# 8.4. Цифрова безпека

Цифрова інформаційна мережа, що обплутала своєю павутиною всі комп'ютери на планеті, неминуче співіснує з такими явищами, як «цифровий слід» і «цифрова тінь». Цифрова тінь - це інформація, яку кожна сучасна людина створює про себе, сама того не підозрюючи, а цифровий слід - це гігабайти інформації, які користувачі щодня самостійно передають через Всесвітню павутину, відправляючи електронні листи з вкладенням, ділячись фільм або публікуючи пости в соціальних мережах. Більш широко, цифровий слід - це віртуальна особистість користувача.

* Пасивний цифровий слід – це дані, які залишаються ненавмисно, наприклад, ІР-адреса пристрою чи історія відвідувань в Інтернеті.
* Активний цифровий слід – це сукупність всього, що робиться усвідомлено – пости у блог, коментарі, листи тощо.

Обсяг цифрового сліду кожної людини щодня постійно збільшується. Відповідальність за зберігання та використання цієї цифрової інформації покладається на певні організації, Інтернет-сервіси, провайдери і дата-центри, де все це розміщується фізично.

## Цифровий слід

Цифровий слід, який лишає людина має кілька складових.

**Візуальна інформація.** Фотографії, відеоролики, сигнал цифрового телебачення і камер зовнішнього спостереження.

Зростання обсягів інформації в гігабайтах вихідних даних, в першу чергу доводиться на візуальні документи. Графічне представлення інформації відіграє головну роль в створенні цифрового світу.

Публікація фотографій та відео, 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 сервері 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.** Записи кожної дії кожного користувача (логи) в Інтернет, 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.

## 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 тіні 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, 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 буквально знімати 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 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.

### Збір даних у Facebook

Соціальна мережа Facebook на 225 сторінках [звіту](https://www.commerce.senate.gov/public/_cache/files/ed0185fb-615a-4fd5-818b-5ce050825a9b/62027BC70720678CBC934C93214B0871.senate-judiciary-combined-7-.pdf) розкрила перелік даних і способи, за допомогою яких збирає інформацію про користувачів.

* Час, частота і тривалість дій у вікні соцмережі (в тому числі, відкрито воно чи знаходиться у фоновому режимі).
* Встановлені в браузері користувача плагіни.
* Пересування мишки на пристрої користувача.
* Використання камери, вбудованої в додаток Facebook.
* Метадані фотографій (в тому числі, час і місце зйомки).
* Встановлені на пристрої користувача додатки.
* Назви і типи файлів на пристрої користувача.
* Ідентифікатори з ігор, додатків та інших облікових записів.
* Доступне місце на диску пристрою користувача.
* Контакти з адресної книги користувача.
* У випадку з Android-пристроями - журнал дзвінків і історію SMS.
* Найближчі до користувача точки доступу Wi-Fi і мобільного зв'язку.
* Інформація мобільних і стаціонарних провайдерів через комп'ютери, телефони, зв'язані телевізори та інші пристрої в мережі.
* Рівень заряду пристрою користувача.
* Параметри та дозволи на пристрої користувача.
* Інформація та фотографії інших користувачів, а також частота взаємодії і спілкування з ними.
* Покупки на сторонніх сайтах.

У компанії додали, що можуть отримувати інформацію про користувачів за допомогою третіх осіб, але яких саме - не уточнюється.

## Безпека в соціальних мережах

Щоб уникнути небажаних наслідків і проблем в соціальних мережах, потрібно ретельно виконати ряд нескладних заходів

**Паролі**

Акаунти нерідко зламуються і крадуться, і при таких діях зловмисників від імені користувача до їх друзів можуть надходити повідомлення з проханням перевести гроші. Щоб уникнути цього і захистити свою сторінку, слід використовувати складні паролі, причому різні для всіх соціальних мереж.

Пароль має складатися мінімально з восьми символів, і система може запропонувати автоматично його згенерувати. Можна придумати пароль самостійно, але не використовувати власне ім'я, номер телефону, дату народження, кличку домашньої тварини.

**Налаштування**

При правильному налаштуванні можна захистити і сторінку і особу. Особливо важливою є приватність, яка дозволяє обмежувати доступ до акаунту і робити його закритим для незнайомців. Переглядати інформацію зможуть лише друзі, а деякі окремі відомості (наприклад, фото) можна за бажанням приховати повністю.

Є кілька можливих варіантів налаштувань (в залежності від конкретної соцмережі), що забезпечують безпечне використання облікового запису:

* Вхід за одноразовим кодом. Кожен раз на прив'язаний до сторінці номер буде приходити код для здійснення входу.
* Конфіденційність: ступінь доступу до сторінці. Визначення, хто зможе переглядати ті чи інші дані (фото, перелік спільнот, подарунки, місце розташування зроблених фотографій, список друзів). Можна закрити доступ для незнайомців, для всіх або лише для деяких зі списку друзів.
* Чорний список. Вносячи туди певних користувачів, забороняються будь-які контакти з ними.

**Особиста інформація**

За деякими акаунтами можна дізнатися про їх власників буквально все: прізвище, місце роботи, район і навіть будинок проживання, захоплення, найбільш часто відвідувані місця і багато іншого. І всі ці дані можуть використовуватися зловмисниками в злочинних цілях. Варто обмежитися мінімумом відомостей, цього буде достатньо.

**Друзі**

У список друзів краще додавати тільки людей, з якими особисто знайомі, причому перевірених і надійних. Є два важливих правила. По-перше, не приймати пропозиції дружби від незнайомих людей. По-друге, періодично перевіряйте список друзів і видаляйте з нього сторінки, на яких помічені сліди злому або сайтів із підозрілою активністю.

**Переписка**

Важливо правильно навчитися вести листування, адже вони можуть бути використані проти особи. Допоможуть прості поради:

* Не ділитися одкровеннями і таємницями за допомогою повідомлень. Дописувач може зберегти переписку з секретами і використовувати її для шантажу чи інших дій.
* Не відповідати на повідомлення, що приходять від незнайомців, навіть якщо вони здаються безневинними і містять фрази типу «Привіт, як справи?» Або «Давай познайомимося». Звичайно, деякі практикують знайомства через соціальні мережі, але також незнайомець може займатися шахрайством або банальним тролінгом.
* Ігнорувати навмисно образливі повідомлення, а дописувачів відразу відправляти до чорного списку чи поскаржитися на них адміністрації сайту. Це дозволить зберегти нерви і уберегти себе від образ, прямих погроз і шантажу.

**Додатки та посилання**

Не переходити за посиланнями, які надсилають незнайомці. Вони можуть містити віруси і бути небезпечними для комп'ютера або мобільного пристрою. Часто, сайти з посилань нерідко містять непристойну або іншу небажану інформацію.

Не варто завантажувати додатки. По-перше, вони можуть запитувати доступ до особистих даних (невідомо, з якою метою інформація може використовуватися). По-друге, деякі програми ініціюють скачування сторонніх додатків: абсолютно непотрібних або платних. По-третє, після завантаження з рахунку можуть дивним чином зникнути гроші.

## Основи цифрової безпеки

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

### Моделювання загроз

Моделювання загроз означає оцінити, наскільки можливо те, що вас можуть зламати. Щоб убезпечити мережне життя, потрібно визначитися, що захищати і від кого.

Асоціація електронних кордонів рекомендує поставити 5 питань під час моделювання загроз:

1. Що ви бажаєте захистити?
2. Від кого хочете захистити дані?
3. Наскільки можливо, що вам знадобиться захист?
4. Наскільки поганими будуть наслідки, якщо захистити дані не вдасться?
5. Наскільки великі складності ви згодні піти, щоб убезпечити себе?

**Базова безпека. Першочергові дії по захисту комп'ютера**

* Встановлення ліцензійних операційних систем і програмного забезпечення. Неліцензійна ОС може містити шкідливі закладки, а також не дозволяти робити оновлення.
* Регулярне оновлення операційної системи, що містять виправлення дірок в безпеці. Створення резервної копії диска.
* Синхронізація локальних папок з «Хмарою». Копіювання важливих для роботи файлів (архів ключів доступу, приватні ключі PGP).
* Встановлення антивірусу, що зменшить ризик зараження комп'ютера.

**Цифрова гігієна**

* Двохфакторна авторизація для пошти і соціальних мереж. Використання складних і різноманітних паролів. Пароль на вхід в систему, що дозволить захистити ОС від стороннього доступу.
* Не підключати до пристрою чужі флешки, мобільні телефони, SD-карти, USB-пристрої та інші носії інформації. Відключити автозапуск для зовнішніх пристроїв, які можуть містити шкідливі програми, що автоматично запускаються і встановлюються.
* Не давати комп'ютер стороннім особам, які можуть встановити небажане ПЗ.
* Не встановлювати програми для підбору ключів (keygen) або інше ПЗ для злому офіційних програм, вони можуть містити шкідливі програми.
* На мобільних телефонах не рекомендується встановлювати програми з неофіційних магазинів додатків. В офіційних магазинах програми проходять перевірку безпеки.

### Додаткова безпека

* Закрити відеокамеру ноутбука. Застосовуючи шкідливе ПЗ, зловмисники можуть використовувати камеру і мікрофон для стеження.
* Створити повну резервну копію важливих документів, які варто зберігати на різних пристроях.
* Локальне шифрування важливих матеріалів (паролі доступу, фінансові та адміністративні матеріали, а також персональні дані третіх).

### Робота в Мережі

* Не підключатися до відкритих Wi-Fi мереж без використання VPN (OpenVPN, Cloak або іншого). Трафік за відкритими безпровідними мережами можна легко перехопити.
* Не можна вводити паролі до ресурсі, якщо не встановлено захищене з'єднання по HTTPS.
* Використовувати складний пароль. Всі паролі повинні містити цифри, великі і малі літери алфавіту і розділові знаки. За можливістю варто додати спеціальні символи.
* Не застосовувати один пароль всюди. Загальний пароль може стати частиною словників паролів, які зловмисники використовують для підбору паролів до різних сайтах.
* Двохфакторна авторизація для пошти та соціальних мереж.
* Не відкривати програми та посилання, які отримано від незнайомих людей.

## Безпека на смартфоні

Майже всі фахівці у світі кібербезпеки вважають, що айфони найбезпечніші смартфони. Одна з причин це те, що iOS дуже захищена.

До того, як потрапити до App Store, програми проходять ретельну перевірку на безпеку. Туди потрапляють лише програми із цифровим підписом Apple. А ще програми App Store не можуть підключатися до інших програм. Завдяки цим функціям хакерам дуже складно зламати найвразливіші частини ОС.

Оскільки Apple контролює інфраструктуру iOS, айфони отримують миттєві та регулярні оновлення безпеки. Критичні оновлення безпеки для пристроїв Android часто публікуються через тижні чи навіть місяці.

Android - ОС, розроблена Google. Вона стала найпопулярнішою ОС у світі завдяки відкритому вихідному коду і тому, що пристрої на ній набагато дешевші за айфони. Оскільки це ОС з відкритим вихідним кодом, оновлення залежить тільки від виробників пристроїв, а вони часто не дуже поспішають з цим.

Бути обережними при встановленні програм, переконатися, що це не підробка. Хакери часто публікують шкідливі програми в Play Store. Наприклад, у 2020 році більше мільйона користувачів Android завантажили фальшиву програму WhatsApp.

Щоб захистити дані на телефоні, переконатися, що на ньому увімкнено повне шифрування диска (зазвичай, Установки - Безпека - Шифрувати телефон). Встановити мобільний антивірус - наприклад Lookout або Zips.

### Безпечні месенджери

Якщо спілкування зашифроване, це означає, що воно зашифроване між кінцевими точками - відправником та одержувачем. Відправник та отримувач можуть бачити повідомлення, якщо повідомлення перехоплять під час передачі, вміст буде відображатися як зашифрований.

### Безпека в соцмережах: протести та мітинги

Соцмережі підпорядковуються наказам судів та запитам даних користувачам. Часто вони можуть передавати інформацію, не повідомляючи про це користувача. Тому всі розміщені пости є публічними.

Думати про безпеку інших людей — кого відзначено у постах чи додано інформацію про їх місцезнаходження. Технології розпізнавання обличь швидко розвиваються, тому навіть якщо не відзначати людей, теоретично алгоритм може просканувати та ідентифікувати людей.

### Мікрофони та камери на пристроях

Через ці пристрої можливо прослуховування або стеження за користувачем, тому варто подбати про їх захист. Наприклад, закрити наклейкою фронтальну камеру, коли її не використовують. Це спосіб захиститися від можливих хакерів та вірусів. Для цього можна купити спеціальні стікери, що знімаються, які не залишають відбитків на камері.

На жаль, немає способу переконатися, що мікрофон нічого не записує.

### Безпечний браузер Tor

Браузер Tor шифрує трафік, перенаправляючи його через кілька комп'ютерів. Щоб використовувати Tor, встановити спеціальний браузер чи плагін на комп'ютер. Він працює так само, як Firefox або Chrome — лише трохи повільніше через приватність, яку він надає. Tor - не бронежилет, це браузер для приватності, а не безпеки.

#### 3 причини, з яких варто використовувати Tor:

* Ви намагаєтеся приховати вашу особу.
* Ви часто використовуєте публічний WiFi.
* Ви намагаєтесь уникнути цензури уряду.

### Шифрування твердого диска на телефоні

Повне шифрування диска означає, що коли пристрій заблоковано або вимкнено, до контенту твердого диска не можна отримати доступ без пароля або шифру.

У багатьох смартфонах вже вшито повне шифрування диска. Потрібно тільки придумати пароль для нього, і особиста інформація в безпеці.

## 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>