# 4.2. Сервіси миттєвого обміну повідомленнями

Месенджери - це програмні додатки, які дозволяють користувачам обмінюватись повідомленнями в режимі реального часу через інтернет. Вони дозволяють людям надсилати текстові повідомлення, а також проводити голосові та відеодзвінки, обмінюватися файлами, фотографіями та іншими медіа-контентом. Месенджери стали популярними завдяки своїй зручній та миттєвій комунікації, що дозволяє людям комунікувати у будь-який час та у будь-якому місці.

Історія месенджерів розпочалася задовго до появи сучасних програм.

* У 1990-х роках розроблено стандарт SMS (Short Message Service) для надсилання текстових повідомлень між мобільними телефонами. SMS став першим способом мобільної комунікації та форматом для обміну повідомленнями.
* У 1996 році з'явився ICQ (I Seek You) – перший популярний інтернет-месенджер. Він дозволяв користувачам надсилати миттєві повідомлення, повідомляти про присутність та обмінюватися файлами. ICQ став феноменом і започаткував популярність месенджерів.
* Наприкінці 1990-х і на початку 2000-х років з'явилися інші месенджери, такі як AOL Instant Messenger (AIM), MSN Messenger (пізніше перейменований у Windows Live Messenger) та Yahoo Messenger. Вони пропонували аналогічний функціонал і стали поширеними серед користувачів інтернету.
* У 2003 році з’явився Skype - це популярна програма для голосового, відео- та текстового спілкування.
* У 2010-х роках з'явилися нові месенджери, які перевершили популярність ранішніх месенджерів: WhatsApp, Facebook Messenger, Telegram. У різних регіонах світу також з'явилися локальні месенджери, такі як WeChat у Китаї, Viber у Східній Європі та Line у Японії. Вони пропонують специфічні функції і адаптовані до місцевих потреб та уподобань користувачів.

Сьогодні месенджери є невід'ємною частиною повсякденної комунікації. Вони дозволяють людям обмінюватися інформацією та підтримувати контакт із друзями, сім'єю та колегами у будь-який час та в будь-якому місці.

### Функціонування месенджерів

Для кожного сервісу миттєвого обміну повідомленнями розроблено власну програму – месенджер. Користувачі бачать лише клієнтську частину месенджера - це або програма на комп'ютері, або додаток на мобільному пристрої. Всі месенджери зав'язані на власні сервера - там відбувається зберігання інформації і обробка даних. Серверна частина забезпечує безпеку акаунтів, зберігає історію спілкувань та контакти.

Месенджери працюють за власним протоколом передачі даних і ці протоколи зазвичай не є сумісними. Розробники кожного з месенджерів прагнуть, щоб користувачі спілкувалися лише в їх сервісі, тоді можна увімкнути рекламу або запропонувати платну послугу. Тому, різні месенджери майже завжди несумісні між собою і для кожного сервісу потрібно встановлювати свого клієнта.

#### Особливості месенджерів:

* Миттєва передача повідомлень. Можливість передавати текст, картинки, відео, довільні файли.
* Можливість вести голосову і відео розмову без додаткової плати за зв'язок, оплачується лише Інтернет трафік.
* Відображення статусу співрозмовника (активний чи немає в мережі) і повідомлення (прочитане чи ні).
* Збереження історії листування.

## Компоненти системи

Кожна система миттєвого обміну повідомленнями повинна мати такі складові:

* Система ідентифікації (адресації) клієнтів.
* Система обліку стану клієнтів (хто підключений, а хто ні).
* Система доставки повідомлень (передача повідомлення через комп'ютерну мережу)

### Система ідентифікації (адресації) клієнтів

Месенджери використовують серверні або безсерверні протоколи, що визначають способи обміну повідомленнями між учасниками.

* Серверні протоколи. Багато месенджерів, таких як WhatsApp, Facebook Messenger та Telegram, використовують власні сервери для обміну повідомленнями. У цьому випадку всі повідомлення проходять через центральні сервери месенджера і сервер відповідає за доставку повідомлень між відправником та одержувачем.
* Безсерверні протоколи P2P (Peer-to-Peer). У цьому підході повідомлення безпосередньо передаються між пристроями відправника та отримувача без проміжних серверів. Це забезпечує високу конфіденційність та мінімізує можливість централізованого зберігання даних.

Обидва підходи мають свої переваги та недоліки. Серверні протоколи можуть надавати більшу стабільність та зручність, але можуть мати питання з конфіденційністю даних. Безсерверні протоколи забезпечують більш високий рівень конфіденційності, але можуть бути менш зручними або вимагати більше ресурсів пристроїв. Вибір протоколу залежить від потреб користувачів та фокусу на безпеці та конфіденційності даних.

У безсерверних протоколів виникають проблеми ідентифікації співрозмовника. Для точної ідентифікації клієнта вони можуть використовувати лише фізичну мережну адресу (IP). Це створює складність, оскільки на одному комп'ютері можуть знаходитися кілька користувачів. Для вирішення цієї проблеми створено серверні протоколи.

У серверних протоколах виділяється сервер, який проводить облік користувачів. На сервері потрібно зареєструватися використовуючи ідентифікатор та пароль.

Ідентифікатори користувачів — це може бути номер (ICQ), номер телефону (WhatsApp, Viber), спеціальне ім'я користувача – логін (Skype, Telegram) або акаунт у соціальній мережі (Facebook Messenger). В деяких протоколах логін подібний до електронних адрес: містить домен і має вигляд ім'я\_користувача@домен

### Система обліку стану користувачів

Більшість месенжерів дозволяє користувачам бачити, чи під’єднані до мережі їхні співрозмовники в цей момент, так званий статус.

Існує три основних статуси, що відображають присутність/відсутність користувача у мережі:

1. В мережі / Онлайн (Online) — користувач під'єднаний до мережі і готовий до спілкування.
2. Не в мережі / Офлайн (Offline) — користувач поза мережею.
3. Невидимий (Invisible) — користувач знаходиться в мережі, але цей спеціальний статус не дозволяє бачити його всім іншим (або лише деяким) користувачам. Натомість вони бачать статус користувача як: «не в мережі».

### Список контактів

Користувач може створювати власний список контактів. Контакти можуть бути згруповані у групи з назвою. Більшість протоколів дозволяють зберігати список контактів на сервері, що створює певні зручності:

* Користувач може отримати його, знаходячись на іншому комп'ютері.
* Користувач може задавати власні правила для контактів. Наприклад, список заблокованих (заборонених) контактів, від яких він не бажає отримувати повідомлення («чорний список»). Або список контактів, для яких його статус завжди видимий.
* Користувач може зберігати власні примітки для контактів.

### Система збереження повідомлень

Повідомлення можуть бути збережені у журналі (історії) повідомлень, який зберігається на сервері.

### Інформація про користувачів

Майже всі поширені протоколи дозволяють користувачам задавати власну інформацію про себе у спеціальних формах. Зазвичай, там містяться такі поля:

* Нік (нікнейм, псевдонім).
* Справжнє ім'я.
* Фотографія користувача або зображення (аватар).
* Адреса.
* Дата народження та вік.
* Інтереси.
* Про себе.
* Контактна інформація (електронна пошта, номери телефонів та інше).

## Популярні месенжери

### ICQ (I Seek You)

ICQ – це один з найстаріших месенджерів, який на сьогодні втратив свою домінуючу позицію після появи інших месенджерів, таких як WhatsApp, Telegram, Facebook Messenger та інші. Тим не менш, ICQ досі існує і використовується деякими користувачами, хоча його популярність значно знизилася. ICQ продовжує надавати свої послуги та розробляти програми для різних платформ.

### Skype

Skype - це популярна програма для голосового, відео- та текстового спілкування. Компанія Skype була заснована в 2003 році в Естонії. За створення месенджера відповідали розробники - Андерсен Хенріксен (Ahti Heinla), Прійт Касперсон (Priit Kasesalu) та Янус Фрііс (Janus Friis). Їхньою метою було розробити програму, яка б дозволила людям обмінюватися голосовими повідомленнями через Інтернет.

Однією з ключових особливостей Skype стала його технологія peer-to-peer (P2P). На відміну від традиційних систем телефонії, де голосові дані проходять через центральний сервер, Skype використовував розподілену мережу, де кожен учасник мережі служив клієнтом і сервером одночасно. Це дозволяло встановлювати прямі з'єднання між користувачами, забезпечуючи надійніший та ефективніший зв'язок.

Спочатку Skype пропонував лише голосовий зв'язок, але згодом його функціональність розширилася. Додано можливість проведення відеодзвінків, обміну миттєвими повідомленнями, передачі файлів та проведення відеоконференцій.

Skype швидко став популярним завдяки своїй простоті використання, високій якості зв'язку та безкоштовною комунікацією між користувачами Skype. За короткий час Skype набрав мільйони користувачів по всьому світу і став однією з найпоширеніших платформ онлайн-спілкування.

У 2011 році компанія Microsoft оголосила про покупку Skype за 8,5 мільярда доларів. Після придбання Skype був інтегрований з іншими продуктами Microsoft, такими як Outlook та Xbox, і став частиною екосистеми Microsoft.

Більшої популярності Skype мав, коли не було гідного конкурента, але з часом Viber, WhatsApp, Telegram виявилися більш зручними. Після придбання Skype компанією Microsoft месенджер став працювати значно повільніше, що пов'язано з поступовою інтеграцією сервісу в Windows. Також, невдалі зміни інтерфейсу та правила використання зменшили ряди прихильників даного месенджеру.

### Viber

Viber - це месенджер та додаток для голосових та відеодзвінків, який розроблено компанією Viber Media та випущений у 2010 році. Акаунти в Viber прив'язуються до номера мобільного телефону, що робить зручним пошук людей через телефонні контакти.

* Viber дозволяє користувачам обмінюватися текстовими повідомленнями, стікерами, фотографіями, відео та аудіозаписами.
* Viber дозволяє створювати групові чати до 250 учасників, що зручно для спілкування та координації у групах. У групових чатах можна надсилати повідомлення, медіафайли і навіть здійснювати групові дзвінки.
* Viber надає безкоштовні високоякісні голосові та відеодзвінки. Він використовує технологію VoIP (голосовий зв'язок за протоколом інтернету), що забезпечує чіткий звук та стабільний зв'язок.
* Користувачі можуть використовувати Viber на різних платформах, включаючи мобільні пристрої (Android, iOS) та настільні комп'ютери (Windows, macOS). Всі повідомлення та дані синхронізуються між пристроями, що дозволяє отримувати доступ до чатів та історії повідомлень незалежно від пристрою.
* Viber забезпечує захист конфіденційності користувачів. Він пропонує шифрування end-to-end для повідомлень, тому прочитати повідомлення можуть лише відправник та одержувач. Viber також дозволяє налаштувати конфіденційності, такі як приховування статусу "онлайн" і блокування небажаних контактів.
* Viber інтегрується з іншими сервісами, такими як Google Drive та Dropbox, що дозволяє користувачам обмінюватися файлами з хмарних сховищ.

### logo-whatsappWhatsApp

WhatsApp - це популярна безкоштовна система миттєвого обміну текстовими повідомленнями для мобільних та інших платформ з підтримкою голосового і відеозв'язку. Акаунт в WhatsApp відповідає номеру телефону, список контактів береться безпосередньо із записника телефону.

WhatsApp розроблено компанією WhatsApp Inc в 2010 році - Джаном Кумаром (Jan Koum) та Браяном Ектоном (Brian Acton). У 2014 році WhatsApp Inc. придбала компанія Facebook Inc., з того часу WhatsApp залишається одним із провідних месенджерів у світі.

* WhatsApp дозволяє користувачам надсилати текстові повідомлення, аудіозаписи, фотографії, відео, контакти, геолокацію та інші типи файлів. Користувачі можуть створювати чати або групові чати з 256 учасниками.
* WhatsApp підтримує голосові та відеодзвінки в рамках програми. Користувачі можуть безкоштовно дзвонити один одному по всьому світу, використовуючи лише інтернет-з'єднання.
* WhatsApp пропонує функцію WhatsApp Web, яка дозволяє користувачам використовувати месенджер на комп'ютері через веб-інтерфейс. Це зручно для тих, хто воліє працювати на великих екранах або мати доступ до чатів прямо з комп'ютера.
* WhatsApp використовує шифрування end-to-end для захисту приватності та безпеки повідомлень. Лише відправник та одержувач можуть прочитати вміст повідомлень, і ніхто інший, включаючи WhatsApp, не має доступу до цих даних.
* WhatsApp пропонує функцію WhatsApp Status, яка дозволяє користувачам публікувати фото, відео та текстові оновлення, які зникають через 24 години.
* WhatsApp є доступним на різних платформах, включаючи Android, iOS, Windows Phone та ін, що забезпечує широку доступність для користувачів.

WhatsApp є одним з найбільш популярних месенджерів у світі, і його перевагами є простота використання, широкий функціонал та шифрування для захисту конфіденційності користувачів.

### Facebook Messenger

Facebook Messenger – це месенджер, розроблений компанією Facebook Inc., та призначений для обміну повідомленнями та комунікації між користувачами Facebook. Спочатку функція обміну повідомленнями була вбудована безпосередньо у соціальну мережу Facebook. У 2008 році Facebook додав функцію "Чат" (Chat), яка дозволяла користувачам обмінюватися миттєвими повідомленнями всередині платформи.

У 2011 році Facebook прийняв рішення відокремити функцію обміну повідомленнями від основної програми Facebook і створив окрему програму під назвою "Facebook Messenger". Це дозволило користувачам надсилати повідомлення без необхідності входити в основну програму Facebook.

Протягом наступних років Facebook Messenger поступово розширював свій функціонал. У 2013 році додано функції голосових та відеодзвінків, а також можливість надсилання фотографій та відео.

У 2015 році Facebook оголосив про запуск платформи Messenger Platform, яка дозволяє розробникам створювати програми та боти, інтегровані з Facebook Messenger. Це дозволило розширити функціональність Messenger та створити нові можливості для комунікації та автоматизації завдань.

У наступні роки Facebook Messenger став інтегруватися з різними сервісами та платформами. Додано підтримку платежів, інтеграцію з Uber для замовлення таксі, інтеграцію з бізнес-сторінками для спілкування з клієнтами та інші функції.

Facebook Messenger продовжує розвиватися та пропонувати нові функції та можливості для своїх користувачів. Він є одним з найпопулярніших месенджерів у світі завдяки своїй широкій базі користувачів на платформі Facebook та різноманітним функціям комунікації.

Всі функції Facebook Messenger спрямовані на те, щоб надати можливість користувачу спілкуватися з друзями на Facebook, не заходячи при цьому в саму соціальну мережу. Рішення Facebook відокремити Messenger від соціальної мережі та перетворити його в автономний додаток, було неоднозначно сприйнято користувачами. По-перше, це створило необхідність встановлювати ще один додаток на свій пристрій. По-друге, користувачі повинні були зробити «додатковий крок», якщо вони хотіли поспілкуватися один з одним.

**Telegram**

Telegram – це месенджер, який розроблено Павлом Дуровим та його командою у 2013 році. Він пропонує низку особливостей, які відрізняють його від інших месенджерів.

* Одна з основних особливостей Telegram – це фокус на безпеці та конфіденційності даних. Він пропонує шифрування end-to-end для секретних чатів, що означає, що повідомлення між користувачами шифруються та можуть бути прочитані лише отримувачем. Telegram пропонує функцію "самознищувальних повідомлень", яка дозволяє встановити час автоматичного видалення повідомлень після прочитання.
* Telegram дозволяє надсилати та отримувати файли будь-якого розміру, включаючи фотографії, відео, аудіозаписи та документи. Завдяки власній інфраструктурі серверів та оптимізації передачі даних, Telegram забезпечує швидке завантаження та вивантаження файлів.
* Telegram підтримує створення групових чатів, де користувачі можуть обмінюватися повідомленнями, медіа-файлами та приєднуватися до обговорень. Telegram пропонує функцію каналів, які дозволяють користувачам створювати публічні чи закриті канали для поширення інформації та контенту.
* Telegram підтримує ботів - автоматизовані облікові записи, які можуть виконувати різні завдання та надавати користувачеві інформацію або послуги. Боти можуть бути використані для отримання новин, інформації про погоду, ігри, бронювання та багато іншого.
* Telegram доступний на різних платформах, включаючи мобільні пристрої (Android, iOS, Windows Phone) та настільні комп'ютери (Windows, macOS, Linux). Всі повідомлення та дані синхронізуються між пристроями, що дозволяє користувачам отримувати доступ до своїх чатів та файлів незалежно від пристрою.

Платформа Telegram постійно розвивається та впроваджує нові функції, щоб задовольнити потреби користувачів у комунікації та обміні інформацією.

## Наскрізне шифрування

Шифрування end-to-end - це метод шифрування даних, який забезпечує високий рівень конфіденційності та безпеки інформації під час передачі через мережу. Дзвінки, повідомлення, відео, аудіо, зображення, документи та інші дані доступні лише для співрозмовників та захищені від попадання в треті руки. Ключі шифрування є також тільки у них. За допомогою цих ключів можна розблокувати і прочитати повідомлення. У контексті месенджерів та комунікаційних програм, таких як WhatsApp, Signal та інші, шифрування end-to-end використовується для захисту повідомлень від доступу третіх осіб, включаючи провайдерів послуг та розробників додатків.

Принципи end-to-end

* Кожен користувач генерує унікальну пару ключів: відкритий і закритий ключі. Відкритий ключ використовується для шифрування повідомлень, а закритий ключ зберігається лише на пристрої користувача та використовується для розшифровування повідомлень.
* Під час надсилання повідомлення відправник використовує відкритий ключ отримувача для шифрування вмісту повідомлення. Розшифрувати та прочитати повідомлення може лише отримувач, який має свій закритий ключ. Навіть якщо хтось перехоплює повідомлення у процесі передачі, воно залишається зашифрованим та недоступним для читання.
* Шифрування end-to-end забезпечує аутентифікацію повідомлень. Воно використовує контрольні суми та цифрові підписи, щоб переконатися, що повідомлення не було змінено в процесі передачі та надійшло від правильного джерела.
* Дані зберігаються у зашифрованому вигляді на серверах. Навіть сам провайдер послуг або розробник програми не має доступу до розшифрованих даних, їх прочитати може тільки користувач з доступом до свого закритого ключа.

Шифрування end-to-end є важливим механізмом для забезпечення приватності та захисту даних у сучасних комунікаційних додатках.

### Основні способи шифрування даних.

**Симетричні криптосистеми** передбачають, що для шифрування і дешифрування застосовується один і той же криптографічний ключ. Головний недолік полягає в тому, що ключ повинен бути розділений між сторонами. Якщо не буде створено безпечний тунель, перехоплювач зможе стягнути ключ і розшифрувати повідомлення (рис.1). За наявності досить великих продуктивних потужностей ключ можна підібрати.

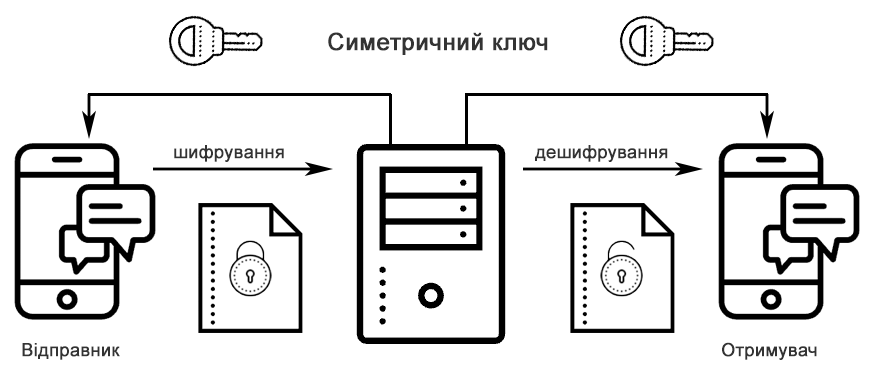


Рис.1. Симетричне шифрування

Щоб забезпечити стійкість криптосистеми від зламу, фахівці безпеки збільшують такі параметри, як довжина ключа, складність і число раундів перетворення.

**Асиметричне шифрування.** Для захисту даних використовуються два ключі - відкритий і закритий. Відкритий потрібен для шифрування даних, але для розшифрування він абсолютно даремний. З цієї причини він доступний всім, хто хоче спілкуватися з власником закритого ключа. Дані можна розшифрувати тільки за допомогою закритого ключа (рис.2).

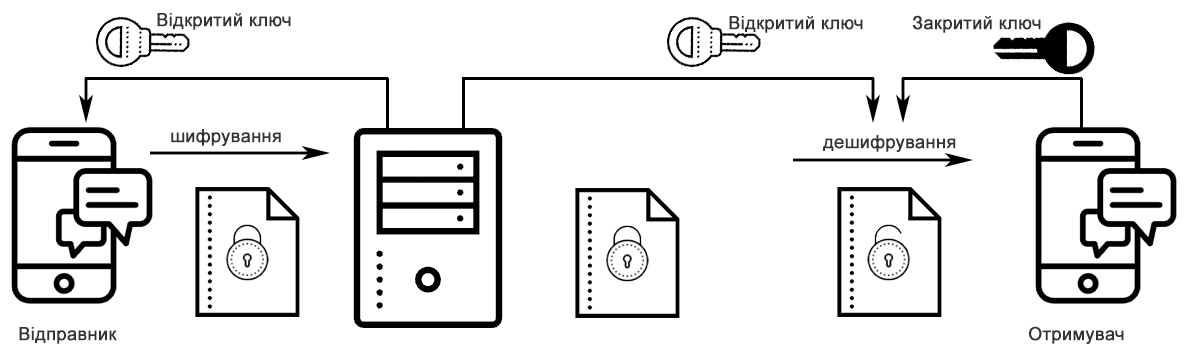


Рис.2. Асиметричне шифрування

Наскрізне шифрування може комбінувати ці два методи. У випадку з месенджерами ключі локалізовані каналом зв'язку і відомі тільки для клієнтів, що спілкуються між собою. Захищений канал дозволяє виключити атаки методом «людини посередині». Таким чином дані, які він перехопить, будуть марні. При перехопленні даних, вони будуть у зашифрованому вигляді.

Ключовою характеристикою месенджерів, що використовують наскрізне шифрування, є приватність і анонімність.

* Під приватними даними розуміють, що жодні дані не доступні для третіх осіб. В популярних месенджерів є певні напрацювання в цьому напрямку. Наприклад, Telegram має функцію самознищення акаунту у разі відсутності активності користувача.
* Анонімність месенджерів виражається в тому, що зв'язок встановлюється через сервера компанії, і IP-адреса віддаленого користувача є прихованою, а клієнт в свою чергу не знає ІР-адресу сервера.

Технології зв'язку, реалізовані в клієнтах, можуть мати й недоліки. Наприклад, в WhatsApp при інтернет-дзвінках існує можливість отримати реальну IP-адресу користувача навіть без встановленого сеансу зв'язку.

Недолік багатьох месенджерів - авторизація за номером мобільного телефону. Спецслужби багатьох країн мають доступ до мобільних провайдерів зв'язку і можуть надсилати СМС з номера користувача без будь-яких повідомлень і користувач про це навіть не дізнається. Для захисту від цього в багатьох месенджерах передбачено функцію оповіщення про активність користувача за допомогою іншого пристрою.

## Проблеми

Злом шифрування end-to-end є вкрай складним завданням і потребує значних обчислювальних ресурсів та експертизи. Однак теоретично деякі методи атак можуть бути застосовані для обходу або компрометації end-to-end шифрування.

### Злом ключів

Шифрування end-to-end залежить від безпеки ключів, які використовуються для шифрування та розшифровування повідомлень. Якщо зловмисник отримує доступ до закритого ключа, наприклад, шляхом злому пристрою або перехоплення ключів у момент генерації, він може розшифрувати повідомлення. Тому важливо забезпечити безпеку пристроїв та ключової інфраструктури.

### Внутрішні атаки «Людина посередині»

Деякі месенджери можуть бути вразливими до атак зсередини, коли розробники або провайдери послуг мають доступ до зашифрованих даних. Хоча серйозні провайдери зазвичай вживають заходів для захисту даних та конфіденційності користувачів, існує потенційний ризик зловживання внутрішніми особами.

Наскрізне шифрування передбачає, що контроль за листуванням здійснюється безпосередньо користувачами. Одним з варіантів обходу наскрізного шифрування для зловмисника є захоплення під свій контроль каналу зв'язку між кінцевими точками, після цього він може спробувати видати себе за отримувача повідомлення, щоб, наприклад, підмінити відкритий ключ. Щоб не дати себе виявити, зловмисник після дешифрування повідомлення може зашифрувати його ключем, який він поділяє з фактичним отримувачем, або його відкритим ключем у випадку асиметричних систем, і знову надіслати повідомлення. Атаки такого типу прийнято називати атаками «людина посередині».

Для запобігання внутрішніх атак більшість криптографічних протоколів використовують аутентифікацію. Для цього можуть використовуватися, наприклад, центри сертифікації. Альтернативним методом є створення відбитків відкритого ключа на основі загальнодоступних відкритих ключів користувачів або загальних секретних ключів. Перш ніж почати розмову сторони порівнюють свої відбитки відкритих ключів з використанням зовнішнього каналу зв'язку, який гарантує цілісність та автентичність зв'язку, при цьому він не обов'язково повинен бути секретним. Якщо відбитки ключив збігаються, значить атака «людина посередині» не була проведена.

### Атака на кінцеві пристрої

Якщо зловмисник отримує фізичний доступ до пристрою, він може використовувати різні методи, такі як зламування паролів або встановлення шкідливого програмного забезпечення, щоб перехоплювати повідомлення до або після їх розшифровки на пристрої одержувача.

Іншим способом обходу наскрізного шифрування є атака безпосередньо на кінцеві точки доступу. Кожний пристрій користувача може бути зламано, з метою вкрасти криптографічний ключ (для створення атаки «людина посередині») або просто прочитати дешифровані повідомлення користувачів. Для уникнення такого роду спроб злому, необхідно забезпечити відповідний захист пристроїв за допомогою програмних або інших методів.

Основними спробами підвищити безпеку кінцевих точок були виведення основних операцій генерації, зберігання і криптографії на смарт-карту. Але, оскільки введення і виведення відкритого тексту видно в системі, то ці підходи не здатні захистити від клавіатурних шпигунів і шкідливого програмного забезпечення, яке може відстежувати розмови в режимі реального часу. Більше надійний підхід полягає у фізичній ізоляції пристрою.

### Backdoor

Backdoor (задні двері) - шкідлива програма, а іноді навмисно залишена лазівка в коді легальної програми, яка надає доступ до пристрою для несанкціонованих дій. Бекдор в точності відповідає своїй назві: приховано впускає зловмисника в систему, наділяючи правами адміністратора.

Компанії можуть (самостійно чи з примусу) впроваджувати у своє програмне забезпечення бекдори, які допомагають порушити узгодження ключа або обійти шифрування.

Альянс «П'ять очей» (Five Eyes), куди входять розвідслужби США, Великобританії, Австралії, Канади та Нової Зеландії, вимагають від технологічних компаній впроваджувати бекдори в зашифровані додатки, щоб можна було надати правоохоронним органам доступ, необхідний для припинення кіберзлочинності. За словами вищих посадових осіб, зростання кількості додатків з наскрізним шифруванням, таких як Signal, Telegram, FaceBook Messenger і WhatsApp, «створюють серйозні проблеми для громадської безпеки».

«Хоча шифрування має життєво важливе значення, а головним пріоритетом повинна бути конфіденційність і кібербезпека, це не повинно здійснюватися за рахунок повного виключення можливості правоохоронних органів і самої технологічної індустрії протистояти небезпечному незаконному контенту і діяльності в інтернеті», - пояснили чиновники.

Прихильники захисту конфіденційності стверджують, що впровадження бекдору, за допомогою яких правоохоронні органи зможуть отримати доступ до повідомлень користувача, може поставити під загрозу дисидентів і посилити вплив деяких диктаторських урядів.

Згідно інформації, розкритої Едвардом Сноуденом в 2013 році, Skype містив бекдор, який дозволяв Microsoft передавати в АНБ повідомлення користувачів, незважаючи на те, що офіційно ці повідомлення піддавалися наскрізному шифруванню.

В цілому, добре реалізоване шифрування end-to-end надає високий рівень безпеки та конфіденційності даних. Однак важливо розуміти, що безпека залежить від багатьох факторів, включаючи безпеку пристроїв, алгоритмів шифрування, ключової інфраструктури та захисту від внутрішніх атак.

## Контрольні питання

1. Які послуги надають сервіси миттєвих повідомлень?
2. Перелічити компоненти системи миттєвих повідомлень.
3. Яку інформацію показує система обліку стану користувачів?
4. Яка інформація про користувача міститься в месенжері?
5. Провести порівняльний аналіз популярних месенжерів.
6. Пояснити причини популярності Telegram.
7. Назвати причини, з яких причин користувачі встановлюють Facebook Messenger? Які переваги від нього має користувач Facebook?
8. Порівняйте якісні характеристики WhatsApp та Viber: зручність інтерфейсу, якість зв’язку, наявність реклами, додавання контактів, групові чати.
9. Для чого використовують наскрізне шифрування в месенжерах?
10. Назвати особливості симетричного шифрування?
11. Назвати особливості асиметричного шифрування?
12. Які існують варіанти обходу наскрізного шифрування?

## Література

1. Шифрування в месенджерах <https://xakep.ru/2018/06/14/useless-encryption/>
2. Криптографія для початківців <https://bitnovosti.com/2020/07/16/kriptografiya-dlya-absolyutnyh-novichkov/>
3. Основи алгоритмів шифрування <https://hacker-basement.ru/2019/08/23/kryptografia-dlay-hakerov-algorytmy-shifrovaniy/>
4. Що таке наскрізне шифрування? <https://bezopasnik.info/что-такое-сквозное-шифрование-типы-ши/>
5. Функції Viber <https://www.viber.com/ru/features/>
6. Корисні функції в WhatsApp <https://androidinsider.ru/polezno-znat/38-funktsij-v-whatsapp-o-kotoryh-vy-ne-znali-chast-1.html>
7. Приховані можливості Facebook Messenger <https://daily.afisha.ru/brain/5394-11-funkciy-facebook-messenger-pro-kotorye-vy-mogli-ne-znat/>
8. Переваги Telegram перед аналогічними продуктами <https://nastroyvse.ru/programs/review/vozmozhnosti-telegram-na-fone-analogichnyx-produktov.html>
9. Як влаштовано шифрування в месенджерах <https://thecode.media/dh/>
10. Безпека переписки в месенджерах <https://safe-surf.ru/users-of/article/666973/>
11. Офіційний сайт Skype - <https://www.skype.com/uk/>
12. Офіційний сайт Viber - <https://www.viber.com/ru/>
13. Офіційний сайт WhatsApp - <https://www.whatsapp.com/?lang=uk>
14. Офіційний сайт Telegram - <https://telegram.org/>
15. Офіційний сайт Facebook Messenger - <https://www.messenger.com>