РЕФЕРАТ

ПЗ: 84 с., 8 рис., 12 табл., 31 джерел.

Приводиться дослідження основних характеристик популярних на сучасному ринці систем обміну миттєвими повідомленнями та соціальних мереж, визначаючих конфіденційність користувацьких даних та тих, що забезпечують таємницю листування, розмов та інших повідомлень. В ході роботи було складено рейтинг соціальних медіа, які відповідають заданим критеріям безпеки.

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

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 та соціальних мереж. Отримані результати є основою для формування системи критеріїв порівняльної оцінки месенджерів та соціальних мереж та обґрунтуванням їх вибору з точки зору безпеки.

АНАЛІЗ, БЕЗПЕКА, ЗАХИСТ ІНФОРМАЦІЇ, КОНФЕДИЦІЙНІСТЬ, МЕСЕНДЖЕР, СОЦІАЛЬНІ МЕРЕЖІ

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

IM – instant messenger

ІБ – інформаційна безпека

SNS – Social networking service

E2EE – end-to-end encryption

HTTPS – HyperText Transfer Protocol Secure

ВСТУП

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 зовсім інша річ, коли мова йде про соціальні мережі. Служба соціальних мереж (SNS - Social networking service або соціальна мережа, або соціальні медіа), така як Facebook не настільки ж безпечна, незважаючи на технології, що застосовуються на їх об'єктах, або на політику, встановлену їхнім персоналом безпеки. Основна причина цього – це інформація, яку користувачі виставляють у соціальні мережі. Згідно зі статтею «A privacy paradox: Social networking in the United States», вражаюча популярність соціальних мереж, які часто використовуються підлітками та людьми, які не мають розуміння конфіденційності та безпеки, веде до величезної кількості потенційної приватної інформації, що розміщується в Інтернеті, де інші можуть отримати доступ до неї. В статті говориться, що взаємодія з людьми не є новим, але це середовище для відносин відносно нове. Також в ній пишеться: «Соціальні мережі стали популярним місцем для вивчення молодіжної культури, відносин та місцем, де можна ділитися культурними цінностями». В іншому джерелі «Social Networking Sites and Their Security Issues» пишеться про те, що дуже легко спілкуватися з іншими людьми, використовуючи соціальні мережі, а також, що вся інформація, яку ви розміщуєте на цих сайтах протягом багатьох років, складається з колекції інформації, яка називається вашим профілем, і майже будь-хто в мережі може її бачити, особливо ваші друзі. Тому при постійному поширенні соціальних мереж існує постійний ризик для безпеки інформації, але не тільки з боку хакерів або злодіїв, а й з фальшивої довіри, яку багато хто має при розміщенні приватної інформації про себе в Інтернеті. Це величезний ризик, але його можна побороти освітою.

Дана стаття також стверджує, що Facebook, Instargam та інші сайти стали частинами наших життів та використання Інтернету. Таким чином, складне величезне

сховище персональних даних в Інтернеті - це недбайливе ставлення та надмірна довіра людей, де люди, особливо підлітки, викладають особисту інформацію. Ця інформація також може міститися у відзнятих фотографіях, наприклад, фотографія, що була знята перед вашим будинком, може містити номер будинку. Люди не дуже уважно ставляться до своєї безпеки та безпеки своєї інформації. Важливо бути обережним, коли ми щось робимо в Інтернеті, адже неуважність може призвести до розміщення інформації, яка не повинна бути доступною для інших [3-4].

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. Для прикладу візьмемо Росію, де достовірні випадки перехоплення переписки в Facebook одиничні, і якщо вірити інформації, що наявна, ця соцмережа співпрацює з російськими органами влади не надто охоче, то Вконтакте з цієї точки зору не найнадійніший – адже доступ російських правоохоронних спецслужб до листування та особистих даних користувачів цієї мережі в Росії на ділі обмежений лише їх особистим бажанням. А тому необхідно звернути увагу на «чистокровні» месенджери, наприклад, WhatsApp, Telegram, Viber, Skype та інші [5].

1. ОГЛЯД СОЦІАЛЬНИХ МЕРЕЖ ТА МЕСЕНДЖЕРІВ

1.1 Соціальні мережі

SNS – це веб-додаток, що використовується людьми для побудови соціальних мереж або соціальних зв'язків з іншими людьми, які поділяють подібні особисті чи кар'єрні інтереси, діяльність або мають реальні зв'язки. Різноманітність автономних та вбудованих служб соціальних мереж, які наразі доступні в Інтернеті, висуває проблеми визначення; однак існують деякі загальні риси:

а) послуги соціальних мереж - це інтернет-додатки;

б) користувальницький контент є джерелом життєдіяльності організацій SNS.

Більшість служб соціальної мережі є веб-ресурсами та забезпечують засобами для взаємодії користувачів через Інтернет, наприклад, електронною поштою, миттєвими повідомленнями та через Інтернет-форуми.

Соціальні мережі змінюються, вони можуть включати в себе низку нових інформаційних та комунікаційних інструментів, що працюють на настільних комп'ютерах та ноутбуках, на мобільних пристроях, таких як планшетні комп'ютери та смартфони. Вони можуть виконувати функції запису цифрових фотографій / відео / обміну та щоденного входу в Інтернет (ведення блогу). Служби соціальних мереж іноді вважаються соціальними мережами, хоча в ширшому сенсі служба соціальної мережі зазвичай надає індивідуальну послугу, тоді як соціальні мережі в Інтернеті зосереджені на групі. Визначаючи як "веб-сайти, які сприяють побудові мережі контактів для обміну різними типами вмісту в Інтернеті", сайти соціальної мережі забезпечують простір для взаємодії. Соціальні мережі дозволяють користувачам обмінюватися ідеями, цифровими фотографіями та відео, публікаціями та інформувати інших про діяльність та події в Інтернеті чи в реальному часі з людьми у своїй мережі. У той час як особисті соціальні мережі - такі як збирання на сільському ринку для обговорення подій - існували з самого раннього розвитку міст, веб-сайти дають змогу людям спілкуватися з

іншими людьми, які живуть у різних місцях, по всьому світу. Залежно від платформи соціальних мереж учасники можуть зв'язатися з будь-яким іншим учасником. Успіх служб соціальних мереж можна побачити в їхньому домінуючому становищі в суспільстві сьогодні. Це можна побачити на прикладі Facebook, який має 2,13 мільярда активних щомісячних користувачів і в середньому 1,4 мільярда активних користувачів в 2017 році. LinkedIn, соціально-мережевий сервіс, зазвичай вимагає, щоб користувач особисто знав іншого користувача в реальному житті, перш ніж він «зв'язався» з ним в Інтернеті. Деякі служби вимагають, щоб учасники мали наявне з'єднання для зв'язку з іншими учасниками.

Основні служби соціальних мереж містять деякі особисті данні (наприклад, вік, професія чи релігія), мають зв'язок із друзями (як правило, з описом сторінок) та систему рекомендацій, пов'язану з довірою. Можна класифікувати соціальні мережі за трьома видами [6]:

а) розмовні соціальні мережі, що використовується переважно для спілкування з друзями (наприклад, Facebook);

б) мережеві соціальні мережі, що використовуються в основному для несуспільних міжособистісних комунікацій (наприклад, LinkedIn, сайт, що орієнтований на кар'єру та на роботу);

в) служби соціальних мереж, які використовуються, перш за все, для того, щоб допомогти користувачам знаходити певну інформацію чи ресурси (наприклад, Goodreads, Github).

2. Месенджери, додатки для смартфонів

Додатки для обміну повідомленнями, месенджер – це програми та платформи, що дозволяють створювати обмін повідомленнями, деякі з яких починалися навколо платформ соціальних мереж [7], але багато з них перетворилися на об’ємні платформи,

що дозволяють оновлювати статус, здійснювати платежі та торгівлю онлайн за допомогою чатів (електронна комерція через чат).

Деякими прикладами популярних програм для обміну повідомленнями є WhatsApp, китайські WeChat і QQ Messenger, Viber, Line, Snapchat, KakaoTalk [8], Google Hangouts, Blackberry Messenger та Zalo. Деякі служби соціальних мереж пропонують послуги обміну повідомленнями як компонент їх загальної платформи, такі як Facebook Messenger, а також функції прямого обміну повідомленнями Instagram і Twitter [9-10].

Месенджери – це найпоширеніші додатки для смартфонів, з яких у 2018 року понад 1,3 мільярди людей є користувачами WhatsApp та Facebook Messenger, 980 мільйонів щомісячно активних користувачів WeChat та 843 мільйони щомісячно активних користувачів QQ Mobile [11].

Програми для обміну повідомленнями відрізняються від попередніх поколінь платформ обміну миттєвими повідомленнями, таких як неіснуючі AIM, Yahoo! Messenger та Windows Live Messenger, тим що в основному вони використовуються через мобільні додатки на смартфонах, а не на персональних комп'ютерах, хоча деякі додатки для обміну повідомленнями пропонують веб-версії або програмне забезпечення для операційних систем для ПК.

Оскільки люди, змінили в 2010-х роках функціональні телефони на смартфони, то вони перейшли від традиційних дзвінків та SMS-повідомлень (які є платними сервісами) до безкоштовних додатків для передавання повідомлень або вимагають лише невеликих витрат на отримання послуг [12].

У програмах обміну повідомленнями є деякі з таких функцій [13]:

а) чат:

1) текстовий чат;

2) груповий чат;

б) списки трансляцій:

1) чатботи (включаючи "бот у групових чатах");

2) «Інтелектуальні відповіді» (запропоновані відповіді на вхідні повідомлення, надані платформою Google's Reply);

в) дзвінки:

1) голосові виклики;

2) відеодзвінки;

г) файлообмінник;

д) ігри;

е) "міні програми" (наприклад, Міні програма WeChat);

є) огляд новин (наприклад, Snapchat Discover);

ж) платежі або мобільний гаманець, наприклад WeChat Pay;

и) особисте (хмарне) сховище;

з) Push-сповіщення;

і) оновлення статусу (статус WhatsApp, WeChat Moments);

ї) наклейки (стікери);

к) віртуальний помічник, наприклад Google Assistant в Google Allo;

л) ефемерні обміни повідомленнями (зображення або текст, які самостійно видаляються через короткий час після отримання або після перегляду одержувачем).

1.3 Становлення соціальних мереж

Засновниками теорії соціальних мереж стали в 1951 році Рей Соломонов та Анатолій Рапопорт. А через вісім років стали з'являтися статті угорських математиків Поля Ердоса і Альфреда Рен`ї. Писали вони в часовому проміжку - 1959-1968 рр. У статтях були викладені принципи формування соціальних мереж як. Поняття «соціальна мережа» з'явилося ще у 1954 році, проте це поняття не відповідало тому, яке розуміння вкладається в нього в сучасному світі. Визначення цього феномену дав Джеймс Барнс, соціолог «Манчестерської школи»: «соціальна мережа» – це соціальна

структура, що складається з групи вузлів, якими є соціальні об'єкти (люди або організації), і зв'язків між ними (соціальних взаємин).

З плином історії соціальних мереж наукова концепція, створена Дж. Барнсом, набувала популярність, спочатку в розвинених капіталістичних країнах, потім і в східній Європі. У міру розвитку інформаційних технологій в суспільстві стали створюватися види комунікацій, відмінні від традиційних. Типи взаємовідносин, існуючих в «реальному світі», стрімко увійшли в соціальну мережу. Так в кінці 60-х Дункан Уоттс і Стівен Строгач представили математичну теорію розвитку соціальних мереж, а також ввели поняття коефіцієнта кластеризації (clustering coefficient), тобто ступеня близькості між неоднорідними групами.

Таким чином, до 70-х років сформувався повний і остаточний комплекс соціологічних і математичних досліджень, який і став науковим фундаментом статистики та аналізу соціальних мереж.

Перша соціальна мережа в історії з використанням комп'ютерної техніки стала технологія електронної пошти в 1971-му, яка використовувалася військовими в мережі ARPA Net [6, 13-14].

1988 подарував технологію «IRC» (англ. Internet Relay Chat), тобто – інтернет-чат, що ретранслюється, який з'єднав користувачів і дозволимо їм спілкуватися в реальному часі. Творцем IRC був 20-річний фінський студент Йаркко Ойкарінен [14-15].

Знаковою подією стало винахід Інтернету, який став публічним в 1991 році, завдяки британському вченому Тіму Бернерс-Лі.

У 1995 році Ренді Конрадом був створений сайт Classmates.com - перша соціальна мережа в більш сучасних визначеннях. Звісно, в сучасному розумінні вельми важко вважати цей сайт соціальною мережею, оскільки спочатку в ньому не було функцій створення профілів і додавання в друзі. Але навіть назва сайту (а переводився вона як «однокласники») – вже стало поштовхом для створення в найближчому майбутньому повноцінних соціальних мереж. Спочатку на сайті

користувачі могли тільки бачити список навчальних закладів та хто навчався в них. Проект став швидко розвиватися. Дана мережа і до цього дня залишається дуже затребуваною і налічує понад 50 мільйонів користувачів. З цього моменту починається бурхливий розвиток соціальних мереж в Інтернеті.

Загалом, світ був готовий до народження повноцінної соціальної мережі. Існує гіпотезу шести кроків, створена експериментом Мілграма з 300 адресатами паперової пошти. Так ось, ця теорія була розроблена і покладена в основу створеної в кінці 1996 (поч. 1997 року) року соціальної мережі SixDegrees [6, 14]. У цьому проекті вже були закладені такі функції як створення власного профілю-сторінки, листа друзів і можливість пошуку друзів по всьому даному проектом. SixDegrees почав набувати популярності. А в 2000-му році був навіть проданий за 125 млн. доларів. Але в 2001-му році ця соціальна мережа перестала існувати.

Близькими до SixDegrees були і інші соціальні мережі, які виникали одна за одною в інтервалі між 1997 і 1999 роками. У 1997-му з'явився універсальний органайзер AsianAvenue, який згодом перетворився в соціальну мережу.

У 1999-му стартує відразу кілька соціальних мереж: Cyworld запущена у вигляді форуму, але функції соціальної мережі були додані лише в 2001 році [6, 12]; QQ стартує як сервіс миттєвих повідомлень; Blackplanet запущена у вигляді онлайн-спільноти.

18 березня 1999 року американським студентом-програмістом Бредом Фіцпатріком був створений Livejournal (Живий Журнал або ЖЖ). Надалі сервіс став масовим хостингом блогів і придбав величезну популярність в країнах СНД. Саме Livejournal вперше надав можливість створювати спільноти і вести в них спілкування.

У 2001 році виникає ресурс для пошуку ділових контактів - Ryze. Фактично ця мережа дала в майбутньому поштовх до розвитку вже широко популярною LinkedIn.

У 2002 році розробляється сайт знайомств Friendster. Його автор - Джонатан Абрамс. Примітно те, що ця соціальна мережа була адаптована для того, щоб допомагати людям знаходити нових друзів і знайомих в списках своїх друзів. А не намагатися познайомити незнайомих один одному, як роблять всі звичайні сайти

знайомств. Дане нововведення зробило цей сайт дуже популярним в перші місяці його існування.

У наступні кілька років відбулася поява не одного десятка аналогічних сервісів. Офіційним початком буму соціальних мереж прийнято вважати 2003-2004 роки, коли були запущені LinkedIn, MySpace і Facebook [13, 16].

У грудні 2002 року було створено LinkedIn. У травні 2003 вона запускається і займає гідне місце серед мереж для професіоналів.

У 2003 році з'явилася нова соціальна мережа MySpace. Тоді вона підкорила багатьох. Можливість створення персональних профілів, зручні настройки зовнішнього вигляду, спільноти за інтересами, розміщення фотографій, а також відео та ауді відомих виконавців, власний блог. Все це дало можливість MySpace у 2006 році стати найпопулярнішою соціальною мережею в усьому світі. Мережа полюбилася рок-колективам, та й багато музикантів стали використовувати мережу для само презентації. А їхні прихильники - для спілкування зі своїми кумирами.

В цей же час виникли і такі, в минулому популярні мережі, як Hi5 (створена Ramu Yalamanchi, в кінці року 2007 в мережі було більше 70 мільйонів зареєстрованих користувачів, більшість з них в Латинській Америці), OpenBC і Tribe.

2004 рік – один з найбільш знакових років. Саме цього року з’явилися такі мережі як [12]: aSmallWorld (приватна мережа з доступом тільки за запрошенням), Piczo, Dogster, Facebook, Mixi, Multiply, Dodgeball, Flickr.

Тут варто відмітити саме Facebook, який розпочав свою діяльність у 2004 році, ставши найбільшим сайтом соціальних мереж у світі на початку 2009 року. Facebook був вперше представлений як сайт соціальних мереж Гарвардського університету. У ньому використовується той самий механізм спілкування, трохи в іншій площині, що призводить до історичної революції в цій області. Ярослав Скворцов, міжнародний журналіст, пише про дітище Марка Цукерберга в такий спосіб: «Facebook – це реальний виклик». Він говорить про те, що з часом природним чином з'являються нові

інструменти для комунікацій і отримання інформації, як колись це було друковане слово, тепер це Facebook.

Безумовно незабутньою подією в історії соціальних мереж стала робота Тіма О'Рейлі. В кінці вересня 2005 року в світ виходить його стаття, яка здійснила переворот в області розуміння нових медіа. Значуще місце в статті Tim O'Reilly «What Is Web 2.0» відводиться в тому числі і «масовому спілкуванню». Особливу увагу автор звертає на користувацьку активність, а також взаємодію з користувачами, завдяки яким вийшли такі вдалі бізнес-проекти як Ebay і Amazon. Тім О'Рейлі вказує на те, що «мережеві ефекти від взаємодії з користувачами – це ключ до ринкового домінування в епоху Веб 2.0».

Першим поколінням мережевих сервісів прийнято вважати той Інтернет, який більшою мірою був місцем, де відвідувачі шукали і використовували інформацію, що вже зберігалася, ніж сервісом, що дозволяє працювати спільно і обмінюватися даними. Веб 1.0, порядковий номер якого був привласнений вже після виникнення Веб 2.0, представляв собою сховище різнопланової інформації, поповнення та редагування якої було складним і трудомістким, недоступним для зміни «звичайними» користувачами, тому виконувалося окремими «привілейованими» людьми або програмними агентами. Становлення платформи Веб 2.0 як суб'єкт-суб'єктної форми комунікації у всесвітній павутині важливо з точки зору масового вторгнення цієї технології в повсякденне життя людей. Поява інтернету привела до технологічних змін, а поява веб 2.0 і потім соціальних мереж призвели до масштабних антропологічним змін, перш за все, тому що вони стали найбільшим в історії сховищем особистої інформації про людство [15].

Twitter був заснований в 2006-му і отримав велику популярність під час конференції SxSW (South by Souhtwest) в 2007-му. Під час конференції твіти примножилися в три рази з 20 до 60 тисяч. Twitter створив соціальну мережу, яка зараз має безліч популярних користувачів. Він також породив ряд сторонніх сайтів і додатків, стаючи більше платформою ніж простим сервісом [1].

Що стосується розвитку соціальних мереж на території України, то слід відміти, що до останнього часу популярними буду такі соціальні мережі як:

а) «Вконтакте», яка була розроблена Павлов Дуровим і почала працювати 10 жовтня 2016 року;

б) «Одноклассники», яка була заснована 12 січня 2007 року Альбертом Попковим;

в) Facebook.

Звісно після заборони російських соціальних мереж на території України виникали спроби створення власних мереж: «Ukrainians», «Nimses», «Сусід. Online». Але прожили ці проекти недовго, тай особливою популярністю серед користувачів вони не користувалися.

Втім, за минулі роки «Ukrainians» – вже далеко не перша спроба створити соцмережу для українців. У 2014 році, з початком війни на сході України, багато українців стали шукати альтернативу російським соцмережах. У 2014 році з'явилася соціальна мережа WeUa, яка була створена на базі Facebook, але проіснувала недовго. Також відомо про такі ресурсах, як UKRFACE, UkrOpen, Ц.укр, weua.info (зараз - inrepublic.com) і druzi.life, ukrainci.org.ua, січ.укр, namaidani.com. Але жоден з них так і не зміг скласти реальної конкуренції забороненим тепер російським соцмережах.

1.4 Месенджери – один з основних засобів комунікації у сучасному світі

Щодо месенджерів то першим, з відомих на сьогоднішній день, став ICQ (назва походить від англійських слів I SEEK YOU - я шукаю тебе), що з'явився в 1996 році. Все почалося з того, що четверо школярів з Ізраїлю створили компанію Mirabilis і почали працювати над програмою для спілкування в Інтернеті і локальних мережах. Створивши програму, вони розіслали її безкоштовно друзям і знайомим. Ті, в свою чергу, приводили в «аську» своїх друзів і знайомих. Кількість користувачів зростала в

геометричній прогресії. А через деякий час талановита четвірка випустила корпоративну версію ICQ. «Аська» стала піонером ринку месенджерів. Слідом за «аською» з'явилися AIM і MSN / WLM, а також Gadu-Gadu, QQ, NateOn, Google Talk, Miranda, QIP, Skype і багато інших, в тому числі єдиний відкритий стандарт - XMPP або Jabber.

Попри всю різноманітність месенджерів було щось, що їх об'єднувало: «статус присутності».

Коли користувач відкривав додаток, перше, що він бачили, - список, що містить всі його контакти і їх статуси, які вказують чи «В мережі» вони. Великі миготливі іконки повідомляли, хто в даний момент доступний, зайнятий або відійшов.

Звукові повідомлення дозволяли дізнатися про зміну статусу друзів. За замовчуванням, при вході в систему користувач також транслював всьому світу, що він в мережі.

Щось обговорювати зі співрозмовником можна було, тільки коли він перебував в мережі. Були й групові чати, але їх використання також було пов'язано з безліччю проблем і обмежень. Приєднатися до групового чату можна було лише увійшовши в мережу, але при цьому учасники чату не обов'язково могли бути в мережі одночасно з користувачем. Будь-яка людина могла бути раптово відключена з будь-якої причини (нестійкість з'єднання або телефонний дзвінок). Вона пропускала всі розмови, що відбувалися в той час, поки вона перебувала оффлайн. Крім того, групові чати були постійно завалені автоматичними повідомленнями про зміну статусу контактів: «Іван приєднався», «Антон відключився».

Деякі служби месенджерів пропонували використання голосу і відео. Але в той час комп'ютери не були оснащені вбудованими веб-камерами, а самі веб-камери коштували цілий статок, і якість їх зйомки була просто жахливою.

Більшість функцій передачі голосу і відео були доступні тільки в розмовах один-на-один, і практично ні один додаток не було сумісний з наземною лінією зв'язку або мобільними телефонами.

Але при цьому безліч людей використовували перші месенджери для передачі один одному файлів, так як в той час відправлення «важких» (2MB і більше) файлів по електронній пошті було просто неможливим: або очікування закінчення передачі файлу і закриття вікна пошти займало дуже багато часу, або сервери мали обмеження за розміром файлу. У месенджерах ж така можливість була, хоч вона і відрізнялася деякою складністю при реалізації. Відправник пропонував файл і чекав, поки приймає погодиться на пересилку файлу і дочекається закінчення його завантаження. Іноді пропозицію прийняти файл могло висіти протягом тривалого часу або взагалі зазнати невдачі. Більшість месенджерів мали обмежену пропускну здатність, а деякі навіть цензуру (деякі формати файлів неможливо було передати з причин безпеки). Крім того, передача файлів враховувалася поза контекстом чату. Жоден маркер в розмові не вказував, які саме файли ви передавали або брали.

Поступово багато проблем першої серії месенджерів були виправлені або зважилися самі собою. З'явилися DSL модеми, які надавали високошвидкісне і набагато більш стабільне підключення, оффлайн-повідомлення та журнали бесід, в яких фіксувалася історія чатів. Прийшов час перших смартфонів, які привели до нових видів месенджерів [17].

Своєю появою нові месенджерів зобов'язана масовому зростанню кількості користувачів смартфонів, яке, в свою чергу, безпосередньо пов'язане з виходом в 2007 році iPhone і в 2008 році Android. Новим об'єднуючим початком став «Додаток», яке привело до повного переосмислення самого поняття месенджера [18].

«Вбивцю» ICQ в 2009 році придумав український емігрант Ян Кум, який з дитинства живе в Каліфорнії. Ідея соціального сервісу прийшла йому в голову, коли він купив iPhone і вивчив магазин додатків App Store.

Спочатку WhatsApp не був месенджером – Кум створив сервіс, який показував статус контактів з телефонної книги: чи в мережі абонент, розмовляє він по телефону, коли у нього сяде акумулятор. Сервіс також дозволяв виставляти свій статус в ручну.

WhatsApp не користувалося попитом до тих пір, поки в червні 2009 року Apple не запустила опцію push-повідомлень. Додатки стали нагадувати про себе, навіть коли власник iPhone не користувався ними. Тепер кожен раз, коли користувач WhatsApp змінював свій статус, сервіс сповіщав про це весь список його контактів. Люди стали відповідати один одному статусами, і додаток сам по собі перетворився на засіб спілкування.

У той час свій месенджер з прив'язкою до номеру телефону був тільки у BlackBerry, але він дозволяв спілкуватися тільки власникам цього смартфона. У iPhone ще не було iMessage; Google Talk, Skype і ICQ програвали WhatsApp, оскільки список контактів в цих сервісах не був прив'язаний до номерів телефонів. До слова, коли Кум створював WhatsApp, він кілька місяців вручну синхронізував його з усіма префіксами, які використовуються в телефонних номерах по всьому світу.

У серпні 2009 року вийшла друга версія WhatsApp – з функцією обміну повідомленнями. Аудиторія сервісу за кілька тижнів зросла до 250 тисяч користувачів. У грудні того ж року додаток навчили відправляти фотографії. WhatsApp став коштувати один долар, але приплив користувачів посилився, хоча додаток і зробився платним. До початку 2011 року WhatsApp став найпопулярнішим додатком в американському App Store.

Ту пору можна вважати початком буму мобільних месенджерів. Майже в кожній країні з розвиненою IT-індустрією вже є власний сервіс для безкоштовного обміну повідомленнями. Особливо вони популярні в Азії. Це пов'язано в першу чергу з високим проникненням мобільного інтернету - майже у кожного жителя Японії, Південної Кореї і Китаю є смартфон. Це стосується і бідного населення – найчастіше телефон замінює біднякам комп'ютер. Тому месенджери для них зручніше, ніж електронна пошта і соцмережі.

У кожній з перерахованих вище країн є свій лідер серед месенджерів. У Китаї це WeChat, в Японії – Line, в Південній Кореї – KakoTalk. Також є сервіси безкоштовного

обміну повідомленнями канадського, ізраїльського і російського походження. Щоб виділитися на тлі інших, вони придумують все нові і нові функції.

Якщо WhatsApp вважається «вбивцею» ICQ, то Viber називали загрозою для Skype. За три роки з моменту запуску Viber, майже не вкладаючись в рекламу, привернув 100 мільйонів активних користувачів. Аудиторія сервісу Skype, існуючого вже більше 10 років, в три рази більше. Секрет швидкого зростання Viber той же, що і у WhatsApp – прив'язка контактів до телефонної книги користувача. До того ж, коли людина встановлює Viber, всім, у кого є його номер телефону, надходить повідомлення про це.

В іншому месенджері ізраїльсько-білоруського виробництва функції незначно відрізняються від можливостей Skype. Основне призначення Viber – безкоштовні дзвінки. У мобільній версії доступні тільки аудіоразговори, проте додаток забезпечує якісну передачу голосу навіть в 2G-мережах. Також в сервісі можна відправляти повідомлення, файли і стікери.

Viber з'явився в кінці 2010 року і був першим месенджером з прив'язкою до контактів і можливістю здійснювати дзвінки. Але з тих пір ця функція з'явилася у більшості мобільних сервісів обміну повідомленнями, в першу чергу - у азіатських. Японський месенджер Line в 2011 році запустив дзвінки, в 2013 році – відеорозмови, а в березні 2014 року додалася можливість дзвонити на мобільні і міські номери за додаткову плату. У 2012 році дзвінки стали доступні користувачам китайського WeChat і південнокорейського KakaoTalk. Тоді ж WeChat запустив і відеорозмови.

У квітні 2014 року можливість дзвонити з'явилася в Facebook Messenger.

Месенджери не хочуть залишатися просто сервісами обміну повідомленнями. Багато з них вже вийшли на ринок соцмереж і блогохостингів. Піонерами в цьому, знову-таки, є азіатські сервіси. За останні три роки вони перетворилися з альтернативи смс в повноцінні соціальні платформи.

У деяких месенджерах можна оплачувати не тільки функції спілкування – стікери і дзвінки, але і купувати справжні товари. У 2013 році в WeChat з'явилася

можливість реєструвати платні акаунти компаній. Спочатку вони могли тільки рекламувати користувачам свої товари, а з літа – ще й продавати за допомогою платіжної системи TenPay, яка, як і WeChat, належить компанії Tencent.

Після відкриттів Едварда Сноудена в 2013 році з'явилася категорія месенджерів, які називають себе захищеними, або кріптомессенджерами. Їх основна функція – захист переданих даних.

Найвідомішим подібним сервісом в Росії є Telegram – проект колишнього гендиректора «ВКонтакте» Павла Дурова. Повідомлення в цьому мессенджері шифруються не на віддалених серверах, а самими мобільними пристроями. Відповідно, навіть сама адміністрація не може розшифрувати повідомлення своїх користувачів. Також в Telegram є функція самознищення повідомлення після відправки.

Telegram – далеко не єдиний сервіс, який набрав популярність на хвилі обговорення стеження американськими спецслужбами за користувачами. У Каліфорнії створили месенджер Wickr, в якому повідомлення теж не зберігаються на серверах компанії і автоматично видаляються з пристроїв користувачів. Причому не тільки зі смартфона відправника, а й з апарату одержувача. Термін, через який видалиться послання, вибирає його автор. До того ж, текст повідомлень не можна скопіювати з сервісу.

На відміну від всіх перерахованих месенджерів, в Wickr контакти не прив'язані до телефонної книги. Щоб додати нового користувача, потрібно знати адресу його електронної пошти. Більш того, щоб прочитати нове повідомлення, необхідно кожен раз вводити свій пароль.

Захищеним також є месенджер Blackberry BBM, який з 2013 став доступний для установки на iOS і Android. У ньому теж не можна зв'язатися з будь-яким користувачем зі своєї книги контактів. Щоб написати якійсь людині, потрібно повідомити йому спеціально згенерований індивідуальний PIN-код [19].

В Україні також представили свій месенджер, який за словами розробників стане альтернативою світовим месенджерам. Компанія FMS розробила у 2017 році месенджер "First" [20].

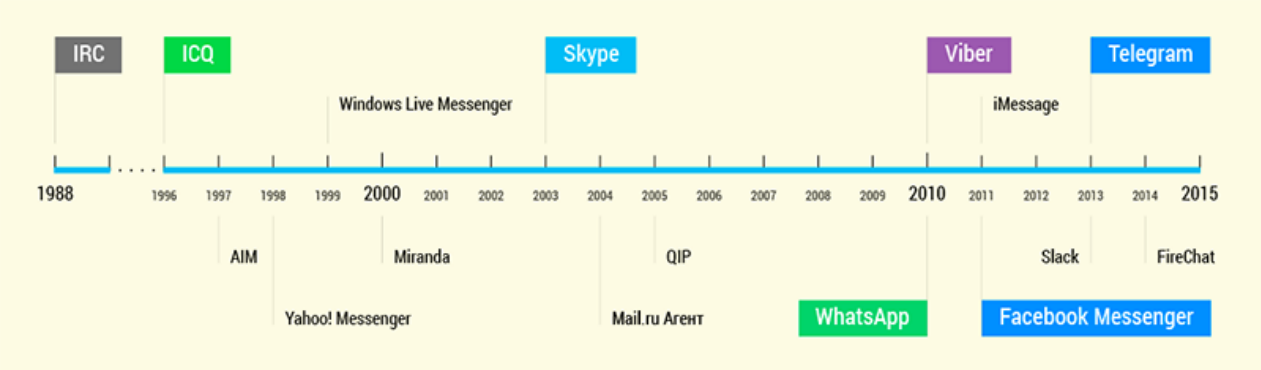


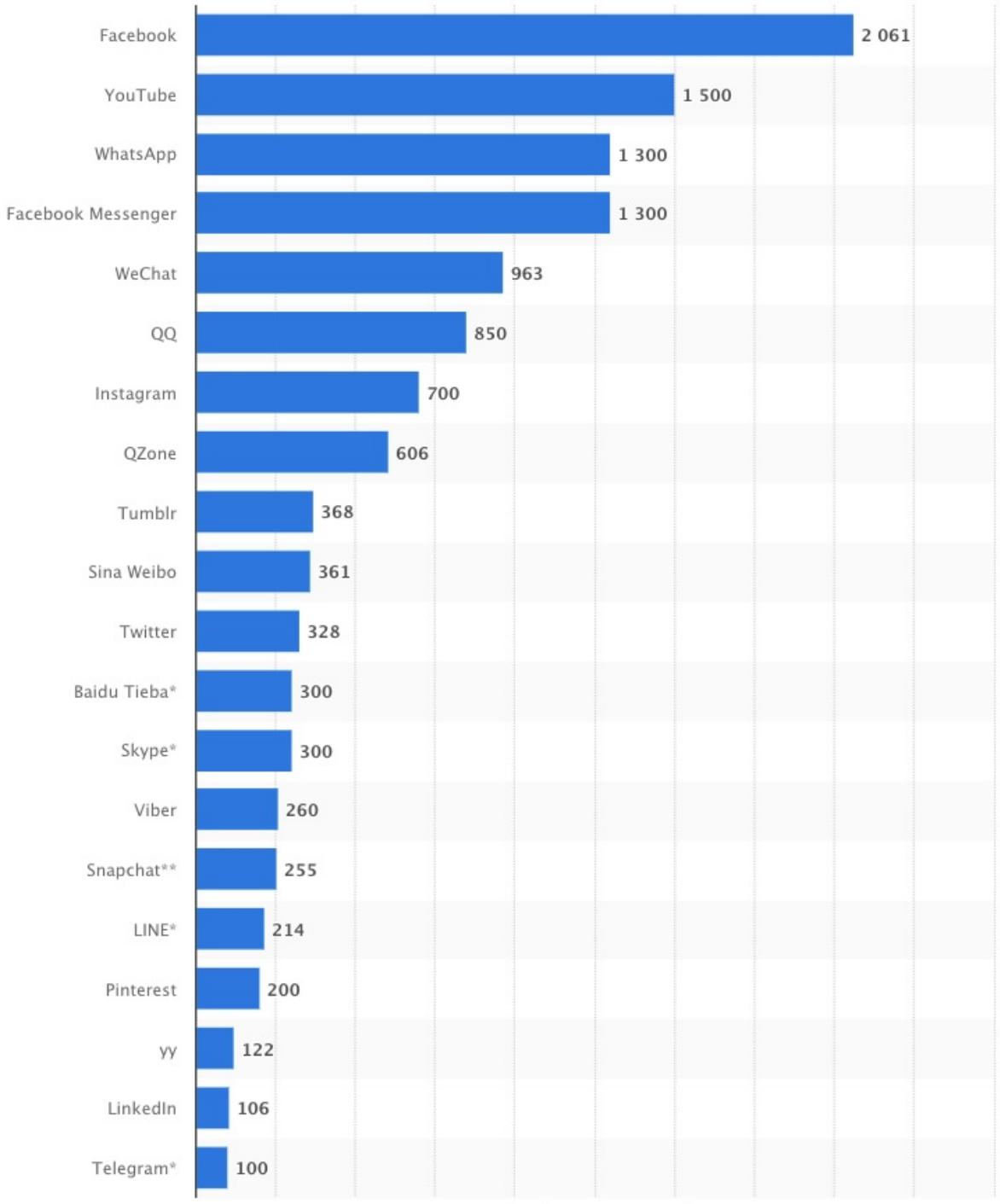
Рисунок 1.1 – Дати появи популярних месенджерів

5. Статистика користувачів соціальних мереж та месенджерів

На сьогодні соцмережі настільки міцно вкоренилися в нашому житті, що список п'ятірки найпопулярніших соціальних майданчиків практично не змінюється з року в рік. Проте, масштаби проникнення і використання цих соцмереж відрізняються в залежності від географії і демографічних чинників. Розуміння цих відмінностей грає велику роль при націлювання на конкретну аудиторію. Порівнюючи найпопулярніші соцмережі, важливо звертати увагу не на кількість зареєстрованих аккаунтів, а на число активних користувачів.

Діаграма, підготовлена аналітичним агентством Statista, дає чітке уявлення про кількість активних користувачів (в мільйонах) в найпопулярніших соціальних мережах світу. Очолює список Facebook. Навряд чи це може когось здивувати. Facebook займає більшу частину ринку завдяки більше 2 млрд активних користувачів. У січні 2017 року найбільш найближчим конкурентом гіганта був WhatsApp, який також належить корпорації Facebook. Тоді він перебував на другому місці. Сьогодні ж на другій сходинці з 1,5 млрд активних користувачів розташувався YouTube. Facebook Messenger і WhatsApp займають третє і четверте місця відповідно (див рис. 1.2).

За ними слідують платформи, більша частина аудиторії яких знаходиться на території Азіатсько-Тихоокеанського регіону (АТР). Це QQ, WeChat і Qzone (з більш ніж 600 млн. активних користувачів). Це вказує на те, що в країнах АТР є цілий ряд популярних соціальних медіа. Після них можна бачимо кластер популярних переважно на Заході площадок - Tumblr, Instagram і Twitter [21].



Рисинок 1.2 – Діаграма кількості активних користувачів в найпопулярніших соціальних мережах світу

Нижче на карті наведено поширення популярних соціальних мереж по країнам (див рис. 1.3).

Рисунок 1.3 – Найбільш популярні сайти соціальних мереж в країнах

Рейтинг соціальних мереж в Україні за 2016-2017 роки буде представлений двома графіками. Перший графік показує середню величину за 12 місяців в період з червня 2016 року по червень 2017 року (див рис. 1.4).

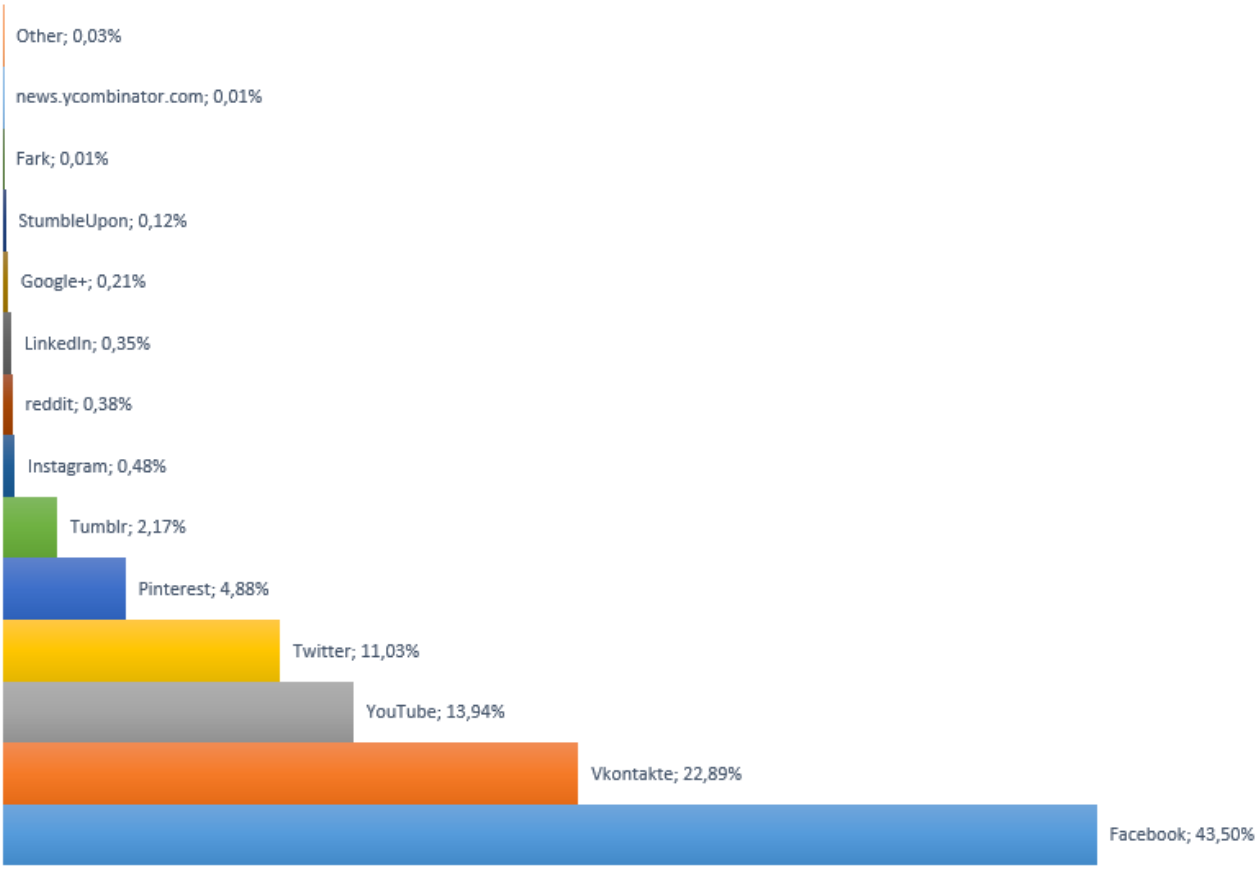


Рисунок 1.4 – Середній показник користувачів за червень 2016 – липень 2017 роки

Другий графік показує цифри станом на червень 2017 року (див рис. 1.5) [22]. Як видно з цих графіків, після заборони соціальної мережі «Вконтакте» її позиції значно змістилися, вона поступилася місцем таким соцмережам як Twitter, YouTube та Pinterest.

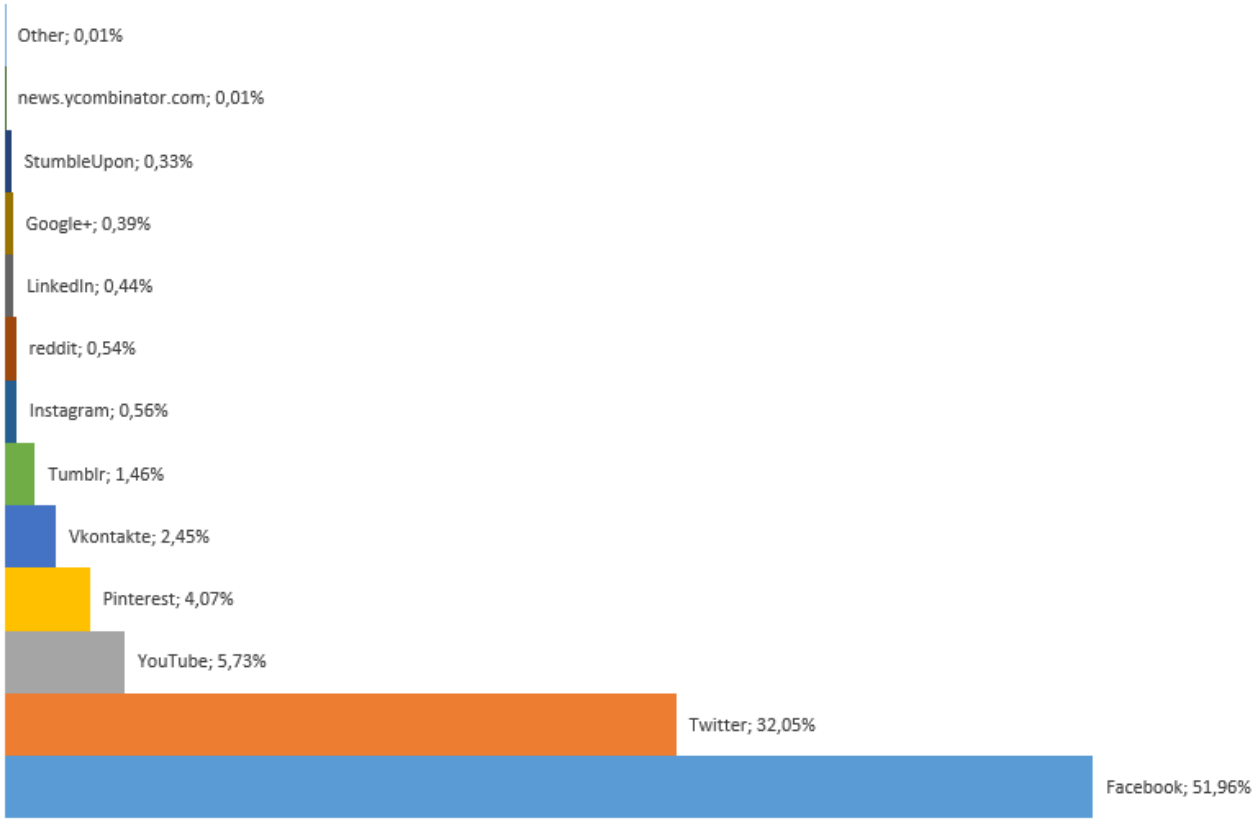


Рисунок 1.5 – Середній показник користувачів за червень 2017 року

За даним лютого 2018 року, статистика змінилася ще більше. Серед соцмереж після заборони російських сайтів в Україні впевнено лідирує Facebook з охопленням 65%. Колись лідируюча соцмережа «ВКонтакте» (39%) сьогодні поступилася місцем Instagram (48% охоплення) і посідає третє місце. Примітно, що на четвертому - Google+ з 13% охоплення, а на п'ятому «Однокласники». Настільки низьку позицію другої російської соцмережі пояснюють тим, що аудиторія «Однокласників» переважно більш зрілого віку і в основному заходить з комп'ютера, а досліджені ж враховували саме додатки.

Серед месенджерів у всьому світі лідирує WhatsApp, а на другому місці Facebook Messenger (за даними Similarweb). Але не в Україні. Беззастережне лідерство належить Viber, яким як мінімум раз на місяць користується 94% власників смартфонів (близько 40% всього населення України). Facebook Messenger займає друге місце з величезним відривом, а третє місце – не здаючи свої позиції в останні роки, месенджера Skype. WhatsApp один з найменш поширених месенджерів. Він охоплює тільки 22% користувачів смартфонів на місяць і його в Україні вже випередив Telegram з охопленням 28% (див рис. 1.6).

В середньому користувач Viber проводить в додатку 30 хвилин в день. 45% цього часу складають дзвінки і відеодзвінки. Один користувач відправляє більше 20 повідомлень в день, а 35% користувачів користуються стікерами. Розмір аудиторії в Україні на сьогоднішній день компанія не розкриває [23].

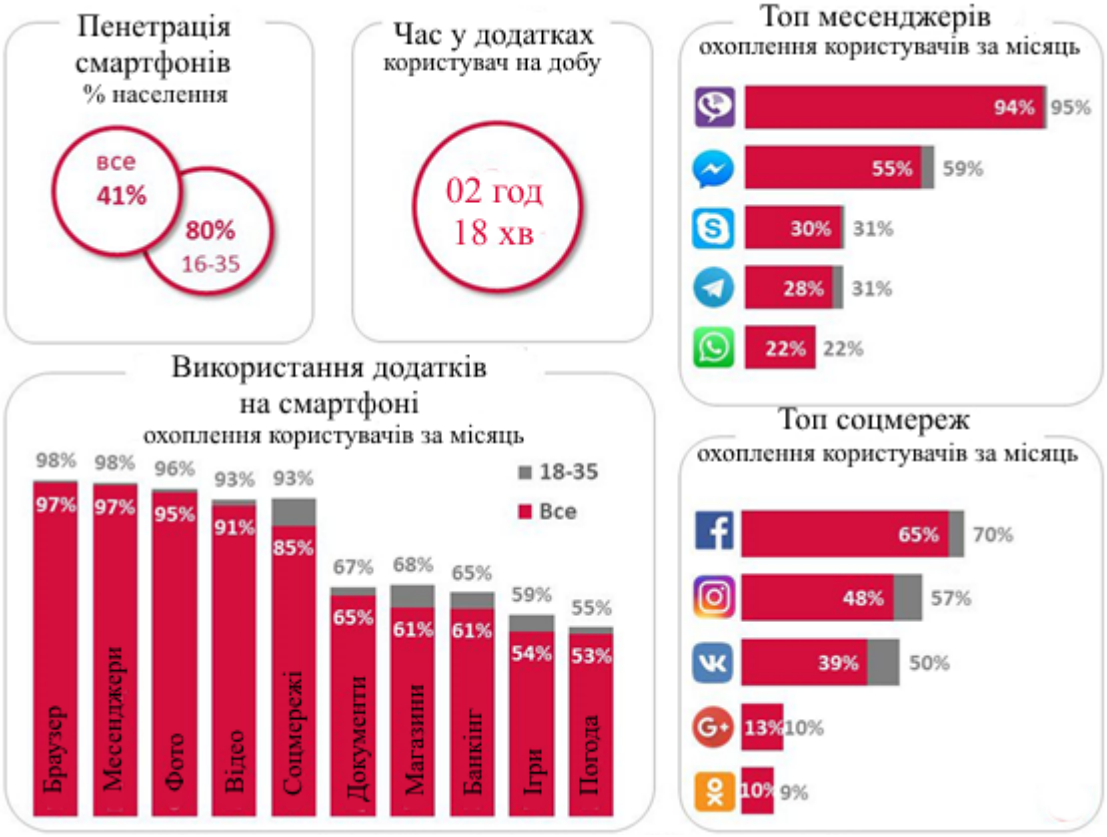


Рисунок 1.6 – Топ найбільш популярних додатків для смартфонів

2 АНАЛІЗ РІВНЯ ЗАГРОЗ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ ТА МЕСЕНДЖЕРАХ

2.1 Безпека і конфіденційність, ризики в соціальних мережах

Соціальні мережі без ризиків для безпеки не існують. Більшість соціальних мереж займаються питанням конфіденційності. В «The impact of polices on government social media usage: Issues, challenges, and recommendations» пишеться, що існує багато проблем з управління інформацією в службах соціальних медіа, в основному в сфері конфіденційності та особистої інформації, а також того, як правильно зберігати та захищати її. Це часто робить інформацію доступною державним установам. Пояснюється це тим, що, як стверджує «A privacy paradox: Social networking in the United States»: «Соціальні мережі створюють центральне сховище особистої інформації, яке продовжує зростати, коли користувачі продовжують додавати до нього нову інформацію». Що ще гірше, це підлітки, які менше турбуються про конфіденційність та безпеку, продовжують публікувати інформацію про себе дуже охоче. Іноді це в ім'я популярності. Іноді це просто чиста недбалість. Це величезна частина проблеми, і можливе рішення, яке має допомогти боротися з цим, буде запропоновано пізніше. Стаття стверджує, що «приватні та публічні межі соціальних медіа-просторів незрозумілі». Стаття продовжує зауважити, що батьки часто не знають або не дбають про те, що їх діти викладають в Інтернеті.

Інший основний ризик конфіденційності та безпеки інформації в соціальних мережах – це централізована архітектура. Як зазначалося раніше, соціальні медіа-сервери – це золота шахта особистої інформації, яку вільно поповнюють підлітки та дорослі користувачі. «Privacy and Security: Online Social Networking» стверджує, що це породжує серйозні конфлікти та може викликати такі речі, як крадіжка особистих даних та продаж даних користувачів третім особам. Користувачі мають наївно довіряють своїм соціальним мережам в питаннях захисту своєї інформації, коли в той же час її часто продають третім особам або хакерам. Вона також зазначила, що, хоча

Facebook додала параметри конфіденційності, які користувач може контролювати, їх налаштування за замовчуванням є загальнодоступними, коли обліковий запис створюється спочатку. Таким чином, новий користувач, який не змінює ці налаштування, щоб зробити їх більш строгими, насправді публікує інформацію, яку можуть переглядати усі охочі. «Privacy and Security: Online Social Networking» продовжує показувати, що кількість інформації, яка викладається користувачами у їхніх профілях на популярних сайтах соціальних мереж, може бути об'єднана для створення портрета користувача, якщо вона вам потрібна, яка містить достатньо інформації, щоб обдурити друзів користувача. Для цього злодій може створити несправжній профіль цієї людини, додати усіх друзів жертви, а потім обдурити друзів у виявленні більш особистої інформації про користувача. «Social Networking Sites and Their Security Issues» називає цю практику "клонуванням профілю". Стаття стверджує, що деякі злодії викрадають інформацію про користувачів з одного сайту, щоб створити підроблений профіль на іншому. Вона заявляє, що інформація також може бути викрадена у користувачів через використання фішингових атак, де інформація збирається про користувачів шляхом створення фальшивих веб-сайтів, які запитують особисту інформацію або навіть паролі та номери соціального забезпечення. Різні інші атаки, відповідно до цієї статті, розроблені для того, щоб або користуватись особистою інформацією користувачів, або заражати їх систему вірусами. Вони включають підключення клавіш, в яку зловмисник публікує відео користувачеві, і коли користувач його відтворює, в систему вводять шкідливий код, а також атаки введення, де використовується взламаний форум, і кожен, хто відвідує форум, заражає свою систему вірусом троянського коня. Інші ризики включають шахрайство та залякування в Інтернеті. Ризик, який приймає будь-який користувач, буде пропорційний кількості особистої інформації, яку вони вибирають для публікації, і як вони встановлюють свої параметри безпеки та конфіденційності.

Найбільша проблема полягає в тому, що багато користувачів не знають про налаштування конфіденційності та про те, як їх використовувати. Вони також «не

знають про ризики, пов'язані з завантаженням конфіденційної інформації». Дослідження показали, що сайти соціальних мереж призначені для обслуговування великої кількості користувачів в одному місці, і багато з яких користувачів не знають про те, як використовувати налаштування конфіденційності. Ці сайти оцінюють «відкритість, підключення та обмін з іншими - на жаль, ті самі аспекти, які дозволяють кібер-злочинцям використовувати ці сайти як зброю для різних злочинів». Співробітники часто публікують інформацію про компанію в соціальних мережах, вносячи ризик для організації, в якій вони працюють.

Таким чином, відповідно до «Privacy and Security: Online Social Networking», зрозуміло, що навіть якщо технології та політика можуть використовуватися на сайтах соціальних мереж так само, як і будь-яка інша організація, централізована структура та величезний репозиторій приватної інформації створюють великі прогалини в галузі безпеки. До них можна звернутися за допомогою більшої політики безпеки, деякого здорового глузду з боку користувачів та деяких архітектурних змін [3].

2.2 Проблеми безпеки в месенджерах

Одночасно з розвитком комунікації йшла еволюція кіберзлочинності. Вірус Мікеланджело з'явився в 1992 році і вважався першим деструктивним вірусом. У 1995 році з'явився макро-вірус, який спочатку поширювався через документи Word. У 1999 році з’явився Happy99, нешкідливий хробак, перший вірус, який поширювався по електронній пошті. Першим вірусом, який отримав прибуток від заражених хостів, був Fizzer, він з'явився в 2003 році.

Не існує ідеального засобу для захисту будь-якої системи. Це завжди компромісний, нескінченний, не одноразовий акт. Те, що сьогодні є безпечним, може бути небезпечним завтра. Дуже важливо постійно робити нову оцінку реалізованій практиці безпеки.

Важливо також зрозуміти, яку інформацію захищає користувач та від кого. Дані можуть зберігатися у місцевому сховищі без доступу до мережі. Метадані практично неможливо сховати. Це дані про дані – все про шматок інформації, крім самої інформації. Не вміст повідомлення, а інформація, хто, кому, коли і де його надіслали. Правові системи часто захищають вміст більше, ніж метадані. Наприклад, у Сполучених Штатах правоохоронці вимагають ордеру прослуховування телефонних дзвінків людини, але заявляє право на отримання списку, в якому вказано кому дзвонила людина.

За даними NowSecure Mobile Security Report, чверть мобільних додатків включає один або декілька недоліків безпеки високого ризику. 35 відсотків повідомлень, надісланих мобільними пристроями, не зашифровано. 43 відсотка користувачів не мають PIN-коду, графічного або цифрового пароля. 50% пристроїв підключаються до незахищеної бездротової мережі принаймні раз на місяць у США. Половина популярних додатків надсилає рекламним компаніям інформацію, таку як номер телефону, ідентифікатор пристрою, інформацію про дзвінки та географічні координати користувача.

Павло Дуров є прихильником концепції безпеки в Інтернеті та засновником програми IM із шифруванням E2E (End-to-End Encryption) під назвою Telegram. Він стверджує, що інтернет-корпорації, такі як Google і Facebook, майстерно викрали конфіденційні дані, переконавши громадськість, що найважливіші речі про конфіденційність приховують загальнодоступні публікації користувачів, фотографії та інші дані користувачів. Додавання відповідних налаштувань дозволяє компаніям заспокоїти увагу громадськості при наданні приватних даних маркетологам та третім сторонам. Джуліан Ассанж також підтримує концепцію безпеки Інтернету, він є головним редактором WikiLeaks, який публікує секретну інформацію та секретні медіа. У своїй книзі "Google Met WikiLeaks" він поділяє подібну точку зору, зазначивши, що Google – американська компанія і тісно співпрацює з політичними та військовими структурами, а не рекламує її для громадськості. Таким чином, у сучасному світі

перевага часто приділяється проекту з відкритим кодом. Інтернет-конфіденційність повинна включати захист приватних даних від підслуховування третіх осіб, як-от рекламодавців, або політиків та військових.

Отже, необхідність для миттєвого обміну повідомленнями – запобігти доступу стороннім особам до переписки між користувачами. У той же час важливо контролювати, щоб постачальник послуг не збирав конфіденційні дані та інформацію про осіб, які використовують ці месенджери. Різний аспект полягає в тому, щоб контролювати, скільки персональних даних можна зібрати зі списку контактів та умов, за яких можна додати нового друга. Дуже важливо зупинити спроби використання соціальної мережі для розвідувальних атак.

Безпечний ІМ спеціалізується на шифруванні вмісту повідомлення, забезпечуючи ключами розшифровування інформації лише фактичних користувачів, які мають доступ. Ідея користувальницького безпечного Messenger – забезпечити безпеку масам, які нічого не розуміють про безпеку. Таким чином, програма повинна бути не тільки безпечною, але і швидкою, потужною та зручною для користувачів.

Коли використовується на робочих місцях, додаток ІМ має багато корисних функцій, але також має ризики та зобов'язання в сфері безпеки, відмінні від описаних вище. Є ризики безпеки та згоди, невідповідне використання та витоку інтелектуальної власності.

Сеанс чату через публічну мережу дозволяє будь-кому в Інтернеті отримувати доступ до даних. Тому сильне шифрування має вирішальне значення. Інформація, передана через миттєві повідомлення, не повинна контролюватися та не реєструватися, щоб сприяти поліпшенню корпоративної безпеки. Смартфони збирають розширену кількість конфіденційних даних, і важливо зберегти незначний проміжок між захистом конфіденційності користувачів та захистом інтелектуальної власності компанії.

Для атакуючого існує три головні цілі: дані, справжність та доступність. Дані означають будь-яку конфіденційну інформацію про інтелектуальну власність особи чи компанії. Вони поставляється за допомогою звичайного тексту, логіну автентифікації та

паролю, приватну інформацію або журнали активності, зібрані програмним забезпеченням [2].

3. E2EE або наскрізне шифрування: опис та принцип роботи

Більшість сучасних сервісів заради безпеки виключають роботу з незашифрованим з'єднанням. Особливо активно в цій сфері працює Google, який до літа 2018 роки збирається спеціальним значком «нагороджувати» сайти, у який не використовується сертифікат HTTPS.

Тема шифрування безпосередньо пов'язана з криптовалютами. Але в світлі останніх подій (ситуація з телеграм і заяву Вконтакте), все частіше користувачі цікавляться специфікою наскрізного шифрування (воно ж кінцеве, end-to-end) [24].

Одним з найбільш популярних засобів захисту особистої переписки, який реалізований у месенджерах – це E2E-шифрування, спосіб передачі даних, коли доступ до повідомлень мають виключно користувачі, які задіяні в спілкуванні.

За рахунок використання криптографічних ключів технологія E2EE передбачає, що контроль над листуванням здійснюється безпосередньо користувачами, а розшифрувати повідомлення не можуть ні перехоплювачі, ні сервери, які передають дані.

Для того, щоб зрозуміти, що з себе представляє метод E2EE, по-перше, необхідно з'ясувати, що не є наскрізним шифруванням. Відомо про шифрування, яке використовується веб-сайтами з метою захисту онлайн активності. Наприклад сервіс https://www.gmail.com, протокол HTTPS на початку адресного рядка свідчить про те, що для шифрування передачі даних між комп'ютером і серверами Google використовуються криптографічні протоколи SSL або TLS. Даний протокол є більш безпечним, ніж HTTP і широко застосовується веб-ресурсами для захисту від перехоплення даних. Головним недоліком технології HTTPS є той факт, що при спілкуванні двох користувачів передані дані проходять через централізовані сервера

(наприклад, GMail), які мають ключі для розшифровки інформації. Щоб виключити сервера з ланцюжка, підвищивши таким чином приватність даних, можна використовувати наскрізне шифрування.

У наскрізному шифруванні кінцевими пунктами передачі є безпосередньо пристрої відправника і одержувача. Повідомлення шифрується локально на пристрої відправника і може бути розшифровано лише на пристрої одержувача. Наскрізне шифрування часто називають «шифрування на стороні клієнта» або «нульовий доступ» через той факт, що шифрування відбувається на пристроях кінцевих користувачів, а не на хмарних серверах. Завдяки даній особливості, наскрізне шифрування запобігає потенційному читанню призначених для користувача даних серверами. При реалізації наскрізного шифрування існує два види криптографічних алгоритмів: симетричний та асиметричний.

2.3.1 Симетрична криптографія

Шифрування з використанням симетричного ключа застосовується для «блокування» повідомлення. Принцип методу заснований на ідеї, що відправник генерує ключ для перетворення повідомлення в криптограму, тобто закодовану версію повідомлення, а потім відправляє цю криптограму одержувачу. Передача ключа одержувачу здійснюється по іншому захищеному каналу, тому в кінцевому підсумку одержувач зможе розшифрувати повідомлення.

Для того, щоб проілюструвати, як в дійсності працює симетрична криптографія, розглянемо передачу повідомлення з поштової адреси сервісу ProtonMail на адресу іншого провайдера послуг електронної пошти. В цьому випадку потрібно задати пароль на повідомлення і передати його вашим одержувачам. Одержувачі отримують повідомлення, що містить посилання на сторінку ProtonMail, де знаходиться зашифрований текст. Потім одержувачі вводять заданий відправником пароль до повідомлення, і повідомлення розшифровується на локальному комп'ютері. Таким

чином, пароль ніколи не покидає комп'ютер відправника і не відправляється на сервера ProtonMail, тому ніхто сторонній не може розшифрувати повідомлення.

2.3.1 Асиметрична криптографія

Головною проблемою використання симетричної криптографії є необхідність пошуку каналу для безпечного обміну ключа з одержувачем (якщо перехоплювач отримав криптограму і ключ, повідомлення буде розсекречено).

Розроблений в 1970-х роках, асиметричний метод вирішує проблему із захистом конфіденційності сгенерованих ключів за рахунок використання двох видів ключів - відкритого криптографічного ключа і пов'язаного з ним математично закритого ключа. Відкритий ключ може бути трансльований, в той час як закритий ключ ніколи не повинен бути виявлений. Відправник використовує відкритий ключ одержувача для перетворення повідомлення в криптограму і потім відправляє зашифровані дані одержувачу. Криптограма може бути розшифрована тільки за допомогою закритого ключа одержувача. Таким чином, перехоплювачі не зможуть розсекретити повідомлення навіть при наявності відкритого ключа.

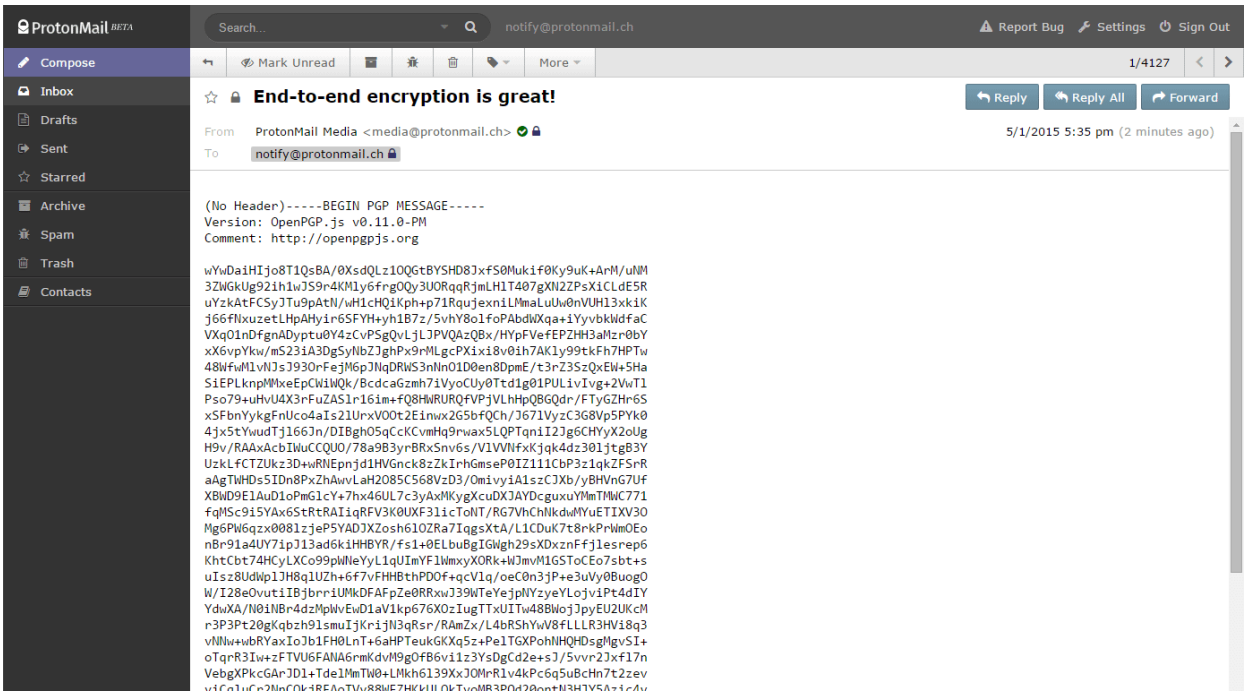


Рисунок 2.1 – Вигляд повідомлення без закритого ключа, яке було зашифроване наскрізним шифруванням

Як реальний приклад роботи асиметричної криптографії, розглянемо, як передаються повідомлення електронної пошти між користувачами ProtonMail. Процес шифрування невидимий для користувачів: для зашифровування повідомлень використовуються відкриті ключі одержувачів, а закриті ключі, які доступні тільки з коректним паролем користувачам, які авторизувалися, застосовуються для розшифрування. ProtonMail не містить паролі користувачів, тому сервіс не може розшифровувати призначені для користувача дані [25].

3 РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ ТА МЕСЕНДЖЕРАХ

3.1 Оцінка захищеності месенджерів та соціальних мереж

Громадська організація Electronic Frontier Foundation, що займається питаннями безпеки в мережі, підготувала і регулярно оновлює рейтинг безпеки месенджерів, куди включені, зокрема, і месенджери деяких соціальних мереж і поштових сервісів.

Кожен месенджер оцінюється за кількома ключовими пунктами:

а) чи зашифроване листування при передачі по мережі;

б) чи може адміністрація сервісу при бажанні прочитати переписку;

в) чи можете ви ідентифікувати контакт користувача при листуванні;

г) чи будуть зловмисникові доступні старі повідомлення в разі доступу до аккаунта;

д) чи відкритий програмний код месенджера для бажаючих його перевірити;

е) чи добре задокументований протокол безпеки;

є) чи перевірений код месенджера.

Результати їх дослідження представлені у таблиці 3.1.

Як видно на прикладі чату Facebook, він відповідає лише першій та останній вимогам, і не може вважатися безпечним засобом спілкування.

Ще більш невтішні показники у колись популярного сервісу відео-спілкування Skype. Месенджер не відповідає жодному пункту, крім шифрування листування.

Не може втішити високим рівнем безпеки і один з популярніших на теренах України месенджерів з можливістю голосового спілкування Viber. З того часу як якісні голосові дзвінки стали доступні майже в усіх месенджерах, користувачі поступово «витекли» з цього клієнта, але деякі їм все ще користуються.

Таблиця 3.1 – Результати тестування найбільш популярних сервісів обміну миттєвими повідомленнями.

Найменування сервісу	Наявне шифрування?	Чи може адміністрація сервісу при бажанні прочитати повідомлення?	Чи можна ідентифікувати контакт користувача при листуванні?	Чи отримають зловмисники доступ до старих повідомлень в разі взлому аккаунта?	Чи відкритий програмний код месенджера для бажаючих?	Чи добре задокументований протокол безпеки?	Чи перевірений код месенджера?
Facebook chat	+	–	–	–	–	–	+
Skype	+	–	–	–	–	–	–
Viber	+	–	–	–	–	–	+
WhatsApp	+	+	+	+	–	+	+
Telegram	+	–	–	–	+	+	+
Telegram (в режимі секретного чату)	+	+	+	+	+	+	+

Як видно у таблиці 3.1, у Viber провал за всіма пунктами крім шифрування листування і перевірки коду.

Значно краще оцінки у месенджера Whatsapp. Як видно, претензії до нього виникли тільки через закритого коду, який теоретично може приховувати вразливості, які використовують хакери, або залишати лазівки розробникам якимось чином отримувати доступ до листування користувача.

Однак більш слабке місце WhatsApp в системі зберігання повідомлень. Вони не зберігаються на сервері, але резервна копія зберігається на смартфоні і, якщо у користувача телефон Android, то і на його Google-диску. Якщо Google-аккаунт

користувача захищений надійним паролем та подвійною автентифікацією, то зламати його складно. Тим не менш, якщо не захищений паролем телефон якимось чином виявиться в руках тямущих зловмисників, то вони зможуть відновити повідомлення безпосередньо з Google-диска. Втім, перейшовши в Налаштування, в пункті «Чати» зберігання резервних копій легко відключити. У той же час резервне копіювання в пам'ять пристрою відключити не можна. Тобто з міркувань безпеки сам телефон повинен бути зашифрований.

Щодо Telegram то було проведено оцінювання в двох його режимах: стандартному та в режимі секретного чату.

У стандартному режимі, яким найчастіше користується більшість користувачів, все листування зберігається на серверах компанії. Це може бути причиною для занепокоєння, нехай на даний момент є деякі підстави вірити тому, що жодна спецслужба доступу до серверів не має.

1. Залишається ризик злому аккаунта в першу чергу, якщо користувач не побудував подвійну аутентифікацію в налаштуваннях.

2. Є ризик доступу до листування з боку недобросовісних співробітників сервісу.

3. У звичайному режимі немає можливості упевнитися, що листування не перехоплено кимось з боку (нехай це і малоймовірно).

У той же час, у Telegram легко включається функція секретного чату, яка дозволяє не тільки безпечно листуватися, не побоюючись злому або перехоплення листування, а й видаляти повідомлення кожному з користувачів на обох пристроях, або виставити таймер самознищення повідомлень - від секунди до тижня (що не дозволить зберегти другому користувачеві листування довше цього терміну, навіть відключившись від мережі). Тому рекомендовано по можливості частіше користуватися саме секретними чатами [5].

Аналітичний відділ Artezio провів комплексне тестування популярних месенджерів та опублікував список кращих програм, які можуть забезпечити високий рівень конфіденційності.

Додатки iOS та Android були оцінені на основі 30 критеріїв, включаючи надійність шифрування даних, рівень захисту персональної інформації (двофакторна аутентифікація), готовність розкривати персональні дані, функціональність систем зберігання листування та рівень захисту від нестандартних способ копіювання інформації. Якість шифрування даних та надійність засобів захисту інформації були основними критеріями для остаточної експертизи. Програми, що не відповідають мінімальним вимогам щодо конфіденційності, були виключені зі списку. Їх дані представлені у таблиці 3.2.

Signal, месенджер з високим рівнем конфіденційності, займає 1 місце з 8 наявних. Він отримав найкращу оцінку за наявність двофакторної аутентифікації, шифрування за замовчуванням, високоякісного протоколу шифрування та готовності розкривати особисті дані. Серед недоліків: немає функцій для видалення вмісту та захисту від скріншотів.

Wickr-messenger займає друге місце. Його рейтинг було знижено фахівцями через наявність платної, більш функціональної версії програми та відсутності даних про розкриття інформації про користувача.

Популярний Telegram займає третє місце в списку, випередивши Confide, Viber, Line, WhatsApp і iMessage.

Експерти Artezio вважають Signal найкращим додатком миттєвих повідомлень для особистої кореспонденції, а підприємствам радять використовувати Wickr.

Експерти вважають, що Facebook Messenger є найбільш небезпечним для конфіденційної кореспонденції. Деякі серйозні недоліки: низький рівень захисту інформації користувачів, включаючи готовність компанії поділитися інформацією користувачів, відсутність інструмента для видалення повідомлень на певних пристроях [26].

Таблиця 3.2 – Дані результатів тестування додатків аналітичним відділом Artezio

	Signal	WhatsApp	iMessage	Confide	Telegram	Wickr	Viber	Line
1	2	3	4	5	6	7	8	9
Шифрування ввімкнено за замовчуванням	+	+	-	+	-	+	+	-
Якість протоколу	5 з 5	5 з 5	2 з 5	2 з 5	4 з 5	4 з 5	3 з 5	4 з 5
Двофакторна автентифікація	+	+	+	-	+	-	+	+
Готовність розкривати дані користувача	5 з 5	1 з 5	2 з 5	немає даних	4 з 5	немає даних	немає даних	немає даних
Ціна	безкоштовний	безкоштовний	безкоштовний	безкоштовний з обмеженнями, 5$ для звичайного користувача, 15$ для бізнес-користувачів	безкоштовний	Безкоштовний з обмеженнями, 25$ для бізнес-користувачів	безкоштовний	безкоштовний
Платформи	IOS, Android, Desktop	IOS, Android	IOS, MacOS	IOS, Android, Desktop	IOS, Android	IOS, Android, Desktop, Windows Phone	IOS, Android, Desktop, Windows Phone	IOS, Android, Desktop, Windows Phone
Видалити повідомлення на певних пристроях	-	+	-	+	+	+	+	+
Самовидалення повідомлень	+	-	+	+	+	+	+	-
Захист від скріншотів	-	-	-	+	-	+	-	-

Місце у рейтинзі	1	7	8	4	3	2	5	6

Експерти аналітичного центру Falcongaze (компанії-розробника програмних рішень в галузі запобігання витоків даних) продовжують оцінювати на предмет безпеки технології та програми, онлайн-сервіси та платформи, без яких сьогодні не уявляють свого життя не тільки компанії і прогресивні користувачі, а й звичайні люди. Цього разу дослідники склали рейтинг популярних соціальних мереж в залежності від того, наскільки дані їх користувачів захищені.

Основою для складання рейтингу послужили два критерії: популярність соціальних мереж серед користувачів та їх безпека. Безпека оцінювалася за сукупністю наступних факторів: наявність двофакторної авторизації, захищеного протоколу, доступністю і безперебійною роботою технічної підтримки, програма баг баунті та інформацією про уразливість і витоках даних користувачів, отриманої з відкритих джерел. Місця в рейтингу присвоювалися виходячи з комплексного поєднання двох зазначених вище факторів на основі оцінки експертів.

Замикає п'ятірку найпопулярніших соцмереж, ранжируваних за ступенем їх надійності з точки зору безпеки інформації користувачів, найбільш відвідувана в світі соціальна мережа (близько 1 мільярда користувачів в день) – Facebook. Дітище Марка Цукерберга забезпечено двофакторною авторизацією, захищеним протоколом, є програма баг баунті. У жовтні 2015 року в Facebook з'явилася система повідомлень про спроби злому аккаунтів, покликана сповіщати користувачів про загрозливі їм кібератаки. Повідомлення приходять тим користувачам, чиї аккаунти, на думку сервісу, можуть бути зламані хакерами, які працюють на замовлення будь-якої країни.

Однак, за відгуками користувачів, з технічною підтримкою сервісу зв'язатися не завжди легко, так само як і отримати відповіді на свої питання.

Крім того, розробники Facebook часто змінюють налаштування конфіденційності, внаслідок чого користувачі змушені повторно повертатися до них і вносити необхідні зміни.

На четвертому місці розташувалася соціальна мережа «ВКонтакте». У травні 2015 року «ВКонтакте» запустила програму баг баунті. Протокол сервісу захищений, з недавнім редизайном соцмережі всі користувачі перейшли на захищене з'єднання HTTPS, в 2014 році з'явилася двофакторна авторизація. При цьому якщо від неї відмовитися і не прив'язати номер мобільного телефону до аккаунту, «ВКонтакте» буде нагадувати про цей прорахунок щоразу, коли користувач побажає «лайкнути» вподобанний пост. Якщо при такому нагадуванні надалі залишати без уваги номер телефону, в якості альтернативи доведеться вводити код з картинки.

Соціальна мережа «Однокласники» розташувалася в середині рейтингу аналітичного центру Falcongaze. В «Однокласниках» є двофакторна авторизація, велика база з питань, оперативна техпідтримка, зв'язатися з якою можна заповнивши форму ok.ru/help. Ще недавно захищений протокол HTTPS можна було включити опціонально, а сторінки соціальної мережі були доступні по нешифрованому протоколу – тепер же соціальна мережа повністю перейшла на захищене з'єднання.

Друге місце серед найбільш захищених соціальних мереж отримує Instagram від експертів Falcongaze.

Перше місце в контексті безпеки отримав сервіс Twitter. У Twitter все в повному порядку: з 2013 року є двофакторна авторизація, використовується захищений протокол, технічна підтримка знаходиться за адресою support.twitter.com/forms, де можна, заповнивши форму, звернутися за допомогою. Також є офіційні аккаунти підтримки на різних мовах, які періодично діляться з читачами різного роду інформацією про оновлення і так далі. До програми баг баунти соціальна мережа Twitter підключилася однією з останніх, в 2014 році [27].

3.2 Message Layer Security – новий протокол безпеки

Технології не стоять на місці і шифрування в тому числі. Інженерна рада інтернету (IETF) опублікувала чорновий варіант нового протоколу безпеки Message Layer Security (MLS). Його завдання, забезпечити захищену передачу повідомлень між двома пристроями. Він описує абстрактні структури даних, які можна використовувати не тільки в чат-додатках, але і для роботи з TLS 1.3 і JSON.

Інженери IETF випустили два документа. Перший описує вимоги до системи обміну повідомленнями для реалізації протоколу MLS, а другий сам протокол MLS.

У розробці архітектури та вимог до MLS взяли участь представники Google, Mozilla, Twitter, MIT, французького дослідницького інституту INRIA і платформи для спілкування Wire. Сам протокол створили люди з Cisco, Facebook, Google і Оксфордського університету.

Система обміну повідомленнями (Messaging Service) включає в себе дві служби, які стежать за безпекою прийому / передачі повідомлень.

Перша-служба автентифікації (Authentication Service). Відповідає за збереження особистих даних: логіна, номера телефону, а також унікальної пари ключів для ідентифікації клієнтів.

Друга-служба доставки (Delivery Service) – зберігає і розподіляє між клієнтами ключі для обміну зашифрованими повідомленнями. Служба доставки оперує тільки тими даними, які потрібні для обміну повідомленнями, і не чіпає особисті відомості про відправників. Це обмежує «слід» метаданих на стороні сервера.

У багатьох системах служби доставки і ідентифікації представлені одним логічним об'єктом або сервером. Однак в MLS це два окремих компонента. Автори вирішили розділити ці процеси, щоб MLS можна було використовувати разом з відкритими протоколами авторизації.

Це дає ще одну перевагу. Навіть якщо провайдер сервісу обміну повідомленнями контролює процеси автентифікації і доставки, метадані будуть надійно

захищені. У провайдера не вийде зв'язати зашифровані повідомлення з відкритими ключами.

Користувачі системи обміну повідомленнями об'єднуються в групи. Для створення групи учасники «складають» свої ключі UserInitKey і формують секрет. UserInitKey представляє собою ключову пару Діффі-Хеллмана і служить для ініціалізації окремих користувачів.

Протокол задіює два типи двійкових дерев. Перше дерево-Меркле (воно ж дерево хешів) – служить для підтвердження автентичності операцій, що проводяться членами групи. Друге Ratchet-дерево – використовується для вилучення їх секретів.

У групі можна проводити наступні базові операції:

а) додавати нового члена групи (створити діалог);

б) оновлювати дані секрету учасника групи;

в) видаляти члена групи.

Якщо член групи A хоче створити діалог з B і C, він в першу чергу завантажує їх ключі ініціалізації (InitKeys). Після чого ці ключі використовуються для формування повідомлень GroupAdd, які повинні додати членів B і C.

Повідомлення GroupAdd розсилаються всій групі і обробляються по порядку B і C. Коли їх відповіді повертаються до A, стан групи оновлюється і в ньому відображаються «новоприбулі». Будь-які інші повідомлення, що посилаються учасниками системи до прийняття в групу, ігноруються.

На відміну від TLS і DTLS, новий протокол не містить фази «рукостискання» як такої. MLS використовує так звані повідомлення рукостискань (Handshake Messages). Учасники листування обмінюються ними кожен раз коли, потрібно додати або видалити нового члена групи.

Handshake Message інкапсулює спеціальне повідомлення про зміну стану групи, а також включає в себе GroupInitKey, щоб новий учасник зміг ініцілюзуватися, і підписи одного з поточних членів групи укупі з доказом Меркле (щоб переконатися в «справжності» людини, яка його поставила)[28].

3.3 Основні заходи із забезпечення безпеки у соціальних інтернет-медіа

Підсумовуючи усе раніше вказане у дипломній роботі, можна скласти список основних заходів, яких необхідно дотримуватися при листуванні у соціальних інтернет-медіа. Вони будуть дещо різними для соціальних мереж та месенджерів.

Для початку, при користуванні соціальними мережами слід дотримуватися основного правила і не викладати особистої інформації, а саме адреси проживання, номеру телефону, фотографій паспорту, ідентифікаційного коду та банківських карток. В більшості соціальних-мережах можна налаштовувати режим доступу до сторінки, тобто обмежувати дані, які видимі для інших користувачів. Найкраще щоб інформацію про вас могли бачити лише ваші знайомі, це стосується і списку ваших друзів та знайомих. Дуже ретельно перевіряти незнайомі профілі, які додаються до вас у друзі. Пароль від вашої сторінки має містити цифри, букви та спеціальні символи та мати від 6 і більше символів. Бажано пароль нікому не повідомляти і не залишати десь записаним на листку паперу. Адже навіть найскладніший пароль буде безсилий, якщо він буде у відкритому доступі. Для більшої надійності пароль необхідно змінювати через певний проміжок часу.

Не переходити за незнайомими посиланнями, бо так зловмисники можуть отримати доступ до вашої сторінки. Відомі випадки, коли на пошту можуть приходити повідомлення нібито від соціальної мережі, в яких написано що сторінка «взламана» і необхідно змінити пароль. Але це можуть бути шахраї, тому необхідно ретельно перевіряти від кого саме прийшло це повідомлення. Адже замість адреси соціальної мережі у відправниках, наприклад help@gmail.com, може бути зовсім інша адреса, яка дуже схожа на офіційну, наприклад help@gmeil.com.

Не використовувати незнайомі флеш-накопичувачі, сітьові пристрої, адже деякі з них можуть бути замаскованими пристроями, які крадуть паролі. Наприклад, пристрій «Poison Tap», який виглядає як звичайний Ethernet-пристрій [29], але насправді це міні-комп'ютер, який краде всі пароль, які зберігає браузер.

Стосовно месенджерів, то тут все дещо простіше, адже немає повноцінних профілів, а тому особистої інформації мінімум. Зазвичай це номер телефону або нікнейм та невеликий опис про себе. Та навіть тут необхідно дотримуватись деяких правил.

По-перше, це встановлення паролю для розблокування телефону або увімкнення розблокування по відбитку пальця/обличчю. Адже якщо телефон, який не має захисту, потрапить до інших людей, то вони з легкість зможуть прочитати усі переписки. Але це лише перший крок до захисту. Багато додатків мають функцію увімкнення паролю для входу саме до додатку. Ця функція також створить додатковий захист.

По-друге, це використання додатків з E2E-шифруванням.

По-третє, регулярно чистити переписки, які хотілось би приховати від сторонніх. Адже ніяке шифрування та паролі не захистять, якщо телефон був «взламан». Для цього можна також використовувати додатки, які через деякий час самостійно видаляють переписки, наприклад додаток Telegram у режимі секретного чату або Confide.

На жаль, усі ці методи не допоможуть захистити десктопні версії більшості додатків. Тому необхідно не залишати без нагляду увімкнений комп'ютер, коли відходите від нього, це стосується і захисту у соціальних мережах.

Вибір захищеного месенджера залежить від вимог, які до нього пред'явлені. Серед найбільш захищених вважаються Telegram, Confide, Threema, Signal, останній рекомендує Едвард Сноуден.

У 2018 році був прийнят Закон «Про основні засади забезпечення кібербезпеки України». Законом визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави,

національних інтересів України у кіберпросторі, повноваження і обов'язки державних органів, підприємств, установ, організацій, осіб та громадян, основних засад координації їх діяльності, а також базових термінів у сфері кібербезпеки. Але на жаль, закон не поширюється, зокрема, на: соціальні мережі, приватні електронні інформресурси в мережі інтернет, якщо вони не несуть інформації, необхідність захисту якої встановлена законом [30].

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

В дипломній роботі проводиться науково-дослідна праця, яка відбувається в офісному приміщенні. Кімната обладнана персональними комп’ютерами, принтером, двома робочими столами, сидіннями та кондиціонером.

4.1 Аналіз потенційних небезпек

Основні небезпечні і шкідливі фактори в приміщенні, що можуть виникнути відповідно до ГОСТ 12.0.003-74 ССБТ «Небезпечні та шкідливі виробничі фактори. Класифікація»:

а) можливість загорання у зв’язку із несправністю електричного обладнання, короткого замикання або через порушення правил протипожежної безпеки персоналом;

б) незадовільні параметри повітряного середовища, вологи, мікроклімату через відсутність, неправильне проектування або несправність вентиляційної системи;

в) відсутність, недостатня або нераціональна організація освітленості робочої зони, що негативно впливає на органи зору;

г) небезпека ураження електричним струмом, що може виникнути в наслідок недотримання правил електробезпеки чи виходу з ладу електрообладнання;

д) підвищений рівень електромагнітних випромінювань;

е) підвищене навантаження на нервову систему через напруженість праці, монотонність праці, емоційне перевантаження, недотримання режиму праці;

є) тривале перебування в одному і тому ж положенні і повторення одних і тих же рухів негативно впливає на опорно-руховий апарат;

ж) нераціональна організація робочого місця, що може призвести до уражень електричним струмом та порушень здоров’я.

Ці проблеми можуть бути вирішені комплексно як з позиції ергономіки, так і з позиції строгої регламентації режимів праці та відпочинку, цілеспрямованої професійної спрямованості, тощо.

4.2 Заходи забезпечення безпеки

При роботі в офісному приміщені головним небезпечним чинником є електроенергія. Кімната, в якій відбувається науково-дослідна робота, відноситься до приміщень без підвищеної небезпеки уражень електричним струмом.

Обладнання, що використовується в приміщенні є споживачем електроенергії, воно живиться від змінного струму 220 В від мережі з заземленою нейтраллю та відноситься до електроустановок до 1000 В закритого виконання. За способом захисту людини від ураження електричним струмом відповідає згідно з ГОСТ 12.2.007.0-75* (2001) «ССБТ. Изделия электротехнические. Общие требования безопасности» I (стаціонарні комп’ютери) та II (освітлювальні прилади, кондиціонери, опалювальні пристрої, ноутбуки, сканери) класу захисту. Згідно цього ж ГОСТу в приміщенні встановлені автоматичні рубильники.

Згідно з «Правилами улаштування електроустановок» (далі «ПУЕ») виконані такі групи заходів з електробезпеки: конструктивні, схемно-конструктивні, організаційні.

Безпека при роботі з електроустановками забезпечується наступними основними заходами:

а) струмопровідні частини недоступні для випадкового дотику;

б) згідно з ГОСТ 12.1.009-76 (1996) «ССБТ. Электробезопасность. Термины и определения» у приладах II класу захисту використовується ізоляції належної якості, у деяких випадках – подвійна;

в) згідно з НПАОП 40.1-1.32-01 «Правила устройства элетроустановок. Электрооборудование специальных установок» офісні приміщення відносяться до класу пожежонебезпечної зони П-IIа, тому передбачений ступінь ізоляції обладнання IP44;

г) проведенням планово-попереджувальних ремонтів і профілактичних випробувань електрообладнання, апаратів і мереж, що знаходяться в експлуатації;

д) проведенням ряду організаційних заходів (спеціальне навчання, атестація і переатестація осіб електротехнічного персоналу, інструктажі та т.д.). Експлуатація електроустановок та електроустаткування проводиться відповідно до НПАОП 40.1-1.01-97 «Правила безпечної експлуатації електроустановок» та НПАОП 40.1-1.21-98 «Правила безпечної експлуатації електроустановок споживачів»;

е) забезпечення орієнтації в електроустановках (електропроводка легко розпізнається і в залежності від провідника, позначена певним кольором)

э) відповідно до розділу VI Правил охорони праці під час експлуатації електронно-обчислювальних машин, затверджені наказом Держгірпромнагляду від 26.03.2010 р. № 65 (далі — Правила № 65) у разі виникнення аварійної ситуації негайно відключається персональний комп’ютер і периферійні пристрої від електричної мережі.

Персональні комп’ютери, периферійні пристрої підключаються до електромережі тільки за допомогою справних штемпельних з’єднань і електророзеток

заводського виготовлення (п. 2.9 Правил № 65). Штемпельні з'єднання та електроустановки, окрім контактів фазового та нульового робочого провідників, маються спеціальні контакти для підключення нульового захисного провідника. Конструкція їх виконана так, щоб приєднання нульового захисника відбувається раніше, ніж приєднання фазового та нульового робочого провідників. Порядок роз'єднання при відключенні є зворотнім. Унеможливлено з'єднання контактів фазових провідників з контактами нульового захисного провідника.

Кожен блок живлення комп'ютера чи периферійного пристрою має мережевий фільтр.

Згідно ПУЕ опір захисного заземлення в офісному приміщенні складає не більше 4 Ом.

Не допускається:

а) експлуатація кабелів та проводів з пошкодженою або такою, що втратила захисні властивості за час експлуатації, ізоляцією;

б) застосування саморобних подовжувачів, саморобного електронагрівального обладнання або ламп розжарювання;

в) користування пошкодженими електровиробами (розетками, розгалужувачами, вимикачами, тощо);

г) використання електроапаратури та приладів в умовах, що не відповідають вказівкам (рекомендаціям) підприємств-виготовлювачів.

4.3 Заходи з виробничої санітарії та гігієни праці

Робочі місця офісних працівників, обладнані персональними комп'ютерами (далі – робочі місця), відповідають вимогам «Правил охорони праці під час експлуатації електронно-обчислювальних машин», затверджених Наказом Державного комітету України з промислової безпеки, охорони праці та гірничого нагляду від

26.03.2010 року № 65 (Правила), та «Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин», затверджених постановою Головного державного санітарного лікаря України від 10.12.98 N 7 (ДСанПіН 3.3.2-007-98). Зазначені нормативно-правові акти встановлюють санітарно-гігієнічні вимоги до приміщення, в якому розташоване робоче місце, власне до робочого місця, освітлення, мікроклімату в приміщенні тощо.

Умови до організації робочого місця користувача ПЕОМ.

1. Відповідно до вимог ДСанПІН 3.3.2.007-98 «Державних санітарних правил та норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» площа на одне робоче місце становить не менше 6 м^2.

2. Робочі місця з ПЕОМ розміщуються на відстані не менше 1 м від стіни з вікнами, так, щоб природне освітлення падало збоку, зліва.

3. Відстань між бічними поверхнями дисплеїв є не меншою 1,2 м. Відстань між тильною стороною одного дисплея та екраном іншого є не меншою 2,5 м.

4. Конструкція робочого місця з ПЕОМ забезпечує оптимальне розміщення на робочій поверхні документів, дисплея, системного блоку, принтера, клавіатури, телефонного апарату і т.д. Системний блок і дисплей встановлені на основному робочому столі.

5. Прохід між рядами робочих місць складає 1 м.

6. Відповідно до НПАОП 0.00-1.28-10 «Правил охорони праці під час експлуатації електронно-обчислювальних машин» розміри робочого столу скадають: висота - 725 мм; довжина - 1400-1600 мм; ширина - 800 мм.

7. Екран відеомонітора від очей користувача знаходитися на оптимальній відстані 600 - 700 мм, але не ближче 500 мм.

8. Дисплей обладнаний поворотним майданчиком, що дозволяє переміщати його в горизонтальній і вертикальній площинах в межах +300 або -300 (вправо-вліво), змінювати кут нахилу екрану до 10-150.

9. Робочий стілець (крісло) підйомно-поворотний і регульований по висоті і кутам нахилу сидіння і спинки. Поверхня сидіння і спинки стільця напівм'які з нековзним, повітронепроникним покриттям, що легко очищається та не електризується.

Для запобігання статистичного навантаження при користуванні ПК використовуються перерви в роботі 10 хв. через кожні дві години. Синдром зап’ястного каналу, або тунельний синдром зап’ястя, який може бути наслідком хронічної травми, трапляється у людей внаслідок тривалої роботи з мишею: постійні напруга і здавлювання приводить до мікротравм, здавлювання нерва прилеглими оточуючими тканинами, через що виникає набряк.

Щоб тунельний синдром не турбував, працівники дотримуються кількох правил організації робочого місця:

а) оптимальна висота клавіатури від підлоги – 65-75 см;

б) наявні ергономічні і зручні особисто для працюючих миші і клавіатури;

в) можна регулювати висоту і нахил клавіатури (відстань від поверхні стола до середини клавіатури – не більше 30 мм, кут підйому клавіатури – від 2° до 15°);

г) у клавіатури є підставки для рук;

д) килимки для миші з захистом від тунельного синдрому (спеціальний виступ забезпечує правильне положення кисті);

е) стільця або крісла з підлокітниками.

У приміщені на робочих місцях забезпечуються оптимальні значення параметрів мікроклімату: температури, відносної вологості й рухливості повітря у відповідності до ГОСТ 12.1.005-88 (1991) «ССБТ. Общие санитарно-гигиенические требования к воздуху рабочей зоны», ДСН 3.3.6-042-99 «Санітарні норми мікроклімату

виробничих приміщень» та ГН 2152-80 «Санітарно-гігієнічні норми допустимих рівнів іонізації повітря виробничих та громадських приміщень». Для цього передбачено обладнання системами водяного опалення згідно з ДБН В.2.5-67:2013 «Опалення, вентиляція та кондиціонування» та встановлен побутовий кондиціонер.

Таблиця 4.1 – Оптимальні значення параметрів мікрокліматичних умов для категорії робіт «легка а-1»

Пора року	Температура повітря, град. С	Відносна вологість повітря, %	Швидкість руху повітря, м/с
Холодна	22-24	40-60	0,1
Тепла	23-25	40-60	0,1

Допустимі мікрокліматичні умови встановлені за критеріями допустимого теплового і функціонального стану людини на період 8 - годинний робочої зміни. Вони не викликають пошкоджень або порушень стану здоров'я, не призводити до виникнення загальних і локальних відчуттів теплового дискомфорту, напруги механізмів терморегуляції, погіршення самопочуття і зниження працездатності.

Приміщення, в якому встановлені персональні комп’ютери, має природне та штучне освітлення відповідно до ДБН В.2.5-28-2006 «Інженерне обладнання будинків та споруд. Природне та штучне освітлення».

Штучне освітлення здійснюється системою загального рівномірного освітлення.

Освітленість на поверхні столу в зоні розміщення робочого документа складає 300 – 500 лк. Допускається установка світильників місцевого освітлення для підсвічування документів. Місцеве освітлення не створює відблисків на поверхні екрану і не збільшує освітленість екрана більш ніж на 300 лк.

Як джерела світла при штучному освітленні застосовуються переважно люмінесцентні лампи типу ЛБ. Можливе застосування ламп накалювання у світильниках місцевого освітлення.

Яскравість світильників загального освітлення в зоні кутів випромінювання від 50 до 90 градусів з вертикаллю в подовжній і поперечній площинах складає не більше 200 кд / м^2, захисний кут світильників – не менше 40 градусів.

Коефіцієнт пульсації не перевищує 5%

Коефіцієнт запасу ($к_з$) для освітлювальних установок загального освітлення - 1,4.

Для забезпечення нормованих значень освітленості в приміщеннях використання ВДТ і ПЕОМ проводиться чистку скла віконних рам і світильників не рідше двох разів на рік і проводиться своєчасна заміна перегорілих ламп.

Рівні шуму на робочих місцях користувачів персональних комп'ютерів не перевищує значень, встановлених СанПіН 2.2.4 / 2.1.8.562-96 і становлять не більше 50 дБА.

Для зниження рівня шуму в приміщенні здійснюється:

а) використовуються більш сучасне обладнання;

б) принтери та різноманітне устаткування колективного користування розташовується на значній відстані від більшості робочих місць працівників;

в) жорсткий диск переводиться в режим сну, якщо комп’ютер не працює протягом тривалого часу;

г) використовуються блоки живлення ПК з вентиляторами на гумових підвісках.

Значення напруженості електростатичного поля на робочих місцях (як у зоні екрана дисплея, так і на поверхнях обладнання, клавіатури, друкувального пристрою) не перевищують гранично допустимих за ГОСТ 12.1.045-84, СН 1757-77. Значення напруженості електромагнітних полів на робочих місцях з ВДТ відповідають нормативним значенням (ГДР № 3206-85, ГДР № 4131-86, СН № 5802-91, ГОСТ 12.1.006-84). Інтенсивність потоків інфрачервоного випромінювання не перевищує

допустимих значень відповідно до СН 4088-86, ГОСТ 12.1.005-88. Інтенсивність потоків ультрафіолетового випромінювання не перевищує допустимих значень відповідно до СН 4557-88.

Таблиця 4.2 – Тимчасові допустимі рівні ЕМП, що створюються ПЕОМ

Найменування параметрів		ВДУ
Напруженість електричного поля	в діапазоні частот 5 Гц - 2 кГц	25 В / м
	в діапазоні частот 2 кГц - 400 кГц	2,5 В / м
Щільність магнітного потоку	в діапазоні частот 5 Гц - 2 кГц	250 нТл
	в діапазоні частот 2 кГц - 400 кГц	25 нТл
Напруженість електростатичного поля		15 кВ / м

Для зниження впливу електростатичного поля:

а) встановлені нейтралізатори статичної електрики;

б) підтримується в приміщенні відносну вологість не нижче 45-50% (чим сухіше повітря, тим більше електростатичний заряд);

в) підлога в приміщенні застелена антистатичним лінолеумом і щодня проводиться вологе прибирання;

г) обмежена кількість полімерних матеріалів в приміщенні;

д) протирається екран і робоче місце спеціальною антистатичною серветкою.

Розрахунок повітрообміну проводиться для кімнати площею 18 м^2, ширина якої 3 м, висота - 3 м, довжина – 6 м.

Продуктивність природної винтеляції (прилив або витяжка повітря) визначається:

$$L = k \cdot V_n, \text{ м}^3/\text{год} \qquad (4.1)$$

де k – кратність повітрообміну (відповідно до галузевих норм становить k=2);

V_n – об'єм приміщення, м^3.

$$V_n = 18 \cdot 3 = 48 \text{ м}^3$$

$$L = 2 \cdot 48 = 96 \text{ м}^3/\text{год}$$

Необхідний повітрообмін в приміщенні, де не виділяється надлишкове тепло визначається:

$$L = l \cdot n, \text{ м}^3/\text{год} \qquad (4.2)$$

l – мінімальна подача повітря до одного працівника відповідно до санітарних норм (при об’ємі приміщення, що припадає на одного працівника, до 20 м^3 – l = 30 м^3/год, при об’ємі більше 20 м^3 – l =20 м^3/год);

n – кількість працівників у приміщенні

$$S = 3 \cdot 6 \cdot 3 = 48 \text{ м}^3 / 2 = 24 > 20 (= 20 \text{ м}^3/\text{год})$$

$$L = 20 \times 2 = 40, \text{ м}^3/\text{год}$$

Необхідний теплообмін в приміщенні визначається:

$$L = \frac{Q}{C\gamma\left(t - t_{пр}\right)}, \text{ м}^3/\text{год} \quad (4.3)$$

де Q – сумарна кількість теплоти, що утворюється в приміщенні;

C – питома теплоємність повітря, що дорівнює 1 кДж/(кг℃);

γ – густина зовнішнього повітря, що дорівнює $\gamma = \frac{353}{\left(273 + t_{пр}\right)}$, кг/м³;

t – температура повітря, що видаляється, ℃;

$t_{пр}$ – температура приточного повітря, $t_{пр}$ =19 ℃;

Кількість зовнішнього повітря розраховується для асиміляції надлишкового тепла у приміщенні в теплий період року при використанні кондиціонування повітря. Температура приточного повітря складає 19 ℃.

$$\gamma = \frac{353}{273 + 18} = 1,2 \quad ^3$$

$$L = \frac{1000}{1 \cdot 1,2(33 - 18)} = 55,6$$

4.4 Заходи з пожежної безпеки.

Закон України «Про пожежну безпеку» визначає загальні правові, економічні та соціальні основи забезпечення пожежної безпеки на території

України, регулює відносини державних органів, юридичних і фізичних осіб у цій галузі незалежно від виду їх діяльності та форм власності.

Пожежна безпека забезпечується виконанням вимог Правил пожежної безпеки в Україні, НПАОП 0.00-1.28-10, ГОСТ 12.1.004-91 «Пожежна безпека. Загальні вимоги». Будинки й ті їх частини, в яких розташовуються ПЕОМ, мають ступінь вогнестійкості не нижче II.

В даному приміщенні знаходиться дерев`яна мебель, електронна апаратура, паперові носії інформації. Клас пожежі у офісному приміщенні (згідно із ДБН В. 1.1.7-2002 «Захист від пожежі. Пожежна безпека об'єктів будівництва») – пожежі твердих речовин, переважно органічного походження, горіння яких супроводжується тлінням (деревина, пластмаса, папір) – визначається як клас А. Категорія приміщення (згідно із НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою») – визначається як категорії П-IIа.

Для забезпечення пожежної безпеки в уставах проводять пожежну профілактику, яка включає в себе комплекс організаційних і технічних заходів, спрямованих на забезпечення безпеки людей, на запобігання пожежі, обмеження її поширення, а також на створення умов для успішного гасіння пожежі.

Для ліквідації пожежі у початковій стадії її розвитку силами персоналу об'єктів застосовуються первинні засоби пожежогасіння. До них відносяться: вогнегасники, пожежний інвентар (покривала з негорючого теплоізоляційного полотна, ящики з піском, пожежні відра, совкові лопати, ломи, сокири тощо), системи автоматичного пожежогасіння.

Комплекс протипожежних заходів для приміщення (офісу) обладнаного персональними комп'ютерами з ВДТ розроблений згідно з вимогами НАПБ А. 01.001-2014 «Правила пожежної безпеки в Україні».

З технічних та організаційних заходів запобігання пожеж в приміщенні (офісі) обладнаному персональними комп'ютерами з ВДТ передбачені наступні

протипожежні заходи. На силовому обладнанні, силових та освітлювальних колах, згідно вимог пункту 3.1 «ПУЕ», встановлені захисні пристрої, що вимикають джерело живлення від ділянки електричного кола, у якій виникло коротке замикання.

Згідно з вимогами НАПБ А.01.003-2009 «Правила улаштування та експлуатації систем оповіщення про пожежу та управління евакуацією людей в будинках та спорудах» і ДБН В.2.5-56:2014 «Системи протипожежного захисту», в приміщенні (офісі) встановлена система пожежної й охоронної сигналізації, яка забезпечує виявлення теплових і димових ознак пожежі і місця виникнення пожежі з точністю до місця розміщення датчика.

Засоби протипожежного захисту утримуються у справному стані. Усі працівники вміють користуватись наявними вогнегасниками та іншими первинними засобами пожежогасіння, знають місце їх знаходження. Відстань від найбільш віддаленого місця приміщення до місця розташування вогнегасника не перевищує 20 м. Відповідно до вимог НАПБ Б.03.002-2004 «Типові норми належності вогнегасників» для гасіння електрообладнання у приміщенні (офісу) обладнаному персональними комп’ютерами з ВДТ, що знаходиться під напругою, передбачені 2 вогнегасника Шар-1 [31]. Відстань між вогнегасниками та місцями можливих загорянь не перевищує 10 м. Вогнегасник розташований на об'єкті, відповідно до вимог ГОСТ 12.4.009 (розділ 2.3) таким чином, щоб він був захищений від дії прямих сонячних променів, будь-яких механічних впливів і інших несприятливих чинників, таких як вібрація, підвищена вологість та інших. Вогнегасник розміщується в легкодоступному і помітному місці. Не допускається зберігання та експлуатація вогнегасника в місцях, де температура може перевищувати 500 С і під прямими променями сонця. При гасінні електроустановок, що знаходяться під напругою, не допускається підведення розтруб ближче 1 м до електроустановки та полум'я. Після застосування вогнегасника в закритому приміщені, приміщення провітрюється. Кожен співробітник офісу в обов'язковому порядку ознайомлений з правилами експлуатації вогнегасників.

4.5 Заходи забезпечення безпеки у надзвичайних ситуаціях

Єдина державна система цивільного захисту, її складові та режими функціонування.

Згідно з Кодексом цивільного захисту України забезпечення захисту населення і територій від НС покладено на Єдину державну систему цивільного захисту (ЄДСЦЗ), яка є сукупністю суб'єктів забезпечення цивільного захисту, котрі здійснюють реалізацію державної політики у сфері цивільного захисту.

Суб'єктами забезпечення цивільного захисту в межах своїх повноважень є:

- Рада національної безпеки і оборони України;
- Кабінет Міністрів України;
- центральний орган виконавчої влади, який забезпечує формування та реалізує державну політику у сфері цивільного захисту (нині це Державна служба України з надзвичайних ситуацій – ДСНС);
- інші центральні органи виконавчої влади;
- місцеві державні адміністрації;
- органи місцевого самоврядування;
- суб'єкти господарювання;
- громадяни України.

Основними завданнями єдиної державної системи цивільного захисту є:

а) забезпечення готовності міністерств та інших центральних та місцевих органів виконавчої влади, органів місцевого самоврядування, підпорядкованих їм сил і засобів до дій, спрямованих на запобігання і реагування на надзвичайні ситуації;

б) забезпечення реалізації заходів щодо запобігання виникненню надзвичайних ситуацій;

в) навчання населення щодо поведінки та дій у разі виникнення надзвичайної ситуації;

г) виконання державних цільових програм, спрямованих на запобігання надзвичайним ситуаціям, забезпечення сталого функціонування підприємств, установ та організацій, зменшення можливих матеріальних втрат;

д) опрацювання інформації про надзвичайні ситуації, видання інформаційних матеріалів з питань захисту населення і територій від наслідків надзвичайних ситуацій;

е) прогнозування і оцінка соціально-економічних наслідків надзвичайних ситуацій, визначення на основі прогнозу потреби в силах, засобах, матеріальних та фінансових ресурсах;

є) створення, раціональне збереження і використання резерву матеріальних та фінансових ресурсів, необхідних для запобігання і реагування на надзвичайні ситуації;

ж) оповіщення населення про загрозу та виникнення надзвичайних ситуацій, своєчасне та достовірне інформування про фактичну обстановку і вжиті заходи;

з) захист населення у разі виникнення надзвичайних ситуацій;

і) проведення рятувальних та інших невідкладних робіт щодо ліквідації наслідків надзвичайних ситуацій, організація життєзабезпечення постраждалого населення;

й) пом’якшення можливих наслідків надзвичайних ситуацій у разі їх виникнення;

к) здійснення заходів щодо соціального захисту постраждалого населення;

л) реалізація визначених законом прав у сфері захисту населення від наслідків надзвичайних ситуацій, в тому числі осіб (чи їх сімей), що брали безпосередню участь у ліквідації цих ситуацій;

м) інші завдання, визначені законом.

Режими функціонування єдиної державної системи цивільного захисту.

1. Єдина державна система залежно від масштабів і особливостей надзвичайної ситуації, що прогнозується або виникла, функціонує у режимах:

а) повсякденного функціонування;

б) підвищеної готовності;

в) надзвичайної ситуації;

г) надзвичайного стану.

2. Положенням про єдину державну систему цивільного захисту визначається перелік заходів, що здійснюються у відповідному режимі, завдання та порядок взаємодії суб'єктів забезпечення цивільного захисту під час функціонування зазначеної системи у відповідному режимі.

3. В особливий період єдина державна система цивільного захисту функціонує відповідно до цього Кодексу та з урахуванням особливостей, що визначаються згідно з вимогами законів України «Про правовий режим воєнного стану», «Про мобілізаційну підготовку та мобілізацію», а також інших нормативно-правових актів.

Режим повсякденного функціонування ЕДСЦЗ встановлюється за умов нормальної виробничо-промислової, радіаційної, хімічної, сейсмічної, гідрометеорологічної, техногенної і пожежної обстановки, гідрогеології, за відсутності епідемій, епізоотій, епіфітотій. У режимі повсякденного функціонування органи управління ЕДСЦЗ і сили ЦЗ:

- забезпечують спостереження і контроль за обстановкою на об'єктах підвищеної небезпеки і прилеглих до них територіях;
- здійснюють цілодобове чергування оперативно-рятувальних і пожежно-рятувальних підрозділів;
- розробляють і виконують цільові і науково-технічні програми по запобіганню виникненню НС і зменшення можливих втрат;
- здійснюють планові заходи по запобіганню НС, забезпеченню безпеки і захисту населення і територій від них;
- забезпечують підготовку органів управління і сил цивільного захисту відносно дій в надзвичайних ситуаціях;

- організовують навчання керівного складу і фахівців цивільного захисту і населення діям в надзвичайних ситуаціях;

- створюють і поновлюють матеріальні резерви для запобігання, ліквідації надзвичайних ситуацій і їх наслідків;

- здійснюють прогнозування обстановки, погіршення якої може привести до виникнення надзвичайних ситуацій;

- створюють і підтримують в постійній готовності системи оповіщення.

Режим підвищеної готовності ЕДСЦЗ встановлюється в межах конкретної території у разі істотного погіршення виробничо-промислової, радіаційної, хімічної, епідемічної (епізоотичної), сейсмічної, гідрометеорологічної обстановки гідрогеології, за наявності загрози виникнення надзвичайної ситуації. У режимі підвищеної готовності органи управління ЕДСЦЗ і сили ЦЗ:

- здійснюють оповіщення населення про загрозу виникнення НС;

- формують оперативні групи для виявлення причин погіршення обстановки і готують пропозиції відносно її нормалізації;

- вводять цілодобове чергування членів комісії з питань техногенно-екологічної безпеки і НС;

- посилюють спостереження і контроль за ситуацією на об'єктах підвищеної небезпеки і прилеглих до них територіях, здійснюють постійне прогнозування можливості виникнення НС і їх масштабів;

- здійснюють заходи по запобіганню виникненню НС;

- уточнюють, розробляють і здійснюють заходи відносно захисту населення і територій від можливої надзвичайної ситуації;

- приводять в стан готовності наявні сили і засоби реагування.

Режим надзвичайної ситуації ЕДСЦЗ встановлюється у разі виникнення НС, залежно від її масштабу, в межах конкретної території. У режимі надзвичайної ситуації органи управління ЕДСЦЗ і сили ЦЗ :

- здійснюють оповіщення населення про надзвичайну ситуацію і про їх дії в умовах цієї ситуації;

- призначають спеціальну комісію і/або керівника робіт по ліквідації НС, які створюють Штаб по ліквідації НС;

- визначають межі території, на якій виникла НС;

- здійснюють постійне прогнозування зони можливого поширення НС і масштабів можливих наслідків;

- організовують роботи по локалізації і ліквідації НС і її наслідків, притягають для цього необхідні сили і засоби;

- організовують і здійснюють заходи по життєзабезпеченню постраждалого населення;

- організовують захист населення і територій в умовах НС;

- здійснюють безперервний контроль за розвитком НС і обстановкою на аварійних об'єктах і прилеглих до них територіях.

Режим надзвичайного стану для єдиної державної системи цивільного захисту у повному обсязі або частково для окремих її територіальних підсистем тимчасово встановлюється у межах території, на якій введено правовий режим надзвичайного стану відповідно до Закону України «Про правовий режим надзвичайного стану».

5 ТЕХНІКО-ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

Вислів «Інформація є найціннішим товаром в сучасному світі» вже не здається дивним або невірним. Швидкий розвиток інформаційних технологій, породив нові засоби добування інформації конкурентами. Тож власники інформації усілякими засобами намагаються захисти свої дані, адже інколи від цієї інформації може залежати матеріальний добробут власника. Вже не стоїть питання захисту лише паперових носії, жорстких дисків, флешок та пошти як це було ще декілька років тому. Сьогодні більшість часу людина проводить в соціальних мережах та месенджерах. Саме там вона здійснює ділову переписку або веде бізнес через сторінку в мережі. Тому актуальність захисту цих засобів комунікації виходить для неї на передній план.

5.1 Визначення трудомісткості та тривалості робіт

Планування дослідження захищеності користувачів у соціальних інтернет-медіа здійснюється за допомогою методу сітьового планування і управління (СПУ), що істотно знижує терміни розробки. В результаті цього етапу визначаються тривалість і трудомісткість робіт з досліджень.

Система СПУ включає:

- складання переліку етапів і визначення тривалості виконання робіт;
- побудова сітьового графіка;
- розрахунок основних параметрів сітьового графіка.

Весь комплекс розробки проекту підрозділяється на етапи. По кожному з етапів розраховується трудомісткість, виконавці і тривалість робіт. Так як в процесі розрахунку трудомісткості робіт є елемент невизначеності, розрахунок ведеться за допомогою імовірнісної оцінки згідно з формулою:

$$t_{оч} = \frac{3t_{\min} + 2t_{\max}}{5} \tag{5.1}$$

де $t_{оч}$ – очікувана оптимальна оцінка часу виконання роботи, днів;

$t_{\min}$ – мінімально необхідний час на виконання роботи при найбільш сприятливих умовах, днів;

$t_{\max}$ – максимальні витрати часу на виконання роботи при несприятливих умовах.

Правильність визначення $t_{оч}$ перевіряється розрахунком дисперсії - розкиду між мінімальною і максимальною оцінками часу. Дисперсія являє собою середнє значення квадрата відхилення тривалості роботи від її очікуваного значення і визначається за формулою:

$$\sigma^2(t) = \left(\frac{t_{\max} - t_{\min}}{5}\right)^2 \tag{5.2}$$

Якщо $\sigma^2(t) \le 1$, то ступінь невизначеності оцінки часу робіт по даному етапу мала. Розраховані згідно (5.1) - (5.2) характеристики робіт наведено в таблиці 5.1.

Таблиця 5.1 – Загальна тривалість етапів робіт

№	Найменування роботи	Тривалість, дні			Дисперсія	Виконавці	
		t_{min}	t_{max}	$t_{оч}$		Спеціальність	Кількість, чол.
1	2	3	4	5	6	7	8
1	Уточнення проектного завдання	1	3	2	0,16	Інженер-консультант	1
2	Узгодження теми	2	4	3	0,36	Інженер	1

Продовження таблиці 5.1 - Загальна тривалість етапів робіт

1	2	3	4	5	6	7	8
3	Ознайомлення з методами аналізу захищеності соціальних інтернет-медіа	5	8	6	0,36	Інженер	1
4	Складання методики дослідження соціальних інтернет-медіа	14	18	16	0,64	Інженер	1
5	Підбір та вивчення літератури	5	8	6	0,36	Інженер	1
6	Аналіз отриманої інформації	7	10	8	0,36	Інженер	1
7	Розробка рекомендацій з вибору методів захисту інформації в соціальних інтернет-медіа	4	7	5	0,16	Інженер	1
8	Складання розділу з охорони праці	7	8	7	0,04	Інженер	1
9	Аналіз економічної частини проектного завдання	7	8	7	0,04	Економіст	1
10	Оформлення проектного завдання	5	7	6	0,16	Інженер-консультант	1

Загалом:	57	80	66	-	-	10

5.2 Побудова сітьового графіка

Сітьовий графік являє собою інформаційно-динамічну модель, в якій зображуються взаємозв'язки і результати всіх робіт, необхідних для досягнення кінцевої мети розробки. Використовуючи таблицю 5.1, складено перелік робіт і подій (таблиця 5.2), побудовано сітьовий графік проведення НДР і розраховано його основні параметри.

Таблиця 5.2 – Перелік робіт сітьового графіка

№	Код роботи	Найменування роботи	Тривалість, дн.
1	*2*	*3*	*3*
1	0–1	Уточнення проектного завдання	2
2	1–2	Узгодження теми	3
3	2–3	Ознайомлення з методами аналізу захищеності соціальних інтернет-медіа	7
4	3-4	Складання методики дослідження соціальних інтернет-медіа	16
5	4-5	Підбір та вивчення літератури	8
6	5-6	Аналіз отриманої інформації	7
7	5-7	Розробка рекомендацій з вибору методів захисту інформації в соціальних інтернет-медіа	7
8	6-8	Складання розділу з охорони праці	7
9	8–9	Аналіз економічної частини проектного завдання	7
10	9-10	Оформлення проектного завдання	7

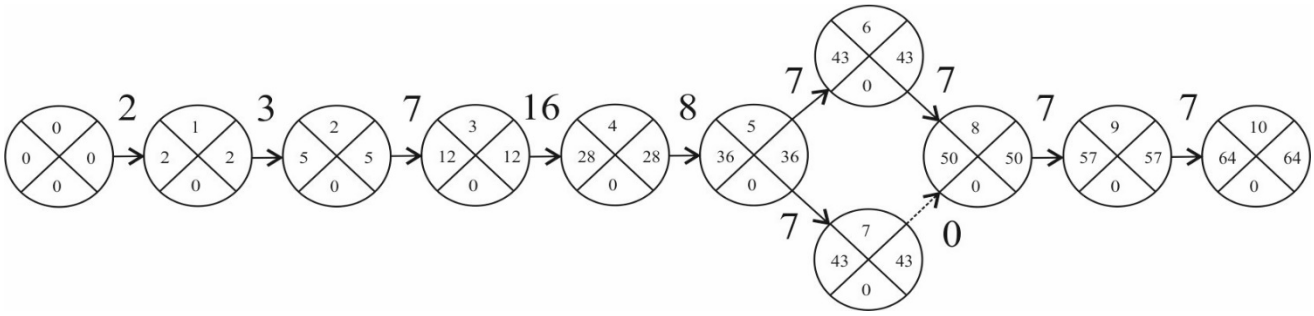


Рисунок 5.1 – Сітьовий графік

Після складання сітьового графіка визначаємо його параметри. Отримані результати наведені в таблицях 5.3, 5.4.

Таблиця 5.3 – Параметри шляхів

№ шляху	Номери подій	Тривалість робіт	Довжина шляху	Резерв часу	$К_н$, %
1	*2*	*3*	*4*	*5*	*6*
1 Критичний	0-1-2-3-4-5-6-8-9-10	2-3-7-16-8-7-7-7-7	64	0	100
2 Найкоротший	0-1-2-3-4-5-7-8-9-10	2-3-7-16-8-7-0-7-7	57	7	75

де K_H – напруженість шляху. Визначається за формулою:

$$K_{Hi} = \frac{L_i - L_i^{кр}}{L_{кр} - L_i^{кр}}, \quad (5.3)$$

де L_i – і-го довжина шляху;

$L_i^{кр}$ – довжина і-го шляху на подіях де він співпадає з критичним;

$L_{кр}$ – довжина критичного шляху.

Таблиця 5.4 - Параметри робіт

Код роботи	t_{ij}	$t_{ij}^{рп}$	$t_{ij}^{рз}$	$t_{ij}^{пп}$	$t_{ij}^{пз}$	$R_{ij}^{п}$	$R_{ij}^{в}$
1	2	3	4	5	6	7	8
1-2	3	2	5	2	5	0	0

Продовження таблиці 5.4 – Параметри робіт

1	2	3	4	5	6	7	8
2-3	7	5	12	5	12	0	0
3-4	16	12	28	12	28	0	0
4-5	8	28	36	28	36	0	0
5-6	7	36	43	36	43	0	0
5-7	7	43	43	43	43	7	0
6-8	7	43	50	43	50	0	0
7-8	7	50	50	50	50	7	7
8-9	7	50	57	50	57	0	0
9-10	7	57	64	57	64	0	0

В таблицях використані позначення:

i – номер події, яка передує роботі;

j – номер події, яка завершує роботу;

t_{ij} – тривалість виконання роботи;

$t_{ij}^{рп}$ – ранній термін початку події;

$t_{ij}^{рз}$ – ранній термін звершення події;

$t_{ij}^{пп}$ – пізній термін початку події;

$t_{ij}^{по}$ – пізній термін звершення події;

$R_{ij}^{п}$ – повний резерв часу роботи;

$R_{ij}^{в}$ – вільний резерв часу роботи.

Тривалість критичного шляху складає 64 днів. При послідовному проведенні дослідження вимагає 66 днів. Виконання НДР за параметрами сітьового планування дозволяє скоротити строки робіт до 64 днів.

5.3 Розрахунок основної заробітної платні

Виплати за цією статтею складаються з планового фонду заробітної платні всіх категорій робітників, що зайняті розробкою проекту.

Розрахунок зарплатні ведеться на основі даних табл. 5.1 та табл. 5.2.

Розрахунок приводяться в табл. 5.5.

Таблица 5.5 – Розрахунок основної заробітної платні

Посада виконавця	Кількість, осіб	Місячний оклад, грн	Середньоденна зарплатня, грн	Кількість роб. днів	Сума зарплатні, грн
Консультант	1	11000	500	9	4500

Інженер	1	7000	318,18	64	20363,52
Економіст	1	12000	545,45	7	3818,15
Усього	3	-	-	-	28681,67

Відрахування в соціальний фонд визначаються у відсотковому відношенні до основної та додаткової зарплатні у відповідності з встановленим нормативом 22% и складають:

$$ЗП_{осн} \cdot 0,22 = 28681,67 \cdot 0,22 = 6309,97 \text{ грн}$$

5.3.1 Розрахунок вартості матеріалі

На цю статтю відносяться витрати з придбання основних матеріалів для проведення досліджень, а також для виготовлення дослідних зразків (таблиця 5.6).

Таблиця 5.6 – Розрахунок вартості матеріалів

Матеріал	Одиниця виміру	Витрати матеріалу, шт.	Ціна за одиницю, грн./шт.	Сума витрат, грн..
Папір	Пачка	1	90	90
Канцелярські товари	Штуки	8	10	80
Картриджі на принтер	Штуки	1	250	250
Разом				420

Транспортно-заготівельні витрати	21
Всього з урахуванням транспортно-заготівельних витрат	441

Ціни на матеріальні ресурси визначені за відповідними прайс-листами.

Транспортно-заготівельні витрати складають 5% від вартості матеріалів.

5.3.2 Розрахунок вартості енергоресурсів

Тариф з електроенергії складає 180 копійок. Звідси витрати на живлення комп'ютера, який поглинув 280 кВт·год, складатимуть:

$$280 \text{ кВт·год} \cdot 180 \text{ коп} = 50400 \text{ копійок}$$

Таблиця 5.7 – Вартість енергоресурсів

Найменування устаткування	Вид енергоресур-сів	Установлена потужність, кВт	Тривалість використан-ня, год.	Вартість енергоресурсів, грн
Комп'ютер	Е/енергія	0,5	560	504 грн
Принтер	Е/енергія	0,1	16	2,88 грн
Усього				506,88 грн

5.3.3 Спеціальне устаткування для науково-експериментальних робіт

В цій статті враховуються витрати на закупівлю, доставку і монтаж лабораторних установок, вимірювальних і регулюючих приладів, пристроїв, випробувальної апаратури і тому подібне (таблиця 5.8).

Таблиця 5.8 - Витрати на спеціальне устаткування

Перелік устаткування	Модель	Кількість	Ціна за одиницю, грн..
1	2	3	4
Рідинно-кристалічний монітор	23" LG Electronics IPS234V-PN	1	3600
Системний блок	ARTLINE Home H25 v07	1	6840
Клавіатура	WIRELESS SOLAR KEYBOARD K750 Y-R0016	1	200

Продовження таблиці 5.8 - Витрати на спеціальне устаткування

1	2	3	4
Комп'ютерна миша	WIRELESS MOUSE M185 M-R0024	1	200
Принтер	Canan Pixma iP7240	1	2500
Разом		13340	
Транспортно-заготівельні витрати		667	

Всього з урахуванням транспортно-заготівельних витрат	14007

5.3.4 Накладні витрати

Накладні витрати (витрати, пов'язані з управлінням, утриманням і експлуатацією устаткування й приміщень, створенням необхідних санітарно-гігієнічних умов) по проведенню науково-дослідницької роботи визначені у відсотках (30%) від основної заробітної плати її виконавців і складають 8604,5 грн.

$$С_{нр} = 28681,67 \text{ грн} \cdot 30\% = 8604,5 \text{ грн}$$

5.3.5 Бальна оцінка економічної ефективності науково-дослідної роботи

Для теоретичних досліджень у більшості випадків важко чи навіть неможливо розрахувати економічний ефект, тому доцільно визначити їхню техніко-економічну ефективність з урахуванням наступних показників:

- важливість дослідження;
- складності розробки;
- результативності й можливості використання.

Важливість теоретичного дослідження оцінюють по його призначенню:

- рішення проблемних питань;
- задоволення вимог спеціальної техніки; пошук принципово нових конструктивних і технологічних рішень і т.п.

Складність виконання роботи визначають порівнянням отриманих результатів даного дослідження з результатами відомих аналогічних досліджень з обліком грошових і трудових витрат на їхнє проведення.

Результативність НДР можна визначити по повноті рішень поставленого завдання: отриманий результат відповідає плановому, задовільний (часткове рішення) чи негативний.

Аналіз залежності між цими показниками й витратами на їхнє досягнення дає можливість кількісної оцінки техніко-економічної ефективності теоретичних НДР по формулі:

$$К_{НДР} = \frac{J^n \cdot R \cdot T}{B_{НДР} \cdot t_{НДР}} \quad (5.4)$$

де $К_{НДР}$ – рівень ефективності дослідження (коефіцієнт техніко-економічної ефективності НДР);

J = 1 – важливість роботи. Таке значення обрали, тому що результати роботи в подальшому стануть основою більш глибоких досліджень;

R = 5 – результативність роботи. Обрали таке значення, тому що всі поставлені дослідницькі задачі виконано;

T = 3 – технічна складність виконання НДР.

$B_{НДР}$ = тис. грн – витрати на проведення НДР;

$t_{НДР}$ = 64 днів – час проведення НДР;

n = 1 – показник використання результатів НДР

При значенні $К_{НДР} \geq 1$ дослідницька робота вважається ефективною.

Отже, розрахуємо $К_{НДР}$:

$$К_{НДР} = \left(1^1 \cdot 5 \cdot 3\right) / \left(44,037 \cdot 0,18\right) = 1,9$$

Після розрахунку (5.4) отримаємо рівень ефективності дослідження $К_{НДР}$ = 1,9 Це більше 1, тому робимо висновок, що дана дослідницька робота є ефективною.

ВИСНОВОК

З вище сказаного досить зрозуміло, що соціальні мережі є великими ризиками для безпеки та конфіденційності. Вони мають цей ризик через їх централізовану архітектуру, їх величезний репозиторій всієї особистої інформації, яку може захопити хакер, і загальне незнання населення про те, як правильно використовувати параметри конфіденційності, щоб поліпшити їх безпеку в Інтернеті. Існує також великий ризик тому, що багато людей, особливо підлітки, занадто довіряють іншим людям і викладають інформацію про себе до соцмереж.

З цим можна боротися лише за допомогою технологічних засобів та розумної політики. Але з кращою освітою та деякими архітектурними змінами соціальні мережі можуть бути використані більш безпечно.

Нарешті, важливо продовжувати дослідження в галузі створення безпечних соціальних мереж, навіть якщо довірливі користувачі розміщують безліч особистої інформації в Інтернеті

Щодо месенджерів то слід зазначити, що всі протоколи безпеки не мають сенсу, якщо сам смартфон погано захищений, або хтось змусить вас ввести всі паролі. Такі випадки відомі, в деяких з них це призвело до кримінальних справ проти власників смартфонів. Тому навіть користуючись безпечним месенджером, рекомендуємо регулярно чистити листування, особливо ті, які б ви хотіли зберегти в секреті.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Мкртчян, Е. История и развитие социальных медиа [Электронный ресурс] – Режим доступу: https://habr.com/post/72136/

2. Nurtdinova, D. Security In Mobile Messaging [Text] / D. Nurtdinova // Information Technology: bachelor's thesis, 6 may 2016. – 51 p.

3. Hiatt, D. Role of Security in Social Networking [Text] / D. Hiatt, Y. B. Choi // (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 2, 2016 – P. 12 - 15

4. Конфіденційність, доступність і цілісність інформації [Електронний ресурс] – Режим доступу: https://stboinf.wordpress.com/2013/03/12/конфіденційністьдоступність-і-цілі/

5. Информационная безопасность: обзор популярных мессенджеров [Электронный ресурс] Коалиция в поддержку правозащитников — сообщество российских правозащитных организаций, 6 грудня 2071 року – Режим доступу: https://hrdco.org/bez-rubriki/informatsionnaya-bezopasnost-obzor-populyarnyh-messendzherov/

6. Social networking service [Electronic Resource] - Режим доступу: https://en.wikipedia.org/wiki/Social_networking_service

7 Lomas, N. Line: We’re A Social Entertainment Platform, Not Just A Free Calls Messaging App [Electronic Resource] – Режим доступу: https://techcrunch.com/2013/03/17/line-the-social-entertainment-platform/

8. Most Popular Social Messaging Apps, December 2013 [Electronic Resource] – Режим доступу: http://trends.e-strategyblog.com/2013/12/13/most-popular-social-messaging-apps/15939

9. Twitter is a messaging app now that it's finally removed the 140 character limit on direct messages [Electronic Resource] – Режим доступу: http://www.businessinsider.com/twitter-becomes-a-messaging-app-by-getting-rid-of-140-character-limit-for-dms-2015-8

10. Twitter now acts more like a messaging app with read receipts, typing indicators & web link previews [Electronic Resource] – Режим доступу: https://techcrunch.com/2016/09/08/twitter-now-acts-more-like-a-messaging-app-with-read-receipts-typing-indicators-web-link-previews/

11. Most popular global mobile messenger apps as of April 2018, based on number of monthly active users (in millions) [Electronic Resource] – Режим доступу: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/

12. Messenger Wars: How Facebook lost its lead [Electronic Resource] – Режим доступу: https://ondeviceresearch.com/blog/messenger-wars-how-facebook-lost-its-lead

13. Messaging apps [Electronic Resource] – Режим доступу: https://en.wikipedia.org/wiki/Messaging_apps

14. История возникновения и развития социальных сетей [Электронный ресурс] – Режим доступу: http://miolaweb.ru/biznes-uroki/istoriya-vozniknoveniya-i-razvitiya-socialnyx-setej/

15. История социальных сетей. Сайты и определения [Электронный ресурс] – Режим доступу: http://smo-i-seo.ru/vneshnee-smosmm/istoriya-socialnyx-setej-sajty-i-opredeleniya.html

16. История [Электронный ресурс] – Режим доступу: https://sites.google.com/site/palovchin/istoria

17. История мессенджеров: первая волна [Электронный ресурс] – Режим доступу: https://www.astrosoft.ru/articles/unified-communications/istoriya-messendzherov-pervaya-volna/

18. История мессенджеров: вторая волна [Электронный ресурс] – Режим доступу: https://www.astrosoft.ru/articles/unified-communications/istoriya-messendzherov-vtoraya-volna/

19. Мобильные мессенджеры: эволюция [Электронный ресурс] – Режим доступу: https://therunet.com/articles/2810

20. Компания FMS представила новый украинский мессенджер "First" [Электронный ресурс] – Режим доступу: https://vesti-ukr.com/strana/241009--kompanija-fms-predstavila-novyj-ukrainskij-messendzher-first

21. Социальные сети в 2018 году: глобальное исследование [Электронный ресурс] – Режим доступу: https://www.web-canape.ru/business/socialnye-seti-v-2018-godu-globalnoe-issledovanie/

22. Самые популярные социальные сети в странах СНГ и мире [Электронный ресурс] – Режим доступу: https://marketer.ua/top-social-media-2017/

23. Топ-5 мессенджеров в Украине: больше 90% пользуются Viber [Электронный ресурс] – Режим доступу: https://ain.ua/2018/04/10/top-5-messendzherov-v-ukraine

24. Что такое end-to-end шифрование + ТОП-7 мессенджеров с оконечным шифрованием [Электронный ресурс] – Режим доступу: https://crypto-fox.ru/faq/end-to-end-shifrovanie/

25. ProtonMail: Сквозное шифрование: описание и принцип работы метода [Электронный ресурс] – Режим доступу: https://www.comss.ru/page.php?id=2468

26. Artezio Presents Top 8 Confidential Messengers [Electronic Resource] – Режим доступу: https://www.artezio.com/pressroom/news/artezio-presents-top-8-confidential-messengers

27. Мощное средство коммуникации или канал утечек информации: рейтинг популярных соцсетей по степени их надежности [Електронний ресурс] - Режим доступу: https://www.securitylab.ru/blog/company/falcongaze/311566.php

28. IETF предложили новый стандарт для обмена сообщениями — что нужно знать [Електронний ресурс] - Режим доступу: https://habr.com/company/it-grad/blog/421811/

29. Абраменко, Л. Устройство съёма информации «Poison Tap». Тиждень науки. Тези доповідей науково-практичної конференції, Запоріжжя, 18–21 квітня 2017 р. [Електронний ресурс] / Лізунов С.І., Абраменко Л.О. Редкол. : В. В. Наумик (відпов.

ред.) Електрон. дані. – Запоріжжя : ЗНТУ, 2017. – 1 електрон. опт. диск (DVD-ROM); 12 см. – Назва з тит. екрана. – с. 596-598.

30. Абраменко, Л. Про основні засади забезпечення кібербезпеки України. Тиждень науки. Тези доповідей науково-практичної конференції, Запоріжжя, 16–20 квітня 2018 р. [Електронний ресурс] / Абраменко Л.О, Лізунов С.І. Редкол. : В. В. Наумик (відпов. ред.) Електрон. дані. – Запоріжжя : ЗНТУ, 2018. – 1 електрон. опт. диск (DVD-ROM); 12 см. – Назва з тит. екрана, с. 911-913.

31. Абраменко, Л. Средства пожаротушения режимных помещений. Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 18-22 квітня 2016 р.: збірник тез доповідей в 5 томах/ Абраменко Л.О, Лізунов С.І. – Запоріжжя, 2016. – Т.1. – С. 316-318.