Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувачка кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього ступеня)

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

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Засоби захисту персональних даних в соціальних мережах та месенджерах»

Виконавець: студентка IV курсу, групи КБ-42

_____ **Юлія МАЙБОРОДА**
(підпис) (ім'я прізвище)

	Прізвище, ініціали	**Підпис**
Керівник	Лариса МИРУТЕНКО	

Нормоконтроль	Олександр ТОРОШАНКО	

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувачка кафедри кібербезпеки
та захисту інформації
_____ Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-42** **Юлії Юріївни Майбороди**
(група) (прізвище ім'я по батькові)

Тема дипломної роботи Засоби захисту персональних даних в соціальних мережах та месенджерах

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Різновиди соціальних мереж та месенджерів, види загроз на персональні дані користувачів соціальних мереж.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно провести аналіз нормативно-правових документів щодо захисту персональних даних, визначити вразливості в політиці конфіденційності в соціальних мережах та месенджерах, проаналізувати найбільш поширені методи злому месенджерів, розробити алгоритм що допоможе користувачу захистити персональні дані.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблені рекомендації можуть бути використані для дієвого захисту персональних даних у соціальних мережах та месенджерах.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29.10.2021 року

Завдання видав _____ (підпис) Лариса МИРУТЕНКО (ім'я, прізвище)

Завдання прийняла до виконання _____ (підпис) Юлія МАЙБОРОДА (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.10.2021 – 22.01.2022	*виконано*
2	Аналіз літератури	29.01.2022 – 11.02.2022	*виконано*
3	Обґрунтування вибору рішення	12.02.2022 – 15.02.2022	*виконано*
4	Аналіз нормативно-правової бази у сфері захисту персональних даних	16.02.2022 – 04.03.2022	*виконано*
5	Визначення вразливостей в політиці інформаційної безпеки в соціальних мережах та месенджерах та способи запобігання порушень безпеки	05.03.2022 – 21.03.2022	*виконано*
6	Аналіз методів злому месенджерів	22.03.2022 – 08.04.2022	*виконано*
7	Розробка алгоритму дій, що допоможе користувачу захистити персональні дані	09.04.2022 – 10.05.2022	*виконано*
8	Оформлення пояснювальної записки	11.05.2022 – 27.05.2022	*виконано*
9	Підготовка до захисту дипломної роботи	28.05.2022 – 13.06.2022	*виконано*

Завдання видав _____ (підпис) Лариса МИРУТЕНКО (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) Юлія МАЙБОРОДА (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, має 59 сторінок основного тексту, 1 таблицю та 11 рисунків. Список використаних джерел містить 33 найменування і займає 3 сторінки.

Об'єкт дослідження- процес забезпечення захисту персональних даних.

Предметом дослідження є методи та засоби захисту персональних даних в соціальних мережах та месенджерах.

Мета роботи - розробка рекомендацій щодо захисту персональних даних в месенджерах і соціальних мережах.

Для досягнення мети мають бути виконані наступні завдання:

- проаналізувати нормативно - правову базу у сфері захисту персональних даних;
- визначити вразливості в політиці інформаційної безпеки в соціальних мережах та месенджерах та способи уникнення порушень конфіденційності інформації;
- проаналізувати методи злому месенджерів;
- розробити алгоритм дій що допоможе користувачу захистити персональні дані.

Методи дослідження дипломної роботи:

- аналіз інформаційних ресурсів щодо даної теми;
- аналіз нормативно-правових документів;
- порівняння політики безпеки месенджерів та соціальних мереж.

Практична значимість дипломної роботи визначена можливостю використання розроблених рекомендацій для дієвого захисту персональних даних та месенджерах.

Ключові слова: загрози, захист даних, месенджери, персональні дані, соціальні мережі.

ЗМІСТ

ВСТУП

Соціальні мережі та месенджери розвиваються дуже бурхливо у всьому світі. Вони є однією з головних платформ для комунікації між людьми.

Порівняно нещодавно Інтернет був досить суворим середовищем і щоб скористатися його послугами потрібно було набирати інструкції в командному рядку UNIX і мати спеціальні знання в галузі програмування. У таких умовах людина, яка вирішує завдання отримання інформації і завжди обмежена в часі, не витрачатиме дорогі (у самому прямому сенсі) хвилини на спілкування в онлайн режимі.

Дослідження цієї теми є актуальним, оскільки соціальні мережі та месенджери є одним із найпопулярніших засобів спілкування в інтернет-просторі. Під соціальною мережею розуміється онлайн-сервіс, призначений задля забезпечення взаємовідносин між людьми чи організаціями в Інтернеті. За даними аналітичного агентства Statista, найпопулярнішою соціальною мережею у світі є Facebook, де налічується понад 3 млрд активних користувачів [1].

Соціальні мережі – це не тільки засіб спілкування, а й популярна платформа для створення, розміщення та просування медіаконтенту.

Месенджер –програма, що може бути мобільним додатком або веб-сервісом для миттєвих обмінів повідомленнями [2].

Найчастіше під месенджером розуміють програму, в яку можна писати повідомлення і де їх можна читати. Як правило, за кожною із таких програм стоїть мережа обміну повідомленнями, що також входить до поняття "месенджер". Мережа може бути як глобальною, так і знаходитись всередині компанії.

Потрібно сказати, що поняття месенджера вже давно не пов'язують лише з текстовими повідомленнями. Сучасні месенджери вже стали повноцінними комунікаційними центрами, які окрім обміну повідомленнями реалізують голосовий та відеозв’язок, обмін файлами, веб-конференції та багато іншого.

Актуальність цієї роботи пов'язані з виникненням потреби вивчення та аналізу засобів захисту персональних даних в соціальних мережах та месенджерах.

РОЗДІЛ 1АНАЛІЗ НОРМАТИВНО - ПРАВОВОЇ БАЗИ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

1.1 Загальний регламент із захисту даних у світі (GDPR)

У січні 2012 року Європейська комісія сформулювала плани щодо реформи

захисту даних у Європейському Союзі, щоб Європа "відповідала духу цифрової ери". Майже через чотири роки було досягнуто згоди про те, що ці перетворення передбачають і як вони будуть реалізовані. GDPR був виданий у 2016 році, набув чинності 25 травня 2018 року та діє не лише на європейському просторі.

Загальний регламент захисту даних (ЄС) 2016/679 ("GDPR") у законодавстві Європейського союзу є положенням про захист даних та конфіденційності для всіх осіб на території Європейського Союзу (ЄС) та Європейської економічної зони (ЄЕЗ). Він також стосується експорту персональних даних за межі ЄС та ЄЕЗ. GDPR спрямований насамперед на надання контролю фізичним особам над їх персональними даними та на спрощення правового регулювання для міжнародного бізнесу шляхом уніфікації становища в рамках ЄС.

Розглянемо ключові принципи GDPR:

1) поняття "персональні дані" означає будь-яку інформацію, що стосується ідентифікованої фізичної особи ("суб'єкт даних");

2) GDPR використовується для опрацювання персональних даних повністю або частково автоматизованими засобами та для обробки персональних даних іншими способами, відмінними від автоматизованих засобів, які є частиною системи реєстрації або призначені для формування системи реєстрації;

3) GDPR застосовується для обробки персональних даних у контексті діяльності установи контролера або процесора в Союзі, та не залежить від того, чи відбувається обробка в Союзі чи ні. Регламент поширюється на опрацювання персональних даних суб'єктів даних, що перебувають у Союзі, контролером або

процесором, не заснованим у Союзі. Якщо ж діяльність з опрацювання зв'язана з пропозицією товарів або послуг, незалежно від того, чи потрібна оплата суб'єкта даних таким суб'єктам даних у Союзі або моніторинг їхньої поведінки в тій мірі, в якій їхня поведінка відбувається на території Союзу;

4) персональні дані обробляються на засадах законності, справедливості та прозорості щодо суб'єкта персональних даних, способом, що забезпечує належну безпеку персональних даних;

5) персональні дані повинні збиратися для певних, чітко виражених та законних цілей і не піддаватися подальшій обробці способом, несумісним із цією метою;

6) персональні дані повинні бути достатніми, релевантними та обмежуватися тим, що необхідно для цілей, для яких вони обробляються; точними та, за необхідності, актуальними; зберігатися не довше, ніж це необхідно для цілей, для яких вони обробляються;

7) обробка здійснюється на підставі згоди суб'єкта даних або інших законних підстав, зазначених у статті 6 GDPR;

8) згода має бути вільно вираженою, визначеною, інформативною та чітко сформульованою вказівкою на побажання суб'єкта даних, за допомогою якого він, шляхом заяви або за допомогою чітких позитивних дій, що висловлюють згоду на опрацювання своїх персональних даних.

Слід звернути увагу до права суб'єкта даних. GDPR значно розширив цю категорію. У GDPR суб'єктам даних надаються такі права:

1) декларація про отримання інформації;
2) право доступу;
3) декларація про уточнення;
4) декларація про знищення;
5) декларація про обмеження обробки;
6) право на переносимість даних;
7) декларація про заперечення;

8) право не піддаватися автоматизованому прийняттю рішень в індивідуальному порядку, включаючи профайлінг, коли рішення матиме правові чи інші суттєві наслідки;

9) право на правовий захист.

Оскільки GDPR вже набув чинності, більшість контролерів і процесорів вже вжили дії з метою відповідності GDPR. Тим не менш, велика кількість компаній за межами Союзу все ще очікують здійснення процедур GDPR і задаються питанням, чи підпадають вони під дію GDPR чи ні. По-перше, вони повинні визначити свій статус відповідно до GDPR, чи є вони "контролером" та/або "процесором". Відповідно до GDPR, поняття "контролер" визначає фізичну чи юридичну особу, державний орган, агентство та ін., який самотужки або з допомогою інших осіб визначає цілі та засоби опрацювання персональних даних. "Процесор" означає фізичну чи юридичну особу, державний орган, агентство або інший орган, який опрацьовує персональні дані за дорученням контролера. По-друге, вони повинні визначити, чи вони опрацьовують персональні дані суб'єктів даних, які перебувають у Союзі. За дотримання цих вимог повинні бути вжиті такі мінімальні заходи:

1) призначення інспектора із захисту персональних даних, який інформуватиме та консультуватиме контролера або процесора та працівників, що здійснюють обробку, щодо своїх зобов'язань, стежити за дотриманням GDPR, співпрацювати з наглядовим органом;

2) розробка згоди, яка повинна відображати, що вона надається вільно, і суб'єкт даних (наприклад, клієнт або співробітник) "проінформований". Згода має містити право відкликати її у будь-який час;

3) проведення відповідних технічних та організаційних заходів для забезпечення рівня безпеки, що відповідає ризику;

4) розробка Кодексів поведінки, що відображають політику підприємства у сфері захисту даних;

5) розробка угод, які мають бути підписані між контролерами та процесорами даних, а також третіми особами, які беруть участь у процедурі обробки даних (аутсорсерами);

6) організація навчання персоналу.

Компанії, які підпадають під дію GDPR, повинні вжити заходів у найкоротший термін, оскільки штрафи досить високі: вони можуть сягати 4% від продажів до максимальної суми 20 млн. євро. Для забезпечення дотримання GDPR у найкоротший термін компанії можуть надавати на аутсорсинг третім особам питання, пов'язані з GDPR, або навчатися через різні освітні програми та отримувати юридичні консультації.

1.2 Нормативно-правова база щодо захисту персональних даних в Україні

Проект Закону України "Про захист персональних даних» регулює правові відносини, пов'язані із захистом та обробкою персональних даних. Він направлений на захист основних прав та свободи громадян України. Зокрема одним із основних аспектів є право не втручатись в особисте життя громадян України, у зв'язку з опрацювання їх особистих даних [3].

Даний Закон поширюється на діяльність з опрацювання персональних даних, що здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на опрацювання особистих даних, що містяться в картотеці або ті, що призначені для занесення в картотеки, із застосуванням ручних засобів.

Проєкт Закону України “Про захист персональних даних” №5628 було зареєстровано у Верховній Раді 7-го червня 2021-го року. Даний проєкт є значно кращим ніж діючий, тому що, він містить в собі більше визначень та детально визначає процедури. Багато норм є схожими або й по суті несуть в собі норми у GDPR Європейського Союзу. Законопроєкт №5628 прагне привести законодавство України про захист персональних даних у відповідність до актів Ради Європи та Євросоюзу. При цьому планується запровадити нові підходи до обробки та зберігання даних.

Найбільш позитивними аспектами проєкту є:

1) деталізованість процедур і визначень;
2) орієнтованість на методи Європейського суду з прав людини (ЄСПЛ);

3) запровадження принципу “захист персональних даних за проєктуванням і за замовчуванням”;

4) права суб’єктів персональних даних та обов’язки контролера й оператора визначені доволі конкретно;

5) добре регламентовано дії контролера у випадку витоків даних (data breach);

6) деталізовано ознаки згоди, питання цілей обробки даних.

Проаналізувавши даний законопроєкт можна виділити наступні недоліки:

1) у даному проєкті немає жодного розділу або навіть статті, що регламентувала б діяльність органу контролю;

2) також, занепокоєння викликають деякі зобов’язання перед контролюючим органом з боку оператора або контролера (наприклад, на вимогу контролюючого органу надавати доступ до свого приміщення, чи надати особисті дані про локацію абонентів);

3) тому, як відсутній реально діючий контролюючий орган всі гарантії, що надає законопроєкт, просто не зможуть функціонувати на практиці;

4) також серйозним ризиком є те що, контролюючий орган немає чіткого визначення компетенції, тому може сам перетвориться на злісного порушника права на приватність;

5) незрозумілість, тобто, який порядок обробки органу контролю персональних даних, які він буде отримувати під час здійснення своїх функцій. Також і про самі функції контролюючого органу мало що відомо;

6) необхідно присвятити частину законопроєкту регламентації роботи органу контролю, або паралельно підготувати окремий законопроєкт про нього;

7) у проєкті також відсутня детальна процедура, що давала б змогу передавати персональні дані між державними органами, так як окремі державні структури володіють великим обсягом персональних даних;

8) санкції, що передбачає проєкт, є надто жорсткими, а самі підстави для їх накладення — занадто широкі та розмиті. Тому, необхідно чітко визначати в них диспозицію, а розмір штрафів можна суттєво зменшувати. Набуття чинності закону в частині накладення санкцій доцільно було б відтермінувати;

9) немає чіткого розуміння, що саме стосується журналістської та творчої діяльності. А саме нема визначення для цих діяльностей. Також потрібно згадати, що самі норми про відео та фото фіксацію у публічних місцях є такими, що приводять до обмеження свободи вираження. Тобто, обмежують діяльність таких професій, як: журналіста, фотографа, оператора, художника тощо;

10) у проєкті також не вистачає визначення деяких термінів (наприклад, немає визначення таких понять як “автоматизоване опрацювання персональних даних”, “кандидат на влаштування на роботу”), деякі терміни вживаються по різному (“автоматизований” і “автоматичний”, “місцезнаходження”, “місце знаходження” та “розташування” тощо). Окремі принципи та норми спотворені положеннями Європейської конвенції з прав людини;

11) хоча відносини щодо опрацювання персональних даних працівника роботодавцем описані в загальному досить непогано. Окремі визначення є можуть бути мало зрозумілими та заплутаними;

12) також є необхідність доопрацювати розділ про передачу персональних даних для інших держав або міжнародних організацій;

13) заборона у відмовлянні надання послуг або товарів у випадку відмови в обробці персональних даних, а також вимога щодо призначання своїх представників в Україні іноземними компаніям є сумнівною;

Необхідно зробити зауваження, що розробляючи такий важливий законопроєкт, варто уважно оцінити всі ризики, що пов’язані з обмеженням свободи слова та стримуванням економічної активності. В більшості нормах законопроєкт №5628 по суттєво копіює GDPR Європейського Союзу, та чимала кількість норм в українському проєкті є навіть дещо жорсткішою за європейські, хоча європейський регламент вважають дуже вимогливим щодо опрацювання даних та їх застосуванням.

Треба сказати, що даний законопроєкт сам по собі є суттєво об’ємним та складним. Якщо ж його положення ретельно вивчити та імплементувати є доцільним для багатьох компаній та державних структур, щоб в свою чергу стане

непосильним тягарем і погіршить не тільки ринкову конкуренцію, а й економічну ситуацію в країні.

Варто зазначити, що у Сполучених Штатах Америки взагалі відсутній федеральний закон для регламентації опрацювання персональних даних в цілому. Такий собі аналог GDPR існує в тільки декількох штатах, зокрема в штаті Каліфорнія. Та дія цих законодавчих актів розповсюджуються лише на великий бізнес і загалом вони є набагато м'якшими ніж європейські норми.

1.3 Вимоги до роботи з персональними даними

Робота з персональними даними починається з їх обробки. Це важливий етап, що має гарантувати право кожного громадянина на недоторканність приватного життя та нерозголошення особистих даних.

Відповідно до Закону України «Про захист персональних даних» стаття 6, можна навести такі загальні вимоги:

1) Мета опрацювання персональних даних формується в законі та інших нормативно-правових актах, положеннях, установчих чи інших документах, що врегульовують діяння власника персональних даних. Також мета повинна відповідати законодавству про захист особистих даних. Обробка персональних даних повинна здійснюватися відкрито та прозоро застосовуючи засоби та способи, що відповідають визначеним цілям даної обробки.

2) Персональні дані повинні бути точними та достовірними, а також оновлюватись в залежності від потреби, що визначена метою їх опрацювання.

3) Стосовно визначеної мети їх обробки персональних даних , вони повинні бути відповідними, адекватними та ненадмірними.

4) Першоджерелами про фізичну особу повинні бути видані на її ім'я документи; що підписані нею; а також відомості, які особа надає про себе.

5) Опрацювання персональних даних повинно виконуватись для конкретних і тільки законних цілей, що визначені за згодою суб'єкта персональних даних, або у

випадках, що передбачає закон України, в порядку, що встановлений законодавством.

6) Обробка даних конфіденційної інформації про фізичну особу не допускається, без її згоди, окрім випадків, що визначені законом, та слідують інтересам економічного добробуту, національної безпеки та прав людини.

7) Опрацювання даних для захисту життєво важливих інтересів суб'єкта персональних даних без його згоди можна до часу, поки отримання згоди стане можливим.

8) Опрацювання персональних даних в історичних, статистичних чи наукових цілях може відбуватися тільки за умов забезпечення їх відповідного захисту.

9) Типовий порядок опрацювання персональних даних повинен затверджуватись Уповноваженим.

Наступним етапом роботи з персональними даними є їх використання.

Використанням персональних даних передбачені будь-які дії власника щодо опрацювання його даних, дій щодо захисту цих даних, а також дій щодо надавання частково або повного права їх опрацювання стороннім суб'єктам відносин, що пов'язані із даними, що здійснюються за згодою їх власника або згідно закону.

Розповсюдження персональних даних без згоди їх власника цих даних або довіреної самим суб'єктом особи дозволено тільки у випадках, що визначені законом, та тільки в інтересах національної безпеки, економічного добробуту або прав людини.

Порушнику чинного законодавства про захист персональних даних загрожує адміністративна чи кримінальна відповідальність, що встановлена законом України.

Наступним етапом є збирання та опрацювання персональних даних.

За умовами поінформованості згодою суб'єкту персональних даних вважається добровільне волевиявлення фізичної особи, щодо надавання дозволу на опрацювання її конфіденційних даних у відповідній сформульованій меті їх опрацювання. Ця згода може висловлюватись як і у письмовому виді так і у формі, що надає можливість формувати висновок про надання згоди.

Конституцією України, а саме Статтею 32, що в свою чергу надає право людині на невтручання в її особисте життя. Не допустимими є: збирати, зберігати, використовувати чи поширювати конфіденційну інформацію про особу без її згоди. Виключенням є випадки, що визначені законом, і тільки в інтересах держави.

Розпорядником персональних даних вважається фізична або юридична особа, якій власник персональних надав право обробляти ці дані від свого імені.

Персональні дані фізичної особи якої обробляються вважається суб'єктом персональних даних.

Контроль за дотриманням законодавства про захист персональних даних здійснюють Уповноважений орган та суди.

За порушення недоторканості приватного життя особа, що скоїла злочин буде притягуватись до кримінальної відповідальності.

Одним із найважливіших аспектів з роботи персональними даними є їх захист.

Захист персональних даних — це заходи, що спрямовані на захист відомостей, що стосуються певної або визначеної на підставі такої інформації фізичної особи.

Відповідно до статті 24 про "Забезпечення захисту персональних даних" відносять наступне:

1. Отримувачі чи розпорядники персональних даних та треті особи повинні забезпечити захист для цих даних від їхньої випадкової втрати або знищення, від незаконних опрацювань, у тому числі незаконних знищень чи несанкціонованого доступу до цих даних.

2. В органах, що здійснюють опрацювання даних, що підлягає повідомленню згідно цього Закону, створюється (призначається) структурний підрозділ або ж відповідальна особа, що повинна організувати роботу, пов'язану із захистом персональних даних при їх опрацюванні.

3. Структурні підрозділи чи відповідальні особи, що організовують роботу, яка пов'язана із захистом персональних даних при їх опрацюванні:

а. повинні інформувати та консультувати власника або розпорядника персональних даних з питань дотримання законодавства про захист персональних даних;

b. взаємодіяти з Уповноваженим Верховної Ради України з прав людини та призначеними ним посадовими особами з питаннями щодо запобіганню та усуненню порушень законодавства, що стосуються захисту персональних даних.

4. Фізичні особи — підприємці, що мають відповідну ліцензію повинні особисто забезпечити захист персональних даних, якими вони володіють, відповідно до вимог закону. До таких фізичних осіб відносяться: адвокати, нотаріуси, лікарі та ін.

1.4 Видалення персональних даних

Персональні дані можуть підлягати видаленню або знищенню у разі:

– закінчення вказаного терміну зберігання даних, що був визначений згодою самого суб'єкту персональних даних на їх опрацювання або законом;

– зупинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником;

– виданням певних приписів Уповноваженого органу або посадових осіб секретаріату Уповноваженого, що визначаються ним;

– набуттям чинності рішення суду щодо видалення персональних даних або їх фізичного знищення (стаття 15 Закону України).

У встановленому законодавством порядку персональні дані що були зібрані з порушенням вимоги Закону України належать до видалення або знищення.

Персональні дані, що були зібрані в результаті виконаних завдань оперативно-розшукових чи контррозвідувальних дій, а також боротьбою із тероризмом, видаляються та знищуються відповідно до вимоги закону України.

Якщо ж ваші персональні дані потрапили в інтернет, то ви можете звернутись до гуглу і він їх видалить. До даних, що підлягають видаленню в даному випадку, відносять ідентифікаційний номер або серія та номер паспорта; номери банківських рахунків; номери кредитних карток; зображення власноручних підписів; зображення документів, які посвідчують особу; особисті, конфіденційні та офіційні записи, як-от

медкарти; особиста контактна інформація (фізичні адреси, номери телефонів і електронні адреси); конфіденційні облікові дані.

Висновки за розділом 1

Проаналізувавши нормативно - правову базу у сфері захисту персональних даних було з’ясовано як саме за законопроєктом №5628 України повинна відбуватись робота з персональними даними на різних етапах. Були розглянуті позитивні та негативні аспекти даного законопроекту. Також виявлено, що в більшості норм законопроєкт №5628 суттєво копіює Загальний регламент захисту даних GDPR Євросоюзу, та встановлено, що чимала кількість норм в українському проєкті є навіть дещо жорсткішою за європейські, хоча європейський регламент вважають дуже вимогливим щодо опрацювання даних та їх застосуванням.

РОЗДІЛ 2 ВИДИ ЗАГРОЗ І ТИПИ АТАК НА ПЕРСОНАЛЬНІ ДАНІ В СОЦІАЛЬНИХ МЕРЕЖАХ ТА МЕСЕНДЖЕРАХ

2.1 Аналіз найбільш поширених соціальних мереж та месенджерів.

Термін «соціальні мережі» стосується використання сайтів соціальних мереж в Інтернеті, щоб постійно спілкуватись з друзями, сім'єю, колегами або клієнтами (рис. 2.1). Соціальні мережі в основному наслідують соціальні цілі, ділові цілі або й те, й інше [8]. До соціальних сайтів, наприклад, належать такі сайти, як: Facebook, Twitter, LinkedIn та Instagram. Вони також є дуже важливою базою для маркетологів, що в свою чергу залучають клієнтів через ці веб-майданчики. За статистикою 2021 року від hromadske.ua Facebook є самою популярною соціальною мережею та налічує найбільшу кількість користувачів. Щомісячно її використовують приблизно 2,91 мільярда людей.

Рисунок 2.1 – Соціальна мережа

На сьогоднішній день соціальні мережі залучили мільйони людей по всьому світу, включаючи молодих, яких приваблює його утримання та корисність у

спілкуванні з різними людьми. Це правда, що вони мають вікове обмеження для реєстрації, але зазвичай це вразливий захід. Той факт, що діти мають доступ до традиційних соціальних мереж, таких як Facebook їх наражає на безліч ризиків. Ці небезпеки можуть змінюватись від перегляду неприйнятного контенту до контакту з незнайомцями.

Без сумніву, соціальні мережі та месенджери є привабливими, але потрібно помірно їх використовувати. Багато молодих людей доходять до того, що мають проблеми зі здоров'ям через непропорційне споживання.

Facebook

Facebook - американський онлайн-сервіс соціальних мереж, що входить до складу компанії Meta Platforms. Facebook був заснований у 2004 році Марком Цукербергом, Едуардо Саверином, Дастіном Московицем та Крісом Хьюзом, усі вони були студентами Гарвардського університету. Facebook став найбільшою соціальною мережею у світі з майже трьома мільярдами користувачів станом на 2021 рік, і близько половини цієї кількості користувалися Facebook щодня. Штаб-квартира компанії знаходиться в Менло-Парк, Каліфорнія.

Доступ до Facebook безкоштовний, а більшість грошей компанія заробляє на рекламі на сайті. Нові користувачі можуть створювати профілі, завантажувати фотографії, приєднуватися до вже існуючої групи та створювати нові групи. Сайт має багато компонентів, зокрема Timeline, простір на сторінці профілю кожного користувача, де користувачі можуть:

- публікувати свої думки, а друзі можуть публікувати повідомлення;
- статус, який дозволяє користувачам сповіщати друзів про їхнє поточне місцезнаходження чи ситуацію;
- стрічка новин - інформує користувачів про зміни профілів і статусу їхніх друзів.

На рисунку 2.2 зображено інтерфейс Facebook.

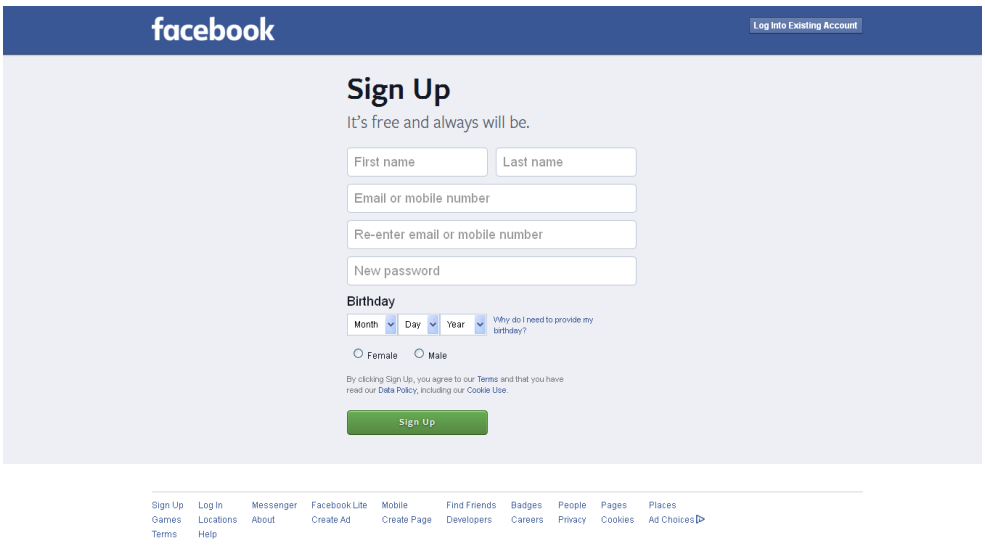

Рисунок 2.2 – Інтерфейс соціальної мережі Facebook

Користувачі можуть спілкуватися один з одним і надсилати один одному приватні повідомлення. Користувачі можуть повідомити про своє схвалення вмісту на Facebook за допомогою кнопки «Подобається», функції, яка також з'являється на багатьох інших веб-сайтах. Іншими сервісами, які входять до складу Meta Platforms, є Instagram, соціальна мережа для обміну фотографіями та відео; Messenger, програма для обміну миттєвими повідомленнями; і WhatsApp, служба текстових повідомлень і VoIP.

Привабливість Facebook частково пояснюється тим, що співзасновник Цукерберг з самого початку наполягав на тому, щоб його члени були прозорими щодо того, хто вони є; користувачам заборонено використовувати фальшиві ідентифікатори. Керівництво компанії стверджує, що прозорість необхідна для формування особистих відносин, обміну ідеями та інформацією та розбудови суспільства в цілому. У ньому також зазначається, що однорангове підключення користувачів Facebook знизу вгору полегшує підприємствам підключення своїх продуктів до споживачів.

Facebook заохочує сторонніх розробників програмного забезпечення використовувати свій сервіс. У 2006 році він випустив свій інтерфейс прикладного програмування (API), щоб програмісти могли писати програмне забезпечення.

Отже, основні плюси Facebook приведені в табл. 2.1.

Таблиця 2.1

Переваги та недоліки соціальної мережі Facebook

Плюси	**Мінуси**
Швидкий старт. Сторінку на Facebook створити можна просто та швидко	Надсилати запрошення на свою сторінку користувач зможе лише заплативши Facebook
Вбудована аудиторія	Популярність Facebook не завжди може бути стабільною
Легко керувати спільнотою	Функціонал Facebook має свої можливості та обмеження
Контроль над контентом користувачів мережі	Користувач не має права запровадити серйозні інновації
Велика кількість додатків, які можна використовувати для просування та розкручування	Функціонал соціальної мережі може бути змінено власником
Економія на розробці сайту	Користувач не володіє на Facebook списком електронних адрес учасників своєї спільноти

Twitter

Твіттер – це соціальна мережа, «фішка» якої полягає в тому, що користувачі можуть залишати лише короткі повідомлення, не довші за 140 символів [12].

Рисунок 2.3 – Інтерфейс соц. мережі Твіттер

Твіттер має кілька позитивних сторін [12]:

• Лаконічні повідомлення. Користувачі, які починають читати і писати короткі твіти, помічають, що їм стає зручний такий формат спілкування та отримання інформації. У тому ж «Facebook» деякі люди не знають міри і розтягують свої міркування на кілька абзаців. Так що якщо користувач цінує свій час та змістовне спілкування, то Twitter йому точно сподобається.

• Зручність у використанні на смартфонах. Більшість користувачів воліє робити та читати твіти саме з мобільних гаджетів.

• Багато функцій сервісу безкоштовні. Навіть за верифікацію облікового запису не потрібно вносити плати.

• Інтуїтивно зрозумілий інтерфейс.

• Постійний розвиток. Розробники компанії не дарма їдять свій хліб і завжди працюють над покращенням сервісу, додаючи нові функції чи вдосконалюючи старі.

Як і в будь-якого іншого сервісу, Твіттер має свої недоліки:

• Політично вмотивовані рішення адміністрації. У 2017-му році в Твіттері заборонили постити рекламу з облікових записів деяких російських ЗМІ, включаючи «Russia Today». Ці дії були неоднозначно оцінені багатьма користувачами, які вважають, що ресурс явно йде на поводу у американської влади.

• Забирає час. Як і інші соціальні мережі, Twitter є "вбивцею" вільного часу. 15-30 хвилин на день, які користувачі витрачають на читання не особливо важливих твітів, можна було б пустити більш корисні заняття.

• Рекламні твіти Часто користувачі натикаються на непотрібну їм рекламу.

• Багато ботів. Багато облікових записів створюється лише для однієї мети – «накрутити» кількість передплатників.

Instagram

Instagram - це соціальна мережа, користуватися якою можна безплатно. Власники акаунтів виставляють власні зображення та відео, обмінюватися

зображеннями та роликами, редагувати контент. Це відкриває багато переваг перед користувачами та перед бізнесменами в інтернеті [13].

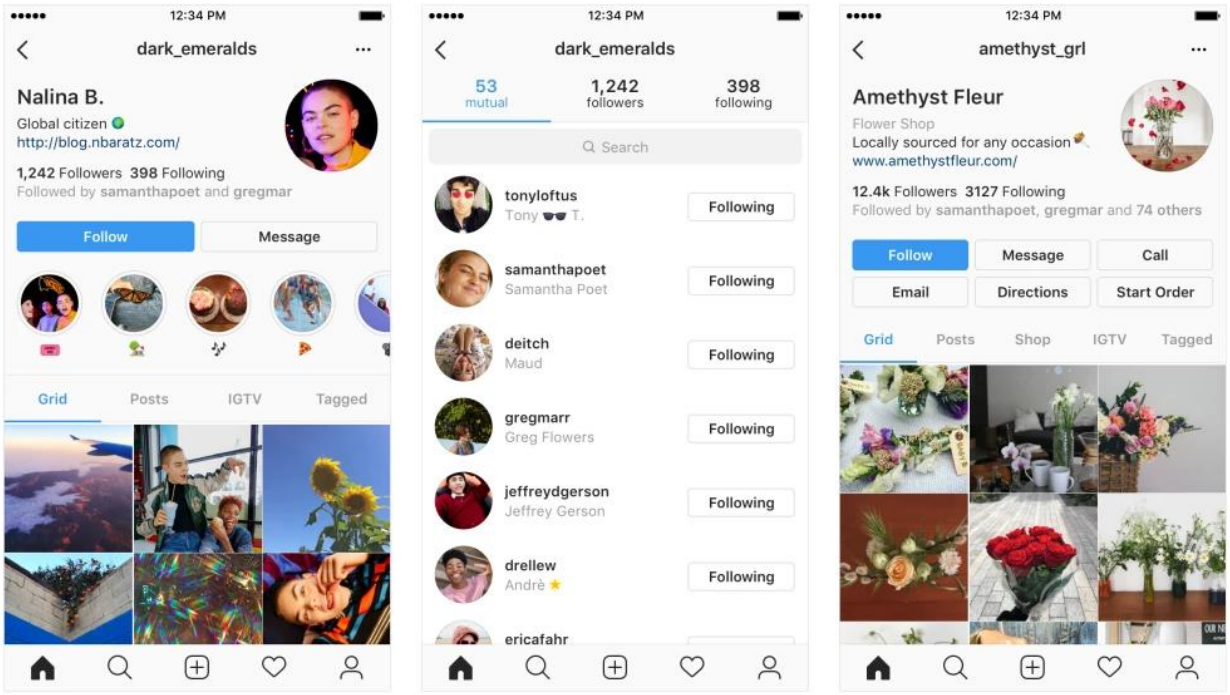

Рисунок 2.4 – Інтерфейс соц. мережі Instagram

Назвемо основні переваги Інстаграму [13]:

• Інстаграм — дуже зручна соціальна мережа для свого блогу. Особливо для фотографій. Гідної альтернативи йому в цьому не знайти.

• Ця соцмережа є найоптимальнішою для ведення бізнесу. У ній є все, щоби підприємець відчував себе комфортно. Якщо приділяти своєму бізнес-профілю належну увагу, то з просування можна отримати багато клієнтів.

• Свій профіль в інтаграмі ведуть топові блогери та селебріті. Якщо у когось із впливових людей немає своєї сторінки, то це скоріше виняток. Завдяки цьому фанати можуть легко відслідковувати активність улюблених зірок.

• Легко шукати цікавий контент завдяки вкладці Explore. Алгоритми платформи пропонують вам цікавий контент, ґрунтуючись на останній активності. Так само можна шукати людей для взаємної активності.

• Формат сторіс — це унікальна фішка Інстаграм. Так, тепер її запроваджують і в інші соціальні мережі, але це лише жалюгідна пародія

неповторного оригіналу. Сторіс в Інстаграм - це унікальна річ, якою користуються всі. Від величезного масштабу зірок, коли їм потрібно зробити анонс нового кліпу, до звичайних обивателів, які вийшли погуляти та застали гарний захід сонця.

• Інстаграм є однією з найпопулярніших соціальних мереж. Розробники працюють над тим, щоб зробити інтерфейс мережі зручнішим для користувачів. І хоча кількість користувачів вже давно побила всі рекорди аналогічних соцмереж, зупинятися на досягнутому ніхто не збирається.

Інстаграм має і недоліки, а саме:

• Інстаграм все ж таки не створено для новин та обговорень якоїсь теми. Соціальна мережа швидше для розваги та бізнесу, ніж для комунікації, тому що в ній немає можливості публікувати великі посади у зручному форматі. Втім, для когось це й не мінус.

• IGTV ніколи не замінить Youtube.

• Дуже багато ботів та масфоловерів. Для більшості з них не важливим є ваш контент, вони не зацікавлені у взаємній активності — їм потрібна лише підписка.

• Якщо ви не звикли до плагіату, то в рамках цієї соціальної мережі доведеться звикати. Є цілі облікові записи, які крадуть чужий контент без вказівки автора. Більшість зловмисників залишаються безкарними, оскільки право поскаржитися на крадіжку має лише сам автор.

• Відсутність нормальної десктопної версії пригнічує тих, хто звик проводити більшу частину часу за персональним комп'ютером. Не вдасться безпосередньо завантажити оброблену у фотошопі фотографію або змонтоване відео, доведеться маніпулювати.

Месенджер - це програмний засіб, мобільний додаток або веб-сервіс для обміну повідомленнями у реальному часі через інтернет [22]. Найчастіше месенджери працюють не самостійно, а підключаються до будь-якого комп'ютера, який є центральним у мережі обміну повідомленнями, він називається сервером. Саме тому месенджери називаються клієнтами. Для широкого кола користувачів

відома певна кількість популярних систем обміну повідомленнями, таких як WhatsApp, Viber, Messenger від Facebook, Telegram, Skype.

Всі мережі були розроблені різними групами розробників, вони використовують різні протоколи та сервери, мають відмінності у своїх умовах та особливостях. Різні мережі не мають прямого зв'язку між собою. Це означає, що користувач Skype не може надіслати повідомлення користувачу What's App, але будь-який користувач може перебувати в кількох мережах. Запущений у 2009 році What's App став першим популярним месенджером, призначеним саме для смартфонів з прив'язкою до номера телефону користувача, що надалі породило безліч копій та варіацій - LINE, Wazapp, Viber, Snapchat, Telegram тощо. А найпопулярніші месенджери на сьогоднішній день - WhatsApp, Viber, Messenger від Facebook, Telegram, Skype; всі перелічені месенджери мають VoIP. Voice over Internet Protocol або IP-телефонія - голосовий зв'язок через інтернет (на відміну від традиційного телефонного зв'язку, що здійснюється через телефонні лінії чи мобільну мережу [22]).

Нижче розглянуто основні переваги та недоліки найпопулярніших серед користувачів месенджерів.

Telegram

«Telegram» – це найбільш популярний месенджер. Його основне призначення – надсилання текстових, голосових, відео повідомлень, а також файлів [23]. Серед політичних активістів та активної молоді поширилася мода на телеграм, як засіб зв'язку. В цілому, Телеграм в будь-якому випадку набагато краще, ніж той же Viber або Facebook.

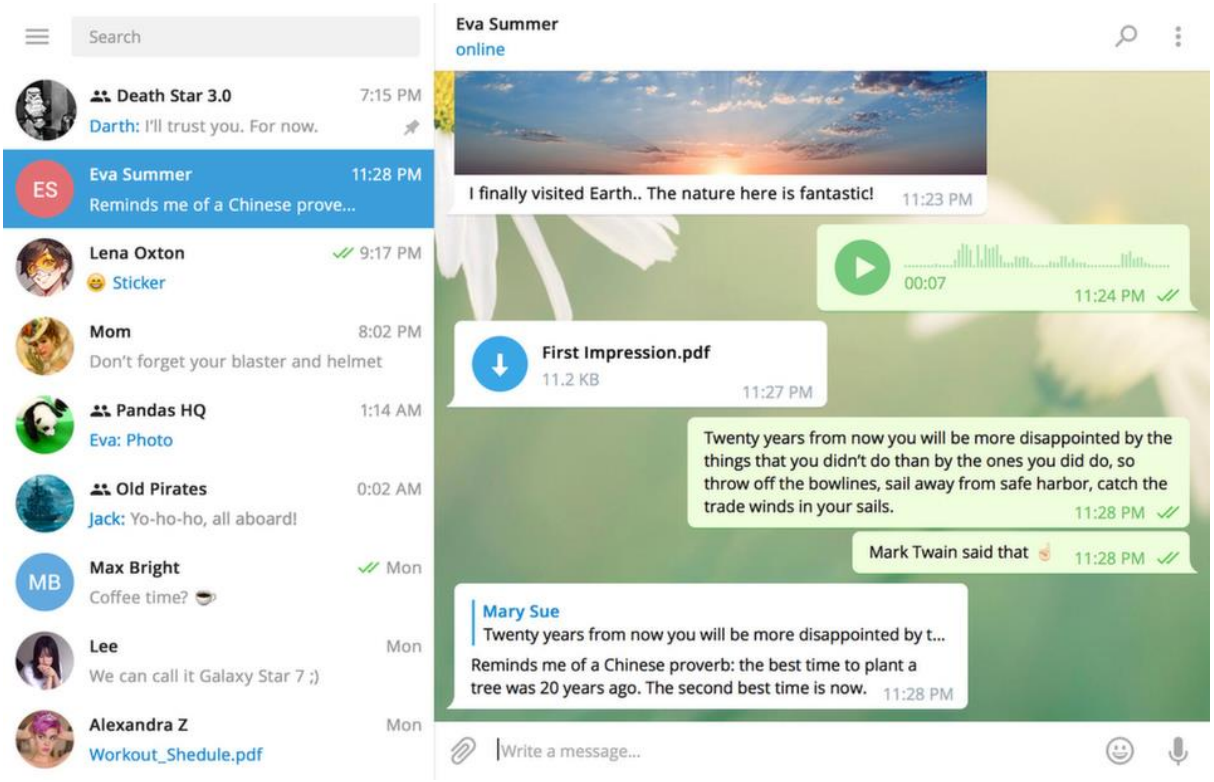

Рисунок 2.5 – Інтерфейс месенджера Telegram

Нижче наведені основні плюси Telegram, які роблять його унікальним популярним продуктом [23]:

• Безліч серверів, що розміщені у світі. Це дає змогу досягти високої швидкості та безпеки, тому у «Telegram» найшвидша доставка повідомлень у порівнянні з іншими месенджерами;

• Відкритий протокол, що дозволяє стороннім розробникам використовувати напрацювання команди "Телеграма";

• Цілком безкоштовний і навіть без реклами;

• Хороший захист від різного роду атак;

• Фактично повна відсутність обмежень за розміром чату та файлів. В одному повідомленні можна надсилати скільки завгодно файлів. Розмір одного файлу не повинен перевищувати 1,5 ГБ;

• Групові чати до 40000 учасників, а також тематичні;

• Надсилання абсолютно будь-яких файлів та документів;

• Секретні чати та групи;

• Легкий у використанні. Споживає мінімум ресурсів пристрою, а також повна кроссплатформенність;

• Зберігати свої файли в хмарі. Тепер файли не займатимуть пам'ять пристрою;

• Можна планувати відправлення повідомлення. Можна вказати проміжок часу, через який повідомлення буде надіслано автоматично.

• Синхронізувати повідомлення між усіма пристроями. Є можливість починати набирати повідомлення в телефоні, а потім закінчити на комп'ютері та навпаки.

• Створювати стікери за допомогою робота.

Недоліки Telegram:

• Прив'язаний до пристрою та надсилає контакти користувача на сервер

• Повідомлення не зашифровані.

• На ПК немає таємних чатів, тільки на телефонах.

• При додаванні нового аватару на пристрій, старий аватар не видаляється автоматично. Його потрібно видаляти вручну.

Facebook Messenger

Facebook Messenger - це сервіс, який призначено для обміну швидкими повідомленнями, посиланнями, відео, знімками та іншою інформацією (рис. 2.6). Безпосередньо пов'язаний із повідомленнями на сайті Facebook [14]. Публікація майданчика Startpack. Цей месенджер схожий на багато інших, але зі своїми особливостями. Він уміє надсилати повідомлення з телефонної книги на конкретний номер, створювати групові чати, прикріплювати до повідомлень медіа-файли, підтримує дзвінки. При цьому листування можна урізноманітнити наклейками та голосовими повідомленнями.

Месенджер від Facebook може синхронізуватися із акаунтом Facebook, та із записником телефону. Варто зазначити ще той факт, що спеціальна версія цього додатку оптимізована під слабкий Інтернет [14].

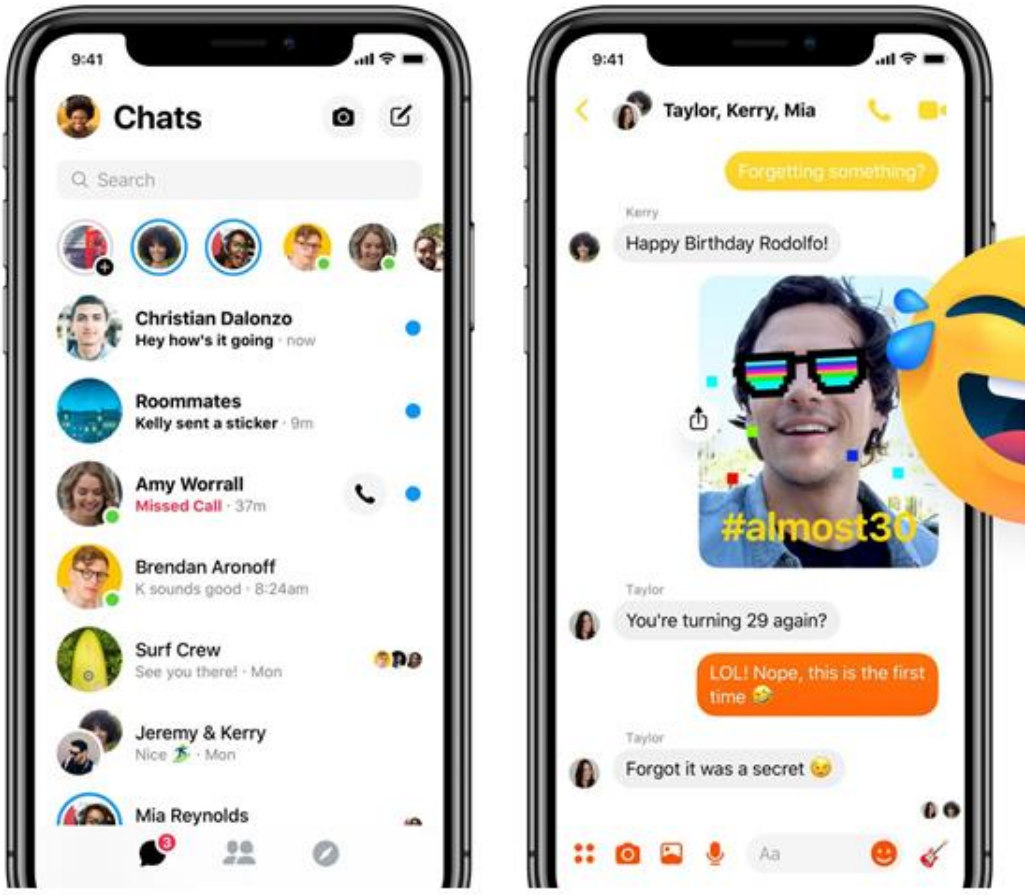

Рисунок 2.6 – Інтерфейс Facebook Messenger

Визначимо основні переваги Facebook:

- можливість здійснювати електронні платежі (щоправда, це можуть робити лише власники карток американських банків);
- є роботи для чатів;
- можна вимкнути повідомлення;
- надає звіт про прочитання повідомлень;
- секретний чат.

Facebook має і недоліки, наприклад:

- сумнівна конфіденційність;
- ви можете видалити повідомлення лише на своєму пристрої;
- надіслані повідомлення не можна редагувати.

Viber

Viber (Вайбер) випустили в 2010-му році (роком раніше, ніж китайський WeChat), причому спочатку він був орієнтований виключно на iOS [14]. Наразі власники Viber розробили багато додатків для інших операційних систем, а також функцій, які мають сучасні месенджери. Мабуть, єдине, що у нього немає, це веб-версія. Інтерфейс месенджера Viber зображений на рисунку 2.7.

Рисунок 2.7 – Інтерфейс Viber

Оскільки на початку основне призначення Viber було – відправка текстових повідомлень, то його головною функцією є передача цих самих повідомлень. При цьому можна надсилати тимчасові повідомлення, які можуть бути доступні лише протягом встановленого користувачем терміну. Також до чату можна додавати GIF-анімації, відео та голосове повідомлення, геолокаційні дані. Крім того, у Вайбер доступні відео- та аудіодзвінки, які працюють і для групових дзвінків до 20 користувачів. Завдяки цьому месенджеру можна здійснювати дзвінок і на звичайний номер, але ця функція платна.

Більшість заходів безпеки персональних даних, що використовуються у Вайбер є стандартними. Так для каналу зв'язку месенджер використовує SSL-шифрування, а для сертифікатів підтвердження – SHA-256RSA.

Також у месенджері передбачено додаткові заходи захисту. До них належать, наприклад, верифікація контактів. Це дозволить синхронізацію ключа із співрозмовником. При підозрі, що контактом користуються треті особи, можна запросити порівняння ключа, а саме пройти верифікацію. Вразі коли ключі не співпадають, можна буде заблокувати такого користувача.

Viber має такі позитивні особливості:

- великий архів емоджі та стікерів;
- унікальна ігрова платформа;
- функція групових чатів;
- можна здійснювати аудіо та відео дзвінки;
- сповіщення працюють навіть в офлайн-режимі;
- визначає місцерозташування користувача.

Можна виділити наступні недоліки Viber:

- проблеми із безпекою;
- дуже популярний месенджер для спаму та реклами.

2.2 Методи злому месенджерів.

Для злому чужих месенджерів використовують кілька методів. Розглянемо їх. Чому складно заволодіти листуванням? Розробники засобів комунікацій розробляють нові системи інформаційного захисту користувачів від зловмисників, але хакери знаходять різні вразливості, що дозволяють обходити захисні системи месенджерів. В інтернеті багато шпигунського софту, хакери викладають платні та безкоштовні програми для злому Viber, Whatsapp, Telegram, Фейсбук. Деякі програми працюють віддалено, деякі слід встановлювати на мобільний телефон контрольованого користувача.

Розібратися в цих складнощах буває непросто, а вибрати потрібний варіант з мінімальними витратами і не нарватися на шкідливе ПЗ, часом неможливо. Не маючи жодних навичок зі злому акаунтів, видобути необхідні відомості не вдасться, тому що рівень шифрування даних досить серйозний. Єдиний спосіб прочитати листування людини і не зламувати телефон - захоплення логіну та паролю

Які бувають причини для злому.

Наприклад, причинами втручання у листування можуть бути спонукання:

1) захистити близьких людей від незворотних помилок (батьки контролюють спілкування важких підлітків, схильних до суїциду родичів, захищають від сексуального домагання дітей);

2) прагнення захистити комерційну інформацію від передачі конкурентам (актуально для роботодавців);підозри у невірності, пошук компромату;

3) з'ясування причетності громадянина до неправомірних дій.

Захоплення чужого листування йде врозріз з уявленнями про законні дії, тому йти на такі заходи слід, маючи суттєві аргументи. Для того, щоб отримати персональні дані або вміст листування абонентів, можна здійснити так:

1) використовувати синхронізацію програми з web-версією (більшість месенджерів підтримує такий формат);

2) заволодіти пристроєм абонента та надіслати архів листування собі на пошту або до хмарного сховища; використовувати програму-шпигун (головне не нарватися на вірусний файл чи шкідливе ПЗ);

3) купити софт для віддаленого перехоплення сесії або захоплення пароля (дорогі програми з непростим інтерфейсом);

4) клонувати sim (дубль сімки буде отримувати всі повідомлення з усіх прив'язаних до номера облікових записів, але у основного власника сім-карта заблокується);

5) перехоплення листування через bluetooth;

6) подарувати смартфон або флеш-карту зі встановленим шпигуном. Бувають ситуації, коли вдається отримати потрібні дані через веб-версію, тільки потрібно.

2.2.1 Кейлоггінг

Кейлоггер (KL) – інструмент, основне призначення якого є реєстрація всіх натискань клавіш або сенсорної панелі будь-якого пристрою. Цей активний запис з клавіатури також названий кейлоггінг або кейстрок логгінг.

Незважаючи на те, що кейлоггер використовується для незаконної діяльності, вони мають кілька позитивних варіантів експлуатації. Наприклад, з його допомогою батьки можуть контролювати своїх дітей або використовуватися роботодавцем для слідкування за своїми співробітники. Кейлоггер також може використовуватися для захисту (запису) паролів та інших даних у разі збою операційної системи.

Треба сказати, що кейлоггер –це програми, що широко використовуються злочинцями як спосіб викрадення персональних даних, а саме:

1) номери кредитних карток;
2) паролі;
3) особисті листи;
4) банківські облікові дані;
5) номери посвідчень водія.

Типи Кейлоггерів.

Отже, є два основні типи пристроїв для кейлоггінгу. Є програмна та апаратна версія. Коли справа доходить до програмних та апаратних кейлоггерів, важливо розуміти відмінність між двома типами.

Апаратне забезпечення кейлоггера:

• складається з невеликого чіпа чи дроту, який фізично прикріплений до технічного пристрою;

• більшість апаратних кейлоггерів можна без проблем видалити;

• добуту інформацію можна переглянути з допомогою спеціальної програми, навіть після фізичного видалення чіпу;

• унікальність програмних кейлоггерів – прошивка апаратного забезпечення, який можна підключити до BIOS комп'ютера та здійснювати запис даних, як тільки включиться комп'ютер;

• бездротові сніфери кейлоггеру здатні перехоплювати зв'язок між бездротовими клавіатурами та комп'ютером.

Програмний Кейлоггер. Як показує практика, програмний кейлоггер складно виявити.

Як правило, він складається з ПЗ, що встановлене хакером на комп'ютер. Це можна здійснити завантаживши вірус на хост комп'ютер (напр., з допомогою фішинг-атак або віддалено). Програмний кейлоггер може записувати не лише активність клавіатури комп'ютера, але здатний виконувати скріншоти та перевіряти буфер обміну.

Дуже малоймовірно, що на комп’ютері жертви може бути апаратний кейлоггер. Однак це можливо у громадських середовищах. Оскільки для роботи апаратного кейлоггера зазвичай використовується USB порт.

При введенні конфіденційної інформації, такої як пароль, можна використати мишку, щоб заплутати кейлоггер, якщо він звісно є. Наприклад, спочатку необхідно ввести останній символ пароля, а потім перемістити курсор, щоб ввести інший символ в іншому місці. Кейлоггер реєструватиме останній символ як перший. Також, як варіант є вибір та зміна тексту під час введення пароля. Однак такі методи не дуже функціональні, і можуть не працювати зі складнішими кейлоггерами, які також записують екран або активність миші.

Щоб запобігти програмному кейлоггеру необхідно встановити хороший антивірус або анти-кейлоггер. Це допоможе убезпечитися.

Необхідно бути особливо обережним із вкладеними файлами електронної пошти та посиланнями. Не натискати на оголошення та сайти від невідомого джерела. Оновлювати свої програми та операційну систему.

Найпростішим способом виявити програмний кейлоггер –перевірка роботи системних процесів. Якщо виявиться щось підозріле, можна здійснити пошук інтернеті і спробувати з'ясувати, чи це легальна програма або кейлоггер. Для того, щоб позбутись програмного кейлоггера непросто спочатку необхідно встановити анти-кейлоггер та перевірити, чи з його допомогою можна щось зробити. Якщо ж є

підозра, що анти-кейлоггер не зміг вирішити проблему, тоді необхідно форматувати жорсткий диск та перевстановити операційну систему.

2.2.2 Зламування з використанням файлів cookie

Файли cookie можуть робити набагато більше, ніж просто відстежувати активність в інтернеті. Тепер хакери знайшли спосіб вкрасти також і наші паролі.

«Cookie» - це невеликий файл, який відвідуваня веб-сайтів зберігають на комп'ютер. Зазвичай вони абсолютно нешкідливі, але дуже корисні. Насправді багато веб-сайтів, які відвідуються кожного дня, використовують файли з «куками» для більш коректної роботи.

Cookie були розроблені для того, щоб стати для веб-сайтів надійним механізмом, що дозволяє пам'ятати необхідну інформацію та записувати історію відвідувань своїх користувачів. Ці крихітні текстові файли можуть бути використані для зберігання реєстраційної інформації та деяких даних про банківську картку, а також вони можуть допомогти рекламодавцям показувати рекламу, яка, на їхню думку, відповідатиме нашим уподобанням.

Файли cookie можуть бути корисними, наприклад, для економії часу, коли потрібно вводити реєстраційні дані на раніше відвіданому веб-сайті. Cookie безпосередньо не відображають паролі, а натомість вони містять хеш, який зберігає пароль. Коли пароль був хешований, він був зашифрований таким чином, щоб прочитати його міг лише той веб-сайт, з якого він був записаний у cookie. Кожен сайт використовує унікальний алгоритм шифрування для кодування хеша та його розкодування.

Зазвичай хакери люблять зламувати паролі, але крадіжка наших файлів із cookie також може принести хакерам власну вигоду. Встановивши наші файли cookie з хешованими паролями у свій веб-браузер, кібер-злочинець може негайно отримати доступ до облікового запису на цьому сайті, при цьому йому не знадобиться вводити реєстраційні дані. Cookie можуть бути використані для того,

щоб швидко і просто можна було зламати облікові записи в соціальних мережах, в електронній пошті та на багатьох інших онлайн-сервісах [20].

Люди з кожним днем стають все розумнішими у питаннях захисту своїх комп'ютерів від шкідливих програм, а тому все частіше встановлюють на комп'ютери надійні антивірусні програми. Внаслідок цього злочинцям доводиться вдаватися до більш досконалих методів, таких як крадіжка інформації, що проходить через публічні мережі Wi-Fi.

Все, що потрібно хакеру, щоб отримати наші cookie, - це, наприклад, розширення для браузера Firefox під назвою Firesheep. Для того, щоб захистити cookie, необхідно використовувати технологію виявлення та копіювання файлів з cookie, що надсилаються бездротовою мережею. Коли розширення виявляє файли з куками, воно створює список на комп'ютері хакера. Потім хакер в себе на комп’ютері може просто натиснути на необхідний файл із «куками», після чого він увійде на відповідний сайт замість користувача (від його імені). Простий, але ефективний спосіб зупинити хакерів від крадіжки особистої інформації - це просто регулярно видаляти файли cookie. Фахівці рекомендують робити це кожні 7-14 днів. Також не потрібно зберігати інформацію про свою банківську картку на сайті, особливо, якщо він не є надійним. Однак видалення файлів з cookie має один недолік- доведеться повторно вводити паролі та особисту інформацію при наступному вході на відповідний веб-сайт. Це може бути незручно і дратівливо, але це набагато безпечніше в довгостроковій перспективі, адже такий підхід дозволить захиститись від крадіжки cookie.

2.2.3 Зламування із використанням хакерських програм Cocospy та Spyier

Соціальні мережі завоювали наш світ, і це ринок цифрової парадигми, що постійно зростає. Всі наші дії записані у соціальних мережах, і це чудова форма спілкування. Це вражаюче нововведення було напрочуд імпровізоване і знаходиться на шляху до зміни нашого світогляду в цілому.

Мільйони підлітків використовують такі програми, як Snapchat, по всьому світу. Сама програма є розважальним способом розпізнати ваш розпорядок дня. Тим не менш, використання цього додатка вже давно піддається критиці через його серйозні небезпеки.

Іноді дуже важливо стежити за своїми близькими, щоб захистити їх від небезпек, запропонованих за допомогою цієї програми. Щоб це сталося, потрібен чудовий інструмент для полегшення проблеми безпеки та відстеження дій цільової людини.

Ось 2 найкращих інструментів, якими ви можете довірити зламати Snapchat, це Spyier та Cocospy. Spyier - один із найкращих додатків для злому в лінійці. Володіючи чудовими функціями злому та шпигунства, Spyier, безсумнівно, займає друге місце на ринку. Spyine має хороші сервіси для зламування чиєїсь облікового запису Snapchat. Крім злому Snapchat, Spyine також займається багатьма іншими речами, такими як злом Facebook, злом Instagram та багато іншого.

Що стосується Spyic, він завжди був одним із найкращих. Spyic довгий час залишався якісним хакером. Найкращі послуги всім відомі. Це хороший варіант, якщо ви шукаєте надійне і те що заслуговує на довіру додаток для злому або стеження. Spyic може не тільки зламати Snapchat, але й досягти успіху в багатьох інших речах. Наприклад, він має кейлоггер, який записує кожен рух або дотик до цільового телефону. Ви бачите кожен дотик, зроблений іншою людиною. Це корисно, тому що ви можете дізнатися паролі за допомогою цієї функції. Cocospy ще один шпигунський чарівник у цій гонці. Ця програма, яка також популярна в різних країнах і використовується багатьма людьми по всьому світу. Ця програма дозволяє вам відстежувати акаунти Snapchat ваших близьких і розкривати все, що відбувається в їхніх акаунтах. Зламувати Snapchat простіше, вигідніше та веселіше з Cocospy.

Cocospy високо цінується такими всесвітньо відомими виробниками веб-контенту, як PC World, New York Times, Top Ten Reviews, Life-хакер, Forbes і тд. Це пояснює ідею про те, що Cocospy є дуже шановним і корисним програмним забезпеченням для клієнтів, а також має величезну популярність і широко

використовується мільйонами людей по всьому світу. Вам не потрібно турбуватися про фізичний доступ до телефону, і це одна з найкращих особливостей цієї програми. Використовуючи його, вам не потрібно робити джейлбрейк або рутувати пристрій, і ви можете читати текстові повідомлення легко. Ви також можете перевірити історію переглядів на цільовому пристрої та дізнатися, що було зроблено на телефоні, за яким шпигують. Ця програма дійсно проста у використанні, тому що команди дуже легко реалізувати. Щоб ця програма працювала на вас, не потрібно звертатися за допомогою до професіоналів [15].

Просто додайте дані облікового запису iCloud на пристрої на випадок, якщо вам потрібно шпигувати за пристроєм iOS, але якщо це телефон Android, вам потрібно один раз встановити програму на пристрої, який ви хочете шпигувати, і дозволити йому робити всю роботу за вас. За винятком надання їм доступу до текстових повідомлень на цільовому телефоні, ви також можете відстежувати їх місцезнаходження та отримувати доступ до контактних номерів, імен, облікових записів соціальних мереж, фотографій, відео та всього іншого, переданого та отриманого через пристрій, включаючи паролі для облікових записів соціальних мереж.

Висновки за розділом 2

Проаналізувавши найпоширеніші соціальні мережі та месенджери було визначено проблеми в політиці конфіденційності для кожного сервісу та розроблено рекомендації, що допоможуть знизити ризик несанкціонованого доступу до персональної інформації. Було проаналізовано методи злому месенджерів, якими найчастіше користуються зловмисники, а саме: кейлоггінг, зламування з використання файлів cookie та таких програм як Cocospy та Spyier. На основі цього аналізу були сформульовані загальні рекомендації, що допоможуть уникнути витоку персональних даних в месенджерах.

РОЗДІЛ ЗРОЗРОБКА ЗАГАЛЬНИХ РЕКОМЕНДАЦІЙ ДЛЯ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО СОЦІАЛЬНИХ МЕРЕЖ ТА МЕСЕНДЖЕРІВ

3.1 Методи та засоби захисту персональних даних в соціальних мережах

Витік персональних даних став однією з найгостріших проблем останніх років. Тому соціальні мережі та інші електронні ресурси (форуми, поштові сервіси, CRM-системи та ін.) постійно вдосконалюють свій функціонал, щоб запобігти несанкціонованому доступу до особистих даних та контенту користувача. Але піклуватися про те, щоб конфіденційною інформацією не скористалися зловмисники, варто не лише соціальним мережам, а й самим користувачам.

Захист персональних даних у соціальних мережах за положенням політики конфіденційності багатьох соціальних мереж, що особисті дані користувача видаляються з серверів ресурсу, якщо користувач видалив свій обліковий запис. Це одне з основних положень політики конфіденційності багатьох соціальних мереж. Але потрібно пам'ятати, що з метою забезпечення користувачеві можливості відновити свій обліковий запис протягом деякого часу після його видалення, соцмережі зберігають всю інформацію протягом певного терміну. Крім того, дані можуть залишитись у кеші пошукових систем та інших електронних ресурсів.

Найпоширеніша помилка, яку роблять користувачі соціальних мереж і якою активно користуються зловмисники, - використання простого, однакового пароля до всіх облікових записів. Такий пароль дуже легко зламати. Інший спосіб, який не втрачає популярності, незважаючи на численні публікації, що стосуються цієї теми, це так звана соціальна інженерія. Зловмисники моделюють ситуації, що дискомфортні для користувача і вимагають від нього швидкого вирішення.

Захист у соціальних мережах - це не в останню чергу критичне ставлення до будь-яких взаємодій, у ході яких від нас намагаються отримати якусь інформацію. Проблема захисту особистих даних у соціальних мережах більш глобальна, ніж

уявляє більшість користувачів. Справа не тільки в тому, що при реєстрації ми передаємо сервісу свою електронну пошту, ім'я та прізвище, іншу інформацію.

Правила безпеки в соціальних мережах, що стосуються персональних даних, можна знайти у розділі «Політика конфіденційності». Зазвичай там зазначено, яку інформацію потрібно буде надати ресурсу, як вона буде використовуватися, як заходи її захисту реалізовані і які заходи слід вжити і куди звертатися у разі порушення конфіденційності, зокрема, злому акаунта.

Оскільки соціальні мережі - це сервіси, головна мета яких полягає у наданні можливості користувачам спілкуватися один з одним та отримувати потрібний їм контент, наші персональні дані та вся активність у соцмережі аналізуються алгоритмами. Це робиться для того, щоб користувач бачив тих людей, пости та рекламу, які можуть його зацікавити. Це відбувається в рамках закону, про це обов'язково вказується у політиці конфіденційності ресурсу («відповідність цілей обробки персональних даних цілям, заздалегідь визначеним та заявленим при зборі персональних даних»).

Крім того, обробка особистої інформації здійснюється на основі принципів: законності та сумлінності. Соціальні мережі не надають особисті дані своїх користувачів третім особам. Рекламодавці можуть використовувати власні рекламні послуги соціальних мереж та адресувати рекламу конкретним групам користувачів за їхніми інтересами, професією, сімейним станом, але ні Facebook, ні ВКонтакте, ні Instagram ніколи не передадуть величезні масиви даних будь-якої іншої компанії безпосередньо.

Програмні засоби, що використовуються для забезпечення конфіденційності персональних даних в соціальних мережах:

- DLP-системи - комплексні системи, що запобігають витоку даних.
- SIEM-системи - комплексні системи управління подіями та інформаційною безпекою, що відстежують у режимі реального часу подій безпеки (тривог).
- Криптографічні засоби - це шифрування інформації, авторизації та дій на сайті та деякі інші інструменти. Заходи, які вживають соціальні мережі для захисту даних своїх користувачів, є відносно надійними.

На жаль, у шахраїв теж є ресурси, щоб створювати свої програмні продукти, які можуть допомогти виявити вразливість у системі захисту. Бази даних користувача - неймовірно дорогий продукт. З практично всебічною цифровізацією суспільства вони стали основним активом будь-якої компанії, що займається комерційною діяльністю. Тому необхідно вживати додаткових заходів, для того, щоб убезпечити себе:

1) не використовувати для реєстрації на загальнодоступних ресурсах пошту, пов'язану з важливими процесами (наприклад, робітниками та фінансовими сервісами);

2) встановлювати свій пароль для кожного ресурсу, уникати класичних комбінацій типу «12345»;

3) для відновлення або підтвердження пароля використовувати мобільний телефон, а не електронну пошту;

4) ділитись особистою інформацією в соцмережах обережно - продумувати, які наслідки може спричинити розміщення;

5) не додавати в друзі незнайомих людей і не переходити по всіх посиланнях поспіль;

6) не публікувати в соцмережах фотографії важливих документів, не надсилати такі документи через особисті повідомлення; не завантажувати пропоновані через соцмережі програми, якщо не впевнені в тому, що це офіційний продукт відомої компанії. І обов'язково підключати двофакторну автентифікацію там, де її реалізовано.

Незважаючи на всі зусилля соціальних мереж, що спрямовані на запобігання витоку персональних даних, захист інформації в соціальних мережах стає все більш актуальним з кожним днем. Це пов'язано насамперед із тим, що традиційні схеми ведення бізнесу вже не працюють, поступово формується нова модель економіки, в якій соціальні мережі стають основним джерелом клієнтів, а матеріали, що публікуються, - важливим соціальним доказом. Захист конфіденційності в соціальних мережах забезпечується потужним програмним забезпеченням, але й хакери розробляють нові і нові інструменти та способи отримання інформації. І ця

загроза актуальна не тільки для фізичних осіб, а й для сторінок брендів, успіх яких залежить від присутності в соцмережах.

Серед основних проблем, пов'язаних із захистом особистих даних, - «друзі» та «дружній» стиль спілкування. Дуже часто пропозиції потоваришувати є небезпечними. Крім того, навіть за профілем людини, яку ви добре знаєте може теоретично ховатися будь-хто - продаж та купівля акаунтів набула небачених раніше масштабів. Нарешті, для ефективного захисту даних у соціальних мережах важливо не забувати встановлювати відповідні установки конфіденційності, якщо комп'ютером, планшетом або телефоном користуються діти. А ще краще - строго обмежувати їм доступ до електронних ресурсів та пояснювати, яку шкоду можуть завдати ті чи інші їхні дії.

3.2 Методи та засоби захисту персональних даних у месенджерах

Для того, щоб оцінити безпеку даних користувача в тому чи іншому месенджері, необхідно визначити ключові критерії безпеки, приватності та анонімності.

Так як сучасні додатки запускаються в «пісочниці» і для них забезпечується інший контроль поведінки, багато що зводиться до того, як саме організована логіка роботи програми на тій чи іншій платформі.

Наприклад, процес біометричної аутентифікації у месенджерах може бути реалізований без використання системних апаратних механізмів. За певних умов (рут-доступ, джейлбрейк) це дозволяє зловмиснику підмінити значення результату роботи локальної функції, що відповідає за автентифікацію в месенджері, та отримати доступ до заблокованої програми.

Apple iOS ретельніше організовує шифрування особистих файлів, які зберігаються на пристрої, але багато залежить від реалізації опцій Data Protection в коді програми. Аналогічна ситуація з Google Android, який також у фінальних версіях значно просунувся в захисті даних користувача.

Можна виділити такі методи та засоби захисту персональних даних у месенджерах:

1) *Наскрізне шифрування* Підтримка наскрізного (end-to-end) шифрування гарантує, що тільки ви та адресат зможете розшифрувати та прочитати інформацію. E2E вважається основним атрибутом будь-якого месенджера, який позиціонує себе безпечним. Важливий момент — чи ця опція програми за замовчуванням увімкнена? Наприклад, у iMessage донедавна шифрування доводилося активувати в налаштуваннях самостійно (сині повідомлення означають, що опція наскрізного шифрування активована, зелені — ні). Тут важливо розуміти, які криптографічні алгоритми застосовуються в організацію шифрування. Де генерується закритий ключ? Чи відбувається хешування метаданих? Чи організовано ротацію ключів через певний часовий інтервал?

2) *Збір даних і метаданих*. Метадані, які кожен із користувачів генерує своїми діями в мережі, схожі на цифровий відбиток особистості. Месенджери також збирають метадані, які можуть описувати нашу особу докладно. По суті це всі дані крім змісту безпосередньо повідомлення: наприклад, з ким з нашого списку контактів ми розмовляємо, як довго і як часто (відправник, одержувач, час відправки, час прочитання). Це якийсь запис нашої активності. Також може збиратися інформація про пристрій, IP-адресу, номер мобільного і т.д. Сюди ж – збір даних про користувачів. Як мінімум це інформація про користувача при реєстрації. У деяких випадках складно визначити, які саме дані збираються, тому що месенджери інтегровані в екосистему корпорації-виробника (Google Messages, Apple iMessage). Компанії можуть бути відомі ідентифікатор користувача, телефон, вміст листування, історія пошуків, переглядів, інформація про покупки, розташування, контакти та багато іншого.

3) *Відкритий вихідний код*. Відкритий вихідний код програми для обміну миттєвими повідомленнями дозволяє здійснювати комплексний аудит безпеки. Любителі, ентузіасти, експерти можуть зробити складання програми, досліджувати його роботу та привернути увагу до слабких місць, до вразливостей як у серверній, так і клієнтській частинах коду. З іншого боку, вільний доступ до коду дещо

підвищує ризик того, що інформація про виявлену вразливість може використовуватися зі злим наміром, доки не буде закрита або хтось інший із спільноти не зверне увагу на слабке місце. Відкритість коду не може гарантувати безпеку даних користувача, але є важливим атрибутом її побудови. Переважна більшість незалежних аудиторів зацікавлені в еволюції надійності та безпеки коду месенджера, а цього можна досягти лише спільними зусиллями.

4) *Передача даних третім особам*. Третіми особами можуть виступати спецслужби, органи громадського порядку, урядові структури. Адміністрація одних месенджерів активно співпрацює з третіми особами, інші принципово відмовляються передавати особисті дані. Зловмисник може представитися будь-ким, у тому числі і співробітником спецслужби, отримавши в результаті необхідні цінні відомості. При виборі безпечної програми це необхідно враховувати, тому що конфіденційні дані можуть потрапити не в ті руки, навіть якщо ви є законослухняним громадянином.

5) *Шифрування бекапів у хмарі.* Далеко не всі месенджери застосовують шифрування для зберігання листування та файлів у хмарі. Успішна атака зловмисника на хмарну інфраструктуру може призвести до витоку конфіденційної інформації. Так само як і у випадку зі збором даних, інформація про те, чи бекап дійсно шифрується, є у відкритому доступі далеко не по всіх месенджерах.

6) *Підтримка однорангового з'єднання*. Однорангове, або пірингове (peer-to-peer) з'єднання виключає участь третьої сторони. Надіслані повідомлення надходять безпосередньо на пристрій адресата. Важливо зауважити, що така сполука вільно дозволяє побачити, з ким і як довго вона встановлена, що, природно, впливає на анонімність і знижує рівень конфіденційності. Підвищити конфіденційність можна додатковим захистом IP-адреси: використовувати VPN або TOR.

7) *Інформація при реєстрації.* При створенні облікового запису в месенджері, наприклад, часто потрібно вказати номер мобільного телефону, який дуже тісно пов'язаний із нашою реальною особистістю. Безпека даних може бути порушена, але анонімність значно знижується. Чим більше даних потрібно під час реєстрації, тим нижче анонімність. Це може бути вимога адреси електронної пошти, програма може

запросити доступ до контактів або вхідних SMS-повідомлень для верифікації. Підтвердження реєстрації може бути реалізовано через дзвінок на номер.

8) *Інші функції безпеки.* Підтримка месенджером двофакторної автентифікації є важливим додатковим елементом безпеки. Другий рівень захисту на основі 2FA (Two-Factor Authentication) може ефективно зупинити зловмисника. Деякі месенджери пропонують користувачеві активувати 2FA за допомогою повідомлення. Тут же - наявність опції, що дозволяє встановити код або парольну фразу для доступу до важливих параметрів безпеки або листування, до чатів; захист інформації, що відображається на екрані (наприклад, коли користувач намагається зробити скріншот секретного листування, другий співрозмовник отримує повідомлення про це); автоматичне блокування екрана, коли користувач відійшов від пристрою; видалення попереднього прив'язаного пристрою з облікового запису і т.д.

На основі вище наведених методів захисту персональних даних у месенджерах, можна зробити такі рекомендації для користувачів:

1) Завантажувати програми месенджерів тільки з сайтів розробників та офіційних магазинів програм.

2) Налаштувати двофакторну автентифікацію у програмі месенджера.

3) Переконатися, що вибрані програми використовують наскрізне шифрування.

4) Заборонити отримання повідомлень від незнайомих контактів.

5) Вимкнути автозавантаження файлів. З підозрою ставитесь до отриманих посилань та файлів, навіть якщо вони надійшли від відомого відправника. Перш ніж переходити за посиланням або відкривати файл, переконатись іншим способом зв'язку, чи ваш знайомий дійсно відправляв їх.

6) Вимкнути функцію, яка дозволяє переглядати профіль усім користувачам (зробити його доступним лише особистих контактів).

7) Уникати обміну конфіденційною інформацією у чатах.

8) Вимкнути функцію збереження резервних копій листування у хмарі, тобто вони зберігаються у незашифрованому вигляді.

9) Бути обережним під час використання месенджерів через загальнодоступні мережі Wi-Fi.

10) Блокувати пристрої пін-кодом.

11) Регулярно оновлювати всі встановлені програми та операційну систему своїх пристроїв.

3.3 Рекомендації щодо забезпечення безпеки даних в месенджері Telegram

Telegram має функцію під назвою «секретний чат», яка не увімкнена за замовчуванням. Секретні чати доступні у версії Telegram з наскрізним шифруванням. Повідомлення видаляються через певний час, який встановлюється користувачем, і не можуть бути відновлені. Розробники Telegram вирішили не включати наскрізне шифрування за замовчуванням з метою зручності: секретні чати пов'язані з конкретними пристроями, і неможливо продовжити розмову там, де не розпочато розмову. Багато звичайних користувачів вважають, що ніхто не може отримати доступ до повідомлень, хоча за фактом просто довіряють безпеці сервера.

Користувачі Telegram можуть створювати облікові записи та виконувати авторизацію за допомогою автентифікаційного коду, який отримується у вигляді текстового повідомлення. Після початкової авторизації користувачі можуть виконувати налаштування та шукати один одного. Telegram також має функцію двофакторної верифікації, якщо є бажання вводити пароль під час кожного входу в обліковий запис.

Необхідно виділити такі проблеми, пов'язані з технічною безпекою Telegram:

1) Схема атаки на Telegram типу «людині-посередині», яка може бути здійснена владою конкретної держави. Атака пов'язана з генеруванням спільних секретів за методом Діффі-Хеллмана для двох жертв, що мають однаковий 128-бітовий візуальний відбиток, і користувачі, які порівнюють відбитки, не зможуть виявити атаку. При реалізації атаки «днів народження» потрібно лише 264 операції. Щоб перевірити ключі та запобігти MITM-атакам, користувачі повинні візуально порівняти сітку квадратів з чотирма відтінками синього. Тут одразу ж спливає

людський фактор. По-перше, користувач може не помітити ледь помітних відмінностей між сітками. По-друге, у користувача взагалі може не бути бажання порівнювати сітки.

2) До 2014 року протокол MTProto використав модифіковану версію схему обміну ключами за методом Діффі-Хеллмана [25]. Замість генерації ключів за допомогою стандартного протоколу на базі алгоритму Діффі-Хеллмана сервер відсилав користувачеві ключ, оброблений операцією XOR разом з довільним числом (nonce). Цей факт дозволяє фальшивому серверу використовувати різні nonce-змінні для двох користувачів, в результаті чого буде той самий ключ, але який буде відомий серверу.

3) У деяких частинах протоколу при хешуванні замість SHA-256 використовується алгоритм SHA-1, який, як відомо, нестійкий до колізій [26]. Розробники Telegram стверджують, що SHA-1 використовується в тих частинах протоколу, де стійкість до колізій не принципова, проте все ж таки сильніша хеш-функція була б доречнішою.

4) Навіть при використанні секретного чату, мобільна версія Telegram дозволяє третій стороні переглядати інформацію про метадані. Наприклад, зловмисник може дізнатися, коли користувачі виходять онлайн і йдуть в офлайн аж до секунд. Telegram не вимагає угоди від обох сторін для встановлення комунікації, і зловмисник може підключитися та отримати інформацію про метадані без відома користувача. Крім того, у зловмисника є хороший шанс виявити, чи спілкуються два користувача між собою за допомогою підключення та аналізу метаданих на обох кінцях дроту.

Отже, як показують проблеми, пов'язані з технічною безпекою Telegram, користувачам не слід повністю довіряти безпеці сервера Telegram.

Як же ж Telegram зазвичай обробляє дані своїх користувачів? Протокол запобігання спаму та зловживанням, який використовує Telegram, включає збір такої інформації, як IP-адреси, відомості про пристрій, історія змін імені користувача та інші конфіденційні дані. Ці дані зберігаються щонайбільше 12 місяців перед видаленням.

Також необхідно враховувати роль «Модератори» Telegram. Вони можуть читати стандартні повідомлення чату, позначені як спам. Це звичайна практика, хоча вона також має на увазі, що хтось читає повідомлення.

Програма також може зберігати метадані користувачів.

Ніщо з цього не є новим (або надмірно тривожним) у сьогоднішньому цифровому середовищі.

На даний момент часу Telegram вважається досить захищеним месенджером проте є деякі секрети, завдяки знанням яких дані можна захистити ще більше.

Досить важливий із них, це встановлення пароля на телефоні та налаштування двоетапної авторизації.

Зробити це можна у розділі з налаштуваннями: («Конфіденційність»). Телеграм буде запитувати пароль при вході до програми з незнайомого пристрою.

Якщо ж використовувати мобільну версію месенджера, наприклад, Telegram для Android, і на смартфоні є сканер відбитків пальців, то можна з його допомогою розблокувати програму. Якщо ж користуватись онлайн-версією месенджера, необхідно щоразу закривати сеанс.

У Телеграмі всі відкриті сеанси можна завершити однією кнопкою. Знаходиться вона також у розділі безпеки. Просто необхідно натиснути напис «Завершити всі інші сеанси».

Таким чином користувач зможе розлогінитись з усіх пристроїв, крім останнього, що забезпечить повну безпеку. Не потрібно нехтувати користуванням секретними чатами, що самі знищуються, після обговорення надважливої інформації.

У Telegram безпека забезпечується зокрема функцією секретних чатів. Також можна заборонити користувачам відстежувати свою активність. Простіше кажучи, приховати час свого останнього візиту. Щоб налаштувати цей параметр, необхідно перейти до меню «Конфіденційність» та знайти рядок «Остання активність». Вибрати, від кого необхідно приховати дані про відвідування.

Також можна налаштувати гнучку систему для підвищення рівня безпеки телеграм: можна приховати час останнього відвідування від конкретних користувачів.

Найкрутіша фішка - можливість налаштувати автознищення акаунта Телеграм. За замовчуванням налаштування виставлено так, що обліковий запис видаляється після півроку бездіяльності.

Отже, як найкраще захистити свій профіль від злому. За допомогою того ж фішингу зловмисник, наприклад, може обманом змусити користувача ввести дані від облікового запису, створивши підроблений веб-сайт Telegram. Щоб не втратити доступ до свого обліку, потрібно:

1) Увімкнути двоетапну автентифікацію. Це дозволить входити до облікового запису через підтвердження коду в SMS. Активувати функцію можна в меню Telegram «Установки» -> «Конфіденційність» -> «Двоетапна автентифікація». І дотримуватися вказівок на екрані.

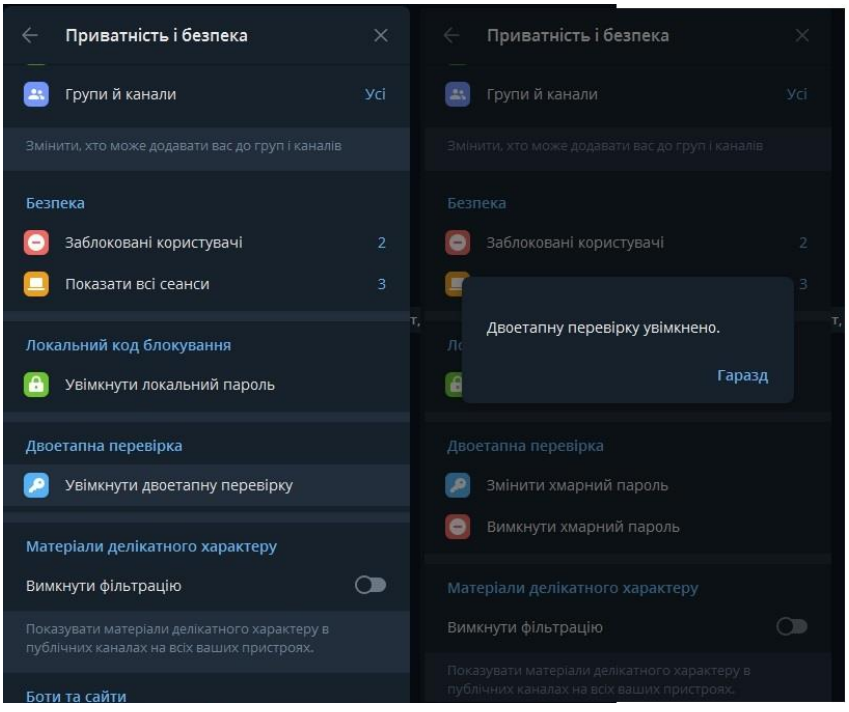

Рисунок 3.1 – Увімкнення двоетапної автентифікації

2) Захистити програму паролем. Це необхідно для того, щоб ніхто не зміг отримати доступ до листування, окрім самого власника облікового запису.

Включається в меню Telegram «Установки» -> «Конфіденційність» -> «Увімкнути локальний пароль».

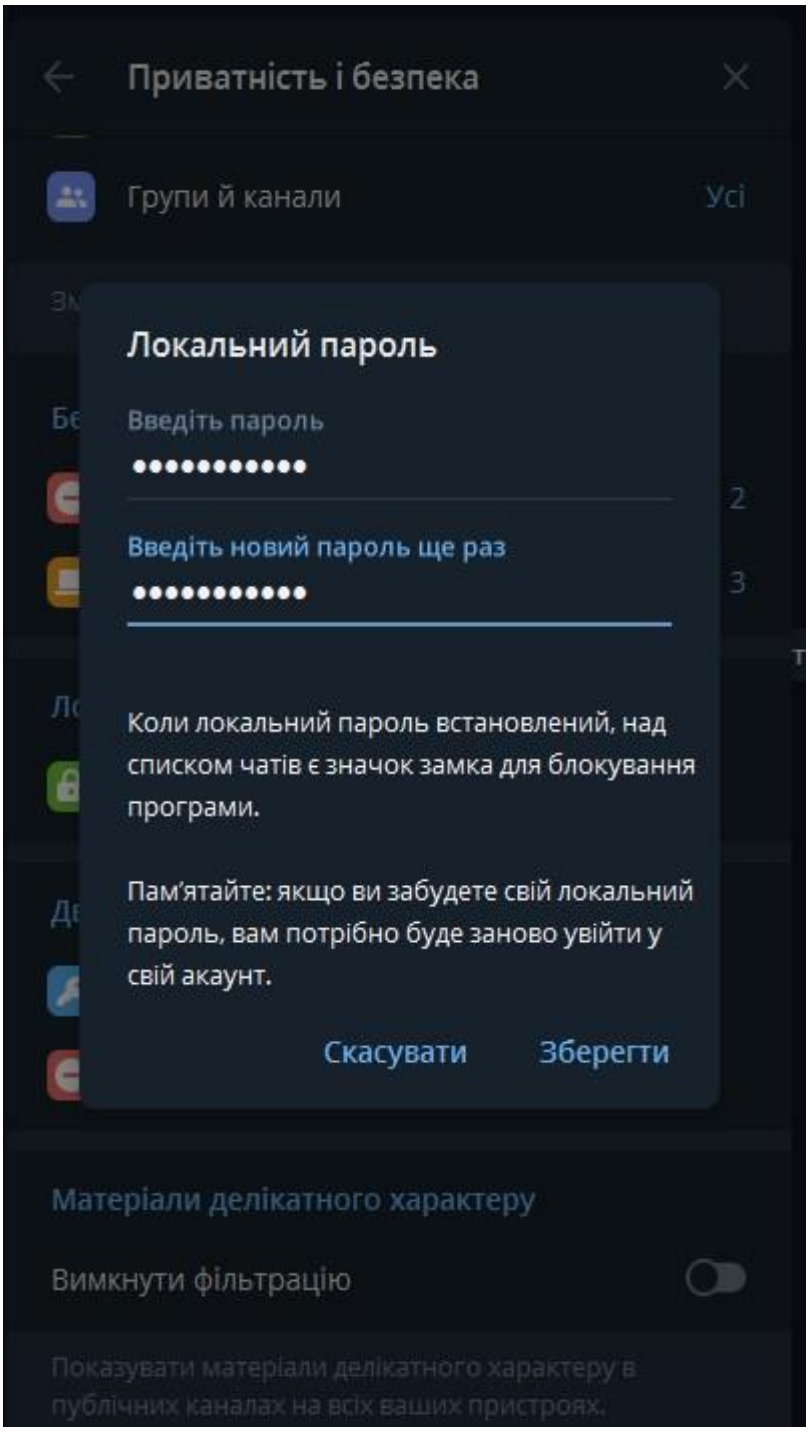

Рисунок 3.2 – Увімкнення локального паролю

Після встановлення коду вхід до програми буде здійснюватися за паролем або відбитками пальців особи.

3) Відстежування пристроїв входу до Telegram. Це можна зробити також через спеціальне меню: Telegram «Установки» -> «Конфіденційність» -> «Активні сеанси».

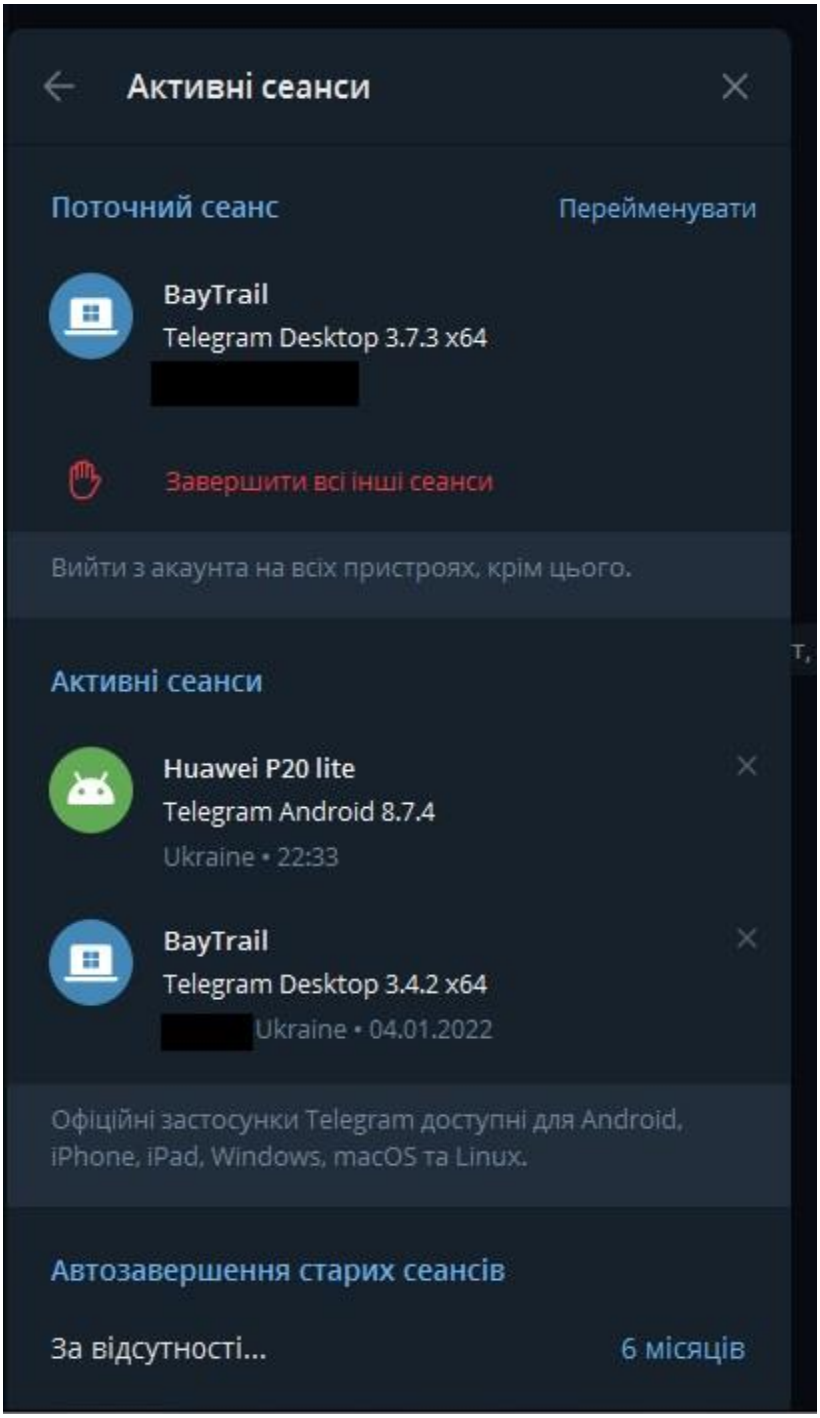

Рисунок 3.3 – Авто закриття старих сеансів

Тут можна віддалено відключити певні сеанси свайпом вліво по девайсу або завершити всі сеанси, крім необхідного.

4) Налаштувати автоматичне видалення акаунту. Якщо користувач з якоїсь причини давно не заходить в Telegram, можна налаштувати автоматичне видалення всіх даних у меню Telegram «Налаштування» -> «Конфіденційність» -> «Якщо я не заходжу» (рис. 3.11).

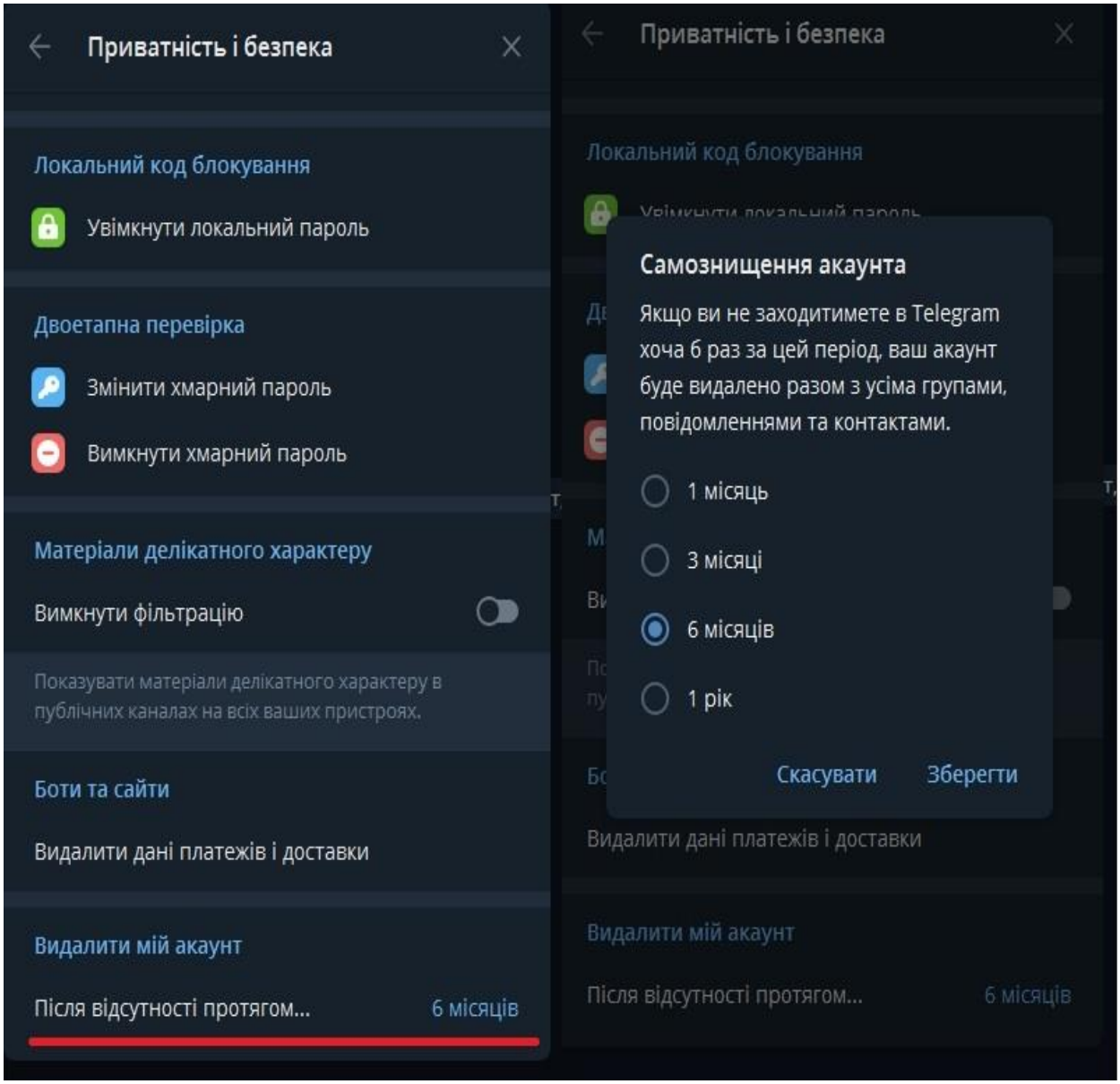

Рисунок 3.4 – Налаштування автоматичного знищення акаунта

Після вибору варіантів 1, 3, 6 або 12 місяців та натискання «Зберегти». Вся інформація зітреться і ніхто не зможе отримати доступ до листування користувача.

5) Додатковим захистом налаштування є «Конфіденційність». Тут є докладний опис кожної функції. Зокрема, є заборона на перегляд номеру телефону власника облікового запису (знайти користувача можна буде тільки по нікнейму,

якщо це, знову ж таки, дозволено в налаштуваннях). У налаштуваннях можна переглянути, хто вже бачить номер облікового запису.

6) Заборона включення облікового запису у групи, канали. Такі дії не варто дозволяти для всіх, у кращому разі – для допускати тільки для відомих контактів. Можна відключити дані функції зовсім і лише за необхідності активувати. Це звісно вимагає додаткового часу, але втрата акаунта — це досить неприємно. Також можна додатково заборонити виклики тим, хто не входить до списку контактів.

7) Відключення функції пересилання повідомлень. У ньому варто повністю відключити посилання на обліковий запис, тому як необхідні контакти і так знають цей обліковий запис. Тоді, якщо хтось процитує повідомлення або перешле його в сторонній чат, групу і так далі, ніхто не зможе перейти до профілю користувача за посиланням, «прив'язаним» до імені (нікнейму).

8) Приховати фотографію профілю облікового запису. Або для всіх, або (і це обов'язковий мінімум) для тих, хто не внесений до списку контактів.

9) Перевіряти синхронізацію контактів. Щоб зберегти дані в хмарі та синхронізувати списки контактів з адресною книгою телефону. Якщо функція активна, всі, хто записаний у телефонній книзі (не Telegram, а саме мобільного телефону), зможуть зв'язатися з користувачем через месенджер (як і користувач з ними). Іноді цю функцію рекомендують відключити, тому як зазвичай у телефонній книзі є чимало малознайомих людей, зокрема випадкових.

Висновки за розділом 3

Проаналізувавши методи та засоби захисту персональних даних в соціальних мережах було визначено, що незважаючи на доволі жорстку політику конфіденційності, обов’язково потрібно вживати додаткові заходи для убезпечення себе від несанкціонованого доступу.

В результаті аналізу методів та засобів захисту персональних даних в месенджерах було виділено наступні методи:

- наскрізне шифрування;
- збір даних і метаданих;
- відкритий вихідний код;
- шифрування бекапів у хмарі;
- підтримка однорангового з’єднання;
- інформація при реєстрації, що використовується для верифікації;
- двофакторна автентифікація.

На основі визначених методів були створені рекомендації для користувачів месенджерів та соціальних мереж, що допоможуть мінімізувати ризик витоку персональних даних.

Проаналізувавши технічні можливості, що дозволяють забезпечити безпеку і конфіденційність даних месенджеру Telegram, можна зробити висновок, що даний сервіс пропонує доволі широкий спектр методів захисту конфіденційності даних.

На основі аналізу технічних проблем Telegram було створено рекомендації при користуванні месенджером, що дозволяють користуватись сервісом з мінімальними ризиками злому акаунта.

Цей алгоритм складається з наступних рекомендацій:

1) увімкнення двоетапної автентифікації;
2) встановлення паролю на сам додаток;
3) перевіряти активні сеанси входу в акаунт;
4) встановити налаштування автоматичного видалення акаунту;
5) приховати номер для інших користувачів;
6) заборонити включення облікового запису у групи та канали;
7) відключити функцію пересилання повідомлень для інших користувачів;
8) приховати фотографії профілю облікового запису;
9) перевірити синхронізації контактів.

ВИСНОВКИ

На сьогоднішній день захист персональних даних – одна з актуальних проблем, що стоїть майже перед кожною людиною, яка живе в суспільстві. В наш час всебічної автоматизації доступ зловмисників до соціальних мереж та месенджерів може призвести до катастрофічних наслідків.

Практично досконалий захист сьогодні, завтра вже може перетворитися лише на невелику перешкоду на заваді зловмисників. На основі аналізу проведеного в предметній області було розроблено загальні рекомендації для захисту персональних даних соціальних мереж та месенджерів.

Аналіз засобів захисту персональних даних в соціальних мережах та месенджерах надав можливість розробити рекомендації захисту від несанкціонованого доступу до інформаційних систем.

Для досягнення мети були виконані всі поставлені завдання, а саме:

- було проведено аналіз нормативно - правової бази у сфері захисту персональних даних;

- було визначено недосконалості в політиці інформаційної безпеки для найпопулярніших соціальних мереж та месенджерів та способи уникнення порушень конфіденційності інформації;

- проаналізовано методи злому месенджерів;

- розроблено рекомендації, що допоможуть користувачу захистити персональні дані при роботі з меседжерами.

У першому розділі роботи було проведено аналіз нормативно - правових документів про захист персональних даних. Розглянуто проект Закону України «Про захист персональних даних» та загальний регламент із захисту даних у світі (GDPR). Було встановлено вимоги до обробки персональних даних на різних етапах роботи з інформацією та використання персональних даних. Також розглянуто можливість забезпечення захисту персональних даних законодавством України.

В другому розділі було розглянуто види загроз і типи атак на персональні дані в соціальних мережах та месенджерах. Також, проведено аналіз методів злому персональних даних у месенджерах та соціальних мережах. Після цього були розроблені методи та засоби захисту персональних даних в месенджерах.

В третьому розділі розроблено методи та засоби захисту персональних даних в соціальних мережах та месенджерах. Також, розроблено рекомендації щодо захисту персональних даних користувача в месенджері Telegram.

Практична значимість дипломної роботи полягає в тім, що її матеріали і результати можуть бути використані для дієвого захисту персональних даних у соціальних мережах та месенджерах. Теоретична значимість – матеріали й результати даної дипломної роботи можуть бути використані як методичний посібник.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналітичне агентство [Електронний ресурс]. – Режим доступу: Statista https://www.statista.com/

2. Месенджери [Електронний ресурс]. – Режим доступу: https://www.voipoffice.ru/tags/messendzhery/

3. Проект Закону України "Про захист персональних даних [Електронний ресурс] Режим доступу. –: https://helsinki.org.ua/articles/analiz-proiektu-zakonu-ukrainy-pro-zakhyst-personalnykh-danykh-5628/

4. Вимоги, що стосуються опрацювання персональних даних [Електронний ресурс]. – Режим доступу: https://i.factor.ua/ukr/law-148/section-636/article-11880/

5. Тлумачення закону про захист персональних даних [Електронний ресурс]. – Режим доступу: https://www.legalaid.gov.ua/publikatsiyi/zahyst-personalnyh-danyh/

6. Опрацювання персональних даних [Електронний ресурс]. – Режим доступу: https://wiki.legalaid.gov.ua/index.php/Захист_персональних_даних

7. Тлумачення статті 24 [Електронний ресурс]. – Режим доступу: https://i.factor.ua/ukr/law-148/section-636/article-11898/

8. Соц. мережі [Електронний ресурс]. – Режим доступу: https://www.investopedia.com/terms/s/social-networking.asp

9. Статистичні дані [Електронний ресурс]. – Режим доступу: https://www.statista.com/

10. Що таке Facebook [Електронний ресурс]. – Режим доступу: https://www.britannica.com/topic/Facebook

11. Плюси та мінуси Facebook [Електронний ресурс]. – Режим доступу: https://dropshipping.ru/raznoe/facebook-minusy-i-plyusy.html#_Facebook

12. Твіттер, плюси та мінуси [Електронний ресурс]. – Режим доступу: https://wikiphile.ru/dlja-chego-tvitter/

13. Плюси та мінуси Instagram [Електронний ресурс]. – Режим доступу: https://zengram.ru/blog/post/instagram-horoshee

14. Facebook Messenger [Електронний ресурс]. – Режим доступу: https://cmsmagazine.ru/journal/items-we-choose-the-messenger/

15. Вайбер [Електронний ресурс]. – Режим доступу: https://sravni.cc/reviews/plyusy-i-minusy-viber/

16. Методи захисту месенджерів [Електронний ресурс]. – Режим доступу: https://www.anti-malware.com/compare/ Messengers-security-and-privacy

17. Дужникова, А. С. Социальные сети: современные тенденции и типы пользования / А. Дужникова. II Мониторинг общественного мнения. - № 5(99). – 2010. - С. 238-251. - [Електронний ресурс]. – Режим доступу: https://wciom.ru/fileadmin/file/monitoring/2010/99/2010_5(99)_16_Duzhnikova.pdf

18. Засурский, Я.Н. Информационное общество, Интернет и новые средства массовой информации // Информационное общество. 2021. — № 2.

19. Игнаткина, В.В. Социальные сети в современном рекрутинге. - М.: Медиаскоп, 2015. - №2, - С. 32.

20. Kapp, H. Бездушность Веб 2.0 /H. Kapp. [Електронний ресурс]. – Режим доступу: http://www.computerra.ru/think/239597.

21. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. – М.: Издательский центр “Академия”, 2015. – 256 с.

22. Месенджер [Електронний ресурс]. – Режим доступу: https://totrdlo.ru/uk/chto-otnositsya-k-internet-messendzheram-chto-takoe-messendzher-v-telefone.html

23. Месенджер Telegram [Електронний ресурс]. – Режим доступу: https://tokar.ua/read/5801

24. Месенджер Viber [Електронний ресурс]. – Режим доступу: https://versus.com/ru/facebook-messenger-vs-viber

25. Протокол Диффи — Хеллмана [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/151599/

26. Алгоритм SHA-256 [Електронний ресурс]. – Режим доступу: https://de.bitcoinwiki.org/wiki/SHA-256

27. Що таке файли Cookie [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%9A%D1%83%D0%BA%D0%B8

28. Загальний регламент про захист даних [Електронний ресурс]. – Режим доступу:https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9_%D1%80%D0%B5%D0%B3%D0%BB%D0%B0%D0%BC%D0%B5%D0%BD%D1%82_%D0%BF%D1%80%D0%BE_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82_%D0%B4%D0%B0%D0%BD%D0%B8%D1%85

29. GDPR [Електронний ресурс]. – Режим доступу: https://gdpr-info.eu/

30. Аналіз проєкту Закону України “Про захист персональних даних” №5628 [Електронний ресурс]. – Режим доступу: https://helsinki.org.ua/articles/analiz-proiektu-zakonu-ukrainy-pro-zakhyst-personalnykh-danykh-5628/

31. Оновлена політика безпеки Telegram [Електронний ресурс]. – Режим доступу: https://www.ukrinform.ua/rubric-technology/2527780-nova-politika-telegramu-personalni-dani-klientiv-pid-zagrozou-vitoku-tak-ci-ni.html

32. Політика конфіденційності Viber [Електронний ресурс]. – Режим доступу: https://www.viber.com/ua/terms/viber-privacy-policy/

33. Оновлена політика безпеки Facebook [Електронний ресурс]. – Режим доступу: https://www.facebook.com/privacy/explanation/