ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

магістра
(освітньо-кваліфікаційний рівень)

на тему *«Дослідження мобільних засобів забезпечення безпеки інформації в месенджерах»*
«Research of mobile means for information security in messengers»

Виконав: студент *6* курсу, групи *6КСМ*
напряму підготовки (спеціальності)
123 «Комп'ютерна інженерія»
(шифр і назва напряму підготовки, спеціальності)
Петрушенко О. М.
(прізвище та ініціали)
Керівник *Козел В.М.*
(прізвище та ініціали)
Рецензент _____
(прізвище та ініціали)

Херсон – 2020 року

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ ТА ПОЗНАЧЕНЬ

IM	instant messenger
ІБ	інформаційна безпека
SNS	Social networking service
E2EE	end-to-end encryption
HTTPS	HyperText Transfer Protocol Secure

ВСТУП

Актуальність проблеми

Розвиток соціальних медіа, інтернет та смартфонів стали невід'ємною частиною сучасного суспільства. Існують такі соціальні мережі, де зареєстрованих користувачів більше ніж населення багатьох країн. Є сайти для завантаження фотографій, відео файлів, сервіси змін статусу, сайти для зустрічі з новими людьми і для знаходження старих друзів [1].

Це допомагає нам бути на зв’язку з іншими людьми та більш легко управляти бізнесом. ІМ (англ. instant messenger – спілкування в реальному часі, в онлайн режимі за допомогою тексту, також «соціальні повідомлення», «програми чату» або месенджери) швидко адаптуються до можливостей цифрової сфери та людських потреб [2]. Використання особою комп’ютера чи будь-якої організацією, що користується комп’ютерами та мережею в повсякденному житті, змушує звернути увагу на питання інформаційної безпеки (ІБ). ІБ – захищеність інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб’єктам інформаційних відносин, зокрема власникам і користувачам інформації та інфраструктури, що її підтримує. Інформаційна безпека повинна бути на першому місці, оскільки значна частина нашої особистої інформації знаходиться саме в Інтернеті. У роботі «Information Security Challenges of Social Media for Companies» зазначається, що ІБ необхідна через сформований ризик, коли технологія використовується для обробки інформації, оскільки інформація може бути розкрита неправильно або не тією людиною. Тому безпека інформації розбита на 3 основні групи, які називаються конфіденційність, цілісність і доступність. Конфіденційність – це захист від несанкціонованого доступу до інформації. Під цілісністю мається на увазі актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни. Доступність – це можливість за прийнятний час одержати необхідну інформаційну послугу. Це

стосується захисту інформації, що зберігається, передається і оброблюється, використовуючи політику, освіту та технології. Багато організацій та компаній, які працюються лише зі щоденними даними, приймають усі необхідні застережливі заходи, щоб запобігти хакерських атак та порушення даних, вони використовують брандмауери, системи виявлення та попередження вторгнень, honeypots (ресурс, що використовуються як приманка для зловмисників), а також відповідне навчання та політику, яка прийнята їх менеджерами безпеки.

Але не лише соціальні мережі несуть в собі загрозу конфіденційності. За останні кілька років месенджери також стали невід'ємною частиною нашого повсякденного життя. Нехай телефонні дзвінки та переписки в соціальних мережах залишаються дуже популярними засобами спілкування, та все більше особистих та ділових розмов, голосових та аудіо-дзвінків відбувається за допомогою програм месенджерів. Не в останню роль це зумовлено різними уявленнями про їх безпеку. Треба одразу зазначити, що під месенджарами маються на увазі не клієнти соціальних мереж – в першу чергу такі як Вконтакте та Facebook. Не дивлячись на зовнішню схожість, наприклад Facebook Messenger з подібними програмами, це лише доповнення до соціальної мережі, що зберігає всі переписки користувачів на своїх серверах, що автоматично ставить їх під загрозу у разі злому аккаунта або інтересу спецслужбами тієї країни, де знаходяться сервера. А тому необхідно звернути увагу на «чистокровні» месенджери, наприклад, WhatsApp, Telegram, Viber, Skype та інші [5].

Ціль роботи є визначення сутності понять соціальних мереж та месенджерів, зробити огляд, дослідження та аналіз питання безпеки в таких явищах та месенджери, характеристику сучасних медіа, проаналізувати рівні захисту захищеності конфіденційних даних.

Для досягнення поставленої мети в кваліфікаційній роботі вирішені наступні задачі:

1) Досліджені й проаналізовані використання соціальних мереж та месенджерів.

2) Досліджені й проаналізовані рівні загроз в соціальних мережах та месенджерах.

3) Виконано дослідження принципів забезпечення безпеки приватної інформації на мобільних пристроях.

4) Виконано порівняльний аналіз існуючих програмних засобів призначенних для обміну приватною інформацією.

5) Розроблено програмне забезпечення з використанням алгоритмів шифрування.

Наукова новизна полягає в тому, що було зроблено спробу систематизації знань з питань захисту конфіденційних даних, що розміщуються на сторінках соціальних мереж, та таємниці листування за допомогою месенджерів. .

Практична цінність результатів роботи полягає в тому, що виконано порівняльний аналіз захищеності за різними критеріями месенджерів. Отримані результати є основою для формування системи критеріїв порівняльної оцінки месенджерів та обґрунтуванням їх вибору з точки зору безпеки.

У якості подальших досліджень можлива доробка існуючої програмної реалізації до еталонної, а також доробка й самої еталонної архітектури. У сучасному світі з'являються всі нові способи атак, тому й засобу захисту повинні розбудовуватися.

Використовуючи це дослідження, будь-яка людина, яка не довіряє стороннім розв'язкам і розроблювачам, здатний при необхідності побудувати свій власний захищений канал для передачі інформації між мобільними обладнаннями.

Публікації. Робота була представлена на конференції VIII Міжнародної науково-практичної інтернет-конференції молодих учених та студентів

«Актуальні проблеми автоматизації та управління». в 2020 році з темою роботи «Дослідження безпеки інтернет месенджерів»

Структура й об'єм роботи

Кваліфікаційна робота складається з вступу, 5 глав, висновку й списку використаних джерел, викладених на 89 сторінках машинописного тексту, що включає 15 таблиць, 9 рисунок і список літературних джерел з 46 найменувань.