідливим ПЗ або спамом, або їх творці були викриті в порушенні Умов надання послуг Twitter. Таке попередження може з'являтися:

- при додаванні посилань у твіт;
- при додаванні посилань у профіль;
- при переході за посиланням через службу скорочення посилань Twitter http://t.co .

3.3. Загальні вимоги безпеки профіля користувача і захисту персональних даних в соцмережах

Нижче представлені основні правила, яких потрібно дотримуватися для збільшення особистої безпеки та захисту персональних даних у соцмережах.

Серйозне ставлення до безпеки в соціальних мережах

Реєструючись у соціальній мережі, користувачі, за рідкісними винятками, не дотримуються анонімності. Більшість діляться світлинами, уподобаннями в музиці, підписками на сторінки, які їх цікавлять - все це елементи профілю, за якими людину знайдуть друзі і знайомі, а також маркетологи або шахраї. Це, в свою чергу означає, що всю цю інформацію можна продати.

Проблема в тому, що багато власників даних за гроші поділяться не лише інформацією про товари, які користувачі шукали онлайн, але і більш особистими даними. Тому контент, який людина не готова афішувати на весь світ, не можна завантажувати в Інтернет узагалі: ні в закриті альбоми, ні в особисті повідомлення. Рекомендується ставитися до цього серйозно і кожному користувачеві заздалегідь враховувати, від опублікування якої інформації можуть з'явитися негативні наслідки в майбутньому.

Контроль за старими акаунтами в соціальних мережах.

Отримавши доступ до закинутого аккаунту, можна використовувати його в дискредитуючій формі, публікувати за допомогою даних акаунтів рекламну і не тільки інформацію. Щоб уникнути цього, варто використовувати інструменти для контролю відразу за декількома акаунтами, що дозволять контролювати роботу багатьох сторінок.

Відстеження заявок у «друзі»

За інформацією The Telegraph, Facebook визнав, що 270 млн. акаунтів у соціальній мережі - фальшиві або дублікати вже існуючих. За визначенням Facebook, фальшивий акаунт - це акаунт, власник якого видає себе за когось неіснуючого, або акаунт вигаданої людини, тварини, організації або знаменитості.

Небезпека таких акаунтів в тому, що їх часто використовують для поширення рекламної інформації, фейкових новин і навіть пропаганди насильства та екстремізму. Наявність такого «друга» в історії може негативно позначитися на репутації сторінки або, що небезпечніше, використовуватися для отримання доступу до персональної інформації користувачів.

Використання складних паролів

Рекомендується уникати таких шаблонних рішень, як безперервна черговість цифр, послідовність простих символів, літер на клавіатурі. Не варто використовувати в якості пароля особисте ім'я, прізвище, країну походження і все те, на що в першу чергу зверне увагу потенційний зломщик аккаунта.

Пароль повинен містити принаймні 10 символів. Це повинна бути практично випадкова комбінація літер різного реєстру, цифр і символів. Щоб запам'ятати таку складну послідовність, можна, наприклад, створювати пароль за принципом абревіатури. Можна придумати фразу (абсурдну або смішну) і використовувати в якості пароля перші літери слів. Потім доповнити цифрами та іншими символами. І, звичайно, в подальшому нікому не розповідати про власний шифр.

Ще один спосіб - використовувати менеджери паролів. Вони допоможуть і підібрати ефективні паролі, і зберегти їх.

Налаштування двофакторної аутентифікації

Ще один традиційний інструмент, що дозволяє підвищити рівень безпеки для сторінки в соціальній мережі, - двофакторна аутентифікація. Більшість соціальних мереж пропонують кілька варіантів такої верифікації: текстові повідомлення з кодом на телефон, коди безпеки з генератора кодів або стороннього додатка, схвалення спроби входу з іншого, вже розпізнаного пристрою і навіть 10 кодів, які користувач може роздрукувати і зберігати в безпечному місці.

Читання користувацьких угод

Рекомендується уважно читати правила соціальних мереж, в яких передбачається реєстрація, перш ніж створити обліковий запис. Особливу увагу слід приділяти політиці безпеки. Не слід ділиться конфіденційною інформацією. Не варто використовувати сторінку в соціальній мережі для реєстрації на сайтах,

які запитують доступ до особистої інформації та інформації про друзів. Багато сайтів зараз пропонують авторизуватися через соціальні мережі, щоб проголосувати в опитуванні, залишити коментар або дізнатися результати тесту.

Крім того, не варто анонсувати на сторінці власні плани на майбутнє. Інформацією про те, що користувач в найближчі вихідні можливо полетить в іншу країну, можуть скористатися квартирні грабіжники [40].

Важливо звертати увагу на те, що публікують і чим діляться користувачі на сторінках. Не рекомендується ділитися забороненим або підозрілим контентом. А також, варто стежити за коментарями. Мова не тільки про коментарі, які користувачі залишають на інших ресурсах, а й про коментарі, які інші залишають на сторінці користувача. Іноді найгірший удар по онлайн-репутації завдають не зломи акаунтів і публікація особистих даних, а необдумані жарти, в яких хтось може побачити грубість, або необережні висловлювання друзів в коментарях.

Видалення неактивних акаунтів

У основної маси користувачів соціальних мереж є кілька сторінок, в тій чи іншій соціальній мережі, про які вже давно забули, але важливо пам'ятати, що там знаходиться особиста інформація, яку швидше за все ніхто не видаляв. Якщо людина вже не користується соціальними мережами, то рекомендується видалити закинуті облікові записи, щоб не залишати персональну інформацію в загальному доступі, навіть якщо вона застаріла, це все одно може стати важелем тиску на людину з боку шахраїв.

Не варто публікувати дати народження

Дата народження - один з головних атрибутів особистості, тому дату народження краще не вказувати. Якщо користувач вирішив опублікувати дані про день народження, рекомендується вказувати тільки день і місяць народження. Цього буде достатньо для привітань від друзів і в той же час більш безпечно.

Закрити відображення сімейного стану

Яким би не був сімейний стан, ця інформація не повинна бути надбанням громадськості. Даний пункт профілю може стати джерелом небажаних наслідків для людини, тому йому краще завжди залишатися порожнім.

Відключити відображення місця розташування

Багато людей сповіщають про своє місцезнаходження в соціальних мережах, що багато фахівців з інформаційної безпеки радять не робити. Відносно розташування рекомендується використовувати тільки минулий час, але не сьогодення і майбутнє.

Не повідомляти, що вдома відсутні люди

Вкрай важливо, щоб батьки переконалися, в тому, що їхні діти не вказують на своїх сторінках інформацію, що зараз вдома самі або будуть без дорослих в певний час, оскільки такою інформацією можуть скористатися шахраї або квартирні злодії.

Користувачі соціальних мереж можуть використовувати найсуворіші правила конфіденційності і розраховувати на безпеку в соціальних мережах, але завжди буде наявний чинник людської безпечності.

Не розміщувати інформацію про дітей

Дуже багато батьків розміщують повні імена власних дітей, дати їх народження, імена родичів і багато іншого. Насправді, подібної інформації може бути цілком достатньо, щоб зловмисники змогли втертися в довіру до дитини. Якщо виникла необхідність розміщення фото дитини, то, принаймні, варто видалити всю особисту інформацію про дитину (прізвище, ім'я, дата народження) [41].

Не застосовувати функціонал «запам'ятати мене» при вході

Якщо комп'ютер загальний і знаходиться на робочому місці в офісі або взагалі випадковий - Інтернет-кафе або вдома у знайомих - не слід залишати в ньому свій пароль і логін. Варто переконатися, що галочка «запам'ятати мене» не стоїть при введенні логіна-пароля і що вони не будуть збережені на цьому пристрої. Подібний захід захистить аккаунт від злому, використання в розсилці спаму, крадіжки особистих даних.

Не відкривати вкладені файли в повідомленнях

Більшість хакерів використовують картинку-вкладення в листі, яка містить хакерський скрипт, створений для перехоплення пароля від соціальної мережі. Якщо користувач не впевнений в особистості автора повідомлення із вкладенням,

не рекомендується відкривати вкладення, а слід переконатися, що спілкування буде вестися саме з цією людиною, а не з кимось іншим. Також варто пам’ятати: чим більш невідомий відправник наполягає на відкритті вкладення, тим більша ймовірність, що це хакер.

Загальні рекомендації щодо безпеки акаунта користувача й забезпечення конфіденційності персональних даних у соцмережах можна представити у вигляді схеми [40,41,42] (Рис. 3.3.).

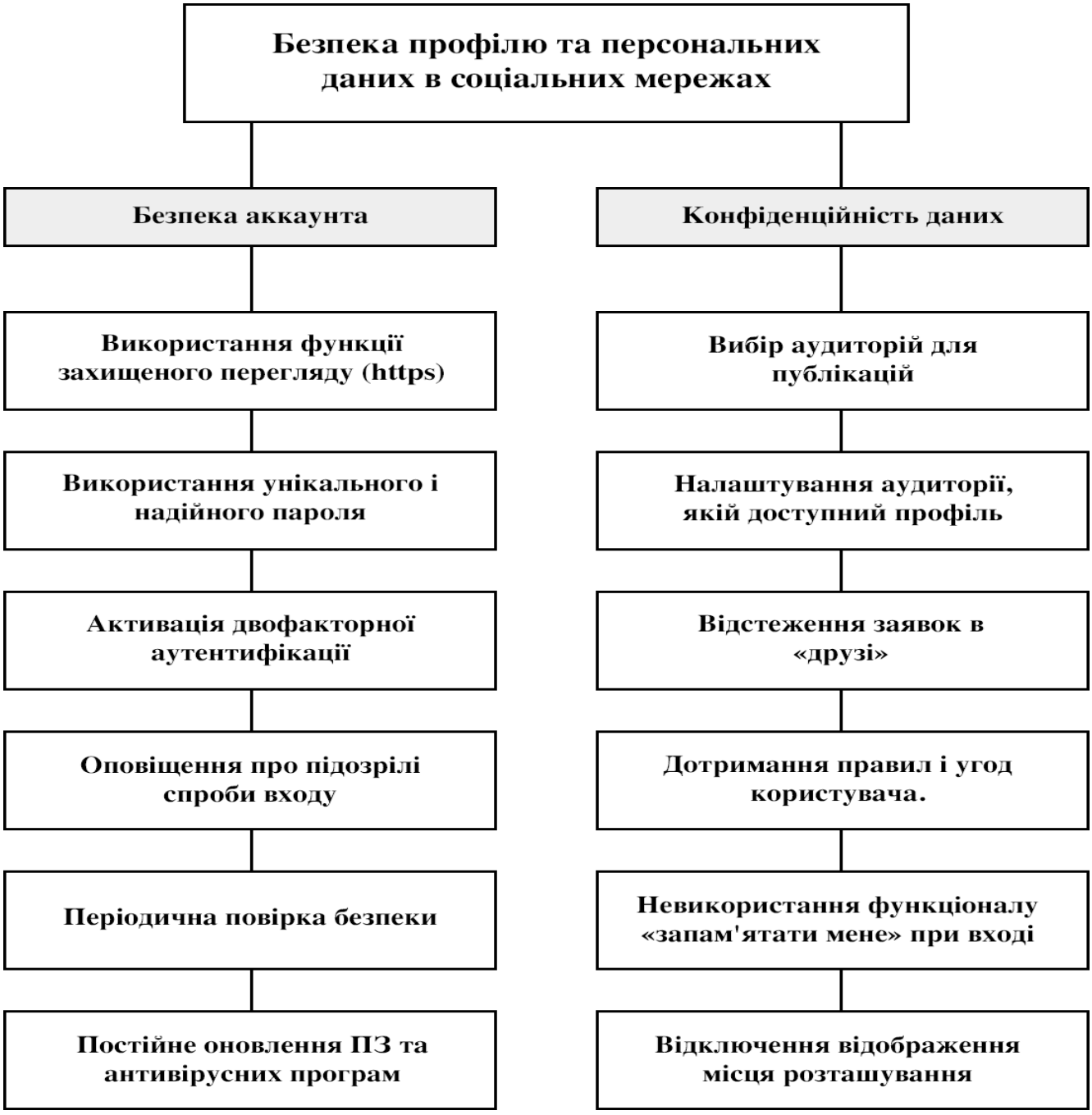

Рис. 3.3. Загальні рекомендації щодо безпеки облікового запису користувача й забезпечення конфіденційності персональних даних у соцмережах.

Висновки до третього розділу

На підставі розгляду технічних можливостей забезпечення безпеки і конфіденційності даних, що надаються в соціальних мережах Facebook і Twitter, зроблено висновок, що обрані соцмережі пропонують своїм користувачам широкий перелік технічних методів захисту конфіденційності даних, зокрема: двофакторну аутентифікацію, генератор кодів, функції перевірки безпеки й одноразових паролів, повідомлення про підозрілі спроби входу, сторонні додатки для додаткової аутентифікації, функцію ключів безпеки, налаштування аудиторій для видимості профілю або опублікованих матеріалів тощо.

Проаналізувавши загальні заходи і рекомендації фахівців з інформаційної безпеки, виділено три основні групи вимог щодо захисту персональних даних, а саме: використання механізмів безпеки, що надаються соціальними мережами, використання загальних механізмів безпеки, не прив'язаних із соціальними мережами, а також безпечне перебування в соціальних мережах, без вчинення дій, що потенційно становлять загрози персональним даним.

ВИСНОВКИ

Вивчення положень Загального регламенту захисту персональних даних ЄС (GDPR) показав, що нормативний акт визначає персональні дані досить широко, відносячи до особистих даних не лише інформацію, яка прямо ідентифікує особу, але й інформацію, яка в сукупності з іншими даними може бути використана для ідентифікації особи. Регламент встановлює основні принципи безпечного використання й обробки персональних даних, зокрема принципи мінімізації даних, обмеження часу їх зберігання, забезпечення цілісності і конфіденційності, підзвітності й відповідальності за обробку персональних даних.

У результаті аналізу нормативно-правової бази щодо забезпечення безпеки та обробки персональних даних в Україні встановлено, що вітчизняна система захисту персональних даних, в тому числі питання збору, обробки та забезпечення їх безпеки, потребують розвитку. При чому вектор цього розвитку має бути спрямований на вивчення і адаптування найбільш прогресивних норм західних нормативних документів, в тому числі GDPR. Оскільки країни Європейського Союзу вже пройшли цей шлях, поступово вибудовували системи, усували слабкі місця і адаптувалися до нових умов.

Розгляд положень призначених для користувача угод соціальних мереж Facebook і Twitter показав, що кожен користувач несе особисту відповідальність за контент, який публікується, в тому числі й персональні дані, і має усвідомлювати наявність загроз і відповідати за свої дії в соцмережі. Використовуючи загальнодоступні дані в особистих цілях, користувач повинен дотримуватись законних прав та інтересів тих осіб, яким належать дані. При створенні облікового запису або додаванні контенту користувач вносить цю інформацію в базу даних, яка належить правовласнику соціальної мережі, відповідно, надає йому виключне право на право використання цих даних.

Встановлено, що для соціальних мереж характерні як інформаційно-технічні, так і інформаційно-психологічні загрози безпеки даних користувачів. Наслідки успішної атаки на персональні дані власника облікового запису можуть включати:

крадіжку особистих даних власника, в тому числі особисту переписку, світлини; використання профілю в шахрайських цілях шляхом експлуатації довіри друзів атакованого користувача; дискредитацію або деанонімізацію власника профілю. Для захисту від інформаційно-технічних загроз використовують традиційні засоби (стійкі паролі, антивірусне ПЗ та ін.), а різні сервіси надають різні способи вирішення цих проблем.

Оскільки соціальні мережі є ідеальним середовищем для маніпулювання інформацією, яка в них циркулює, і здійснення різних впливів на свідомість користувачів, найбільш поширеними прикладами інформаційно-психологічних загроз є методи використання соціальної інженерії. Питання захисту користувачів соціальних мереж від інформаційно-психологічних загроз сьогодні опрацьовано недостатньо, і безпека даних користувачів у переважній більшості залежить від їх правильної поведінки, знання і виконання вимог інформаційної безпеки.

Вивчення методів атак на персональні дані і пов'язаних з ними шахрайських дій дозволило виділити такі основні види зазначених протиправних дій в соцмережах як: опитування, тести і конкурси для збору даних, скорочені URL-адреси, повідомлення про надзвичайні ситуації, підроблені Plug-in, запити дозволів, підробні додатки, крадіжки маркерів доступу.

Масштаби і різноманітність злочинів, спрямованих на оприлюднення і незаконне використання персональних даних в соціальних мережах, постійно зростають, і про це свідчать випадки масового злому акаунтів користувачів соцмереж, витоків даних багатьох мільйонів їхніх користувачів, незаконного збору особистої інформації власників акаунтів в соцмережах часто з метою подальшого маніпулювання їх свідомістю або фінансового шахрайства.

На підставі розгляду технічних можливостей забезпечення безпеки і конфіденційності даних, що надаються в соціальних мережах Facebook і Twitter, зроблено висновки, що обрані соцмережі пропонують своїм користувачам широкий перелік технічних можливостей забезпечення безпеки і конфіденційності даних, зокрема: двофакторну аутентифікацію, генератор кодів, функції перевірки безпеки й одноразових паролів, повідомлення про підозрілі

спроби входу, сторонні додатки для додаткової аутентифікації, функцію ключів безпеки, налаштування аудиторій для видимості профілю або опублікованих матеріалів і багато іншого.

Проаналізувавши загальні заходи і рекомендації фахівців з інформаційної безпеки, виділено три основні групи вимог до захисту персональних даних: використання механізмів безпеки, що надаються соціальними мережами, використання загальних механізмів безпеки, не прив'язаних до соціальних мереж, а також безпечне поводження в соціальних мережах, без вчинення дій, що потенційно становлять загрози персональним даним.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Nadeau M. General Data Protection Regulation (GDPR): What you need to know to stay compliant. URL: https://www.csoonline.com/article/ 3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html (дата звернення: 25.12.2020)

2. General Data Protection Regulation. GDPR. URL: https://gdpr-info.eu/(дата звернення: 25.12.2020)

3. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481

4. Куценко С. Захист особистих та персональних даних в Інтернеті: проблеми законодавчого врегулювання. URL: https://ukrainepravo.com/scientific-thought/legal_analyst/zakhist-osobistikh-ta-personalnikh-danikh-v-interneti-problemi-zakonodavchogo-vregulyuvannya (дата звернення: 25.12.2020)

5. Куничак О. Чи має GDPR майбутнє в Україні? URL: https://biz.ligazakon.net/ analitycs/193376_chi-magdprmaybutn-v-ukran (дата звернення: 25.12.2020)

6. Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних: Закон України від 06.07.2010 № 2438-VI. Відомості Верховної Ради України (ВВР), 2010, N 46, ст.542.

7. Про захист фізичних осіб при обробці персональних даних про вільне переміщення таких даних: Директива Європейського Парламенту і Ради від 24.10.1995 № 95/46/ЄС. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text

8. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481

9. Журлов Н. Соцсети и общедоступные данные пользователей. URL: https://vc.ru/legal/64191-socseti-i-obshchedostupnye-dannye-polzovateley (дата звернення: 25.12.2020)

10. Черниш Р. Соціальні мережі як один із інструментів накопичення та протиправного використання персональних даних громадян. *Проблеми законності*. 2017. Вип. 136. С.205-214. URL: http://plaw.nlu.edu.ua/article/viewFile/93352/92225 (дата звернення: 25.12.2020)

11. Facebook Terms of Service. URL: https://www.facebook.com/terms (дата звернення: 25.12.2020)

12. Twitter Terms of Service. URL: https://twitter.com/en/tos (дата звернення: 25.12.2020)

13. Проноза А., Чечулин А., Комашинский Н. Угрозы безопасности в социальных сетях и защита от информации. *Региональная информатика и информационная безопасность: сборник трудов.* 2017. СПОИСУ. Санкт-Петербург. 2018. Вып. 6. С. 259-261.

14. Социальные сети: актуальные киберугрозы и способы защиты. URL: https://itbiz.ua/socialnye-setiaktualnye-kiberugr (дата звернення: 25.12.2020)

15. Christopher Hadnagy. Social Engineering: The Art of Human Hacking. Second Edition, 2010. 416 p.

16. Гавловський В. До питання захисту персональних даних у соціальних мережах. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2011. № 24. С.252-262.

17. Атагимова Э. «Кража личности» как самостоятельное преступление или разновидность мошенничества. URL: https://cyberleninka.ru/article/n/krazha-lichnosti-kak-samostoyatelnoe-prestuplenie-ili-raznovidnost-moshennichestva (дата звернення: 25.12.2020)

18. Актуальные киберугрозы – 2018. Тренды и прогнозы. URL: https://www.ptsecurity.com/ruru/research/analytics/cybersecurity-threatscape-2018/ (дата звернення: 25.12.2020)

19. Актуальные киберугрозы. I квартал 2019 года. URL: https://www.ptsecurity.com/ruru/research/analytics/cybersecurity-threatscape-q1-2019/ (дата звернення: 25.12.2020)

20. Бураева Л. А. Социальные сети как угроза информационной безопасности. URL: https://cyberleninka.ru/article/v/sotsialnye-seti-kak-ugroza-informatsionnoy-bezopasnosti (дата звернення: 25.12.2020)

21. Прудка Л. Психологічні особливості шахрайства в мережі Інтернет. Південноукраїнський правничий часопис. *Протидія злочинності: проблеми практики та науково-методичне забезпечення*. 2018. №2. С.30-33.

22. Дезінформація та маніпуляції. Клікбейт. VERIFIED: онлайн-курс з медіаграмотності. URL: https://verified.ed-era.com/ua/manipulation/part-b (дата звернення: 25.12.2020)

23. Артемов Н. Психологические приемы. Социальная инженерия – технология «взлома» человека. URL: https://emisare.medium.com/socialnaya-ingeneria-9f16e0ba7fa5 (дата звернення: 25.12.2020)

24. What is "Likejacking"? URL: https://www.sophos.com/en-us/security-news-trends/security-trends/what-is-likejacking.aspx (дата звернення: 25.12.2020)

25. Седов О. Угрозы социальных сетей. URL: https://www.osp.ru/cio/2011/12/13012286 (дата звернення: 25.12.2020)

26. Подробнее о мошенничестве в социальных сетях. URL: https://support.norton.com/sp/ru/ru/home/current/solutions/v97291099 (дата звернення: 25.12.2020)

27. Романтические аферисты: кто попадает на их крючок. URL: https://www.psychologies.ru/articles/romanticheskie-aferistyi-kto-popadaet-na-ih-kryuchok/ (дата звернення: 25.12.2020)

28. Распространенные виды мошенничества на Facebook. URL: https://ru-ru.facebook.com/help/1674717642789671 (дата звернення: 25.12.2020)

29. Борисов П. Cambridge Analytica: компания, которая научилась «взламывать» выборы через Facebook. URL: https://meduza.io/feature/2018/03/19/cambridge-analytica-kompaniya-kotoraya-nauchilas-vzlamyvat-vybory-cherez-facebook (дата звернення: 25.12.2020)

30. Mark Zuckerberg testifies before Congress. URL: https://edition.cnn.com/politics/live-news/mark-zuckerberg-testifies-congress/index.html (дата звернення: 25.12.2020)

31. Twitter-мошенничество с биткойнами (2020). URL: https://www.wikiwand.com/ (дата звернення: 25.12.2020)

32. Хакеры продают данные миллионов пользователей сети LinkedIn. URL: https://www.bbc.com/russian/international/2016/05/160518_linkedin_accounts_hacked (дата звернення: 25.12.2020)

33. Сотни аккаунтов в Instagram были захвачены хакерами. URL: https://www.securitylab.ru/blog/company/PandaSecurityRus/344711.php (дата звернення: 25.12.2020)

34. 235 млн профилей пользователей Instagram, TikTok и YouTube оказались в открытом доступе. URL: https://internetua.com/235-mln-profilei-polzovatelei-instagram-tiktok-i-youtube-okazalis-v-otkrytom-dostupe (дата звернення: 25.12.2020)

35. Обеспечение безопасности аккаунта Facebook. URL: https://ru-ru.facebook.com/help/235353253505947/?helpref=hc_fnav (дата звернення: 25.12.2020)

36. Предупреждения о входе и двухфакторная аутентификация. URL: https://ru-ru.facebook.com/help/235353253505947/?helpref=hc_fnav (дата звернення: 25.12.2020)

37. Конфиденциальность пользователя Facebook. URL: https://ru-ru.facebook.com/help/235353253505947/?helpref=hc_fnav (дата звернення: 25.12.2020)

38. Безопасность учетной записи Twitter. URL: https://help.twitter.com/ru/safety-and-security/account-security-tips (дата звернення: 25.12.2020)

39. Конфиденциальность в Twitter. URL: https://help.twitter.com/ru/safety-and-security#ads-and-data-privacy (дата звернення: 25.12.2020)

40. Власко С. 7 правил безопасности в социальных сетях. URL: https://delo.ua/special/7-pravil-bezopasnosti-v-socialnyh-setjah-341379/ (дата звернення: 25.12.2020)

41. Горохов П. 10 вещей, которые нельзя публиковать в соцсетях. URL: https://www.ridus.ru/news/196092 (дата звернення: 25.12.2020)

42. Соцсети и общедоступные данные пользователей. URL: https://vc.ru/legal/64191-socseti-i-obshchedostupnye-dannye-polzovateley (дата звернення: 25.12.2020)