# 10.3. Цифрова безпека

Цифрова інформаційна мережа, що накрила своєю павутиною всі комп'ютери на планеті, неминуче співіснує з такими явищами, як «цифровий слід» і «цифрова тінь» - це два терміни, що використовуються для опису діяльності користувача в цифровому просторі.

* Цифровий слід (Digital Footprint). Цифровий слід є інформацією, що залишена користувачем в інтернеті в результаті онлайн-активності: відвідані сайти, використані додатки, пошукові запити, активність у соціальних мережах тощо. Цифровий слід може бути використаний для аналізу та виявлення патернів у поведінці людини у цифровому просторі.
* Цифрова тінь (Digital Shadow). Цифрова тінь найчастіше асоціюється з даними та інформацією, які можуть бути використані без свідомого втручання людини або без її явної згоди. Цифрова тінь також може включати дані, що зібрані через різні додатки, пристрої IoT (інтернету речей), давачі, сенсори та інші технології без прямої участі користувача.

В обох випадках важливо усвідомлювати, які дані залишаються та як вони можуть використовуватись. Захист цифрової тіні та сліду стає важливим аспектом забезпечення приватності та безпеки в цифровій епосі.

## Цифровий слід

Цифровий слід складається з інформації, яку користувач активно чи пасивно розміщує онлайн.

Залежно від характеру та джерела інформації, виділяються такі категорії цифрового сліду:

**Активний цифровий слід.** Це інформація, яку користувач усвідомлено та активно розміщує в Інтернеті. До такого сліду належать:

* Публічна інформація, яку користувач навмисно робить публічно доступною. Це можуть бути профілі у соціальних мережах, блоги, форуми, коментарі та інші публічні платформи, де користувач ділиться інформацією про себе.
* Активність користувача в соціальних мережах. Публікації, коментарі, фотографії та відеозаписи, лайки та репости у соціальних мережах, таких як Facebook, Instagram, Twitter та інші.
* Публікації на власних блогах, участь в обговореннях на форумах та інших онлайн-спільнотах.
* Надіслані та отримані електронні листи, включаючи вкладення.
* Активність на різних онлайн-платформах, таких як YouTube, Twitch, LinkedIn, GitHub та інші.

**Пасивний цифровий слід.** Це інформація, яка збирається та зберігається сторонніми сервісами чи організаціями без активної участі користувача. До такого сліду належать:

* Історія відвіданих веб-сайтів, пошукові запити, куки, уподобання, рекламних оголошення та інша інформація, що збирається браузерами та пошуковими системами. Збирається інформації про поведінку користувача в мережі.
* Історія покупок, переваги та інтереси, що збирається інтернет-магазинами та рекламними платформами.
* Дані про використання мобільних додатків, розташування, обмін повідомленнями та інша інформація що збирається мобільними пристроями та додатками. Це можуть бути дані про точку доступу Wi-Fi, мережі або географічні координати GPS.
* Онлайн-транзакції. Під час здійснення онлайн-покупок або використання фінансових сервісів, таких як інтернет-банкінг, цифровий слід може включати інформацію про транзакції, рахунки, платіжні дані та інші фінансові деталі.

**Професійний цифровий слід.** Це інформація, пов'язана із професійною діяльністю користувача. До такого сліду належать:

* Профіль та активність на професійних мережах, таких як LinkedIn.
* Інформація про роботу, що подається в резюме та портфоліо: навички, досягнення та досвід роботи. Ця інформація розміщена на спеціалізованих сайтах або платформах.
* Публікації та коментарі на професійних блогах, форумах чи наукових платформах.

Цифрові сліди можуть бути використані компаніями та організаціями для різних цілей, таких як персоналізація контенту та реклами, аналіз поведінки користувача, покращення продуктів та послуг, а також для прийняття рішень про кредитоспроможність або найму на роботу.

Цифровий слід може бути постійним, і інформація, розміщена в Інтернеті, може бути доступною та впливати протягом тривалого часу. Користувачі можуть вживати заходів для керування своїми цифровими слідами, такі як налаштування конфіденційності та безпеки в онлайн-сервісах, використання інструментів контролю даних та усвідомлена поведінка в Інтернеті.

#### Види інформації у цифрових слідах

**Візуальна інформація.** Фотографії, відеоролики, картинка чи відео з камер зовнішнього спостереження, де присутній користувач. Один раз з'явившись в онлайні, ці матеріали залишаються там назавжди, навіть якщо автор їх видалить. Це початок цифрового сліду того, хто опублікував фотографію і цифрової тіні всіх присутніх там людей.

Різні веб-архіви, копії баз даних, що постійно поновлюються не дадуть цим матеріалам зникнути безслідно. Багато фото-хостингів підкреслюють як перевагу довічне зберігання фотографій, а більшість з них взагалі не видаляють завантажені клієнтами матеріали, тільки якщо ті порушують закон.

**Текстова інформація.** Використання текстової інформації, такої як електронні листи, розміщені документи, онлайн спілкування, опубліковані статті, пости і тому подібне.

Це більше відноситься до цифрового сліду людини, але за наявності вмінь завжди можна витягнути приховану інформацію про інших осіб. Сучасні користувачі, зазвичай, мають акаунти в більшості сервісів обміну повідомленнями. Абсолютно все листування з друзями, колегами, сторонніми людьми залишається на серверах протягом тривалого часу, зберігається в резервних копіях і може бути використане третіми особами.

Це стосується багатьох сервісів електронної пошти та цифрових копій документів, які передаються і в яких є відомості про користувача. Наприклад, Gmail радить не видаляти кореспонденцію, а просто архівувати. І більшість людей так і роблять.

Часто користувачі для спілкування або реєстрації створюють логіни та нікнейми, які характеризують віртуальну індивідуальність особи. Такі відомості також стають частиною цифрового сліду.

**Голосова інформація.** Технологія VoIP, звичайні аналогові мережі, мобільний зв'язок. Голосова складова цифрового світу найбільш проста для розуміння. Оператори зв'язку часто записують розмови своїх абонентів, хоча офіційно це не підтверджують, але вкладають гроші в обладнання для запису мільйонів своїх абонентів. Це зазвичай робиться для тестування алгоритмів щодо запобігання злочинної діяльності. Запис розмов є самим малопоширеним типом цифрового сліду і тіні.

VoIP-мережі страждають цим легальним шпигунством в меншій мірі, але існує ймовірність, що співрозмовник завжди має можливість записати розмову з метою використання отриманої цифрової тіні проти користувача.

**Часова інформація.** Журнал записів кожної дії кожного користувача в Інтернет - логи, які ведуться провайдерами і серверами веб-сайтів. Така докладна інформація зважаючи на величезну обсягу (десятки гігабайт в день для відвідуваного сайту) недовговічна - лог-файли автоматично очищуються раз в кілька днів. Але витягнуті з логів суттєві дані зберігаються вічно.

Навіть в ситуації, коли людина не спілкується в Інтернеті і відімкнула телефон, вона постійно знаходиться під наглядом. У великих містах в місцях масового скупчення присутнє приховане і явне відео спостереження. Прогрес дійшов до того, що зняті кадри передаються не на пульт оператора, а в Інтернет, отримати доступ до яких можна прямо з вікна браузера на домашньому комп'ютері, знаючи потрібну ІР-адресу і, за необхідності, пароль.

Камери дорожнього спостереження реєструють пересування всіх транспортних засобів з їх номерами і швидкістю. Звичайні веб-камери і охоронні системи офісів і будинків записуючи всі пересування людей, є прекрасними помічниками для тих, хто хоче обчислити маршрути і навіть розпорядок дня особи.

Подібна інформація збирається, в основному, для правоохоронних органів, але навіть цей факт не може компенсувати неприємний осад від того, що Великий Брат постійно в курсі всіх наших переміщень і справ. І вже зовсім не гарантує вашу конфіденційність.

#### Способи зменшити цифрові сліди в онлайн-середовищі:

* Керування конфіденційністю у соціальних мережах. Переглянути налаштування конфіденційності у соціальних мережах та обмежити доступ до особистої інформації. Встановити приватні налаштування для своїх профілів та контенту, щоб обмежити його видимість лише для довірених контактів.
* Розумне використання особистої інформації. Бути обережним з розкриттям особистої інформації в онлайн-середовищі. Уникати публікації повного імені, адреси, телефонного номера, фінансових даних та іншої конфіденційної інформації на публічних платформах.
* Обмеження використання публічних Wi-Fi. Уникати використання відкритих та ненадійних Wi-Fi мереж, особливо під час передачі конфіденційної інформації. За потреби підключення до публічної мережі використовувати віртуальну приватну мережу (VPN), щоб зашифрувати дані та забезпечити безпечне підключення.
* Обережність в електронній пошті та повідомленнях. Бути уважними при відкриванні електронних листів та повідомлень, особливо від незнайомих відправників. Уникати відкривання підозрілих посилань або вкладень, які можуть містити шкідливі програми або фішингові атаки.
* Керування акаунтами. Періодично переглядати власні облікові записи та видаляти неактивні чи непотрібні облікові записи. Це допоможе зменшити кількість інформації, пов'язаної з особистістю користувача, яка може бути доступна онлайн.
* Використання анонімних режимів та проксі-серверів. За потреби анонімного відвідування сайтів використовувати режими приватного перегляду або проксі-сервери, які можуть допомогти приховати особу користувача та зменшити слід в онлайн-середовищі.

Важливо відзначити, що повне видалення цифрового сліду практично неможливо, оскільки деяка інформація може зберігатися в онлайн-середовищі незалежно від дій користувача. Однак, дотримання цих практик допоможе зменшити кількість особистої інформації та слідів, які можуть бути пов'язані з користувачем в онлайн-середовищі.

## Цифрова тінь

Цифрова тінь зазвичай формується без відома людини. Наприклад, випадкове потрапляння машини користувача в кадр чужої фотокамери, але фотографію публікують в Інтернеті. Хтось починає обговорювати цю машину, з’ясовується номер і інформація про господаря з'являється на форумі. Починається обговорення, і генерується багато ключових слів, за якими можна знайти цю машину на фотографії. І тепер ця фотографія сформувала цифрову тінь для власника машини.

Ще один простий приклад - спорт. Перед грою команда фотографується, створюючи одну фотографію об'ємом кілька мегабайт. В процесі гри кожен з футболістів створює мало не гігабайти цифрової тіні, потрапляючи в об'єктиви фото, відеокамер і мобільних телефонів. Навіть виходячи зі стадіону, гравець продовжує генерувати цифрову тінь, ховаючись від папараці.

Отже, чим людина є менш помітною, тим менше його цифрова тінь, але повністю це проблему не вирішує. Навколо існує мільйони людей, що щомиті клацають фотоапаратами і записують відео. Для пересічних людей, небезпека може бути тільки від недоброзичливців і шахраїв, які легко вирахують відомості, якщо доберуться до цифрової тіні: де працює, якими маршрутами їздить, де відпочиває, які напої п'є, з ким зустрічається. Для тих, хто щось приховує, наступають нелегкі часи: сховатися буде неможливо.

Поки що цифрова тінь не структурована. Вона хаотична, і знайти людину в величезному або навіть меншому обсязі інформації важко. Для її обробки потрібні потужні комп'ютери і та програми. Але вже сьогодні можна на прикладі сучасних офісів бачити, як зменшується конфіденційність, що пов'язана з можливістю ідентифікації людини. Електронний пропуск або відбитки пальців є ключем, що допомагає знайти людину в великому обсязі цифрових даних.

Для звичайної людини такими ключами є дві речі: мобільний телефон і особистість. Віднайти людину в натовпі, базуючись на пересуванні його мобільного телефону - непросто, але стрімко розвиваються алгоритми розпізнавання особи, вдосконалюються алгоритми аналізу змісту фотографій. Фотографії можна індексувати не лише за мета-інформацією, а й за змістом.

Цю технологію вже втілюють пошуковими в своїх сервісах, що вибирає у збірці фотографій лише ті, де є певна особа або сам власник. І маючи одну фотографію людини, взяту з його сторінки в соціальній мережі, можна знайти всю його цифрову тінь, де особа потрапила в об'єктив камери. А EXIF-інформація з мета даними, що зашита в фотографію, покаже точний час або навіть місце розташування зробленого кадру.

### Конфіденційність даних та цифрова тінь

На сьогодні головним засобом для збільшення цифровий тіні людини стали мобільні телефони з вбудованими камерами, що дозволяють знімати буквально кожен крок, блоги, електронні щоденники і соціальні мережі. Сучасні Інтернет сервіси поєднують і засоби спілкування, і файловий сервер під зберігання фотографій, і навіть хостинг потокового відео.

Зараз людство поширює особисту інформацію з величезною швидкістю, використовуючи соціальні мережі і файлові хостинги. Значна кількість людей під час реєстрації вказує справжні прізвище та ім’я, домашню адресу, телефони і іншу особисту інформацію. На сьогоднішній день мільйони людей по всьому світу з задоволенням прагнуть викласти побільше своїх фотографій, відео та контактних даних, щоб їх онлайн-друзі могли подивитися та залишити коментарі. При цьому ніхто не підозрює, що навіть закрита від відвідувачів сторінка завжди доступна для адміністраторів і хакерів. І вже відомі факти масового злому і викрадення баз даних з подібних сервісів.

Цифрова тінь - явище доволі небезпечне. З поліпшенням якості фото- та відео- техніки, зростанням обсягу пам’яті та швидкості Інтернету, вона буде ставати все більш осяжною і небезпечною. Найголовніша небезпека цифровий тіні полягає в тому, що люди не в змозі її контролювати. З часом вона буде структурована, між тінню і цифровим слідом вже не залишиться різниці, і саме тоді настане кінець конфіденційності. А поки слід не здійснювати вчинків, за які доведеться виправдовуватися або відповідати за законом, адже ваша цифрова тінь вже сьогодні формує вашу «цифрову честь» та порядне ім’я.

## Збір даних у пошукових системах

Пошукові системи збирають персональну інформацію користувача в різний спосіб.

* Пошукові запити. Пошукова система записує запит і пов'язує його з унікальним ідентифікатором. Це дозволяє пошуковій системі аналізувати уподобання користувача та надавати більш релевантні результати в майбутньому.
* Історія пошуку. Пошукові системи зберігають історію пошукових запитів користувача, щоб надавати персональні рекомендації та рекламу. Це дозволяє пошуковій системі краще зрозуміти інтереси користувача.
* IP-адреса. Пошукові системи можуть реєструвати IP-адресу, яка є унікальним ідентифікатором пристрою користувача в мережі. IP-адреса може використовуватися для визначення розташування користувача та надання місцево орієнтованих результатів пошуку.
* Куки та трекінг. Пошукові системи використовують куки (невеликі текстові файли), які зберігаються на пристрої користувача, щоб відстежувати його активність та надавати персональний контент та рекламу. Куки можуть містити інформацію про пошуковий запит, переваги та історію пошуку.
* Аутентифікація облікового запису. В обліковому запису пошукової системи вказують персональну інформацію, яка може бути використана для надання більш персоналізованого досвіду пошуку.
* Веб-аналітика. Пошукові системи використовують інструменти веб-аналітики для відстеження активності користувачів на сторінках результатів пошуку. Це дозволяє їм аналізувати поведінку користувачів, покращувати свої сервіси та надавати більш релевантні результати.

Збір персональної інформації користувача пошуковими системами зазвичай здійснюється з метою поліпшення досвіду користувача, надання релевантної інформації та персоналізованої реклами. Однак, деякі користувачі можуть бути стурбовані збереженням та використанням їх даних. Тому важливо ознайомитися з політикою конфіденційності пошукової системи та вжити відповідних заходів, таких як видалення історії пошуку або використання анонімного режиму перегляду, якщо потрібно обмежити збір персональної інформації.

## Збір даних у соціальних мережах

Соціальна мережа – це структура, що створена для різного роду комунікації користувачів на базі одного ресурсу, об’єднаних за певними параметрами. Мережа утворює зв’язки між особами, групами осіб, організаціями тощо.

Основними принципами соціальної мережі є:

1. **Ідентифікація.** Вказування особистої інформації користувача.
2. **Присутність.** Можливість дізнатись список активних контактів, останнє відвідування мережі контактом.
3. **Відносини.** Можливість створити соціальний зв’язок між двома контактами.
4. **Спілкування.** Наявність засобів для пересилання повідомлень.
5. **Групи.** Формування різного роду спільнот всередині мережі, учасники яких об’єднані спільними інтересами.
6. **Обмін.** Засоби для пересилання матеріалів до інших учасників.

Сучасні соціальні мережі пропонують вказати максимум інформації про себе. Деякі відомості є приватними, але більшість інформації є у публічному доступі і доступна через API. Також є можливість глобального пошуку користувачів за кількома критеріями, такими як прізвище, рік народження, країна тощо.

Користувачі соціальних мереж є стимульованими для створення нових зв’язків. Такий тип зв’язку у більшості мереж називається «друг» і він надає доволі багато інформації до загального портрету користувача. Соціальні мережі часто надають рекомендації щодо додавання нових друзів. Зазвичай, вказуються особи, які є у відповідному колі кількох або одного з наявних друзів.

Одною з ключових особливостей соціальної мережі є велика кількість потоків інформації. Користувач може їх фільтрувати та змінювати джерела в залежності від власних потреб. Дописи, поширення, вподобання – це є важливі фактори, які надаються до аналізу профілю користувача.

Доступність інформації в соціальних мережах, а також її стрімке поширення стають причиною використання особистої інформації користувачів третіми особами. Дані, які зібрала соціальна мережа, можуть бути передані, в тому числі у правові структури. Навіть після видалення акаунту дані не зникають, оскільки з бази даних вони не видаляються. Зібрана у мережі інформація, в додатку з іншими сервісами (Instagram, Ask), може бути використана для формування психологічного портрету, в принципі це може зробити будь-який користувач, оскільки інформація є повністю публічною.

## Віртуальна приватна мережа VPN

Віртуальна приватна мережа (VPN) — це технологія, яка забезпечує безпечне та приватне з'єднання між пристроєм користувача та інтернет-сервером. VPN створює зашифрований тунель через загальнодоступну мережу, таку як Інтернет, і маршрутизує весь мережний трафік користувача через цей тунель. Це дозволяє користувачам обмінюватися даними в безпечному та захищеному середовищі, забезпечує приватність і захист від небажаного прослуховування або доступу до інформації.

VPN використовує різні протоколи шифрування, такі як SSL (Secure Sockets Layer) або IPSec (Internet Protocol Security), для захисту даних, що передаються між пристроєм користувача та сервером. Це робить інформацію недоступною для третіх осіб, таких як хакери чи інтернет-провайдери.

При використанні VPN IP-адреса пристрою користувача в мережі заміняється IP-адресою VPN-сервера. Це робить активність користувача в Інтернеті більш анонімною та запобігає відстеженню його особистої інформації чи місця розташування.

VPN дозволяє виконувати географічні обмеження, які можуть бути накладені на деякі веб-сервіси чи контент. Підключаючись до VPN-серверу в певній країні, можна отримати доступ до онлайн-ресурсів, які зазвичай доступні лише для користувачів з цієї країни.

При використанні громадських мереж Wi-Fi, таких як в аеропортах, кафе або готелях, ваша приватність і безпека можуть бути під загрозою. VPN захищає активність користувача і дані від можливих атак або перехоплює інформацію через такі мережі.

VPN дозволяє створити безпечне з’єднання з корпоративною мережею або іншими видаленими ресурсами. Це дозволяє віддаленим працівникам підключатися до внутрішніх систем і працювати поза межами офісу.

#### Переваги використання VPN

* Дивитися трансляції з будь-якої точки світу. Якщо користувач перебуває за кордоном і намагається увійти в обліковий запис для трансляцій, якою користується в своїй країні, то може виявити, що деякі шоу не працюють. Але якщо вибрати IP-адресу, що розташована на батьківщині, то все улюблені шоу будуть доступними.
* Отримувати доступ до заблокованих веб-сайтів. Деякі установи (школи, бібліотеки, офіси) обмежують доступ до певних веб-сторінок, наприклад до соціальних мереж, але зашифроване VPN-підключення пройде крізь всі бар'єри.
* Обійти цінову дискримінацію. Цінова дискримінація - це коли, за один і той же товар, різні групи споживачів платять різні кошти. Перша причина - виходячи з місця перебування користувача. У великих містах вартість життя вище, а це означає, що вище і доходи. Маркетологи це знають і програмують свої сайти так, щоб люди з цих регіонів бачили більш високі ціни (такий підхід часто зустрічається серед авіаліній). Друга причина дискримінації: провайдери та інші сервіси відстежують покупки і переваги своїх клієнтів. Дізнавшись, що клієнт регулярно купує певний товар, вони теоретично можуть продати цю інформацію виробнику товару, який підвищить для цього клієнта ціну, оскільки знає, що він точно його купить. Завдяки конфіденційності та анонімності в мережі VPN користувач буде вільний від подібного цільового впливу.
* Позбавитися від стеження. Не надавати такої можливості зловмисникам, кіберзлочинцям, корпораціям і навіть власному постачальнику послуг інтернету стежити за собою.

#### Проблеми при використанні VPN

* Можливо уповільнення роботи. При підключенні через VPN потік даних проходить більше етапів, ніж зазвичай, що може викликати помітне уповільнення роботи. Оскільки це популярна скарга щодо VPN, розробники взяли це до відома. Багато з них настільки досягли успіху в оптимізації швидкості і продуктивності, що їх користувачі VPN можуть без найменших проблем грати в ігри і дивитися трансляції.
* Труднощі, пов'язані з QoS. QoS означає «якість обслуговування» і описує продуктивність служби або мережі. Для мереж VPN поки немає будь-якого стандарту, який можна заміряти і повідомити показники. А оскільки немає показників для аналізу, потрібно покладатися на професійні огляди та відгуки користувачів, щоб дізнатися, які служби є надійними.
* Блокування VPN. Деякі компанії розуміють, що мережі VPN надають їх користувачам багато можливостей. Щоб протистояти цьому, вони починають блокувати доступ для відомих IP-адрес VPN. Проте, служби VPN натомість використовують нові IP-адреси.
* Відсутність повної конфіденційності. Хоча мережа VPN справляється з шифруванням і збереженням конфіденційності користувача, файли cookie, що знаходяться у браузері все одно можуть його впізнати. Виходом буде вимкнення збереження cookie.

### Принцип функціонування VPN

При використанні віртуальної приватної мережі ніхто не побачить реальну IP-адресу, оскільки замість неї тепер буде розпізнаватися адреса VPN-сервера (рис.3).

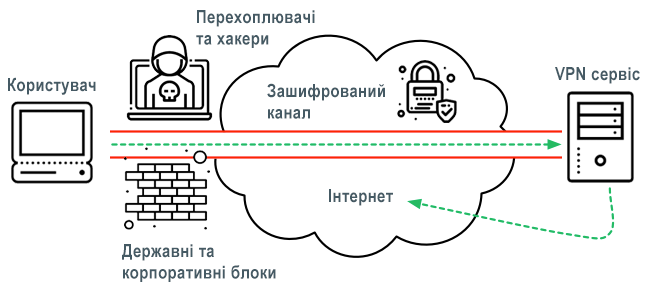


Рис. 3. Принцип функціонування мережі VPN

Саме підключення до Інтернету буде зашифровано, тому, ніхто не побачить дані, які користувач завантажуєте, вивантажує або надсилає. Шифрування - це спосіб перетворення тексту в складний набір кодів. Існує три основних види шифрування: хешування, симетричне і асиметричне шифрування. В кожного виду свої переваги і недоліки, але всі вони шифрують дані так, що в чужих руках вони будуть марними.

Додатковий рівень захисту, який є у більшості служб VPN - їх власна система DNS. DNS - система доменних імен - це телефонна книга інтернету, в якій текстові URL-адреси ототожнені з відповідними IP-адресами. Система DNS дозволяє замість довгої послідовності цифр вводити назву сайту, наприклад site.ua. Кіберзлочинці можуть спостерігати за запитами DNS, щоб відстежувати дії користувача в інтернеті, але система DNS в службах VPN розроблена так, щоб за допомогою додаткового шифрування перешкодити їм.

Слід пам'ятати, що не вся інформація шифрується. У різних VPN-провайдерів можуть відрізнятися такі характеристики як ступінь шифрування, приховування факту підключення до сервера, зберігання логів (журнал, в який зберігається інформація про відвідуваних сайтах, реальні IP адреси тощо) і співпраця при видачі інформації третім особам.

Якщо VPN-провайдер взагалі не записує логи, то передавати третім особам просто нічого. А приховування факту підключення до сервера - вже більш рідкісна послуга. При некоректному підключенні або різкому розриві з'єднання може статися витік частини даних.

### Вибір VPN-сервісу

При виборі VPN-сервісу рекомендується звернути увагу на такі фактори, як швидкість з'єднання, наявність серверів у потрібних країнах, рівень безпеки, політику зберігання логів і ціну. Кожен із перелічених сервісів має свої особливості, тому рекомендується ознайомитися з їхньою функціональністю та вибрати той, який найкраще відповідає потребам.

Вибір правильного VPN-сервісу впливає на безпеку та конфіденційність. Рекомендується вибирати надійних та перевірених провайдерів VPN, які забезпечують високий рівень шифрування, не зберігають логі активності користувача та мають хорошу репутацію.

#### Популярні VPN-сервіси

* ExpressVPN пропонує широке географічне охоплення та високу швидкість з’єднання. Забезпечує високий рівень безпеки за допомогою сильного шифрування та не зберігає логи активності користувачів.
* NordVPN відома своєю надійністю та безпекою. Велика кількість серверів у різних країнах і додаткові функції, такі як подвійне шифрування та захист від витоку DNS.
* CyberGhost пропонує простий у використанні інтерфейс і хороший рівень безпеки. Широкий набір серверів у багатьох країнах, а також функції блокування небажаної реклами та захисту від шкідливих програм.
* Surfshark є відносно новим на ринку VPN, але вже завоював популярність завдяки своїй доступній ціні та надійному захисту. Пропонує необмежену кількість пристроїв підключення до одного облікового запису.
* Private Internet Access (PIA) відомий своїми низькими цінами та сильним захистом. Має багато серверів у різних країнах і не зберігає логи користувальницької активності.

### Використання VPN

Щоб скористатися VPN, потрібно дотримуватися загальних кроків:

1. Вибрати один із рекомендованих VPN-сервісів і перейти до сайту сервісу. Там потрібно створити обліковий запис та вибрати план передплати.
2. Після підписки на VPN-сервіс, завантажити та встановити відповідну програму VPN на пристрій. Додатки VPN доступні для різних операційних систем, таких як Windows, macOS, iOS (iPhone/iPad), Android та інші.
3. Запустити програму VPN і увійти до облікового запису.
4. У програмі VPN надається список доступних серверів, розташованих у різних країнах. Вибрати сервер, до якого потрібно підключитися. Програма встановить захищене з'єднання з вибраним сервером.
5. Після успішного підключення до VPN-сервера весь трафік користувача буде проходити через захищений тунель. IP-адреса пристрою користувача буде замінена на IP-адресу VPN-сервера, і з'єднання буде зашифровано. Так можна безпечно та приватно користуватися Інтернетом.
6. У програмі VPN зазвичай доступні додаткові функції, такі як вибір протоколу шифрування, налаштування блокування реклами або захисту від шкідливих програм. Можна налаштувати ці параметри відповідно до потреб.

Процедура встановлення та використання VPN може відрізнятися залежно від вибраного VPN-сервісу та операційної системи пристрою. Рекомендується ознайомитися з інструкціями та посібниками, які надає провайдер VPN, для отримання детальної інформації про налаштування та використання VPN-з'єднання.

## Основи цифрової безпеки

Цифрова безпека - це комплекс заходів, спрямованих на захист конфіденційності, цілісності та доступності інформації від вірусних атак і несанкціонованого втручання.

* Сильні паролі. Використовувати унікальні та складні паролі для всіх онлайн-акаунтів. Паролі повинні містити комбінацію літер (у верхньому та нижньому регістрах), цифр та спеціальних символів. Уникати використання особистих інформаційних даних у паролях.
* Багатофакторна аутентифікація. Увімкнути багатофакторну аутентифікацію (МФА) для онлайн-акаунтів, де це можливо. МФА додає додатковий рівень захисту, вимагаючи не лише пароль, але й додатковий код перевірки або пристрій для входу в обліковий запис.
* Оновлення програмного забезпечення. Регулярно оновлювати операційні системи та програмне забезпечення на всіх пристроях. Оновлення часто містять виправлення вразливостей та забезпечують захист від нових загроз.
* Безпечне підключення до мережі. Уникати використання відкритих та ненадійних Wi-Fi мереж. При підключенні до відкритої мережі, використовувати віртуальну приватну мережу (VPN), щоб зашифрувати дані та забезпечити конфіденційність.
* Обережність в інтернеті. Бути обережними при відкриванні посилань в електронних листах, повідомленнях та на незнайомих веб-сайтах. Уникати завантаження та встановлення програм з ненадійних джерел.
* Антивірусне програмне забезпечення. Встановити надійне антивірусне програмне забезпечення на пристрої та регулярно його оновлювати. Антивірус допомагає виявляти та блокувати шкідливі програми.
* Захист конфіденційної інформації: Бути обережним з розкриттям особистої та фінансової інформації в онлайн-середовищі. Уникати надсилання конфіденційних даних через незахищені канали зв'язку.
* Освіта та поінформованість. Постійно дізнаватися про нові загрози та методи захисту. Бути уважним до цифрової безпеки та навчати колег про базові принципи цифрової безпеки.

Крім цих основних принципів, існує багато інших заходів та практик, які можуть бути застосовані для захисту цифрової інформації користувачів. Важливо постійно стежити за новими загрозами та бути пильним в онлайн-середовищі.

## Контрольні запитання

1. Які типи інформації лишають цифровий слід? Перелічити дії користувача, які залишають цифровий слід.
2. Як формується і чим небезпечна є цифрова тінь? Які негативні наслідки вона може причинити?
3. Перелічити способи, які використовує Facebook для збору інформації про користувача.
4. Як формується тіньовий профіль користувача в Facebook?
5. Яким чином можна захистити конфіденційність приватних даних?
6. Перелічити заходи, що надають безпеку в соціальних мережах?
7. Перелічити комплекс заходів що потрібні для загальної безпеки в Інтернеті.
8. Які заходи безпеки можна вжити для мобільних пристроїв.
9. Порівняти операційні системи iPhone та Android щодо захисту приватної інформації користувача.
10. Назвати причини, з яких варто використовувати мережу Tor.

## Літературні джерела

1. Основи цифрової безпеки <https://vps.ua/blog/digital-security-guide/>
2. Інформаційна безпека в Інтернеті - <https://lastday.club/informatsionnaya-bezopasnost-v-seti-zametaem-tsifrovoj-sled/>
3. Цифрова тінь та цифровий слід - <https://narasputye.ru/archives/3810>
4. Цифрова безпека: терміни та технології - <https://te-st.ru/2018/05/25/digital-security-terms/>
5. Що знає Facebook <https://webznam.ru/blog/znaet_o_vas_socialnaja_set_facebook/2016-09-15-344>
6. Що Google дійсно знає про вас? - [https://ru.vpnmentor.com/blog /год-что-google-действительно-знает-о-вас/](https://ru.vpnmentor.com/blog%20/год-что-google-действительно-знает-о-вас/)
7. Як захистити акаунти в соцмережах? <https://tass.ru/obschestvo/10223771>