**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

# КВАЛІФІКАЦІЙНА РОБОТА

на тему: "**ТЕХНОЛОГІЇ ШИФРУВАННЯ ТА АНОНІМІЗАЦІЇ ДЛЯ ЗАХИСТУ КОРИСТУВАЧІВ В ІНТЕРНЕТІ**"

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

*Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело*
_____ Денис КАПУСТЕНКО

*(підпис)* *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Денис КАПУСТЕНКО

Керівник: Світлана ЛЕГОМІНОВА
*Д.е.н., професор*

Рецензент: Андрій КОТЕНКО
*к.т.н., доцент*

**Київ 2025**

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**Навчально-науковий інститут кібербезпеки та захисту інформації**

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

**ЗАТВЕРДЖУЮ**
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

# ЗАВДАННЯ
# НА КВАЛІФІКАЦІЙНУ РОБОТУ

Капустенко Денис Ігорович

*(прізвище, ім’я, по батькові здобувача)*

- Тема кваліфікаційної роботи “Технології шифрування та анонімізації для захисту користувачів в Інтернеті”,
  керівник кваліфікаційної роботи ЛЕГОМІНОВА Світлана, д.е.н., професор,
  *(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)*

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “24“ лютого 2025 р. №56.

- Строк подання кваліфікаційної роботи “12” травня 2025р.
- Вихідні дані до кваліфікаційної роботи: *технологія, шифрування, захист, користувач, інтернет, міжнародні стандарти, наукова та технічна література.*
- Перелік питань, які мають бути розроблені:
  4.1. Проаналізувати сучасні підходи до шифрування та анонімізації в Інтернеті;
  4.2. Дослідити сучасні технології шифрування даних та технології анонімізації у кібербезпеці;
  4.3. Визначити шляхи імплементації технологій шифрування та анонімізації для захисту користувачів в Інтернеті, розробити практичні рекомендації.
- Перелік ілюстративного матеріалу: *презентація PowerPoint*
- Дата видачі завдання “10“ березня 2025 р.

# КАЛЕНДАРНИЙ ПЛАН

| № з/п | Етапи кваліфікаційної роботи | Термін виконання етапів роб | Примітка |
|---|---|---|---|
| 1. | Визначення об’єкту, предмету, мети та завдань дослідження. | 18.03.2025 | |
| 2. | Збір та аналіз літератури. | 29.03.2025 | |
| 3. | Аналіз сучасних підходів до шифрування анонімізації в Інтернеті | 08.04.2025 | |
| 4. | Дослідження сучасних технол шифрування даних та технологій анонімі у кібербезпеці | 15.04.2025 | |
| 5. | Визначення шляхів імплементації технол шифрування та анонімізації для захи користувачів в Інтернеті, розробле практичних рекомендацій | 22.04.2025 | |
| 6. | Формулювання висновків за результатами проведеногодослідження. | 29.04.2025 | |
| 7. | Оформлення роботи. | 06.05.2025 | |
| 8. | Оформлення презентації. | 09.05.2025 | |
| 9. | Отримання рецензії на роботу. | __.06.2025 | |
| 10. | Захист в ЕК. | __.06.2025 | |

| | | |
|---|---|---|
| Здобувач вищої освіти | _____ *(підпис)* | Денис КАПУСТЕНКО *(Ім’я, ПРІЗВИЩЕ)* |
| Керівник кваліфікаційної роб | _____ *(підпис)* | Світлана ЛЕГОМІНОВА *(Ім’я, ПРІЗВИЩЕ)* |

# ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

## ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
**на здобуття освітнього ступеня бакалавра**

Направляється здобувачка Капустенко Денис Ігорович

до захисту кваліфікаційної роботи

за спеціальністю 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою
*(назва)*
на тему: "Технології шифрування та анонімізації для захисту користувачів в Інтернеті)"

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

### Висновок керівника кваліфікаційної роботи

Здобувач КАПУСТЕНКО Денис у кваліфікаційній роботі проаналізував сучасні підходи до шифрування та анонімізації в Інтернеті, визначив актуальні технології шифрування даних та технології анонімізації у кібербезпеці, запропонував шляхи імплементації технологій шифрування та анонімізації для захисту користувачів в Інтернеті, розробив практичні рекомендації. КАПУСТЕНКО Денис показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявила себе як організований, відповідальний виконавець. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача КАПУСТЕНКА Дениса на оцінку "добре" та присвоїти їй кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

### Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Капустенко Д. І. допускається до захисту даної роботи в Екзаменаційній комісії.

| | | |
|---|---|---|
| Завідувач кафедри управління кібербезпекою та захистом інформації | _____ | Світлана ЛЕГОМІНОВА |
| | *(підпис)* | *(Ім'я, ПРІЗВИЩЕ)* |

# ВІДГУК РЕЦЕНЗЕНТА

## на кваліфікаційну бакалаврську роботу

здобувач вищої освіти КАПУСТЕНКО Денис
на тему “ Технології шифрування та анонімізації для захисту користувачів в Інтернеті ”

**Актуальність.**

У контексті зростаючих кіберзагроз та загальної цифровізації суспільства, питання захисту персональних даних та анонімності користувачів в Інтернеті набувають особливої ваги. Дослідження сучасних технологій шифрування та анонімізації є важливим і актуальним науковим завданням, що має як теоретичне, так і практичне значення для сфери інформаційної безпеки.

**Позитивні сторони.**

1.У роботі проведено комплексний аналіз методів шифрування та технологій забезпечення анонімності в мережі, включаючи VPN, TOR та I2P.

2.Кваліфікаційна робота відповідає вимогам щодо структури, мови та оформлення. Логічна послідовність викладу матеріалу дотримана, наведені аргументовані висновки за результатами кожного розділу.

3.Автор опрацював значний масив джерел, включаючи сучасні наукові та технічні публікації англійською мовою та галузеві ресурси.

4.Практична частина роботи містить аналіз ефективності brute-force атак на алгоритм AES, що підтверджує глибоке розуміння теми та вміння застосовувати знання на практиці.

**Недоліки.**

Доцільно було б доповнити дослідження порівняльним аналізом юридичних та етичних аспектів використання технологій анонімізації в різних країнах, а також оцінити вплив цих технологій на цифрову політику.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

**Висновок:** Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “добре”, а здобувач КАПУСТЕНКО Денис заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: Андрій КОТЕНКО
к.т.н., доцент *підпис*

# РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню технологій шифруання та анонімізаії, які використовуються для захисту користувачів в Інтернеті. Робота складається зі вступу, трьох розділів, що містять 2 рисунки, 1 таблицю, висновки і списку використаних джерел із 33 найменувань. Загальний обсяг роботи становить 69 аркушів, з яких 4 аркушів займають перелік умовних скорочень, додатки та список використаних джерел.

***Мета роботи*** **–** проведення комплексного аналізу сучасних технологій шифрування та анонімізації, призначених для захисту користувачів в Інтернеті, з метою оцінки їхньої ефективності, виявлення вразливостей, визначення оптимальних сфер застосування та розробки практичних рекомендацій щодо захисту персональних даних.

***Об'єкт дослідження*** **–** методи і технології захисту персональних даних та забезпечення анонімності користувачів у мережі Інтернет.

***Предмет дослідження*** – сучасні технології шифрування та анонімізації для захисту персональних даних користувачів в Інтернеті (криптографічні алгоритми AES, RSA; мережі VPN, Tor, I2P; протоколи SSL/TLS, IPsec, SSH) та оцінка їх ефективності й вразливостей, включно з моделюванням brute-force атаки на AES-128.

***Методи дослідження.*** В роботі застосовано методи системного аналізу, моделювання, експериментного оцінювання, порівняльного аналізу, а також практичного тестування (зокрема, можелювання brute force атаки на AES).

Як результат у роботі проведено аналіз основних криптографічних та анонімізуючих технологій визначено їх переваги та недоліки, здійснено практичну перевірку криптостійкості алгоритму AES методом перебору, а також надано рекомендації щодо ефективного застосування для захисту користувачів. Також приділено увагу деанонімізації та способам її уникнення.

***Галузь застосування.*** Отримані результати можуть бути використані в організаціях, які надають онлайн послуги, а також окремими користувачасм для підвищення рівня приватності та безпеки своїх даних в Інтернеті.

Ключові слова: ШИФРУВАННЯ, АНОНІМІЗАЦІЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, VPN, TOR, I2P, SSL/TLS, AES, RSA, ПРИВАТНІСТЬ В ІНТЕРНЕТІ.

# ABSTRACT

The qualification work is devoted to the study of encryption and anonymization technologies used to protect users on the Internet. The work consists of an introduction, three chapters containing 2 figures, 1 table, conclusions and a list of references with 33 titles. The total volume of the work is 69 pages, of which 4 pages are occupied by the list of abbreviations, appendices and the list of references.

The purpose of the study is to conduct a comprehensive analysis of modern encryption and anonymization technologies designed to protect users on the Internet in order to assess their effectiveness, identify vulnerabilities, determine the optimal areas of application and develop practical recommendations for the protection of personal data.

Object of research - methods and technologies for protecting personal data and ensuring the anonymity of users on the Internet.

The subject of the research is modern encryption and anonymization technologies for protecting personal data of users on the Internet (cryptographic algorithms AES, RSA; VPN, Tor, I2P networks; SSL/TLS, IPsec, SSH protocols) and evaluation of their effectiveness and vulnerabilities, including modeling of a brute-force attack on AES-128.

The methods of system analysis, modeling, experimental evaluation, comparative analysis, and practical testing (in particular, simulation of a brute force attack on AES) are used in this work.

As a result, the paper analyzes the main cryptographic and anonymizing technologies, identifies their advantages and disadvantages, performs a practical verification of the cryptographic strength of the AES algorithm by brute force attack, and provides recommendations for effective use to protect users. Attention is also paid to deanonymization and ways to avoid it.

***Field of application.*** The obtained results can be used by organizations that provide online services, as well as by individual users to increase the level of privacy and security of their data on the Internet.

Keywords: ENCRYPTION, ANONYMIZATION, INFORMATION SECURITY, VPN, TOR, I2P, SSL/TLS, AES, RSA, INTERNET PRIVACY.

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

| | |
|---|---|
| Wi-Fi | Wireless Fidelity - бездротова мережа |
| SPF | Sender Policy Framework - захист поштових доменів |
| DKIM | DomainKeys Identified Mail - криптографічна перевірка електронної пошти |
| DMARC | Domain-based Message Authentication, Reporting, and Conformance - політика перевірки email |
| AES | Advanced Encryption Standard - симетричний алгоритм шифрування |
| VPN | Virtual Private Network - віртуальна приватна мережа |
| TOR | The Onion Router - система анонімного інтернет-серфінгу |
| I2P | Invisible Internet Project - анонімна мережа для приватних комунікацій |
| E2EE | End-to-End Encryption - наскрізне шифрування |
| HTTPS | HyperText Transfer Protocol Secure - захищений протокол передавання гіпертексту |
| HTTP | HyperText Transfer Protocol - незахищений протокол передавання гіпертексту |
| SSL | Secure Shell — захищений протокол віддаленого доступу |
| TOR | The Onion Router - технологія маршрутизації для забезпечення анонімності |
| SSL/TLS | Secure Sockets Layer / Transport Layer Security - протоколи захисту передавання даних в Інтернеті |
| OSINT | Open Source Intelligence - розвідка з відкритих джерел |
| IPsec | Internet Protocol Security - набір протоколів захисту даних на рівні IP |
| DNS | Domain Name System - система доменних імен |

# ВСТУП

***Актуальність теми.*** В наш час, коли державні установи, приватні компанії та звичайні користувачі стають об’єктами кібератак, питання забезпечення інформаційної безпеки набуває особливої ваги. З кожним роком через стрімкий розвиток технологій зростають загрози, що стосуються конфіденційної інформації, цілісності та доступності даних. Здебільшого слабкою стороною інформаційної безпеки є людський фактор. Саме тому потрібно мати належний рівень обізнаності та компетенції у сфері захисту інформації.

***Мета роботи –*** проведення комплексного аналізу сучасних технологій шифрування та анонімізації, призначених для захисту користувачів в Інтернеті, з метою оцінки їхньої ефективності, виявлення вразливостей, визначення оптимальних сфер застосування та розробки практичних рекомендацій щодо захисту персональних даних.

***Об’єкт дослідження –*** методи і технології захисту персональних даних та забезпечення анонімності користувачів у мережі Інтернет.

***Предмет дослідження*** – сучасні технології шифрування та анонімізації для захисту персональних даних користувачів в Інтернеті (криптографічні алгоритми AES, RSA; мережі VPN, Tor, I2P; протоколи SSL/TLS, IPsec, SSH) та оцінка їх ефективності й вразливостей, включно з моделюванням brute-force атаки на AES-128.

***Методи дослідження*** – в роботі застосовано методи системного аналізу, моделювання, експериментного оцінювання, порівняльного аналізу, а також практичного тестування (зокрема, можелювання brute force атаки на AES).

***Практичне значення отриманих результатів.*** Запропоновано модель тестування AES-128, яка може використовуватись для демонстрації принципів Brute force атак. Сформульовано практичні рекомендації щодо вибору технологій шифрування та анонімізації у різних контекстах використання.

Проведено огляд методів деанонімізації та способів протидії їм, що є корисним для підвищення цифрової грамотності.

***Апробація результатів*** кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 27 лютого 2025 року.

# Розділ 1 АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО ШИФРУВАННЯ ТА АНОНІМІЗАЦІЇ В ІНТЕРНЕТІ

## 1.1 Основні загрози безпеці користувачів в Інтернеті

У сучасних умовах цифровізації та глобального поширення Інтернету, користувачі постійно піддаються ризикам, пов’язаним із кіберзагрозами. Щодня тисячі осіб стають жертвами кіберзлочинців, які експлуатують вразливості інформаційних систем та використовують шкідливе ПЗ з метою отримання конфіденційної інформації. Відсутність базових знань з кібербезпеки у користувачів значно підвищує ймовірність потрапляння у ситуації несанкціонованого доступу до персональних даних або втрати інформації.

Для підвищення рівня користувачів в Інтернеті необхідно мати чітке уявлення про основні типи загроз. Усвідомлення природи таких загроз дозволяє формувати ефективну стратегію захисту пристроїв, персональних даних.

У цьому розділі буде розглянуто найпоширеніші типи кіберзагроз для користувачів, зокрема фішингові атаки, шкідливе ПЗ, а також ризики пов’язані з використанням незахищених бездротових мереж Wi-Fi.

Однією з найбільш розповсюджених загроз є Фішинг - це атака, яка намагається викрасти ваші гроші або вашу особу, змушуючи вас розкрити особисту інформацію - наприклад, номери кредитних карток, банківські реквізити або паролі - на веб-сайтах, які видають себе за легітимні.

Кіберзлочинці зазвичай видають себе за авторитетну компанію, друзів або знайомих у фальшивому повідомленні, яке містить посилання на фішинговий веб-сайт.

**Як розпізнати фішингову атаку?**

Оскільки фішингові електронні листи розроблені так, щоб імітувати легітимних осіб та організації, їх може бути важко розпізнати з першого погляду. Ось кілька поширених ознак, на які слід звернути увагу.

Електронний лист не пройшов перевірку SPF, DKIM або DMARC. Три записи DNS - Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) і Domain-based Message Authentication Reporting and Conformance (DMARC) - використовуються для перевірки походження електронного листа.

Якщо електронне повідомлення не проходить одну або кілька з цих перевірок, його часто позначають як спам або не доставляють адресату. З цієї причини в папках зі спамом рідко можна знайти легітимні електронні листи.

Адреса електронної пошти відправника не пов’язана з легітимним доменним ім’ям. Домен повинен відповідати назві організації, від якої нібито надійшов лист.

Наприклад, якщо всі адреси електронної пошти компанії Legitimate Internet Company відформатовані як "employee@legitinternetcompany.com", фальшивий лист може бути надісланий з адреси, яка звучить схоже, наприклад, "employee@legitinternetco.com" [1].

Фішингові електронні листи часто створюють хибне відчуття терміновості, щоб переконати користувачів діяти. Наприклад, вони можуть обіцяти подарункову картку, якщо користувач відповість протягом 24 годин, або стверджувати про витік даних, щоб змусити користувача оновити свій пароль.

Така тактика інколи пов'язана з реальними термінами або наслідками, оскільки вона спрямована на те, щоб змусити користувача вжити заходів до того, як у нього виникнуть підозри.

Посилання в тексті повідомлення не відповідають домену відправника. Більшість легітимних запитів не перенаправляють користувачів на веб-сайт, який відрізняється від домену відправника. Натомість фішингові спроби часто перенаправляють користувачів на шкідливий сайт або маскують шкідливі посилання в тексті листа.

Загалом, чим складніша спроба фішингу, тим менша ймовірність того, що ці елементи з'являться в електронному листі. Наприклад, деякі фішингові листи використовують логотипи та графіку відомих компаній, щоб надати своєму

повідомленню легітимного вигляду, тоді як інші зловмисники можуть закодувати все поле тіла листа як шкідливе гіперпосилання.

Шкідливе програмне забезпечення(Malware) - це будь-яке нав'язливе програмне забезпечення, розроблене кіберзлочинцями (яких часто називають хакерами) з метою крадіжки даних, пошкодження або знищення комп'ютерів і комп'ютерних систем [1].

**7 видів шкідливого ПЗ(malware)**

Віруси - це підгрупа шкідливих програм. Вірус - це шкідливе програмне забезпечення, прикріплене до документа або файлу, яке підтримує макроси для виконання свого коду і поширюється від комп'ютера до комп'ютера. Після завантаження вірус перебуває в сплячому режимі доти, доки файл не буде відкрито та використано. Віруси призначені для порушення працездатності системи. Як наслідок, віруси можуть спричинити значні операційні проблеми та втрату даних [2].

Хробак - це тип шкідливого програмного забезпечення, яке швидко розмножується і поширюється на будь-який пристрій у мережі. На відміну від вірусів, хробакам не потрібні програми-хости для розповсюдження. Хробак заражає пристрій через завантажений файл або мережеве з'єднання, перш ніж він розмножується і поширюється з експоненціальною швидкістю. Як і віруси, хробаки можуть серйозно порушити роботу пристрою і призвести до втрати даних [2].

Троянські віруси маскуються під корисне програмне забезпечення. Але як тільки користувач завантажує його, троянський вірус може отримати доступ до конфіденційних даних, а потім змінити, заблокувати або видалити ці дані. Це може вкрай негативно вплинути на роботу пристрою. На відміну від звичайних вірусів і хробаків, троянські віруси не призначені для самовідтворення [2].

Рекламне ПЗ - це шкідливе програмне забезпечення, яке використовується для збору даних про використання вашого комп'ютера та надання вам відповідної реклами. Хоча рекламне ПЗ не завжди є небезпечним, в деяких випадках воно може спричинити проблеми для вашої системи. ПЗ

може перенаправляти ваш браузер на небезпечні сайти і навіть містити троянських коней та шпигунські програми. Крім того, значний рівень рекламного ПЗ може помітно сповільнити роботу вашої системи. Оскільки не всі рекламні програми є шкідливими, важливо мати захист, який постійно та розумно сканує ці програми [2].

Програми-вимагачі - це шкідливе програмне забезпечення, яке отримує доступ до конфіденційної інформації в системі, шифрує цю інформацію так, щоб користувач не міг отримати до неї доступ, а потім вимагає фінансову виплату за видачу даних. Програми-вимагачі зазвичай є частиною фішингового шахрайства. Перейшовши за замаскованим посиланням, користувач завантажує програму-здирник. Зловмисник починає шифрувати певну інформацію, яку можна відкрити лише за допомогою відомого йому математичного ключа. Коли зловмисник отримує оплату, дані розблоковуються [2].

Безфайлове шкідливе програмне забезпечення - це різновид шкідливих програм, що живуть у пам'яті. Як випливає з назви, це шкідливе програмне забезпечення, яке працює з пам'яті комп'ютера жертви, а не з файлів на жорсткому диску. Оскільки немає файлів для сканування, його важче виявити, ніж традиційне шкідливе програмне забезпечення. Це також ускладнює криміналістичну експертизу, оскільки шкідливе програмне забезпечення зникає після перезавантаження комп'ютера-жертви [2].

Використання незахищених мереж Wi-Fi  в епоху, коли ми завжди на зв'язку, обізнаність про мережеву безпеку є більш важливою, ніж будь-коли. Зважаючи на зручність громадського Wi-Fi у кожній кав'ярні, бібліотеці та аеропорту, легко забути про потенційні небезпеки, що ховаються за цими з'єднаннями. Отже, що саме означає незахищена мережа? Незахищена мережа WiFi - це тип мережі, яка не використовує шифрування для передачі даних, що робить пристрої вразливими до таких загроз безпеки, як підслуховування та перехоплення даних.

**Чим небезпечне використання незахищеної мережі?**

Щоразу, коли ви підключаєтеся до Wi-Fi, ваш пристрій створює зв’язок з роутером, обмінюючись інформацією та надаючи вам доступ. Захищені мережі (наприклад, з шифруванням WPA2 або WPA3) зберігають цей зв’язок приватним, тоді як незахищені залишають його вразливими для підслуховувачів, хакерів або шкідливого програмного забезпечення, яке може використати ваше інтернет-з'єднання. Підключаючись до незахищеної мережі, ви, по суті, ділитеся цим простором з усіма, хто перебуває в зоні досяжності [3].

## 1.2 Методи атак на персональні дані та механізми їх перехоплення

Оскільки говорити про вище наведені теми без опису їх методів атак на персональні дані користувачів не є можливим, одразу перейдемо до механізмів їх перехоплення.

Почнемо як і в минулому пункті з “Фішингу”. Як ми вже знаємо фішингові атаки спрямовані на користувачів аби змусити їх розкрити особисту інформацію шляхом обману.  Як запобігти фішинговим атакам? Як і будь-яку іншу небажану електронну пошту (яку часто називають "спамом"), фішингові електронні листи неможливо повністю усунути за допомогою засобів захисту або служби фільтрації. Однак користувачі можуть вжити певних заходів, щоб зменшити ймовірність успішної атаки.

Перевіряйте електронні листи на наявність підозрілих елементів. У заголовках листа можуть міститися оманливі імена відправників або адреси електронної пошти, а в тексті - вкладення та посилання, які маскують шкідливий код. Користувачам слід бути обережними, відкриваючи повідомлення від незнайомого відправника [1].

Не діліться особистою інформацією. Навіть якщо ви спілкуєтеся з людиною, якій довіряєте, ніколи не обмінюйтеся особистою інформацією - наприклад, номерами соціального страхування, банківськими реквізитами, паролями тощо - в електронному листі.

Використовуйте протоколи безпеки електронної пошти. Методи автентифікації електронної пошти, такі як записи SPF, DKIM та DMARC, допомагають перевірити джерело електронного листа. Власники доменів можуть налаштувати ці записи так, щоб зловмисникам було складніше видавати себе за їхні домени під час підміни доменів [1].

Блокувати спам. Більшість поштових клієнтів мають вбудовані спам-фільтри, але сторонні сервіси фільтрації можуть надати користувачам більш детальний контроль над своєю електронною поштою. Інші рекомендації щодо уникнення спаму включають відписку від списків розсилки, відмову відкривати спам-листи та збереження адреси електронної пошти в таємниці.

Також можна використати MFA(мультифакторна автентифікація) яка додає додатковий рівень безпеки, вимагаючи декількох форм перевірки. Хоча він неефективний для запобігання спробам фішингу, він дуже ефективний проти несанкціонованого доступу, тому навіть якщо хтось став жертвою фішингу і його облікові дані були скомпрометовані, зловмисники все одно не зможуть отримати доступ до облікового запису, захищеного MFA. Будь-яка організація, велика чи мала, яка прагне захистити конфіденційні дані, повинна впровадити MFA[4].

У наш час існують так названі антифішингові програмні забезпечення. Антифішингове програмне забезпечення може допомогти виявити та запобігти спробам фішингу:

Фільтрування електронних листів: Антифішингове програмне забезпечення може сканувати вхідні електронні листи на наявність ознак фішингу, таких як підозрілі адреси відправників і посилання на відомі фішингові сайти. Ці листи можуть бути автоматично заблоковані або відправлені до карантинної папки.

Блокування шкідливих веб-сайтів: Антифішингове програмне забезпечення може запобігти доступу співробітників до відомих фішингових веб-сайтів, допомагаючи знизити ризик успішних атак.

Моніторинг мережевої активності: Антифішингове програмне забезпечення також може відстежувати мережеву активність, шукаючи ознаки фішингової активності та попереджаючи IT-персонал про потенційні загрози.

Забезпечення захисту в режимі реального часу: Антифішингове програмне забезпечення може забезпечити захист від фішингових атак у режимі реального часу, допомагаючи організаціям випереджати ці нові загрози.

Навчання користувачів найкращим практикам уникнення шкідливого програмного забезпечення (наприклад, не завантажувати і не запускати невідоме програмне забезпечення, не вставляти наосліп "знайдені носії" в комп'ютер), а також тому, як виявити потенційне шкідливе програмне забезпечення (наприклад, фішингові електронні листи, несподівані програми/процеси, що запускаються в системі), може мати велике значення для захисту вас або вашої організації.

Створення регулярних резервних копій. Регулярне резервне копіювання в автономному режимі може стати різницею між легким відновленням після руйнівної вірусної атаки або атаки з вимогою викупу та стресовим, шаленим копіюванням, що призводить до дорогого простою або втрати даних.

Ключовим моментом тут є регулярне резервне копіювання, яке підтверджено, що воно відбувається на очікуваній регулярній основі і може бути використане для відновлення. Старі, застарілі резервні копії менш цінні, ніж свіжі, а резервні копії, які не відновлюються належним чином, не мають ніякої цінності.

**Використання незахищених мереж Wi-Fi**

Най ефективніший спосіб запобігти витоку даних, це просто не підключатись до таких мереж, але є кілька способів, що дозволять вам з меншим ризиком використовувати громадський Wi-Fi.

Використовуйте VPN. Один з найефективніших способів захистити інформацію в загальнодоступній мережі - це використання VPN. Віртуальна приватна мережа (VPN) шифрує ваш мережевий трафік, маскує вашу IP-адресу, щоб забезпечити вам більше конфіденційності, а також допомагає обійти

цензуру або отримати доступ до потокового контенту з географічними обмеженнями створюючи безпечний тунель між вашим пристроєм та інтернетом [3].

Проте, слід зазначити, що використання не тих VPN можуть ставити під загрозу вашу особисту інформацію та наражати вас на ще більший ризик. Тож треба використовувати перевірені VPN, щоб захистити свої дані. Хоча VPN підвищує рівень конфіденційності та безпеки, вона також може дати вам хибне відчуття захищеності.

Навіть маючи VPN-з'єднання, ви все одно вразливі до таких небезпек, як шкідливе програмне забезпечення та хакери, оскільки VPN не заважає вам відвідувати шкідливі веб-сайти.

Повертаючись до незахищених мереж, слід вимкнути автоматичне підключення. Функція автоматичного підключення вашого пристрою може здатися зручною, але вона небезпечна при роботі з незахищеними мережами.

Щоб запобігти автоматичному підключенню пристрою до будь-якого доступного Wi-Fi, вимкніть цю функцію. Підключення вручну дозволяє вам контролювати, до яких мереж ви приєднуєтеся, і допомагає уникнути випадкового впливу загроз безпеки.

Один із найпростіших і водночас найефективніших способів зміцнити мережеву безпеку - це постійно оновлювати свої пристрої та програмне забезпечення. Ставтеся до оновлень як до необхідної підтримки вашого цифрового життя. Застарілі пристрої та програмне забезпечення можуть містити вразливості, які хакери прагнуть використати [3].

Виробники та розробники регулярно випускають оновлення, щоб виправити ці вразливості та покращити функції безпеки. Забезпечуючи постійне оновлення своїх пристроїв і програмного забезпечення, ви закриваєте двері для потенційних зловмисників і значно ускладнюєте кіберзлочинцям доступ до ваших даних.

Налаштуйте свої пристрої на автоматичне оновлення, коли це можливо, і регулярно перевіряйте наявність оновлень для своїх програм та операційних

систем. Такий проактивний підхід може суттєво допомогти у підтримці надійної мережевої безпеки [3].

## 1.3 Огляд криптографічних технологій: історичний розвиток та сучасні підходи

Криптографія, що походить від грецьких слів, які означають "приховане письмо", - це практика шифрування переданої інформації таким чином, щоб її міг інтерпретувати лише передбачуваний одержувач. З часів античності практика надсилання таємних повідомлень була поширена майже у всіх великих цивілізаціях [5].

У наш час криптографія стала критично важливим елементом кібербезпеки. Від захисту повсякденних особистих повідомлень і автентифікації цифрових підписів до захисту платіжної інформації в інтернет-магазинах і навіть захисту надсекретних урядових даних і комунікацій - криптографія робить можливим цифрову приватність.

Хоча ця практика налічує тисячі років, використання криптографії та ширшої галузі криптоаналізу все ще вважається відносно молодим, досягнувши величезного прогресу лише за останні 100 років. Початок цифрової ери, що збігся з винайденням сучасної обчислювальної техніки в 19 столітті, також ознаменував народження сучасної криптографії.

Як найважливіший засіб встановлення цифрової довіри, математики, інформатики та криптографи почали розробляти сучасні криптографічні методи і криптосистеми для захисту важливих даних користувачів від хакерів, кіберзлочинців і сторонніх очей [5].

Більшість криптосистем починаються з незашифрованого повідомлення, відомого як відкритий текст, який потім шифрується в нерозбірливий код, відомий як зашифрований текст, за допомогою одного або декількох ключів шифрування. Зашифрований текст передається одержувачу.

Якщо шифрограму перехоплено, а алгоритм шифрування стійкий, то вона буде марною для будь-якого несанкціонованого підслуховування, оскільки він не зможе зламати код. Однак, цільовий одержувач зможе легко розшифрувати текст, за умови, що у нього є правильний ключ розшифровки [5].

**Розвиток криптографії**

Шифр цезаря - близько 58 року до н.е. Юлій Цезар використовував спеціальну техніку у своїх військових кампаніях, щоб ускладнити ворогам розуміння його наказів. Він робив це, переставляючи кожну літеру у своїх командах. Ворогу доводилося докладати додаткових зусиль, щоб перехопити і розшифрувати, що означає команда [6].

Це був перший у світі зафіксований шифр заміни, який використовувався у світі. Пізніше ця техніка стала більш популярною як метод шифрування і була названа шифром Цезаря на честь свого винахідника. Завдяки своїй простоті та легкості у використанні, шифр Цезаря створив основу для сучасних криптографічних методів [6].

Шифр Цезаря запровадив ідею заміни однієї літери іншою - базовий, але важливий принцип криптографії. Його простота дійсно заклала основу для створення більш досконалих і безпечних методів шифрування. Люди часто використовують шифр Цезаря в різних освітніх програмах для навчання основам шифрування та дешифрування [7].

Це може бути чудовим початком для розуміння більш складних тем, таких як: Ідея фіксованого зсуву в шифрі Цезаря з часом розвинулася в більш складні методи, такі як шифр Віженера, який використовує змінний зсув на основі ключового слова. Цей перехід від простого фіксованого методу до більш складного змінного показує, як криптографічні методи розвивалися, щоб задовольнити потребу в кращій безпеці.

Скитала - стародавня форма шифрування, поширена в Стародавній Греції. Це різновид шифру перестановки, коли літери в повідомленні переставляються перед тим, як їх розшифрує одержувач. Цей метод передбачав використання циліндра, навколо якого обертали пергамент і писали на ньому повідомлення.

Одержувач читав послання за допомогою палички тих самих розмірів. З огляду на простоту, його легко розшифровував і ворог [6].

Метод частотного аналізу Аль-Кінді - Арабський математик Аль-Кінді винайшов метод частотного аналізу для розкриття шифрів, що стало одним з найбільш грандіозних проривів у криптоаналізі. Частотний аналіз використовує лінгвістичні дані - такі як частота певних літер або буквосполучень, частин мови і побудови речень - для реінжинірингу приватних ключів дешифрування.

Методи частотного аналізу можуть бути використані для прискорення атак грубої сили, в яких зловмисники намагаються методично розшифрувати закодовані повідомлення, систематично застосовуючи потенційні ключі в надії врешті-решт знайти правильний.

Моноалфавітні шифри підстановки, які використовують лише один алфавіт, особливо чутливі до частотного аналізу, особливо якщо приватний ключ короткий і слабкий. Роботи Аль-Кінді також охоплюють методи криптоаналізу поліалфавітних шифрів, які замінюють відкритий текст зашифрованим текстом з декількох алфавітів для додаткового рівня безпеки, набагато менш вразливого до частотного аналізу.

Шифр Віженера - тип шифру заміни, що використовується для шифрування даних, в якому вихідна структура відкритого тексту дещо прихована в зашифрованому тексті за допомогою декількох різних моноалфавітних шифрів заміни, а не одного [8].

Кодовий ключ вказує, яка саме заміна буде використана для шифрування кожного символу відкритого тексту. Такі результуючі шифри, відомі як поліалфавітні, мають довгу історію використання.

Системи відрізняються, головним чином, способом вибору ключа з набору моноалфавітних правил заміни. Шифр був винайдений у 1553 році італійським криптографом Джован Баттіста Белласо, але протягом століть його приписували французькому криптографу 16-го століття Блезу де Віженера, який розробив подібний шифр у 1586 році. Протягом багатьох років цей тип шифру вважався неприступним і був відомий як "незламний шифр" [8].

Машина "Енігма" - це знаменита шифрувальна машина, яку німці використовували під час Другої світової війни для передачі закодованих повідомлень. Машина "Енігма" дозволяє мільярди і мільярди способів кодування повідомлень, що робить неймовірно складним для інших країн зламати німецькі коди під час війни - на деякий час код здавався незламним.

Алан Тьюрінг та інші дослідники використали кілька слабких місць у реалізації коду "Енігми" і отримали доступ до німецьких шифрів, що дозволило їм сконструювати машину під назвою "Бомба", яка допомогла зламати найскладніші версії "Енігми". Деякі історики вважають, що розкриття "Енігми" було найважливішою перемогою союзників під час Другої світової війни.

Використовуючи інформацію, яку вони розшифрували у німців, союзники змогли запобігти багатьом атакам. Однак, щоб уникнути підозр нацистів у тому, що вони мали доступ до німецьких комунікацій, союзники були змушені дозволити здійснити деякі атаки, незважаючи на те, що вони мали знання, які могли б їх зупинити. Машини Enigma використовують форму шифрування підстановки [9].

Шифрування підстановкою - це простий спосіб кодування повідомлень, але ці коди досить легко зламати. Простим прикладом схеми шифрування підстановки є шифр Цезаря. Шифр Цезаря зсуває кожну літеру алфавіту на певну кількість місць. Шифр Цезаря зі зсувом на 11 кодує літеру A як B, M як N, Z як A і так далі. Але машини Enigma набагато потужніші, ніж простий шифр Цезаря.

Уявіть собі, що кожного разу, коли одна буква зіставлялася з іншою, змінювалася вся схема кодування. Після кожного натискання клавіші ротори рухаються, а повторне натискання цієї ж клавіші спрямовує струм по іншому шляху до іншої відкритої літери. Таким чином, при першому натисканні клавіші генерується одне кодування, при другому натисканні клавіші - інше кодування і так далі [9].

Це значно збільшує кількість можливих конфігурацій кодування. Кожного разу, коли натискається клавіша на машині Enigma, ротори

обертаються, і код змінюється. Це означає, що повідомлення "AA" може бути закодоване як щось на кшталт "TU", навіть якщо ту саму клавішу було натиснуто двічі [9].

Асиметрична криптографія - також відома як криптографія з відкритим ключем - це процес, який використовує пару пов'язаних ключів - один відкритий ключ і один закритий ключ - для шифрування і розшифрування повідомлень і захисту їх від несанкціонованого доступу або використання.

Відкритий ключ - це криптографічний ключ, який людина може використовувати для шифрування повідомлення, щоб його міг розшифрувати тільки той, кому воно призначене, за допомогою свого приватного ключа [10].

Приватний ключ - також відомий як секретний ключ - доступний лише ініціатору ключа. Коли хтось хоче надіслати зашифроване повідомлення, він витягує відкритий ключ одержувача з публічного каталогу і використовує його для шифрування повідомлення перед відправкою. Одержувач може розшифрувати повідомлення за допомогою свого приватного ключа.

Якщо відправник зашифрує повідомлення за допомогою свого приватного ключа, то розшифрувати повідомлення можна лише за допомогою відкритого ключа цього відправника, таким чином автентифікуючи відправника. Ці процеси шифрування і дешифрування відбуваються автоматично; користувачам не потрібно фізично блокувати і розблоковувати повідомлення [10].

Багато протоколів покладаються на асиметричну криптографію, включаючи захист транспортного рівня (TLS) і рівень захищених сокетів (SSL), які роблять можливим використання HTTPS. Процес шифрування також використовується в програмному забезпеченні, яке повинно встановлювати безпечне з'єднання через незахищену мережу, наприклад, у веб-браузерах, або яке повинно перевіряти цифровий підпис [10].

Підвищена безпека даних є основною перевагою асиметричної криптографії. Це найбезпечніший процес шифрування, оскільки користувачі ніколи не зобов'язані розкривати або передавати свої приватні ключі, що

зменшує ймовірність того, що кіберзлочинець виявить приватний ключ користувача під час передачі даних.

## Висновки до розділу 1

У результаті аналізу сучасних кіберзагроз, що виникають у цифровому середовищі, встановлено, що найбільш поширеними ризиками для користувачів Інтернету є фішингові атаки, розповсюдження шкідливого програмного забезпечення, а також використання незахищених бездротових мереж. Визначено, що основною вразливістю є недостатній рівень цифрової грамотності користувачів, що сприяє успішному застосуванню методів соціальної інженерії та перехопленню персональних даних.

Проведений аналіз асиметричної криптографії на прикладі RSA засвідчив її значущість у реалізації цифрових підписів, захищених протоколів (наприклад, SSL/TLS) та процесів автентифікації. Водночас підкреслено, що асиметричне шифрування є обчислювально більш ресурсоємним, тому доцільним є його поєднання із симетричними методами у гібридних схемах.

Таким чином, перший розділ закладає теоретичну базу для подальшого аналізу сучасних криптографічних технологій і методів забезпечення анонімності в цифровому просторі, що є важливою передумовою для досягнення цілей дослідження.

# Розділ 2 СУЧАСНІ ТЕХНОЛОГІЇ ШИФРУВАННЯ ДАНИХ ТА ТЕХНОЛОГІЇ АНОНІМІЗАЦІЇ У КІБЕРБЕЗПЕЦІ

## 2.1 Симетричні та асиметричні алгоритми шифрування: принципи та порівняльний аналіз

Із зростанням обсягів цифрових даних та необхідності їх захисту, криптографія стала ключовим інструментом у сфері інформаційної безпеки. Однією з базових класифікацій криптографічних алгоритмів є поділ на симетричні та асиметричні алгоритми шифрування. Ці два типи відрізняються підходом до управління ключами, рівнем безпеки, швидкістю обробки даних та сферою застосування.

**Симетричне шифрування**

Симетричне шифрування - це найстаріший вид шифрування, в якому один і той самий ключ використовується як для шифрування, так і для розшифрування. Існує дві основні функції, які використовуються для приховування відкритого тексту в шифрах симетричного шифрування: підстановка і транспозиція [11].

Сучасні криптографічні алгоритми використовують обидві функції у досить лабіринтовий спосіб; у першому підрозділі ми коротко розглянемо деякі класичні криптографічні алгоритми, щоб простіше представити кожну з цих функцій.

Симетричні шифри також можуть працювати або з частинами вхідних даних, або з кожним бітом вхідних даних послідовно. Якщо шифр оперує фрагментами або блоками вхідних даних як єдиним цілим, він називається блоковим шифром, тоді як якщо він оперує кожним бітом послідовно, в потоці, то він називається потоковим шифром.

Основна відмінність полягає в тому, що потокові шифри мають переваги в продуктивності та енергоспоживанні над блоковими шифрами, і їх легше

реалізувати на апаратному рівні, однак потокові шифри набагато вразливіші до певних атак, і тому зазвичай використовуються лише тоді, коли це підвищення продуктивності є абсолютно необхідним [11].

Симетрична схема шифрування складається з п'яти компонентів, як показано на схемі нижче. Рис.1

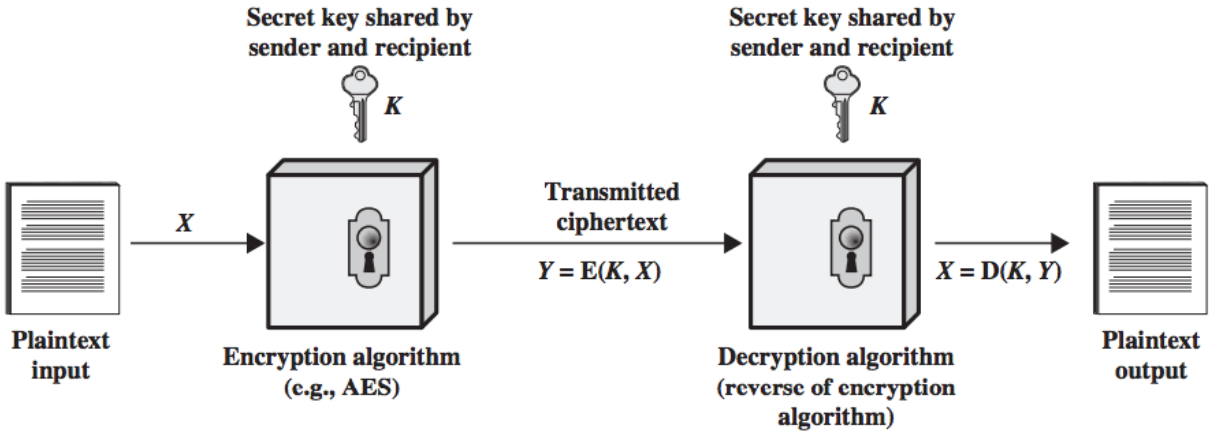


Рис.1 - Компоненти симетричної схеми шифрування

Це спрощена модель звичайного шифрування.

1. Відкритий текст: це оригінальне повідомлення або дані, які подаються в алгоритм як вхідні дані [12].

2. Алгоритм шифрування: Алгоритм шифрування виконує різні заміни і перетворення над відкритим текстом [12].

3. Секретний ключ: Секретний ключ також подається на вхід алгоритму. Від ключа залежать точні заміни і перетворення, які виконує алгоритм [12].

4. Зашифрований текст: Це зашифроване повідомлення, яке ми отримуємо на виході. Він залежить від відкритого тексту і секретного ключа. Для даного повідомлення два різних ключі дають два різних зашифрованих тексти [12].

5. Алгоритм розшифрування: Це, по суті, алгоритм шифрування, який виконується у зворотному порядку. Він бере зашифрований текст і той самий секретний ключ і створює оригінальний відкритий текст [12].

Існує дві вимоги для безпечного використання симетричного шифрування:

По-перше, нам потрібен стійкий алгоритм шифрування. Як мінімум, ми хотіли б, щоб алгоритм був таким, щоб опонент, який знає алгоритм і має доступ до одного або декількох зашифрованих текстів, не зміг би розшифрувати зашифрований текст або підібрати ключ [12].

Ця вимога зазвичай формулюється в більш жорсткій формі : Опонент не повинен бути в змозі розшифрувати зашифрований текст або знайти ключ, навіть якщо він або вона володіє кількома зашифрованими текстами разом з відкритим текстом, який породив кожен з них [12].

По-друге, відправник і одержувач повинні отримати копії секретного ключа у безпечний спосіб і повинні зберігати ключ у безпеці. Якщо хтось може розкрити ключ і знає алгоритм, вся комунікація з використанням цього ключа буде читабельною [12].

Важливо відзначити, що безпека симетричного шифрування залежить від секретності ключа, а не від секретності алгоритму. Тобто, передбачається, що розшифрувати повідомлення на основі зашифрованого тексту плюс знання алгоритму шифрування/розшифрування недоцільно. Іншими словами, нам не потрібно тримати в секреті алгоритм, нам потрібно тримати в секреті тільки ключ [12].

Деякі приклади того, де використовується симетрична криптографія: Платіжні додатки, такі як карткові транзакції, де необхідно захистити PII, щоб запобігти крадіжці особистих даних або шахрайським платежам. Перевірки для підтвердження того, що відправник повідомлення є тим, за кого себе видає. Генерація випадкових чисел або хешування [12].

**Переваги та недоліки симетричного шифрування**

Симетричне шифрування має кілька переваг, серед яких:

Безпека: Симетричне шифрування забезпечує надійний захист даних, оскільки для шифрування та розшифрування використовується один і той самий ключ. До поширених алгоритмів симетричного шифрування належать Advanced Encryption Standard (AES), Data Encryption Standard (DES) та

International Data Encryption Algorithm (IDEA). Це ускладнює доступ до даних для неавторизованих користувачів [13].

Швидкість: симетричне шифрування, як правило, швидше за інші типи шифрування, оскільки для шифрування і розшифрування використовується один і той самий ключ. Це робить його гарним вибором для програм, які потребують швидкого шифрування та розшифрування даних.

Ефективність: Симетричне шифрування вимагає менше обчислювальної потужності і ресурсів для шифрування і розшифрування даних, що може заощадити час і гроші.

Простота: Симетричне шифрування легко реалізувати і використовувати, оскільки воно вимагає лише одного ключа для шифрування і розшифрування. Це робить його популярним вибором для додатків, які потребують простого і зрозумілого шифрування [13].

Сумісність: Симетричне шифрування широко використовується і підтримується більшістю програмних і апаратних платформ, що робить його сумісним з широким спектром систем і пристроїв. Це означає, що його можна легко інтегрувати в існуючі програми та системи, не вимагаючи значних модифікацій.

Однак недоліком симетричного шифрування є те, що воно може бути менш безпечним, ніж асиметричне. Якщо ключ потрапить до чужих рук, дані можуть бути скомпрометовані. Тому важливо забезпечити надійне зберігання ключа і надавати його лише авторизованим користувачам [13].

**Як працює асиметрична криптографія (RSA)?**

Конфіденційні повідомлення проходять через процес шифрування та дешифрування за допомогою відкритих і закритих ключів.

Алгоритм запускає процес. Математична функція генерує пару ключів. Кожен ключ є окремим, але вони пов'язані між собою математично [14].

Протоколи генерації ключів відрізняються, і ключі, які вони створюють, також відрізняються. У середовищі Microsoft, наприклад, вам потрібно близько

чотирьох рядків коду, щоб почати розробку пари асиметричних ключів. Інші програми працюють подібним чином.

Наприклад, якщо хтось хоче відправити зашифроване повідомлення іншій людині. Процес виглядає так:

Реєстрація: Користувач і відправник зв'язалися з офіційною організацією, яка згенерувала відкритий і закритий ключі.

Пошук: Відправник шукає в каталозі відкритих ключів інформацію про відкритий ключ одержувача.

Шифрування: Відправник створює повідомлення, шифрує його за допомогою відкритого ключа одержувача і надсилає.

Розшифрувати: Одержувач використовує приватний ключ, щоб розшифрувати повідомлення.

Відповісти: Якщо одержувач хоче відповісти, процес рухається у зворотному напрямку [14].

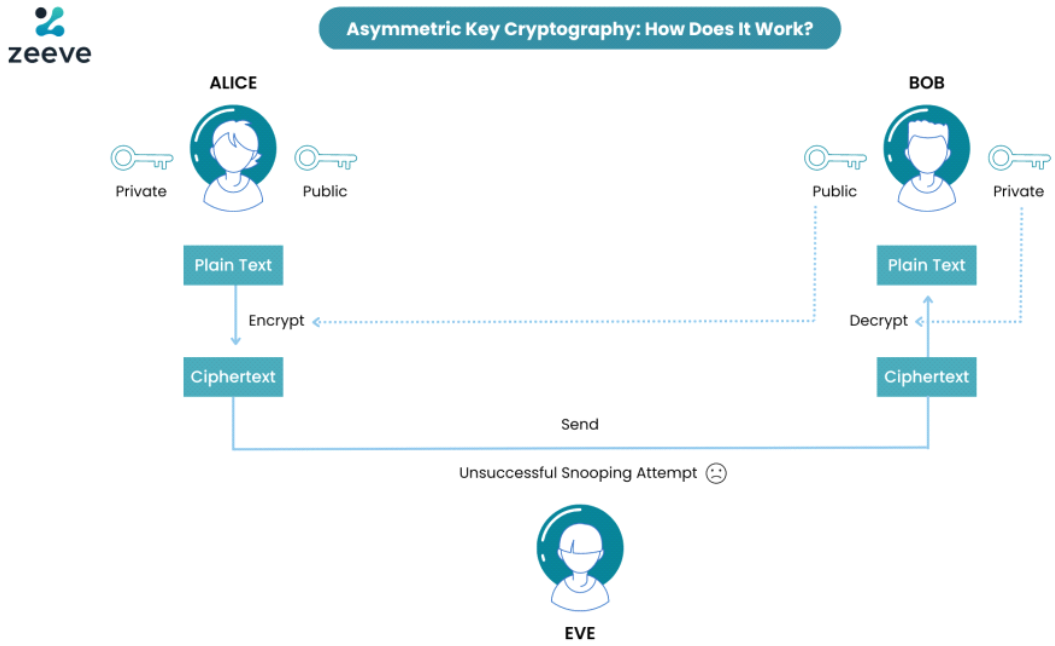


Рис.2 - Приклад роботи асиметричного шифрування

**Переваги асиметричної криптографії**

Підвищена безпека: Асиметричне шифрування забезпечує вищий рівень безпеки в порівнянні з симетричним шифруванням, де для шифрування і дешифрування використовується лише один ключ, а при асиметричному шифруванні для кожного процесу використовується окремий ключ, а приватний ключ, який використовується для дешифрування, зберігається в таємниці одержувачем, що ускладнює зловмиснику перехоплення і дешифрування даних.

Аутентифікація: Асиметричне шифрування може використовуватися для автентифікації, що означає, що одержувач може перевірити особу відправника. Це досягається тим, що відправник шифрує повідомлення своїм приватним ключем, який може бути розшифрований тільки за допомогою свого відкритого ключа, якщо одержувач може успішно розшифрувати повідомлення, це доводить, що воно було відправлено відправником, який має відповідний приватний ключ [15].

Неможливість відмови від повідомлення: Асиметричне шифрування також забезпечує неможливість відмови, що означає, що відправник не може заперечити відправлення повідомлення або зміну його вмісту, тому що повідомлення зашифровано за допомогою закритого ключа відправника, і тільки його відкритий ключ може розшифрувати його. Таким чином, одержувач може бути впевнений, що повідомлення було надіслано відправником і не було змінено [15].

Універсальність: Асиметричне шифрування може використовуватися для широкого спектру застосувань, включаючи безпечне спілкування електронною поштою, банківські операції в Інтернеті та електронну комерцію, а також для захисту SSL/TLS-з'єднань, які зазвичай використовуються для захисту інтернет-трафіку.

Рандомізація - це один з варіантів отримання ключів. Враховуючи, що відкритий ключ може бути широко розповсюджений, можна зашифрувати

приватний ключ, а потім надіслати його особі, якій він адресований. Це стає можливим завдяки широкому розповсюдженню відкритого ключа [13].

**Недоліки асиметричного шифрування**

Швидкість: Асиметричне шифрування працює повільніше порівняно з симетричним. Це пов'язано з тим, що алгоритми асиметричного шифрування складніші і вимагають більше обчислювальних ресурсів.

Розподіл ключів: Асиметричне шифрування вимагає безпечного способу розповсюдження відкритих ключів. Якщо відкритий ключ перехоплять або підроблять під час передачі, це може поставити під загрозу безпеку системи.

Розмір ключа: Асиметричне шифрування вимагає більшого розміру ключа порівняно з симетричним, що робить його більш ресурсоємним [14].

**Порівняльний аналіз Симетрчного та асиметричного шифрування**

**Суть підходів**

Симетричне шифрування використовує один ключ для шифрування та дешифрування даних.

Асиметричне шифрування використовує два ключа, один відкритий для шифрування, другий приватний для дешифрування.

**Швидкість**

Симетричне шифрування значно швидше бо обчислення менш складні.

Асиметричне шифрування повільніше, через складні математичні операції.

**Безпека**

Симетричне шифрування вважається дуже надійним при правильному зберіганні ключа, але вразливе через потребність передавати ключ іншій стороні.

Асиметричне шифрування закриває недолік симетричного, бо має два ключа, один з яких можна спокійно передавати іншій особі, що значно підвищує безпеку при з’єднанні.

**Основні застосування**

Симетричне шифрування використовують загалом для захисту великих обсягів даних, VPN - з’єднання, Wi-Fi мережі, та алгоритмів AES, DES, ChaCha20.

Асиметричне шифрування використовують для безпечного обміну ключами, цифрових підписів та сертифікатів, електоронних комерцій таких як SSL/TLS, та алгоритмів RSA, ECC, ElGamal.

## 2.2 Протоколи безпечного з’єднання: SSL/TLS, IPsec, SSH

В наші дні забезпечення безпечного передавання даних через мережі є критично важливою задачею. Саме для цього використовуються спеціальні протоколи безпечного з’єднання, які шифрують дані та гарантують їх цілістність та автентичність передавання. Найбільш відомі з них - SSL/TLS, IPsec, SSH. Отже спочатку познемо з SSL/TLS.

**Що таке SSL/TLS?**

SSL, або протокол захищених сокетів (Secure Sockets Layer) - це заснований на шифруванні протокол безпеки в Інтернеті. Вперше він був розроблений компанією Netscape у 1995 році з метою забезпечення конфіденційності, автентифікації та цілісності даних в інтернет-комунікаціях. SSL є попередником сучасного шифрування TLS, яке використовується сьогодні. Веб-сайт, який використовує SSL/TLS, має в своїй URL-адресі "HTTPS" замість "HTTP"[16].

**Як працює SSL/TLS?**

Щоб забезпечити високий рівень конфіденційності, SSL шифрує дані, які передаються через Інтернет. Це означає, що будь-хто, хто спробує перехопити ці дані, побачить лише спотворену суміш символів, яку майже неможливо розшифрувати.

SSL ініціює процес автентифікації, який називається рукостисканням між двома пристроями, щоб переконатися, що обидва пристрої дійсно є тими, за кого себе видають.

SSL також накладає цифровий підпис на дані, щоб забезпечити їхню цілісність, перевіряючи, що дані не були підроблені до того, як вони потраплять до адресата.

Існувало кілька ітерацій SSL, кожна з яких була більш безпечною, ніж попередня. У 1999 році SSL було оновлено і перетворено на TLS.

TLS розвинувся з попереднього протоколу шифрування під назвою Secure Sockets Layer (SSL), який був розроблений компанією Netscape. TLS версії 1.0 фактично почав розроблятися як SSL версії 3.1, але назва протоколу була змінена перед публікацією, щоб вказати, що він більше не асоціюється з Netscape. Через цю історію терміни TLS і SSL іноді використовуються як взаємозамінні [16].

З'єднання TLS ініціюється за допомогою послідовності, відомої як рукостискання TLS. Коли користувач переходить на веб-сайт, який використовує TLS, між пристроєм користувача і веб-сервером починається рукостискання TLS.

Під час TLS-рукостискання пристрій користувача і веб-сервер обмінюються даними:

Вказують, яку версію TLS вони будуть використовувати. Вирішують, які набори шифрів вони будуть використовувати. Перевіряють ідентичність сервера за допомогою сертифіката TLS сервера. Генерують сеансові ключі для шифрування повідомлень між ними після завершення рукостискання.

Рукостискання TLS встановлює набір шифрів для кожної сесії зв'язку. Набір шифрів - це набір алгоритмів, який визначає деталі, наприклад, які спільні ключі шифрування або сеансові ключі будуть використовуватися для цього сеансу. TLS може встановлювати відповідні сеансові ключі через незашифрований канал завдяки технології, відомій як криптографія з відкритим ключем [17].

Рукостискання також обробляє автентифікацію, яка зазвичай полягає в тому, що сервер підтверджує свою ідентичність клієнту. Це робиться за допомогою відкритих ключів.

Відкриті ключі - це ключі шифрування, які використовують одностороннє шифрування, тобто будь-хто, хто має відкритий ключ, може розшифрувати дані, зашифровані закритим ключем сервера, щоб переконатися в їх автентичності, але тільки оригінальний відправник може зашифрувати дані за допомогою закритого ключа. Відкритий ключ сервера є частиною його сертифіката TLS.

Після того, як дані зашифровані та автентифіковані, вони підписуються кодом автентифікації повідомлення (MAC). Одержувач може перевірити MAC, щоб переконатися в цілісності даних. Це схоже на захисну фольгу на пляшці аспірину: споживач знає, що ніхто не втручався в його ліки, тому що фольга не пошкоджена, коли він купує їх [17].

**Послуги які надає TLS**

TLS надає три основні послуги, які допомагають забезпечити безпеку та захист даних, якими обмінюються за допомогою цього протоколу:

**Автентифікація**

Автентифікація дозволяє кожній стороні комунікації переконатися, що інша сторона є тією, за кого вона себе видає.

**Шифрування**

Дані шифруються під час передачі між користувацьким агентом і сервером, щоб запобігти їх прочитанню та інтерпретації неавторизованими сторонами.

**Цілісність**

TLS гарантує, що між шифруванням, передачею та розшифруванням даних жодна інформація не буде втрачена, пошкоджена, підроблена або сфальсифікована.

З'єднання TLS починається з етапу рукостискання, на якому клієнт і сервер домовляються про спільний секрет і узгоджують важливі параметри,

такі як набори шифрів. Після узгодження параметрів і режиму обміну даними відбувається обмін прикладними даними, такими як HTTP [18].

**Що таке IPsec (Internet Protocol Security)?**

IPsec - це група протоколів для захисту з'єднань між пристроями. IPsec допомагає захистити дані, що надсилаються через публічні мережі. Його часто використовують для налаштування VPN, і він працює за допомогою шифрування IP-пакетів, а також автентифікації джерела, звідки надходять пакети [19].

У терміні "IPsec" "IP" означає "Інтернет-протокол", а "sec" - "безпечний". Інтернет протокол, це основний протокол маршрутизації, який використовується в Інтернеті. Він визначає, куди будуть передаватися дані за допомогою IP-адрес. IPsec є безпечним, оскільки додає до цього процесу шифрування та автентифікацію.

**Як працює IPsec?**

IPsec-з'єднання складається з наступних кроків:

Обмін ключами: Ключі необхідні для шифрування; ключ - це рядок випадкових символів, який можна використовувати для "блокування" (шифрування) і "розблокування" (дешифрування) повідомлень. IPsec встановлює ключі за допомогою обміну ключами між підключеними пристроями, щоб кожен пристрій міг розшифровувати повідомлення іншого пристрою.

Заголовки та трейлери пакетів: Усі дані, які надсилаються мережею, розбиваються на менші частини, які називаються пакетами. Пакети містять як корисне навантаження, тобто власне дані, що надсилаються, так і заголовки, тобто інформацію про ці дані, щоб комп'ютери, які отримують пакети, знали, що з ними робити. IPsec додає кілька заголовків до пакетів даних, що містять інформацію про автентифікацію та шифрування. IPsec також додає трейлери, які йдуть після корисного навантаження кожного пакета, а не перед ним [19].

Автентифікація: IPsec забезпечує автентифікацію для кожного пакета, подібно до штампу автентичності на колекційному предметі. Це гарантує, що пакети надходять з надійного джерела, а не від зловмисника.

Шифрування: IPsec шифрує корисне навантаження в кожному пакеті та IP-заголовок кожного пакета (якщо не використовується транспортний режим замість тунельного - див. нижче). Це забезпечує безпеку та конфіденційність даних, що надсилаються через IPsec.

Передача: Зашифровані пакети IPsec переміщуються через одну або декілька мереж до місця призначення за допомогою транспортного протоколу.

На цьому етапі IPsec-трафік відрізняється від звичайного IP-трафіку тим, що в якості транспортного протоколу найчастіше використовується UDP, а не TCP. TCP, протокол управління передачею, встановлює виділені з'єднання між пристроями і гарантує, що всі пакети будуть доставлені.

UDP, протокол користувацьких дейтаграм, не встановлює ці виділені з'єднання. IPsec використовує UDP, оскільки це дозволяє пакетам IPsec проходити через брандмауери.

Розшифровка: На іншому кінці зв'язку пакети розшифровуються, і програми можуть використовувати доставлені дані [19].

**Які протоколи використовуються в IPsec?**

Протокол - це визначений спосіб форматування даних таким чином, щоб будь-який комп'ютер у мережі міг їх інтерпретувати. IPsec - це не один протокол, а набір протоколів. Наступні протоколи складають набір IPsec:

AH (Authenticator Header): Протокол AH гарантує, що пакети даних походять з надійного джерела і що дані не були підроблені, подібно до пломби на споживчому товарі. Ці заголовки не забезпечують ніякого шифрування, вони не допомагають приховати дані від зловмисників.

ESP (Encapsulating Security Protocol): ESP шифрує IP-заголовок і корисне навантаження для кожного пакета - якщо не використовується транспортний режим, в якому шифрується тільки корисне навантаження. ESP додає власний заголовок і трейлер до кожного пакету даних.

Security Association (SA): SA відноситься до ряду протоколів, що використовуються для узгодження ключів та алгоритмів шифрування. Одним з найпоширеніших протоколів SA є Internet Key Exchange (IKE) [19].

**Що таке протокол SSH?**

Протокол Secure Shell (SSH) - це метод безпечного надсилання команд на комп'ютер через незахищену мережу. SSH використовує криптографію для автентифікації та шифрування з'єднань між пристроями. SSH також дозволяє тунелювання або переадресацію портів, коли пакети даних можуть перетинати мережі, які інакше вони не змогли б перетнути. SSH часто використовується для віддаленого керування серверами, управління інфраструктурою та передачі файлів [20].

Власник магазину, від'їжджаючи у відпустку, може давати своїм працівникам інструкції на відстані, щоб забезпечити безперебійну роботу магазину під час своєї відсутності. Аналогічно, SSH дозволяє адміністраторам керувати серверами та пристроями на відстані. Старіші протоколи віддаленого керування, такі як Telnet, передавали команди адміністраторів у формі, яку міг бачити будь-хто.  На відміну від Telnet, SSH є безпечним - звідси і назва Secure Shell [20].

**Що робить SSH?**

Віддалені зашифровані з'єднання: SSH встановлює з'єднання між користувацьким пристроєм і віддаленим комп'ютером, часто сервером. Він використовує шифрування для зашифрування даних, які передаються через з'єднання. Сторона, що перехоплює, знайде лише щось на кшталт статичних - випадкових даних, які нічого не означають, якщо їх не розшифрувати. (SSH використовує методи шифрування, які роблять розшифровку надзвичайно складною для сторонніх).

Можливість тунелювання: В мережевих технологіях тунелювання - це метод переміщення пакетів через мережу за допомогою протоколу або шляху, який вони зазвичай не можуть використовувати. Тунелювання працює шляхом обгортання пакетів даних додатковою інформацією, яка називається

заголовками, щоб змінити їх місце призначення. Тунелі SSH використовують техніку переадресації портів для пересилання пакетів з одного комп'ютера на інший [20].

**Як працює і для чого використовують SSH?**

SSH працює поверх набору протоколів TCP/IP, на якому базується більша частина Інтернету. TCP/IP транспортує і доставляє пакети даних. Використання TCP є однією з відмінностей SSH від інших тунельних протоколів, деякі з яких використовують швидший, але менш надійний протокол UDP.

Технічно SSH може передавати будь-які довільні дані по мережі, а тунелювання SSH може бути налаштоване для безлічі цілей. Однак найпоширеніші випадки використання SSH такі:

Віддалене керування серверами, інфраструктурою та комп'ютерами співробітників.

Безпечна передача файлів (SSH безпечніший за незашифровані протоколи, такі як FTP).

Доступ до хмарних сервісів без відкритих портів локального комп'ютера в Інтернеті.

Віддалене підключення до сервісів у приватній мережі та обхід обмежень брандмауера [20].

**Чим SSH відрізняється від інших протоколів тунелювання?**

Однією з основних відмінностей між SSH та іншими протоколами тунелювання є рівень OSI, на якому вони працюють. GRE, IP-in-IP і IPsec - це протоколи мережевого рівня. Як такі, вони не знають про порти (концепція транспортного рівня), натомість працюють між IP-адресами. (Точна приналежність SSH до рівня OSI строго не визначена, але більшість джерел описують його як протокол рівня 7/прикладного рівня, як HTTP, FTP і SMTP).

Ще однією відмінністю є використання SSH протоколу TCP. TCP, як описано вище, є протоколом транспортного рівня і одним з основних протоколів, що використовуються в Інтернеті. Іншим широко

використовуваним протоколом транспортного рівня є UDP, протокол користувацьких дейтаграм.

UDP - це транспортний протокол "найкращих зусиль" - надсилання пакетів без забезпечення їх доставки, що робить його швидшим, але іноді призводить до втрати пакетів. Хоча TCP повільніший за UDP, він гарантує доставку всіх пакетів в порядку, а тому є більш надійним.

IPsec використовує виключно UDP замість TCP, щоб дозволити IPsec-пакетам проходити через брандмауери. Тому тунелі IPsec зазвичай швидші за тунелі SSH, але можуть втрачати пакети під час транзиту. GRE і IP-in-IP можна використовувати з TCP або UDP.

Нарешті, SSH шифрує тільки одну програму за раз, а не весь трафік, що йде на пристрій і з нього. Це відрізняє SSH від IPsec, який шифрує весь мережевий трафік, незалежно від того, від якої програми він надходить. З цієї причини SSH не використовується для налаштування VPN [20].

## 2.3 Квантова криптографія: перспективи та загрози для класичних алгоритмів

Дотепер традиційного шифрування даних було достатньо для підтримання безпечного зв'язку в більшості ситуацій, пов'язаних з кібербезпекою. Однак розвиток квантових обчислень створює екзистенційну загрозу навіть для найбезпечніших традиційних криптографічних алгоритмів.

Як і квантова криптографія, квантові обчислення - це технологія, що швидко розвивається і також використовує закони квантової механіки. Порівняно з нашими найшвидшими і найсучаснішими класичними комп'ютерами, квантові комп'ютери мають потенціал для вирішення складних завдань на порядки швидше.

Наразі найбільш поширені криптографічні алгоритми, зокрема AES Та RSA, забезпечують високий рівень криптостійкості завдяки значній

обчислювальній складності, необхідний для їх злому класичними комп’ютерами. Зокрема для алгоритмів симетричного шифрування таких як AES, повний перебір ключів потребує часу, що перевищує обчислювальні можливості найпотужніших комп’ютерів, доступних на сьогодні.

Однак, поява квантових обчислень становить потенційну загрозу для сучасної криптографії. Зокерма алгоритм Шора, який ефективно виконує факторизацію великих чисел та обчислення дискретного логарифма на квантових комп’ютерах, суттєво знижує складність криптографічних атак на алгоритм типу RSA та інші подібні схеми [21].

**Що таке Квантова криптографія**

Квантова криптографія відноситься до різних методів кібербезпеки для шифрування і передачі захищених даних, заснованих на природних і незмінних законах квантової механіки [21].

На відміну від традиційної криптографії, яка побудована на математиці, квантова криптографія побудована на законах фізики. Зокрема, квантова криптографія спирається на унікальні принципи квантової механіки, наприклад:

Частинкам притаманна невизначеність: на квантовому рівні частинки можуть одночасно існувати в більш ніж одному місці або в більш ніж одному стані одночасно. І неможливо передбачити їхній точний квантовий стан.

Фотони можуть бути виміряні випадковим чином у двійкових позиціях: Фотони, найменші частинки світла, можуть мати певні полярності або спіни, які можуть слугувати двійковими аналогами одиниць і нулів класичних обчислювальних систем.

Квантову систему не можна виміряти, не змінивши її. Відповідно до законів квантової фізики, основний акт вимірювання або навіть спостереження квантової системи завжди матиме вимірюваний вплив на цю систему.

Частинки можна клонувати частково. Хоча властивості деяких частинок можна клонувати, вважається, що 100% клон неможливий [21].

**Види квантової криптографії**

Квантовий розподіл ключів (Quantum key distribution - QKD)

Системи QKD працюють, надсилаючи окремі світлові частинки фотонів через оптоволоконний кабель. Цей потік фотонів рухається в одному напрямку, і кожен з них представляє один біт, або кубіт, даних - нуль або одиницю.

Поляризаційні фільтри на стороні відправника змінюють фізичну орієнтацію кожного окремого фотона на певну позицію. А приймач використовує два доступні розгалужувачі променя, щоб зчитувати положення кожного фотона в міру їх надходження. Відправник і одержувач порівнюють положення надісланих фотонів з розшифрованими положеннями, і той набір, який збігається, стає ключем [21].

Хоча переваги QKD були доведені як в лабораторних, так і в польових умовах, існує багато практичних проблем, що перешкоджають широкому впровадженню, насамперед, вимоги до інфраструктури.

Фотони, що надсилаються через оптоволоконні кабелі, погіршуються на відстанях від 248 до 310 миль. Однак нещодавні досягнення дозволили розширити радіус дії деяких систем контролю якості на континентах завдяки використанню захищених вузлів і фотонних ретрансляторів [25].

**Квантове підкидання монети**

Квантове підкидання монети - це тип криптографічного примітиву, який дозволяє двом сторонам, що не довіряють одна одній, домовитися про набір параметрів. Уявіть, що Людина 1 і Людина 2 розмовляють по телефону і хочуть зробити ставку на підкидання монети, але тільки Людина 1 має доступ до монети. Якщо Людина 2 ставить на орла, як вона може бути впевнена, що Людина 1 не збреше і не скаже, що монета впала на решку, навіть якщо вона впаде на орла?

Таку ставку 50:50 можна здійснити, якщо Людина 1 надішле Людині 2 серію фотонів, поляризованих на основі однієї з двох орієнтацій. Він записує спін кожного фотона як одиницю або нуль, а також фільтри, які він використовує для встановлення їхньої полярності. Потім Людина 2 може здогадатися, який фільтр використовувати, щоб зчитати поляризацію для кожного окремого фотона.

На основі цього вона може порівняти свої показання з записами Людини 1 і здогадатися, чи вибрала Людина 1 той чи інший набір полярностей. Якщо Людина 1 або Людина 2 підозрюють один одного в шахрайстві, вони можуть порівняти показники, отримані за допомогою поляризаційних фільтрів, для перевірки автентичності [21].

## 2.4 VPN, TOR, I2P: принципи роботи та ефективність забезпечення анонімності

У сучасному інформаційному суспільстві зростає усвідомлення небезпек, пов’язаних з використанням мережі Інтернет. Деякі користувачі поступово адаптуються до зростаючих кіберзагроз, вдаючись до використання спеціалізованих програмних засобів та сервісів, призначених для забезпечення приватності й анонімності в мережі. Застосування таких інструментів дозволяє суттєво підвищити рівень захисту персональних даних, запобігти небажаному відстеженню дій користувача, а також ускладнити ідентифікацію джерела трафіку.

У цьому підпункті розглядаються принципи функціонування та рівень ефективності найбільш поширених сучасних технологій анонімізації – VPN (Virtual Private Network), TOR (The Onion Router) та I2P (Invisible Internet Project). Аналіз вказаних рішень дає змогу оцінити їх переваги, обмеження та практичну доцільність у контексті забезпечення інформаційної безпеки й конфіденційності користувача в Інтернеті.

**Як працює VPN?**

VPN працює шляхом маршрутизації інтернет-з'єднання пристрою через приватний сервіс, а не через звичайного інтернет-провайдера користувача. VPN виступає посередником між користувачем і підключенням до інтернету, приховуючи його IP-адресу.

Використання VPN створює приватний, зашифрований тунель, через який пристрій користувача може отримати доступ до інтернету, приховуючи при цьому свою особисту інформацію, місцезнаходження та інші дані. Весь мережевий трафік надсилається через безпечне з'єднання через VPN. Це

означає, що будь-які дані, що передаються в інтернет, перенаправляються на VPN, а не з комп'ютера користувача [22].

Коли користувач підключається до Інтернету за допомогою VPN, його комп'ютер надсилає інформацію на веб-сайти через зашифроване з'єднання, створене VPN. Потім VPN пересилає цей запит і надсилає відповідь із запитуваного веб-сайту назад на з'єднання.

VPN маскує справжнє місцезнаходження користувача під те, на яке він встановив VPN. Це дозволяє користувачеві отримати доступ до контенту або веб-сайтів, які зазвичай обмежені для цього регіону. Наприклад, користувач у США може встановити своє місцезнаходження у Великій Британії і дивитися контент з потокових веб-сайтів, орієнтованих на британську аудиторію. Громадянин США також може продовжувати дивитися свої улюблені шоу, навіть перебуваючи за межами країни у відпустці [22].

**Найпоширеніші способи використання VPN.**

**Захист історії веб-бруазера**

Інтернет-провайдери та веб-браузери можуть відстежувати все, що робить користувач під час підключення до Інтернету. Вони також зберігають історію відвіданих користувачами веб-сайтів і прив'язують цю інформацію до використовуваної IP-адреси, а потім часто показують таргетовану рекламу, пов'язану з цією пошуковою інформацією, або навіть продають дані веб-перегляду користувачів. Збереження цих даних у таємниці може бути дуже важливим для людей, особливо якщо вони користуються спільним пристроєм або веб-браузером.

VPN дозволяє користувачам зберігати пошукову інформацію - наприклад, про стан здоров'я, необхідну операцію або лікування, плани подорожей або навіть пошук ідей для подарунків - приватною, а також запобігає показу пов'язаної з нею реклами їхнім провайдером і веб-браузером [22].

**Захист -адреси та даних про місцезнаходження**

IP-адреса - це інтернет-еквівалент зворотної адреси на листі, написаному від руки. Тому будь-хто, хто знає IP-адресу користувача, може отримати доступ

до інформації, яку він шукав в Інтернеті, і де він був, коли її шукав. Крім того, історію пошуку користувача можна переглянути, якщо він підключиться до веб-браузера на громадському або робочому комп'ютері.

VPN використовують IP-адреси, які не належать користувачеві, що дозволяє йому анонімно підключатися і переглядати веб-сторінки, зберігаючи при цьому свою конфіденційність в Інтернеті. Використання VPN також дозволяє користувачам запобігти збору, перегляду та продажу даних їхньої історії пошуку [22].

**Захист девайсів**

VPN також має вирішальне значення для захисту пристроїв користувачів, таких як комп'ютери, ноутбуки, смартфони та планшети, від перехоплення кіберзлочинцями. Зловмисники часто націлені на пристрої, які підключаються до інтернету через певні мережі, наприклад, публічну мережу Wi-Fi. VPN допомагає користувачеві приховати місцезнаходження свого пристрою та захистити дані на ньому від потенційних хакерів.

В цілому VPN має досить високу ефективність, хоча як вже ми дізналися з першого розділу, є ризик натрапити на поганий VPN і втратити дані [22].

**Що таке TOR і як він працює?**

TOR - це абревіатура від "The Onion Routing project", оригінальна назва програмного забезпечення. TOR базується на "цибулевій маршрутизації", розробленій у 1990-х роках 2 американськими дослідниками для анонімізації комунікацій американської розвідки. Проект став публічним у 2000-х роках.

TOR представлений як безкоштовний веб-браузер з відкритим вихідним кодом, який можна завантажити на їхньому офіційному сайті. На відміну від інших веб-браузерів, таких як Chrome, Firefox, Brave або Safari, TOR реалізує додатковий модуль, який дозволяє йому використовувати принцип маршрутизації цибулини, щоб зробити наші комунікації анонімними [23].

Припустимо, я хочу відвідати сайт анонімно через TOR. Я запускаю браузер TOR і вводжу URL сайту на який хочу зайти. Під час запуску браузер

TOR створює канал, який використовується для пересилання всіх пакетів для цього сеансу перегляду. Давайте подивимося, як створюється ця схема.

Спочатку TOR-браузер з'єднується зі сторожем входу. Він використовує публічний список IP-адрес усіх вузлів TOR, щоб знайти його. Потім він просить його "розширити ланцюг" до середнього реле. Це означає, що середній ретранслятор бачить лише адресу входу, але не нашу адресу.

Ще раз наш браузер TOR просить (через частково встановлений ланцюг) середній вузол продовжити ланцюг до вихідного вузла. На цьому ланцюг завершується. Кожен вузол може бачити лише адресу свого попередника і наступника, не знаючи більше нічого.

Вхідний вузол бачить адресу хоста, але не знає адреси пункту призначення. Вихідний вузол може бачити адресу місця призначення, але не може бачити адресу хоста. Таким чином, забезпечується конфіденційність.

Все це можна зробити завдяки можливостям криптографії. Зокрема, того, що ми називаємо гібридною криптографією. Не вдаючись в деталі, основна ідея полягає в тому, щоб створити секретний ключ для кожного вузла і безпечно розподілити його між ними, використовуючи їхній довгий ключ. Чому не використовувати безпосередньо їхній довгий ключ?

В основному з міркувань продуктивності. Коли ланцюг завершено, ми ділимося унікальним секретним ключем з кожним вузлом ланцюга, і кожен вузол знає тільки свого попередника і свого наступника. Потім ми можемо послідовно шифрувати наші пакети всіма секретними ключами, які ми обговорили на етапі налаштування ланцюга. Звідси і походить назва "цибулинна" маршрутизація. Послідовність всіх цих шарів шифрування виглядає як цибулина.

TOR є високоефективним засобом анонімізації, але є мінус в його швидкості роботи, на відміну від тогож VPN. Але рівень анонімізації значно вищий [23].

**Що таке I2P і принципи його роботи**

I2P - це проект з побудови, розгортання та підтримки мережі, що підтримує безпечну та анонімну комунікацію. Люди, які використовують I2P, контролюють компроміси між анонімністю, надійністю, використанням пропускної здатності та затримкою. У мережі немає центральної точки, на яку можна було б чинити тиск, щоб поставити під загрозу цілісність, безпеку або анонімність системи.

Мережа підтримує динамічну реконфігурацію у відповідь на різні атаки, і була розроблена таким чином, щоб використовувати додаткові ресурси, коли вони стають доступними. Звичайно, всі аспекти мережі є відкритими та вільно доступними [24].

На відміну від багатьох інших анонімізуючих мереж, I2P не намагається забезпечити анонімність, приховуючи відправника повідомлення, а не одержувача, або навпаки. I2P розроблена для того, щоб дозволити користувачам, які використовують I2P, спілкуватися один з одним анонімно - як відправник, так і одержувач не можуть бути ідентифіковані один для одного, а також для третіх осіб.

Наприклад, сьогодні існують як веб-сайти в I2P (що дозволяють анонімну публікацію/хостинг), так і HTTP-проксі до звичайного Інтернету (що дозволяють анонімний перегляд веб-сторінок). Можливість запускати сервери всередині I2P є дуже важливою, оскільки цілком ймовірно, що будь-які вихідні проксі-сервери до звичайного Інтернету будуть відстежуватися, відключатися або перехоплюватися для спроб більш зловмисних атак [24].

I2P працює як повністю децентралізована мережа, яка шифрує і перенаправляє трафік через кілька вузлів, керованих волонтерами. Це забезпечує анонімність в Інтернеті та стійкість до цензури, що робить його безпечним способом доступу до прихованих сервісів і децентралізованих додатків [25].

I2P функціонує як оверлейна мережа, тобто працює поверх існуючого інтернету, але незалежно від традиційних механізмів маршрутизації. Його

архітектура базується на розподіленій мережі однорангових пристроїв, відомих як маршрутизатори, які допомагають передавати зашифровані повідомлення між користувачами.

Вона оптимізована для внутрішніх комунікацій, дозволяючи користувачам розміщувати приховані сервіси, відомі як "eepsites". Це робить його ідеальним для безпечного обміну файлами, децентралізованого обміну повідомленнями та додатків, орієнтованих на конфіденційність [25].

I2P є ефективним методом анонімізації у внутрішній мережі, проте має обмеження щодо швидкісті та інтеграції з загальнодоступними ресурсами Інтернету.

## 2.5 Методи деанонімізації користувачів та способи їх нейтралізації

Перед тим як розповідати про методи деанонімізації, пропоную спочатку зрозуміти, що із себе вона представляє.

**Що таке деанонімізація?**

Деанонімізація - це метод, що використовується в дата-майнингу, який намагається повторно ідентифікувати зашифровану або приховану інформацію. Деанонімізація, яку також називають повторною ідентифікацією даних, полягає у зіставленні анонімізованої інформації з іншими доступними даними з метою ідентифікації особи, групи або транзакції [26].

**Методи деанонімізації**

Моніторинг мережевого трафіку. Передбачає постійний контроль з боку зловмисника за всіма діями, які користувач виконує в мережі. Завдяки цьому можна ідентифікувати його пристрій і розкрити IP-адресу. Це не буде проблемою і не викличе ніяких труднощів, якщо користувач не використовує в своїй роботі VPN або мобільні проксі-сервери, браузери, які можуть забезпечити достатній рівень анонімності [27].

Кореляція даних. У цьому випадку передбачається, що кіберзлочинці будуть комбінувати інформацію, отриману з різних джерел, для того, щоб з'ясувати потрібну їм інформацію, зокрема, особистість людини. У цьому випадку аналізуються соціальні активності в тих же соціальних мережах, форумах, письмові коментарі, а також інші джерела, що містять публічні дані користувачів.

Перевірка метаданих. Це параметри, які містять детальну інформацію про кожне повідомлення або файл, що надсилається через Інтернет. Тут буде присутня така інформація, як дата і час відправлення, геолокація і ряд інших параметрів. Отримана інформація також допоможе зловмисникам встановити справжю особу користувача.

Атаки на анонімайзери. Здебільшого подібним впливам піддаються браузери, які забезпечують анонімність роботи користувачів в Інтернеті, наприклад, браузер TOR.

Використання шкідливого ПЗ. Якщо таке програмне забезпечення потрапляє на пристрій користувача, зловмисник може легко отримати доступ до комп'ютера, а разом з ним і до всієї інформації, що зберігається на ньому.

Хакерські атаки на сесії та файли cookie. Це те, за допомогою чого система відстежує дії користувача. Правда, спочатку це було необхідно для того, щоб надавати максимально коректні та швидкі відповіді на запити користувачів. Але сьогодні цією можливістю часто користуються недобросовісні особи [27].

**Як відбувається деанонімізація користувачів?**

Отримати дані про інтернет-користувачів можна різними способами. У цьому можуть брати участь всілякі стрімінгові сервіси, маркетингові агентства, бренди, провайдери, постачальники і продавці програмного забезпечення, смартфонів, більшовиків та інших цифрових пристроїв.

Ми перерахували лише ті категорії, яким відома особиста інформація про користувачів, хоча вони безпосередньо не використовують її для завдання шкоди своїм клієнтам і не планують продавати цю інформацію третім особам.

Таким чином вони просто збирають портрет своєї цільової аудиторії, щоб персоналізувати рекламу, а разом з нею і товари та послуги, що надаються [27].

Але більшість користувачів Інтернету, самі того не усвідомлюючи, розкривають досить багато інформації про себе, в тому числі й тієї, яка не повинна бути публічною. Це означає, що зловмиснику не потрібно витрачати багато часу і зусиль, щоб отримати потрібну йому інформацію про користувача. Більше того, сьогодні існує ефективно працююча технологія збору даних про окремих користувачів або компанії з відкритих джерел.

Вона отримала назву OSINT - це абревіатура від open source intelligence (розвідка з відкритим кодом). Вона була створена понад 80 років тому американськими спецслужбами і за цей час не втратила своєї актуальності. Сьогодні її використовують детективи, журналісти, які проводять власні розслідування, та соціальні інженери. Хакери також взяли його на озброєння для збору даних користувачів [27].

**Як запобігти деанонімізації?**

Напевно, було б несправедливо стверджувати, що кіберзлочинці завжди на крок попереду експертів з безпеки, але вони постійно вигадують нові та креативні способи використання вразливостей у системах, якими ми користуємося щодня. Іншими словами, інструменти анонімізації, які працюють сьогодні, можуть виявитися неефективними завтра, саме тому дуже важливо докладати свідомих зусиль для захисту своєї приватності [28].

Відмова від Chrome або Edge на користь більш безпечного та приватного браузера була б хорошим початком, а використання хорошого захисту від шкідливого програмного забезпечення є обов'язковим. Але жодне програмне забезпечення не захистить вас, якщо ви не візьмете за звичку проявляти обережність і звертати увагу на те, скільки інформації про себе ви розкриваєте в Інтернеті.

Ніхто не має часу читати сторінки й сторінки політики конфіденційності перед тим, як завантажити програму на свій смартфон або комп'ютер, але не завадить провести невелике дослідження перед використанням програми, і

важливо уникати продуктів, які, як відомо, збирають набагато більше даних, ніж слід [28].

## Висновок до розділу 2

У ході дослідження принципів роботи симетричних криптографічних алгоритмів, зокрема AES, встановлено їхню високу швидкодію та ефективність при обробці великих обсягів даних. Підтверджено, що стійкість таких систем значною мірою залежить від секретності ключа, що вимагає впровадження безпечних методів його передачі та зберігання.

Проведений аналіз асиметричної криптографії на прикладі RSA засвідчив її значущість у реалізації цифрових підписів, захищених протоколів (наприклад, SSL/TLS) та процесів автентифікації. Водночас підкреслено, що асиметричне шифрування є обчислювально більш ресурсоємним, тому доцільним є його поєднання із симетричними методами у гібридних схемах.

# Розділ 3 РЕКОМЕНДАЦІЇ ЩОДО ІМПЛЕМЕНТАЦІЇ ТЕХНОЛОГІЙ ШИФРУВАННЯ ТА АНОНІМІЗАЦІЇ ДЛЯ ЗАХИСТУ КОРИСТУВАЧІВ В ІНТЕРНЕТІ

## 3.1 Розробка або тестування алгоритму для забезпечення безпеки комунікацій

Для реалізації цього пункту, було вирішено протестувати як алгоритм AES впорається проти метода грубої сили (Brute Force). Як ми знаємо, AES використовує 128, 192 та 256 бітні ключі. Також досить відомим є факт того, що AES стійка до грубої сили. Наведу приклад із 128 бітною версією ключа.

AES-128 шифрує відкриті дані, використовуючи ключ довжиною 128 біт. AES-128 шифрує дані за допомогою 10 раундів перетворення і найкраще підходить для захисту секретної урядової інформації, рекомендованої Агентством національної безпеки [29].

Розмір блоку даних, зашифрованих за допомогою AES, завжди становить 128 біт. 128 біт є найменш захищеним серед інших варіантів алгоритму AES. Оскільки інші варіанти, такі як 192-бітний і 256-бітний, використовують більше раундів для перетворення, AES-128 є порівняно менш безпечним.

Зважаючи на те, що AES стійкий до грубої сили, було вирішено перевірити на практиці. Змоделювавши просту brute force атаку на зашифроване повідомлення, зашифрованим AES-128. Оскільки повноцінний перебір всіх варіантів ключів AES-128 є обчислювально неможливим навіть для сучасних компьютерів.

Тому для моделювання було вирішено використовувати 15 байтів ключа, а перебір здійснювався по останньому байту. Таким чином модель дозволяє побачити як працює brute force, хоч і не відображає реальної складності зламу повноцінного AES-128. Код було реалізовано на мові програмування pyton з використанням бібліотеки pycryptodome:

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad, unpad import os
def simulate_aes_bruteforce(): # Генеруємо випадковий 15-байтовий ключ (без останнього байта) partial_key = os.urandom(15)
# Генеруємо останній байт ключа (який будемо підбирати)
last_byte = os.urandom(1)
full_key = partial_key + last_byte
print(f"Повний ключ (який ми намагаємось знайти): {full_key.hex()}")
# Створюємо тестове повідомлення для шифрування
message = b"Hello, AES world!"
cipher = AES.new(full_key, AES.MODE_ECB)
ciphertext = cipher.encrypt(pad(message, AES.block_size))

print("\nПочинаємо перебір останнього байта ключа...")

# Brute force по останньому байту (0-255)
for guess in range(256):
    guessed_key = partial_key + bytes([guess])

    try:
        cipher = AES.new(guessed_key, AES.MODE_ECB)
        decrypted = unpad(cipher.decrypt(ciphertext), AES.block_size)

        # Перевіряємо, чи розшифроване повідомлення має сенс
        if decrypted == message:
            print(f"\nЗнайдено правильний ключ: {guessed_key.hex()}")
            print(f"Потрібно було перевірити {guess + 1} варіантів.")
            return

    except ValueError:
        # Неправильне доповнення - продовжуємо перебір
```

```
        continue

print("\nКлюч не знайдено. Щось пішло не так.")
 if name == "main": simulate_aes_bruteforce()
```

Експеримент показав, що для підбору одного байта в середньому потрібно 128 спроб. Також виявили, що час виконання на сучасному обладнанні становить меньше 1 секунди, що підтверджує експоненційне зростання складності при збільшенні довжини ключа.

## 3.2 Аналіз ефективності розробленого рішення та його порівняння з альтернативними підходами

Розроблене рішення, що моделює brut force атаку на останній байт ключа алгоритму AES-128, дозволяє провести експериментальну оцінку базових механізмів атаки перебором. Хоча така модель значно спрощує реальні умови криптоаналізу, вона є ефективною для демонстрації принципів шифрування, декодування та зростання складності атаки зі збільшенням довжини ключа.

**Ефективність моделі**

В ході експерименту було змодельовано ситуацію, коли з 16 байтового ключа AES-128 відомо 15 байтів, а підбір здійснюється лише в останньому байту. Цей підхід дозволив штучно зменшити простір ключів з 2^128 до 2^8 = 256 можливих комбінацій, що дає змогу протестувати атаку в межах декількох секунд на звичайному комп’ютері.

**Переваги моделі:**

Низькі обчислювальні вимоги - тестування не потребує спеціалізованого обладнання.

Гарна наочність - добре показує принцип роботи brute force, а також залежність успішної атаки від довжини ключа.

Можливість розширення - модель легко адаптується до атаки по 2 або більше байтах, що дозволяє експериментувати з маштабом складності

**Недоліки моделі:**

Низька реалістичність - повноцінна атака brute force AES-128 залишається обчислювально неможливою. Тобто для цього потрібно кілька мільярдів років.

Відсутність сторонніх атак - не враховані потенційні атаки з використанням часу виконання, витоку через побічні канали тощо.

**Порівняння з альтернативними підходами**

Для об’єктивного аналізу ефективності розробленох моделі, доцільно порівняти її з іншими методами криптоаналізу, що треоритично або практично можуть бути застосовані до AES. Для зручності зробимо таблицю.

Таблиця 3.1

| Підхід | Суть | Перевеги | Недоліки |
|---|---|---|---|
| **Brute force (частковий)** | Перебір 1 байта ключа | Швидко виконується, наочно демонструє принцип роботи | Не відображає повної криптостійкості AES-128 |
| **Повноцінний Brute force AES-128** | Перебір усіх 2^128 варіантів ключа | Абсолютна точність криптоаналізу | Нереалістичний навіть для суперкомп’ютерів |
| **Dictionary Attack** | Підбір ключа з наперед заданого списку | Швидкийй при слабких паролях | Малоефективний проти випадкових бітових ключів |
| **Side – Channel Attack** | Використання побічних ефектів (час, енергія) | Успішна при доступі до обладнання | Високий рівень складності реалізації |
| **Алгоритм Гровера (квантовий)** | Квантова атака, що зменшує складність до 2^64 | Потенційна загроза в майбутньому | Нереалізована через відсутність квантових комп’ютерів |

## 3.3 Рекомендації щодо оптимального вибору технологій для різних сценаріїв використання технологій шифрування та анонімізації для захисту користувачів в інтернеті

Захист користувачів в інтернеті потребує правильного підходу до вибору відповідних технологій залежних від контексту використання. Різні сценарії - передача конфіденційних даних або інформації, захист конфіденційності листування в месенджерах мають свої вимоги шифрування, рівня анонімності та доступності рішення. Нижче наведено класифікацію поширених випадків та рекомендації щодо вибору технологій.

**Захист листування**

Для захисту своїх повідомлень можна використовувати месенджери з наскрізним шифруванням(E2EE). E2EE - це безпечний комунікаційний процес, який шифрує дані перед передачею на іншу кінцеву точку. Дані залишаються зашифрованими під час передачі і розшифровуються на пристрої одержувача [30]. Додатки для обміну повідомленнями, SMS та інші комунікаційні сервіси покладаються на E2EE для захисту повідомлень від несанкціонованого доступу.

Наскрізне шифрування вважається найбільш конфіденційним і безпечним методом передачі даних через мережу.

Як і інші методи шифрування, E2EE перетворює читабельний відкритий текст на нечитабельний зашифрований текст за допомогою криптографії. Цей процес допомагає замаскувати конфіденційну інформацію від несанкціонованих користувачів і гарантує, що доступ до конфіденційних даних отримають лише ті, кому вони призначені - з правильним ключем розшифрування.

Однак E2EE відрізняється від інших методів шифрування тим, що забезпечує безпеку даних від початку до кінця. Він шифрує дані на пристрої

відправника, зберігає їх у зашифрованому вигляді під час передачі і розшифровує лише тоді, коли вони досягають кінцевої точки одержувача.

Цей процес гарантує, що постачальники послуг, які сприяють комунікації, такі як Signal та WhatsApp, не зможуть отримати доступ до повідомлень. Лише відправник та отримувач можуть їх прочитати.

Не рекомендовано використовувати такий месенджер як Telegram, через те, що він не використовує E2EE за замовченням [30].

**Безпечна передача даних в Інтернеті**

Безпечна передача даних передбачає використання методів шифрування та автентифікації для захисту процесу передачі даних з одного місця в інше. Вона спрямована на збереження конфіденційності та безпеки даних, водночас захищаючи фінансову та особисту інформацію клієнтів.

Завдяки використанню безпечних протоколів передачі даних, таких як SSL-сертифікати, організації можуть уникнути зловмисних атак або несанкціонованого доступу. Ви також можете активувати платний SSL-сертифікат на своєму веб-сайті за допомогою cPanel [31].

**Які методи слід використовувати для захисту даних?**

Використовуйте VPN, тобто віртуальні приватні мережі, захищають весь трафік веб-сайтів від перехоплення конфіденційної інформації. Коли ви підключаєте свій пристрій до публічної мережі Wi-Fi, передача даних, якими ви обмінюєтеся, стає легкодоступною для зловмисників. Тому рекомендується використовувати VPN, щоб запобігти крадіжці конфіденційних файлів. Це також заборонить зловмисникам отримати доступ до ваших даних.

Налаштуйте MFA на своїх пристроях перед авторизацією доступу. Тільки авторизовані користувачі, чиї особи підтверджені, повинні мати доступ до файлів. Ви можете налаштувати MFA на своїх пристроях як за допомогою тексту, так і за допомогою біометричних даних, таких як розпізнавання обличчя або відбиток пальця.

Використання захищеного хмарного сховища для зберігання файлів - чудовий спосіб забезпечити надійну та безпечну передачу даних. Завдяки легкому доступу до них буде набагато простіше ділитися файлами з колегами або клієнтами, незалежно від того, який пристрій чи платформу вони використовують.

Зберігання файлів у хмарних сховищах також може забезпечити резервне копіювання, що дозволить легко відновити їх у разі катастроф, стихійних лих, відключень електроенергії та інших кризових ситуацій.

**Обхід геоблокування**

Інколи буває так, що потрібно зайти на конкретний сайт, але через геоблокування він просто не відкривається, а також висвічується повідомлення, що “Цей контент недоступний у вашій крїні”. Для обходу геоблокування, краще за все, використовувати VPN, він допоможе обійти блокування від сайту [32].

Також геоблокування можна обійти і без використання VPN. Використовуючи Smart DNS. Smart DNS - цей метод працює, перенаправляючи лише DNS-запити - в основному, запити, які ваш пристрій надсилає для пошуку веб-сайтів - через сервер в іншій країні.

Я використовував Smart DNS у ситуаціях, коли не хотів жертвувати швидкістю, оскільки він не шифрує все ваше з'єднання, як VPN. Якщо для вас важлива швидка робота в Інтернеті, це може бути хорошим варіантом, хоча він не буде працювати для всіх типів географічних обмежень.

Проксі-сервери діють як посередники, надсилаючи ваші запити через сервер, розташований в іншій країні. Хоча їх легко використовувати для базових завдань, вони можуть бути повільнішими і менш безпечними, ніж інші варіанти, особливо безкоштовні. Якщо ви просто хочете розблокувати простий контент, проксі-сервер може чудово спрацювати, але для чогось чутливого краще шукати більш безпечні альтернативи [32].

**Повна анонімність в Інтернеті**

Для зберігання повної анонімності в Інтернеті потрібно робити чимало дій. Використання VPN  це крок у правильному напрямку для зберігання анонімності. Проте цього буде замало, тож нижче вказано можливі способи для повної анонімності своїх пристроїв в Інтернеті [33].

Замість того, щоб використовувати звичайні месенджери, краще користуватися тими, що шифрують повідомлення перед відправкою. Такі месенджери як Signal наскрізно шифрують повідомлення, щоб сама компанія не могла бачити ваші повідомлення.

Google як всім відомо збирає дані. Замість того, щоб використовувати Chrome краще використовувати TOR браузер, він шифрує вашу Ip - адресу та веб активність. Хоча він не в змозі шифрувати інші веб програми, тому в парі з ним доцільно використовувати VPN.

Використовуйте безпечні електронні сервіси. Оскільки ми знаємо, що Google збирає інформацію, вони також зберігають всі наші приватні повідомлення Gmail, на своїх серверах. Однак існують і безпечні варіанти, такі як ProtonMail. ProtonMail базується у Швейцарії, яка не є членом альянсу "Five Eyes", тому компанія не може бути змушена передавати дані про клієнтів уряду. Навпаки вся електронна пошта має наскрізне шифрування з відкритим вихідним кодом, а сервіс є безкоштовним для користувачів Android, iOS та Інтернету.

Повертаючись до Google, всі ми зберігаємо якісь документи, фото тощо, на Google Диску, що не є гарним вибором для конфіденційності. Існують деякі провайдери які використовують наскрізне шифрування для зберігання даних наприклад Sync, Tresorit і ProtonDrive [33].

Перевіряйте дозволи програм, зазвичай ми навіть не читаємо які саме дозволи запитують програми які ми встановлюємо. Наприклад передивитись котрі програми запитують дозвіл на геолокацію, і чи потрібна вона йому або ви можете вимкнути? Зазвичай більшість додатків запитують якомога більше дозволів, тож від вас залежить як саме їх контролювати.

Використовуйте блокувальники реклами. Рекламне ПЗ - це програмне забезпечення, яке розміщує рекламу на вашому комп'ютері, телефоні або планшеті, але навіть якщо у вас немає рекламного ПЗ, більшість веб-сайтів і додатків містять рекламу в тій чи іншій формі, яка може дратувати. Окрім видалення рекламного ПЗ, ви можете скористатися блокувальником реклами, наприклад, AdBlock або Adblock Plus.

Перевіряйте сайти на наявність HTTPS. Відвідуйте лише ті посилання які починаються з HTTPS а не з  HTTP. HTTPS означає “захищений протокол передачі гіпер тексту” використовує SSL для шифрування всього обміну даними між вашим браузером і веб сайтами які ви відвідуєте, HTTP цього не робить.

Вимикайте файли Cookie. Файли cookie - це дані про ваші дії в Інтернеті, які формують таргетовану рекламу. Іноді вони анонімні та агреговані, а іноді ні.

Не використовуйте Google. Нагадаю Google збирає інформацію, іноді це дуже особиста інформація. Замість того, щоб використовувати пошукову систему Google, скористайтесь пошуковоє системою DuckDuckGo. Яка не збирає інформацію для таргетованої реклами. Натомість сервіс створює на рекламу на основі того, що ви шукаєте, і всі пошукові дані анонімізуються, як і IP-адреси [33].

Використовуйте захищені операційні системи. Навіть із захищеними поштовими серверами, браузерами, пошуковими системами тощо, якщо ви використовуєте операційну систему від великої технологічної компанії, ваші дані все одно можуть бути записані.

На відміну від них, операційні системи з відкритим вихідним кодом, такі як Linux, відгороджують кожного користувача. Tails та Whonix - деякі інші безпечні варіанти ОС.

Вимкнути JavaScript. JavaScript - це мова програмування, яка дозволяє створювати анімовану графіку, інтерактивні карти та інші спеціальні функції на веб-сторінках. На жаль, хакери можуть використовувати вразливості в JavaScript для модифікації та крадіжки даних користувача, тому краще

вимкнути його, особливо якщо ви користуєтеся популярними браузерами, такими як Chrome або Firefox [33].

## Висновки до розділу 3

Практичне моделювання brute force атаки на AES-128 підтвердило його криптостійкість за умови використання достатньої довжини ключа. Разом з тим, показано доцільність використання надійних джерел випадкових чисел та оновлення ключів у критичних застосуваннях для запобігання можливим атакам при тривалому використанні одного ключа.

В результаті практичного аналізу технологій забезпечення анонімності, зокрема роботи мереж Tor, I2P та VPN, встановлено, що ефективність приховування особистих даних користувачів значною мірою залежить від архітектурних особливостей кожної технології. Мережі Tor та I2P, які базуються на концепції маршрутизації через декілька анонімних вузлів із багаторівневим шифруванням, демонструють високий рівень анонімності, проте мають обмежену швидкість та схильні до потенційних атак на кінцеві вузли.

Здійснений аналіз показав, що VPN-технології надають користувачам можливість створення захищеного каналу передачі даних, що істотно підвищує конфіденційність онлайн-активності. Однак рівень захисту значною мірою залежить від довіри до VPN-провайдера, політики зберігання логів та налаштувань безпеки. Таким чином, вибір оптимальної технології має здійснюватися з урахуванням конкретних потреб користувача та загрозової моделі.

# ВИСНОВКИ

У процесі виконання кваліфікаційної роботи здійснено комплексне дослідження актуальних загроз інформаційній безпеці користувачів у мережі Інтернет та проаналізовано сучасні технології забезпечення конфіденційності, зокрема методи криптографічного шифрування та засоби анонімізації мережевого трафіку.

На основі детального аналізу принципів функціонування криптографічних алгоритмів (AES, RSA), а також протоколів захищеного з'єднання (SSL/TLS, IPsec, SSH), підтверджено їхню ключову роль у забезпеченні конфіденційності, цілісності та автентичності даних при передачі через відкриті канали зв'язку. Особлива увага приділена симетричному шифруванню як найбільш ефективному засобу захисту великих обсягів даних, а також асиметричному шифруванню як інструменту безпечного обміну ключами та автентифікації.

Розглянуто особливості функціонування основних технологій анонімізації (VPN, Tor, I2P), їх архітектурні підходи, механізми маршрутизації, шифрування трафіку та стійкість до атак на приватність. Встановлено, що ефективність використання зазначених технологій безпосередньо залежить від специфіки сценарію застосування, рівня загроз, обраної конфігурації та довіри до проміжних сервісів.

У ході практичного моделювання brute force-атаки на алгоритм AES-128 емпірично підтверджено його високу криптостійкість, що засвідчує доцільність використання цього алгоритму у системах, які вимагають надійного симетричного шифрування при належній організації управління ключами.

Розроблено низку практичних рекомендацій щодо комбінованого використання технологій шифрування та анонімізації для забезпечення комплексного захисту інформації. Зокрема, доведено ефективність

багаторівневого шифрування у поєднанні з анонімізуючими сервісами при побудові стійких до деанонімізації цифрових комунікацій.

Таким чином, поставлена мета дослідження досягнута: доведено ефективність сучасних технологій шифрування та анонімізації як ключових засобів захисту користувачів в Інтернеті. Отримані результати мають як теоретичну цінність для подальших наукових розвідок у сфері кібербезпеки, так і практичне значення для впровадження у політики інформаційної безпеки в державному, корпоративному та приватному секторах.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. How to Prevent Phishing. Cloudflare. URL: https://www.cloudflare.com/learning/email-security/how-to-prevent-phishing/

2. What is Malware? Cisco. URL: https://www.cisco.com/site/us/en/learn/topics/security/what-is-malware.html

3. What Does Unsecured Network Mean. MysteriumVPN. URL: https://www.mysteriumvpn.com/blog/what-does-unsecured-network-mean

4. Top Phishing Prevention Techniques. CanIPhish. URL: https://caniphish.com/blog/top-phishing-prevention-techniques

5. History of Cryptography. IBM Think. URL: https://www.ibm.com/think/topics/cryptography-history

6. 11 Cryptographic Methods That Marked History. Interesting Engineering. URL: https://interestingengineering.com/innovation/11-cryptographic-methods-that-marked-history-from-the-caesar-cipher-to-enigma-code-and-beyond?group=test_a

7. Caesar Cipher. Splunk. URL: https://www.splunk.com/en_us/blog/learn/caesar-cipher.html

8. Vigenère cipher. Britannica. URL: https://www.britannica.com/topic/Vigenere-cipher

9. Enigma Machine. Brilliant. URL: https://brilliant.org/wiki/enigma-machine/

10. Asymmetric Cryptography. TechTarget. URL: https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography

11. Symmetric Encryption. ScienceDirect. URL: https://www.sciencedirect.com/topics/computer-science/symmetric-encryption

12. What is Symmetric Encryption. LinkedIn (Priya Jangid). URL: https://www.linkedin.com/pulse/what-symmetric-encryption-principles-priya-jangid-

13. Symmetric vs Asymmetric Encryption. Device Authority. URL: https://deviceauthority.com/symmetric-encryption-vs-asymmetric-encryption/

14. Asymmetric Encryption. Okta. URL: https://www.okta.com/identity-101/asymmetric-encryption/

15. What is Asymmetric Encryption? GeeksforGeeks. URL: https://www.geeksforgeeks.org/what-is-asymmetric-encryption/

16. What is SSL? Cloudflare. URL: https://www.cloudflare.com/learning/ssl/what-is-ssl/

17. What is TLS? Cloudflare. URL: https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

18. TLS Overview. MDN Web Docs. URL: https://developer.mozilla.org/en-US/docs/Web/Security/Transport_Layer_Security

19. What is IPsec? Cloudflare. URL: https://www.cloudflare.com/learning/network-layer/what-is-ipsec/

20. What is SSH? Cloudflare. URL: https://www.cloudflare.com/learning/access-management/what-is-ssh/

21. Quantum Cryptography. IBM Think. URL: https://www.ibm.com/think/topics/quantum-cryptography

22. How Does VPN Work? Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/how-does-vpn-work

23. Tor: How Does it Work? Medium. URL: https://medium.com/swlh/tor-how-does-it-work-d0be02ddb539

24. How I2P Works. I2P Project. URL: https://geti2p.net/en/docs/how/intro

25. What is I2P? ExpressVPN. URL: https://www.expressvpn.com/blog/what-is-i2p/

26. Deanonymization. Investopedia. URL: https://www.investopedia.com/terms/d/deanonymization.asp

27. Deanonymization. Investopedia. URL: https://www.investopedia.com/terms/d/deanonymization.asp

28. What is De-anonymization? MakeUseOf. URL: https://www.makeuseof.com/what-is-de-anonymization/

29. Understanding AES-128 Encryption. Doverunner. URL: https://doverunner.com/blogs/understanding-aes-128-encryption-and-its-significance/

30. End-to-End Encryption. IBM Think. URL: https://www.ibm.com/think/topics/end-to-end-encryption

31. Secure Data Transfer Methods. MilesWeb. URL: https://www.milesweb.com/hosting-faqs/secure-data-transfer-methods/

32. Avoiding Geo-blocking. CyberNews. URL: https://cybernews.com/privacy/avoiding-geo-blocking-and-content-restrictions/

33. VPN and Anonymity. Security.org. URL: https://www.security.org/vpn/anonymity/