5. МЕРЕЖЕВА КІБЕРБЕЗПЕКА

5.1. Відстеження особистості та цифровий слід.

5.2. Безпека браузерів.

5.3. Технології Proxy, VPN, DNSFilter, Firewall, Wi-Fi.

5.1. Відстеження особистості та цифровий слід.

Цифровий слід (digital footprint) – це унікальний слід даних про діяльність, дії, повідомлення або транзакції користувача в цифрових носіях інформації. Цей слід можна залишити в Інтернеті, на комп'ютерах, мобільних пристроях чи інших носіях. Цифровий слід може використовуватися для відстеження діяльності та пристроїв користувача.

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 фільмом або публікуючи пости в соціальних мережах.

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

Цифровий слід, який лишає людина має кілька складових.

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

Публікація фотографій та відео, де присутній користувач. Один раз з'явившись в Мережі, 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 із них взагалі не видаляють завантажені клієнтами матеріали, лише за умови, що вони порушують закон.

2. Текстова інформація. використання текстової інформації, такої як електронні листи, 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.

3. 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 та тіні.

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

4. Часова інформація. Записи кожної дії кожного користувача (логи) в Інтернет, які ведуться провайдерами і серверами вебсайтів. Така докладна інформація зважаючи на величезні обсяги (десятки гігабайт у день для відвідуваного сайту) недовговічна – лог-файли автоматично видаляються раз у декілька днів. Але витягнуті з логів важливі дані зберігаються довго.

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

Цифрова тінь зазвичай формується без відома людини. Наприклад, випадкове потрапляння машини користувача в кадр чужої фотокамери, але цю фотографію публікують в Інтернеті. Дехто починає обговорювати цю машину, з'ясовується номер та 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.

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

Значна кількість людей під час реєстрації вказує справжні прізвище та ім'я, домашню адресу, телефони та 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 із 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.

Файли cookie – інформація у вигляді текстових або бінарних даних, отриманих від вебсайту, яку збережено у клієнта для відправлення на той самий сайт при повторному відвідуванні. Вони також можуть зберігати облікові дані, щоб полегшити вам вхід на раніше відвіданий сайт.

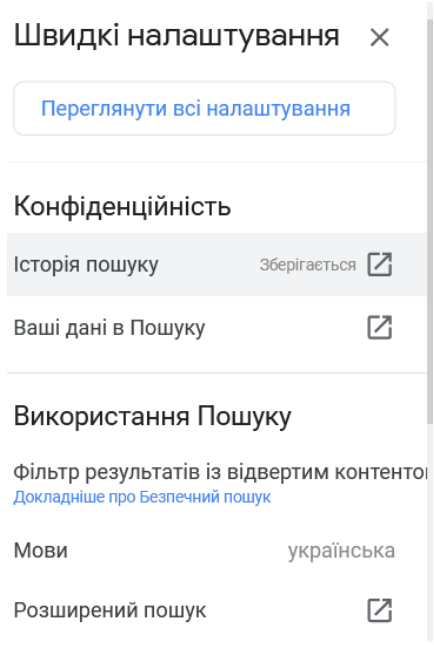
Сесійні файли cookie існують лише під час перебування на вебсайті. Після виходу з цього вебсайту cookie автоматично зникає.

Інші файли cookie називаються стійкими. Вони певний час залишаються на вашому жорсткому диску (іншому пристрої зберігання даних) й використовуються для автентифікації.

Також існує певний різновид стійкого файлу cookie – сторонні файли cookie. Вони генеруються на інших вебсайтах, ніж той, який ви відвідуєте. Зазвичай, сторонні файли cookie пов’язані з рекламою та використовуються рекламодавцями для відстеження активності користувача на всіх сайтах, що містять їх оголошення. Ці файли cookie збирають багато інформації: що саме ви шукаєте в Інтернет-магазині, місцезнаходження (через IP-адресу), конфігурацію пристрою, скільки часу ви провели на певному сайті, публікації у Facebook та багато іншого.

Вебсайти, які використовують файли cookie, законодавством змушені інформувати вас про цю ситуацію та пропонувати кнопку прийняти або відхилити їх.

Зібрати дані про користувачів сьогодні легко, здебільшого вони самі їх надають в обмін на використання різних сервісів. Величезна кількість корисних продуктів Google доступна для користувачів безкоштовно, але натомість потрібно погодитися на збір і обробку персональних даних. Google постійно збирає статистику про своїх користувачів: пам'ятає запити, відвідані сайти, геодані, кількість надісланих листів, фотографій, часто вживані слова. Google підлаштовується під користувача, а отже, знає і його звички.



Єдиний спосіб зламати та отримати ці дані – отримати доступ до облікового запису Google. Тому обліковий запис Google захищає двоетапна аутентифікація та якісна реалізація безпеки для мобільних пристроїв (наприклад, можна віддалено заблокувати смартфон або акаунт).

Користувач може дозволити чи заборонити стежити за певними активностями для покращення підбору інформації: особиста інформація користувача; дані в обліковому запис Google і його місце перебування; дії користувача; поточний пошуковий запит; історія пошуку; діяльність облікового запису Google; взаємодії з оголошеннями; сайти, які він відвідував; дії в мобільних додатках; дії на інших пристроях під власним акаунтом в Google; час доби; інформація, яку користувач надав рекламодавцю. Наприклад, адреса електронної пошти, вказана при підписці на розсилку.

Також Google зберігає інформацію про всі додатки та розширення, які є на вашому пристрої. Компанії відомо, як часто, де і з ким ви використовуєте їх. Ця функція зберігає дані з телефонів і планшетів: контакти, календарі, додатки, музика, інформація щодо пристрою (наприклад, рівень заряду батареї, версія Android, місцезнаходження).

Листи Gmail – дані про електронне листування, відстежується кількість отриманих і відправлених листів. Сам інтерфейс Gmail містить блоки з рекламними оголошеннями. Процес показу оголошень в Gmail повністю автоматизовано, і реклама підбирається з врахуванням дій користувача в обліковому записі Google.

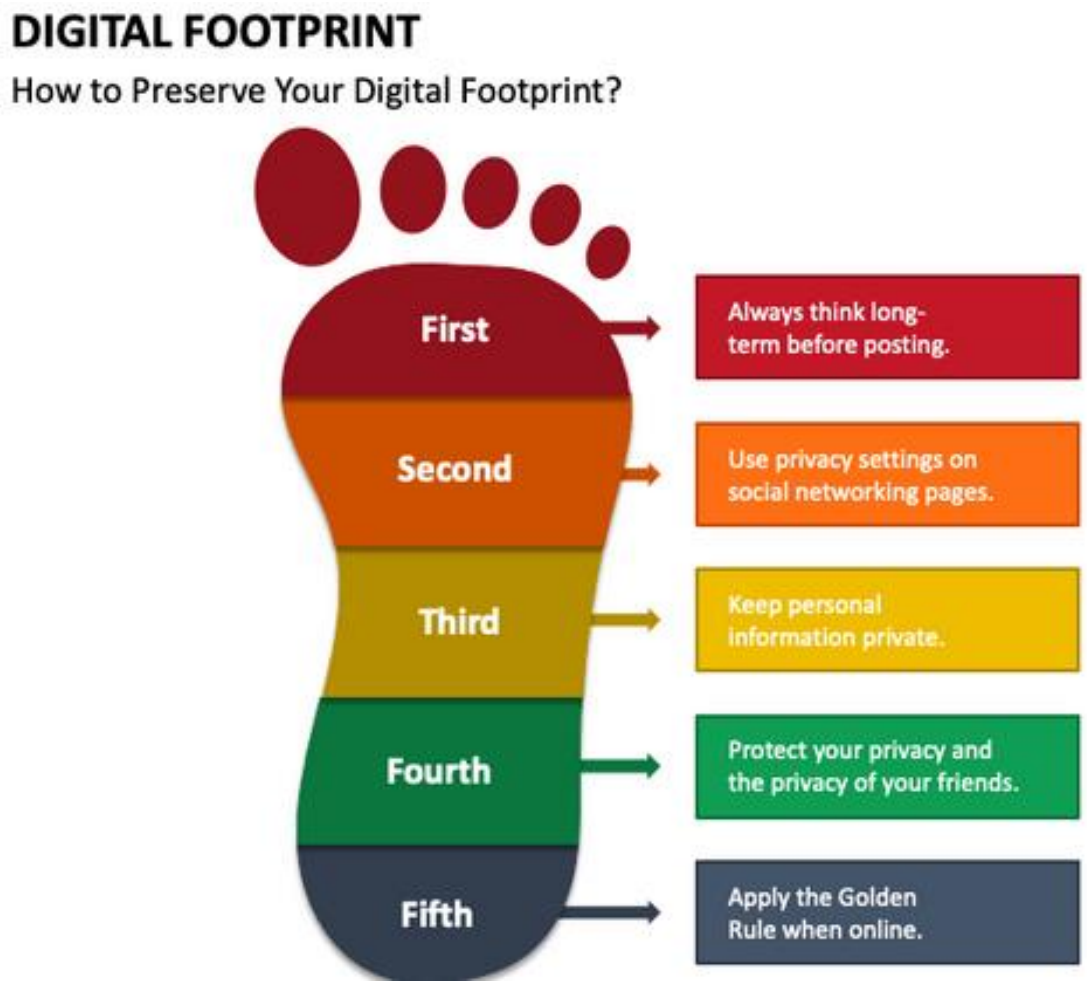
Ситуації зі збором даних не можна розглядати лише з одного боку. Дізнавшись більше інформації про користувача, рекламодавці зможуть запропонувати йому дійсно корисний продукт. Причому саме в потрібний час і в потрібному місці. Найчастіше користувачеві навіть не доводиться нічого шукати. Необхідні товари, місця і послуги приходять до нього самі. Такий підхід відмінно економить час і допомагає швидше знайти потрібну інформацію. Цей досвід можливий при дотриманні певних умов: дані повинні збиратися і зберігатися у відповідності до політики конфіденційності та законодавства.

Як зменшити цифровий слід та цифрову тінь.

1) Розділіть акаунти. Придумуйте випадкові імена акаунтів електронної пошти для особистого використання. Створюйте окремі акаунти для фінансових операцій, реєстрації в соцмережах і загального призначення. Не використовуйте справжню дату народження, не вводьте повне ім’я або використовуйте вигадані імена для кожного акаунту. Для непублічних акаунтів, використовуйте випадкові зображення профілю.

2) Не повторюйте паролі. використовуйте менеджер паролів щоб генерувати окремі паролі для кожного онлайн-сервісу. Для додаткового захисту налаштуйте двухфакторну аутентифікацію.

3) видаляйте метадані, приховуйте геолокацію.



4) Приховуйте підказки. видаляйте EXIF (якщо це не відбувається автоматично) перед публікацією фото в соцмережах. Але залишаються підказки на самому фото: силуети будівель, рекламні вивіски, відображення в дзеркалі, документи на робочому столі. Такі деталі полегшують ідентифікацію особистості, пошук місця розташування офісу або домашньої адреси, а також складають уявлення про спосіб життя цілі.

5) Навчіться мовчати. Розміщення контенту в мережі – загроза конфіденційності. Перш, ніж опублікувати коментарі або фото, подумайте: чи дає це зловмисникові інформацію для створення досьє на людину або компанію.

Перевірте налаштування конфіденційності в соцмережі: хто саме може переглядати ваші публікації та особисті дані та яку кількість інформації можуть бачити відвідувачі. У список друзів краще додавати лише людей, з якими ви особисто знайомі, бажано перевірених й надійних. Далі необхідно очистити існуючий список друзів: почніть із видалення з друзів усіх незнайомців, яких ви

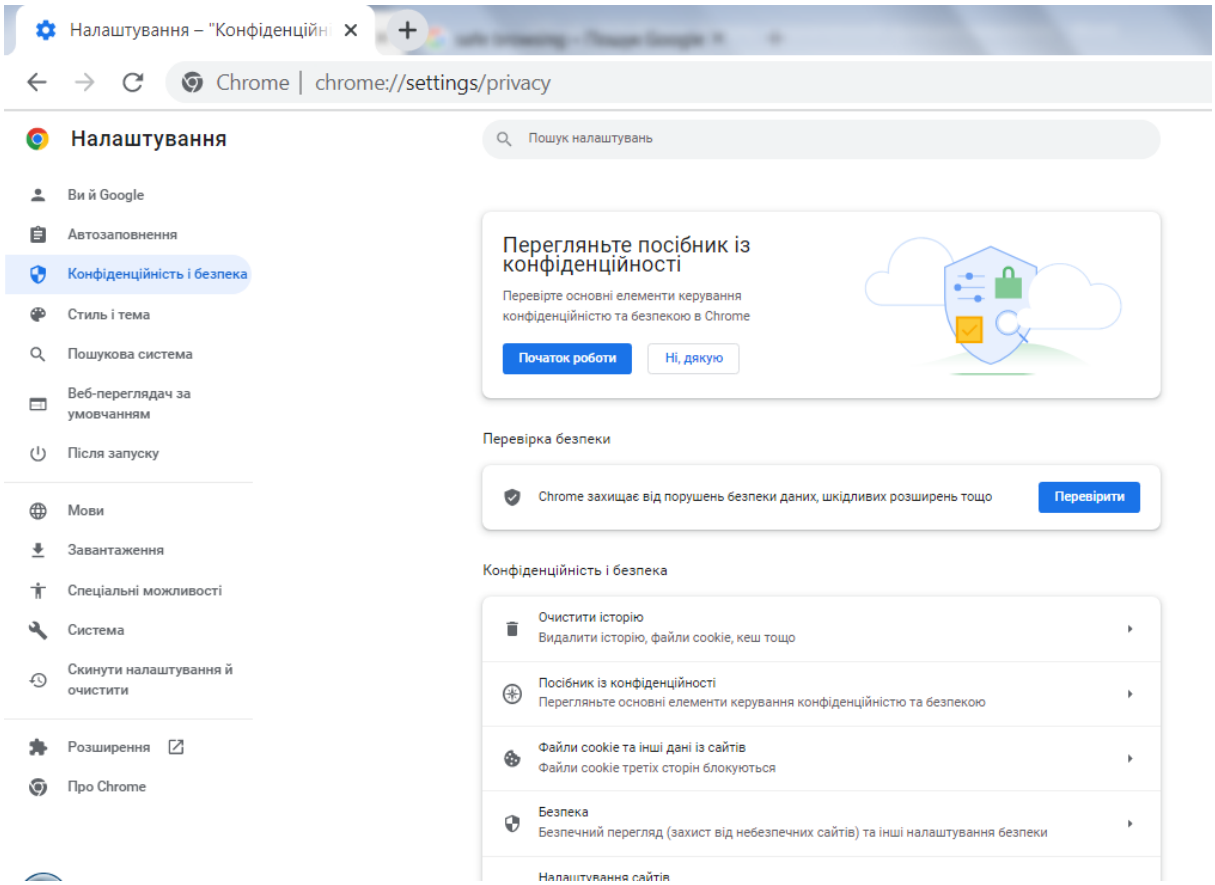
навіть не пам’ятаєте, а потім переходьте до знайомих, яких ви не дуже добре знаєте, а також до людей, з якими перестали спілкуватися.

Не ділитися таємницями за допомогою повідомлень. Дописувач може зберегти переписку з секретами і використовувати її для шантажу чи інших дій. Не відповідайте на повідомлення, які приходять від незнайомців, навіть якщо вони здаються буденними й містять фрази типу «Привіт, як справи?» Або «Нумо познайомимося». Ігноруйте навмисно образливі повідомлення, а дописувачів відразу відправляйте до чорного списку чи поскаржиться на них адміністрації сайту.

5.2. Безпека браузерів.

Google Chrome забезпечує високий захист від шкідливих сайтів, але, водночас, він збирає інформацію щодо користувачів. Із випуском Chrome 76.10 в грудні 2019 року, користувачі можуть отримувати попередження, якщо їхні паролі будуть виявлені в списках і базах, раніше зламаних хакерами та виставлених в загальний доступ. Сам Chrome гарантує, що його можна вважати найбезпечнішим браузером, завдяки своїм трьом функціям:

- безпечний перегляд сторінки, який попереджає про можливі загрози при відкритті фішингового або шкідливого вебсайту;
- режим пісочниці, який надає додатковий рівень захисту і запобігає автоматичному встановленню шкідливих програм (особливо в фоновому режимі);
- автоматичні оновлення, що дозволяють встановлювати всі оновлення і усувати недоліки безпеки;
- унікальні паролі генеруються і зберігаються у веб-браузері автоматично;
- браузер має режим інкогніто і пропонує налаштування параметрів конфіденційності вручну.



Mozilla Firefox є одним із найближчих конкурентів Google Chrome. Ще у 2017 році версія Mozilla Quantum містила такі можливості:

- Linux Sandboxing, який запобігає спробам злому;
- захист від стеження, який блокує компоненти відстеження на відвідуваних користувачем вебсайтах;
- покращений центр управління, що дозволяє отримувати доступ до численних параметрів і налаштовувати їх для забезпечення найбільш безпечних і приватних сеансів перегляду, які може запропонувати браузер;
- Contextual Feature Recommender (CFR) — система, яка рекомендує доповнення та функції, що спираються на досвід перегляду контенту користувача;
- поліпшений захист від стеження, який повністю вимикає стеження.

Opera – ще один браузер в списку «найбезпечніших браузерів». Із 2016 десктопна версія цього браузера на базі Chromium включала вбудований блок захисту від реклами. Opera пропонує кращу конфіденційність користувачів, додавши вбудовану віртуальну приватну мережу – VPN.

Інші функції безпеки, які надаються розробником:

- значки безпеки пропонують перевірену інформацію про сторінку;
- захист від шахрайства і шкідливих програм – попереджає про сайти, що становлять потенційну небезпеку;
- блокування реклами працює як будь-який інший сторонній додаток, що дозволяє блокувати рекламу.

Але браузер збирає деяку інформацію про користувачів і може ділитися нею з довіреними партнерами та компаніями.

Експерти антивірусної лабораторії Zillya! підготували список із семи кращих додатків для браузера, які допоможуть зробити Інтернет-серфінг безпечним.

Adblock Plus – один із найпопулярніших додатків для браузера. Adblock Plus дозволяє блокувати настирливу рекламу, спливаючі вікна та інші неприємні об'єкти на сторінці. Доповнення приховує не всю рекламу, а лише ту, яка не відповідає критерієм «ненав'язливості». Правильно оформлена реклама потрапляє в так званий білий список і відображається користувачеві. Підтримувані браузери: Internet Explorer, Firefox, Chrome, Opera, Safari. Офіційна сторінка доповнення: https://adblockplus.org/.

NoScript – це доповнення підвищує рівень безпеки користувача шляхом тотального блокування JavaScript, Java та іншого контенту в браузері, який завантажується з вебсайтів або запускається на ПК користувача. Таким чином NoScript захищає користувача від різноманітних скриптів, XSS-атак, хакерських маршрутизаторів, тощо. Підтримувані браузери: Firefox, SeaMonkey. Офіційна сторінка доповнення: http://noscript.net/getit.

AdwCleaner – дозволяє позбутися від рекламного ПЗ на комп'ютері. Програма сканує систему і виявляє будь-яке рекламне ПО, надбудови та програми, які підпорядковують собі комп'ютер користувача. Підтримувані браузери: Internet Explorer, Firefox, Chrome. Сторінка доповнення: http://www.bleepingcomputer.com/download/adwcleaner/.

Ghostery – це доповнення захищає конфіденційну інформацію користувача при відвідуванні сайтів в Інтернеті. Ghostery відстежує «невидиму» сторону Мережі, в якій знаходяться шпигуни, мережеві жучки і маяки, розміщені на сайтах рекламними агентами різних компаній, які дозволяють збирати дані про користувачів в Інтернеті. Доповнення Ghostery надає користувачеві інформацію про кожну виявлену компанію, доповнюючи звіт посиланнями на політики конфіденційності та налаштування збору інформації цих компаній. Підтримувані браузери: Internet Explorer, Firefox, Chrome, Opera, Safari. Офіційна сторінка доповнення: https://www.ghostery.com.

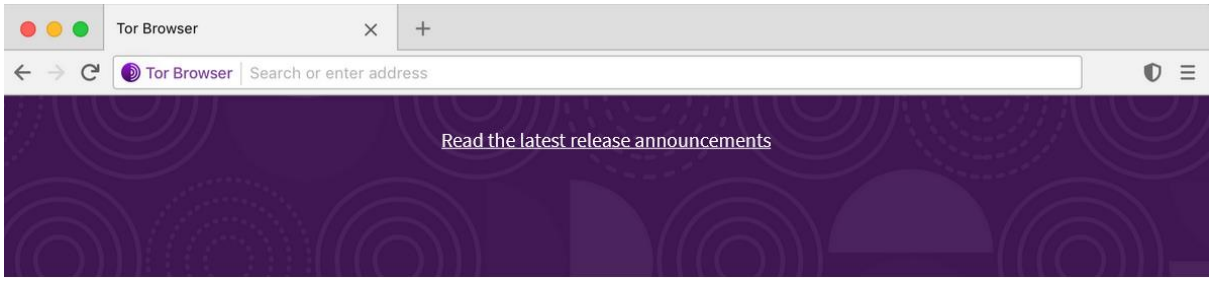
AVG PrivacyFix – це доповнення для управління налаштуваннями конфіденційності соціальних мереж, пошуковиків та вебсайтів. AVG PrivacyFix виконує сканування налаштувань профілів користувача в соціальних мережах і визначає проблеми конфіденційності. Якщо профілі налаштовані таким чином, що приватна інформація користувача наражається на небезпеку, то додаток допоможе це виправити. Доповнення AVG PrivacyFix так само, як і Ghostery, може визначити компанії, які шпигують за діяльністю користувача в Інтернеті та подивитися політику конфіденційності цих компаній. Підтримувані браузери: Firefox, Chrome. Офіційна сторінка доповнення: https://www.privacyfix.com/start/install.

PrivDog – сканує відвідувані вебсайти щодо наявності шкідливого контенту, блокуючи непотрібні рекламні об’єкти. Також, PrivDog прискорює швидкість відкриття сайтів шляхом зменшення кількості cookies, шпигунів і реклами. Підтримувані браузери: Internet Explorer, Firefox, Chrome. Офіційна сторінка доповнення: http://www.privdog.com/.

WOT (Web of Trust) – це надбудова до браузера, яка попереджає користувача про сайти з низькою репутацією. WOT – це своєрідне співтовариство користувачів, кожен із яких, перебуваючи на тому чи іншому Інтернет-ресурсі, може поставити йому оцінку. На основі цих оцінок створюється репутація ресурсу. Рейтинги сайтів постійно оновлюються багатомільйонною аудиторією. Підтримувані браузери: Internet Explorer,

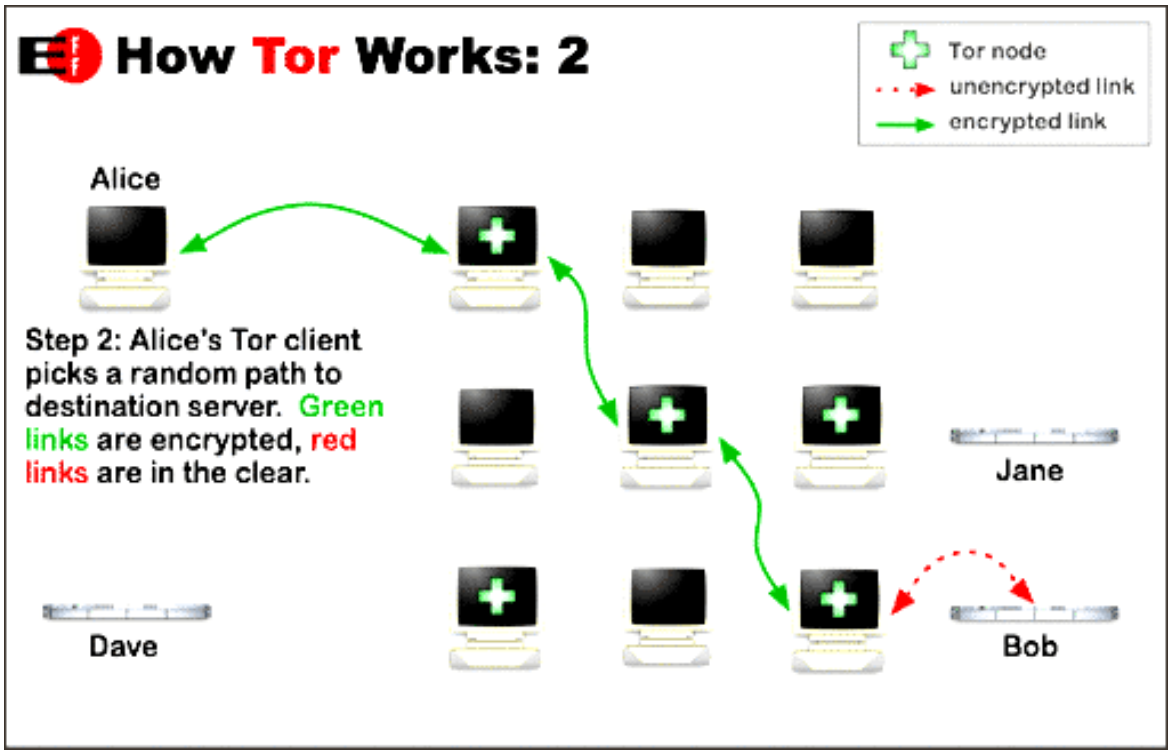
Firefox, Chrome, Opera, Safari. Офіційна сторінка доповнення: https://www.mywot.com.

Браузер Tor – безкоштовна, відкрита та некомерційна програма, яка дає користувачам анонімний доступ до Інтернету. Основна ідея проекту – забезпечити вільний та безпечний доступ до Мережі. Для звичайних користувачів – це спосіб захистити себе та свій трафік не тільки від влади, а й від провайдерів, власників публічних Wi-Fi-точок та сайтів, а також спосіб обійти блокування деяких сайтів.



Tor існує завдяки величезній мережі комп'ютерів-волонтерів, які розкидані по всьому світу. Назва Tor – The Onion Router англійською, або цибульний маршрутизатор – відсилає до принципу роботи браузера. Tor зашифровує ваш трафік тричі, ніби створюючи три шари цибулини. Зашифрований трафік прямує до комп'ютера А, який знімає перший шар шифрів і бачить адресу комп'ютера В. Комп'ютер В, знімаючи ще один шар, бачить адресу комп'ютера С, не знаючи при цьому, звідки трафік прийшов спочатку і куди він прямує зрештою. І лише через комп'ютер С ви виходите в Інтернет.

Хто б не стежив за вами чи вашим трафіком –провайдер чи влада – вони можуть дізнатися, що ви користуєтеся браузером Tor, але не вашу мету. Щоразу ви потрапляєте в Інтернет за допомогою випадкового комп'ютера-волонтера, а сам браузер за замовчуванням не зберігає історію ваших дій, тому в Інтернеті ніхто не дізнається, хто ви, і не зможе отримати інформацію про вас.



Через цибульну структуру браузер Tor уповільнює швидкість вашого Інтернет-з'єднання. Стрім відео чи музики через Tor, швидше за все, буде особливо повільним. Браузер не зможе захистити вас, якщо ви самі видаєте інформацію про себе в Інтернеті або якщо на вашому комп'ютері є віруси чи програми, які стежать за вашим Інтернет-користуванням.

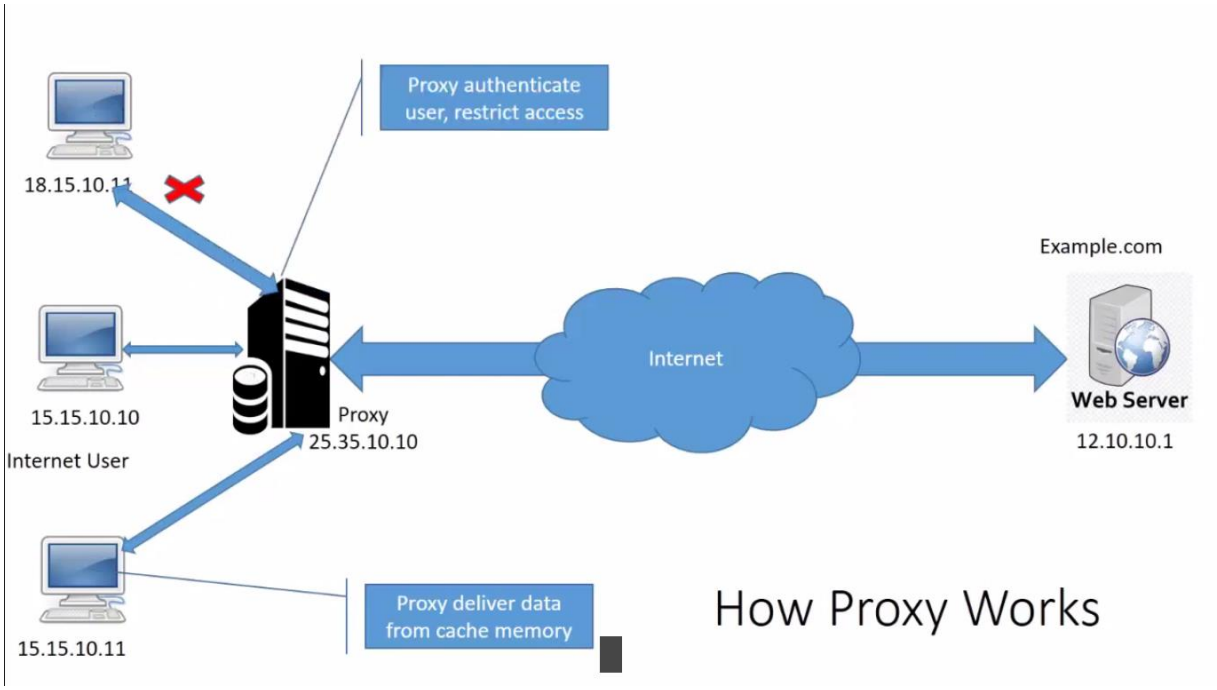
5.3. Технології Proxy, VPN, DNSFilter, Firewall, Wi-Fi.

5.3.1. Проксі сервер (proxy – «представник, уповноважений», право користуватися чимось від чужого ім'я) – це служба в комп'ютерних мережах, що дозволяє клієнтам виконувати непрямі запити до інших мережних служб. Спочатку клієнт підключається до такого сервера і запитує у нього деякий ресурс, що розташований на іншому сервері в Інтернеті. Далі сервер або підключається до вказаного сервера й отримує ресурс у нього, або надає ресурс із власного кешу.

Технологію проксі застосовують з метою:

- забезпечення доступу з комп'ютерів локальної мережі до Інтернету;
- кешування даних – якщо часто відбуваються звернення до одних і тих самих зовнішніх ресурсів, можна тримати їх копію на сервері та видавати за

запитом, знижуючи цим навантаження на канал у зовнішню мережу і прискорюючи отримання клієнтом запитаної інформації;



- стиснення даних – сервер завантажує інформацію з Інтернету та передає інформацію кінцевому користувачеві в стислому вигляді;
- захисту локальної мережі від зовнішнього доступу – наприклад, можна налаштувати сервер так, що локальні комп'ютери будуть звертатися до зовнішніх ресурсів тільки через нього, а зовнішні комп'ютери не зможуть звертатися до локальних взагалі;
- обмеження доступу з локальної мережі до зовнішньої – наприклад, можна заборонити доступ до певних вебсайтів, обмежити використання Інтернету певним локальним користувачам, встановлювати квоти на трафік або смугу пропускання, фільтрувати рекламу та віруси;
- анонімізації доступу до різних ресурсів. Проксі-сервер може приховувати інформацію про джерело запиту або користувача. У такому разі цільовий сервер бачить лише інформацію про сервер, наприклад IP-адресу, але не має можливості визначити справжнє джерело запиту. При звертанні до web-серверів proxy «підмінить» IP-адресу користувача на свою й зловмисник буде намагатися вторгнутися не до користувача, а на proxy-сервер (у якого набагато більш потужна система захисту).

Але не всі proxy-сервера в Internet є анонімними (підміняють IP-адресу користувача). Більшість із них призначено для прискорення доступу в Internet й не приховують вашу IP-адресу. Для пошуку анонімних проксі-серверів доцільно скористатися сервісом Proxy Checker або аналогічним.

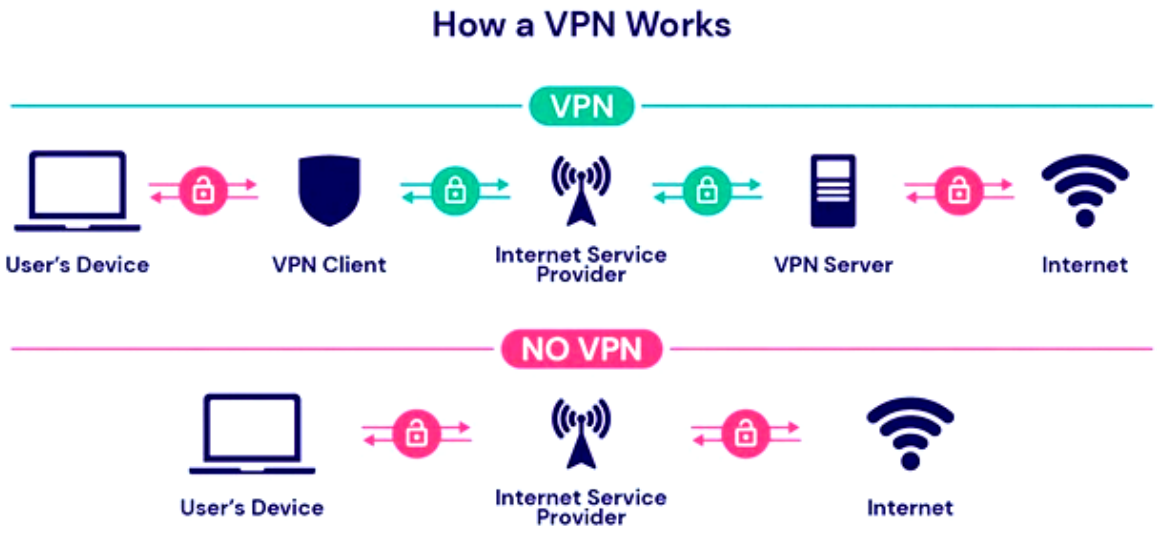
Проксі сервери бувають декількох типів:

- FTP проксі використовуються для завантаження даних на сервери FTP;
- CGI проксі (анонімайзери) допомагають відкрити будь-який вебсайт прямо у браузері. Жодних додаткових налаштувань не потрібно. Найчастіше такі проксі виконані у вигляді вебсайту, де можна ввести адресу сайту, яку необхідно відвідати;
- SMTP, POP3 та IMAP проксі використовуються для надсилання та отримання електронної пошти;
- HTTP та HTTPS проксі призначені для перегляду веб-сторінок;
- Socks проксі передає всі дані на кінцевий сервер як клієнт, тому вважається найбільш анонімним протоколом.

При роботі з будь-яким проксі ви повинні пам’ятати, що проксі сервер здатний вести логи (звіти роботи), зберігаючи всю інформацію про вашу IP-адресу та всі запити, які виконувались з неї, включаючи паролі, логіни та інші важливі конфіденційні дані. Також проксі сервера можуть бути під контролем спецслужб або зловмисників, а часом їх створюють спеціально для перехоплення та аналізу трафіку.

5.3.2. VPN (Virtual Private Network, віртуальна приватна мережа) – узагальнена назва технологій, які дозволяють створювати віртуальні захищені мережі поверх інших мереж із меншим рівнем довіри. VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному пристрою чи користувачу бути повноцінним учасником віддаленої мережі та користуватися її сервісами – внутрішніми сайтами, базами, принтерами, політиками виходу в Інтернет. Безпека передавання інформації через загальнодоступні мережі

реалізована за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. Технологія VPN дозволяє об'єднати декілька географічно віддалених мереж (або окремих клієнтів) в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.



Коли ви підключені до VPN-серверу, то весь ваш Інтернет-трафік шифрується. Це означає, що ніхто не може відстежити, що ви робите в Інтернеті – навіть ваш Інтернет-провайдер. Окрім того, Інтернет-провайдер не зможе обмежити швидкість вашого підключення. Шифрування також запобігає отриманню хакерами доступу до вашої чутливої та важливої інформації, яку ви вводите на вебсайтах, наприклад, до паролів. використання VPN у смартфоні особливо важливо, якщо ви використовуєте відкриті публічні WiFi-мережі, оскільки кіберзлочинцям дуже просто відстежувати ваше підключення до публічних мереж.

VPN приховує вашу справжню IP- адресу. Існує декілька причин, чому варто використовувати VPN-з'єднання. По-перше, ваша IP-адреса може бути використана для визначення вашого реального місцезнаходження, що в свою чергу загрожує вашій конфіденційності, особливо в поєднанні з іншою персональною інформацією.

По-друге, багато вебсайтів, таких як Netflix, HBO, Hulu, BBC iPlayer, Amazon Prime Video та багато інших, на підставі вашої IP-адреси визначають, доступ до якого контенту ви отримаєте. Крім того, через наявність

геопросторових блоків, ви не можете отримати доступ до багатьох популярних ТВ-каналів, особливо поза межами країн їх трансляції. Єдиним способом обійти гео-просторове блокування є маскування вашої реальної IP-адреси та підміна її на іншу, а саме це й робить VPN.

Також VPN блокує підозрілі сайти, рекламу та трекери. Найкращі VPN мають вбудований захист від кібератакі та здатні запобігти завантаженню шкідливих програм і трекерів із підозрілих сайтів на ваш пристрій. Деякі з них також блокують рекламу та спливаючі вікна.

Існує два основних класи мереж VPN. Шлюз захищеного віддаленого доступу до VPN дозволяє користувачам підключитися до іншої мережі (до Інтернету або внутрішньої системи своєї компанії) за приватним зашифрованим тунелем. Інший клас – VPN типу «мережа-мережа», чи VPN між маршрутизаторами. Цей вид мережі VPN в основному використовується в корпоративному середовищі, особливо якщо підприємство має штаб-квартири з різним розташуванням. VPN типу «мережа-мережа» використовується для створення закритої внутрішньої мережі, де всі офіси можуть підключатися один до одного. Ця технологія відома як інтранет.

Існує кілька протоколів VPN. Найстаріший з них – PPTP (протокол тунелювання «точка-точка»), який досі застосовується, але вважається одним із найбільш ненадійних протоколів. Інші – IPSec, L2TP, SSL, TLS, SSH і OpenVPN. Багато хто віддає перевагу протоколу OpenVPN, оскільки це програмне забезпечення з відкритим вихідним кодом.

На що слід звернути увагу при виборі VPN для захисту конфіденційності та забезпечення безпеки:

- 256-бітне шифрування AES;
- автоматичне аварійне відключення. У випадку втрати підключення під час використання VPN, функція автоматичного аварійного відключення призупинить ваш трафік до тих пір, доки не буде відновлено захищене з’єднання із сервером. Без цього інструменту ви будете наражатися на

випадкові витоки даних, через що ваша конфіденційність вже не буде захищеною;

- політика відмови від реєстрації дій користувачів;
- захист від витоків даних через DNS або IPv6. Існує декілька шляхів витоку ваших даних в мережу під час використання VPN, але ці два є найбільш поширеними.

Недоліки VPN:

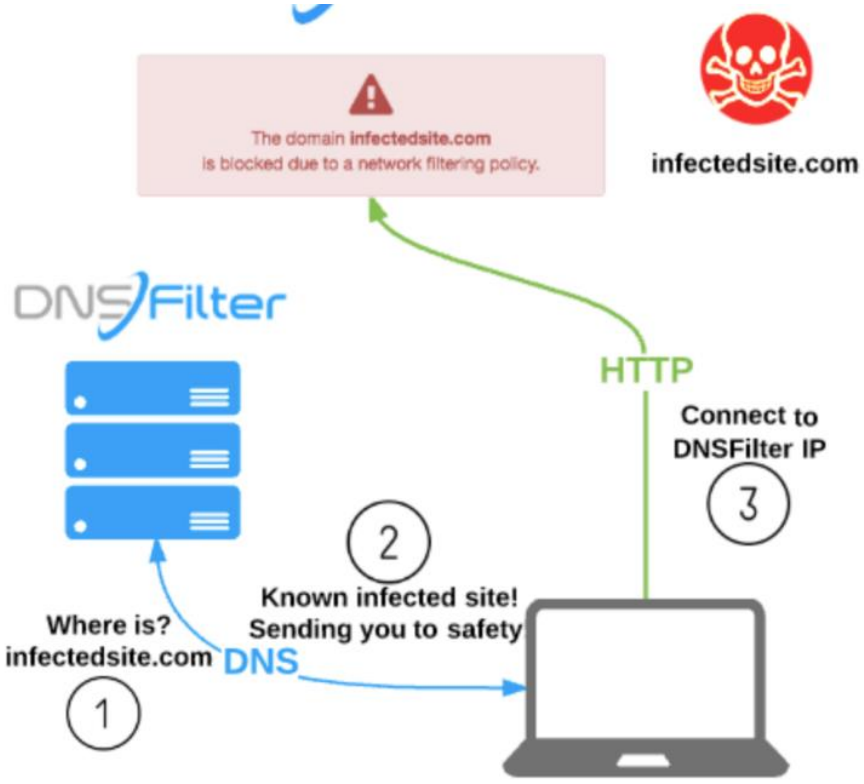
- зниження швидкості з'єднання з Інтернетом;
- неперевірені VPN можуть скомпрометувати ваш захист;
- деякі вебсайти блокують VPN.

5.3.4. DNSFilte (domain name system) – система доменних імен, яка працює за допомогою DNS-серверів. Кожен DNS-сервер за вказаною адресою сайту визначає IP-адресу веб-сервера, на якому знаходиться сайт.

DNS-фільтрація передбачає фільтрацію доменних імен та є методом запобігання доступу до певних веб-сторінок або IP-адрес, які здаються підозрілими. ви також можете заблокувати певні URL-адреси вручну. Особливо зручним цей спосіб є у випадку, коли вам потрібно захистити не один комп'ютер, а декілька, які підключені до мережі Інтернет через роутер. Окрім комп'ютерів, таким чином можна захистити інші пристрої, підключені до роутера через Wi-Fi. Якщо використовувати стандартні налаштування мережі, то всі запити до сайтів йдуть через сервер провайдера, який надає доступ до мережі Інтернет. Як правило, сервер провайдера не фільтрує запити користувачів і надає доступ до всіх затребуваних сайтів (якщо доступ до них не заборонено законодавством).

Але в мережі Інтернет існують DNS-сервери, які збирають інформацію про сайти, що містять інформацію, шкідливу для дітей, або сайти, які були

помічені в різних шахрайських схемах. Якщо в налаштуваннях свого комп'ютера або роутера вказати IP-адресу такого DNS-сервера, то всі запити до сайтів проходитимуть через цей сервер. Сервер фільтруватиме адреси затребуваних сайтів і не надаватиме доступ до заборонених сайтів.



DNS-фільтр перевіряє вхідний та вихідний трафік та блокує підозрілий, ґрунтуючись на певних заданих параметрах. Він дозволяє мережі отримувати та відправляти лише безпечний трафік. DNS-фільтр також може захистити Wi-Fi людини від експлойтів, що є чудовою додатковою функцією програми.

Можна навести наступний практичний приклад використання фільтрації DNS: якщо керівник заблокував доступ своїх користувачів до facebook.com у робочий час, і вони намагатимуться відкрити цей сайт, нічого не вийде. У робочий час їхній запит буде відхилений – сайт стане недоступним.

Переваги DNS-фільтрації:

- на деяких платформах це єдиний спосіб фільтрувати весь системний трафік. Наприклад, на iOS лише Safari підтримує блокування контенту у звичному сенсі. Фільтрувати трафік усіх інших браузерів та програм допоможе лише DNS-фільтрація;

- з деякими формами стеження (наприклад, CNAME-трекінг) може впоратися лише DNS-фільтрація;
- етап обробки DNS-запиту – перша ступінь, яка може заблокувати рекламу чи трекер. Це допомагає трохи заощадити час життя батареї та трафік.

Недоліки DNS-фільтрації:

- DNS-фільтрація – «грубий» метод. Це означає, що з її допомогою не вийде прибрати, наприклад, білі порожні блоки, що залишаються після заблокованої реклами. Багато видів складної реклами не можуть бути заблоковані на рівні DNS (точніше, можуть, але лише ціною повного блокування домену, який також використовується для інших корисних цілей);
- неможливо визначити джерело DNS-запиту, тобто ви не зможете розрізняти трафік різних програм на DNS-рівні. Це завадить веденню докладної статистики і унеможливить створення правил, що працюють лише для конкретних додатків.

Загальнодоступні DNS-фільтри.

Публічний DNS-сервер Google. Цей сервер по суті створювався не для фільтрації, а для прискорення роботи Інтернету, але він так само фільтрує фішингові та шкідливі сервери. Крім того, даний сервер вміє працювати по IPv6.

Адреси DNS Google:

IPv4 8.8.8.8, 8.8.4.4

IPv6 2001:4860:4860::8888, 2001:4860:4860::8844.

OpenDNS – мабуть найстаріший DNS-фільтр. Є платні та безкоштовні можливості. Вміє виправляти неправильно набрані адреси сайтів, а також показує сторінку з пошуком та рекламою, якщо адресу виправити не вдалося автоматично. Має профілі для батьківського контролю доступні безкоштовно після реєстрації. Без реєстрації декларується фільтрація шкідливих серверів.

Адреси DNS OpenDNS:

208.67.222.222

208.67.220.220

https://www.opendns.com/

1.1.1.1 DNS Family. Приватний сервер DNS від CloudFlare. Декларується як один із найшвидших та приватних. Є варіанти із блокуванням шкідливих сайтів та дорослого контенту.

Адреси DNS 1.1.1.1:

1.1.1.1 – швидкий приватний;

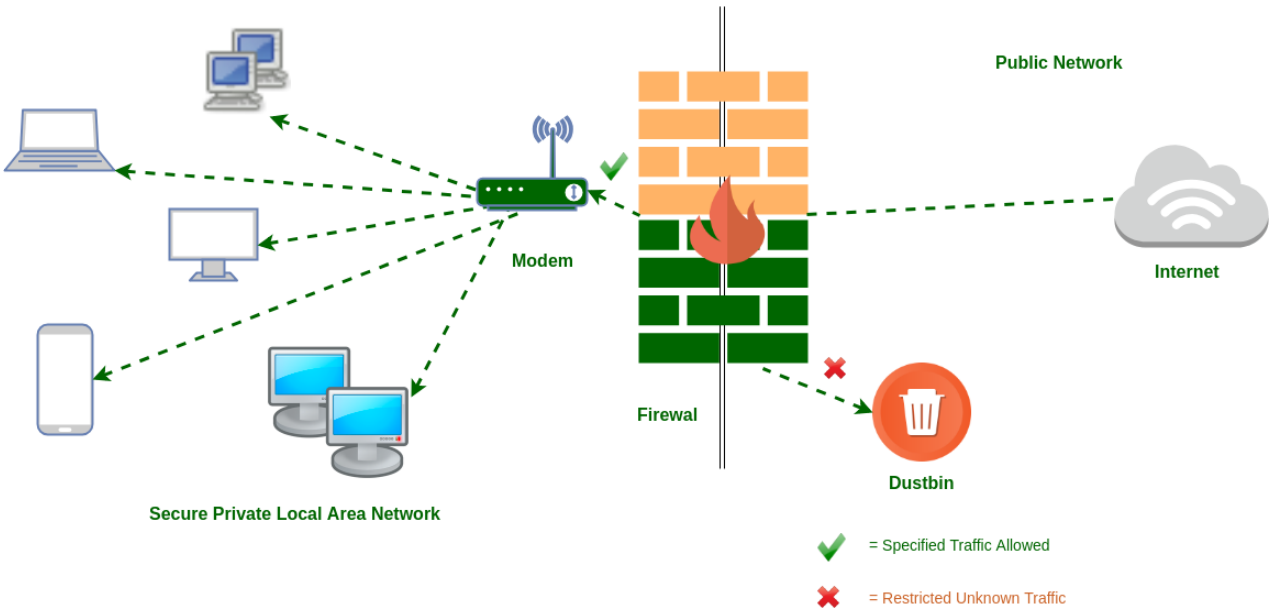
1.1.1.2, 1.0.0.2 – з блокуванням шкідливих сайтів;

1.1.1.3, 1.0.0.3 – з блокуванням шкідливих сайтів та дорослого контенту.

https://1.1.1.1/family/.

5.3.5. Мережевий екран (firewall, міжмережевий екран або мережевий екран, брандмауер) – комплекс апаратних чи програмних засобів, що здійснює контроль і фільтрацію мережевих пакетів, які проходять через нього, відповідно до заданих правил. Термін походить від англійського слова «firewall» – протипожежна стіна, яка перешкоджає поширенню вогню.

Основним завданням мережевого екрану є захист комп'ютерних мереж або окремих вузлів від несанкціонованого доступу. Також мережеві екрани часто називають фільтрами, оскільки їх основне завдання – не пропускати (фільтрувати) пакети, що не задовольняють критерії, які визначені в конфігурації.



Деякі мережеві екрани також дозволяють здійснювати трансляцію адрес – динамічну заміну внутрішньомережевих (сірих) адрес або портів на зовнішні, які використовуються за межами локальних мереж.

Мережеві екрани поділяються на різні типи залежно від таких характеристик:

- чи забезпечує екран з'єднання між одним вузлом і мережею або між двома та більше різними мережами;
- на рівні яких мережевих протоколів відбувається контроль потоку даних;
- чи відслідковується стан активних з'єднань.

Залежно від рівня, на якому відбувається контроль доступу, існує поділ на мережеві екрани, що працюють на:

- мережевому рівні, коли фільтрація відбувається на основі адрес відправника і одержувача пакетів, номерів портів транспортного рівня моделі OSI та статичних правил, заданих адміністратором;
- сеансовом рівні (також відомі як stateful) – відстежують сеанси між додатками, не пропускають пакети, які порушують специфікації TCP/IP, та часто використовуються у зловмисних операціях – скануванні ресурсів, зломи через неправильні реалізації TCP/IP, обриви/уповільнення з'єднань, ін'єкції даних.
- рівні додатків, фільтрація на підставі аналізу даних програми, переданих всередині пакету. Такі типи екранів дозволяють блокувати передачу небажаної і потенційно небезпечної інформації на підставі політик та налаштувань.

Мережеві екрани з фільтрацією пакетів являють собою маршрутизатори або працюють на сервері програми, сконфігуровані таким чином, щоб фільтрувати вхідні та вихідні пакети. Тому такі екрани називають іноді пакетними фільтрами. Фільтрація здійснюється шляхом аналізу IP-адреси джерела і приймача, а також портів вхідних TCP- та UDP-пакетів і порівнянням їх із сконфігурованою таблицею правил. Ці мережеві екрани прості у

використанні, дешеві, надають мінімальний вплив на продуктивність обчислювальної системи. Основним недоліком є їх вразливість при підміні адрес IP. Крім того, вони складні при конфігуруванні: для їх установки потрібно знання мережевих, транспортних і прикладних протоколів.

Шлюзи сеансового рівня контролюють допустимість сеансу зв'язку. Вони стежать за підтвердженням зв'язку між авторизованим клієнтом і зовнішнім хостом (і навпаки), визначаючи, чи є запитуваний сеанс зв'язку допустимим. При фільтрації пакетів шлюз сеансового рівня грунтується на інформації, що міститься в заголовках пакетів сеансового рівня протоколу TCP, тобто функціонує на два рівні вище, ніж мережевий екран з фільтрацією пакетів. Окрім того, зазначені системи зазвичай мають функцію трансляції мережевих адрес, яка приховує внутрішні IP-адреси, тим самим, виключаючи підміну IP-адреси. Однак у таких мережевих екранах відсутній контроль вмісту пакетів, що генеруються різними службами. Для виключення зазначеного недоліку застосовуються шлюзи прикладного рівня.

Шлюзи прикладного рівня перевіряють вміст кожного пакету, який проходить через шлюз пакета і можуть фільтрувати окремі види команд або інформації в протоколах прикладного рівня. Це більш досконалий і надійний тип мережевого екрану, що використовує програми-посередники (proxies) прикладного рівня або агенти. Агенти складаються для конкретних служб мережі Інтернет (HTTP, FTP, тощо) і служать для перевірки мережевих пакетів на наявність достовірних даних.

Шлюзи прикладного рівня знижують рівень продуктивності системи через повторну обробку в програмі-посереднику. Це непомітно при роботі в Інтернеті по низькошвидкісних каналах, але істотно при роботі у внутрішній мережі.

Мережеві екрани експертного рівня поєднують у собі елементи всіх трьох описаних вище категорій. Як і мережеві екрани з фільтрацією пакетів, вони працюють на мережному рівні моделі OSI, фільтруючи вхідні та вихідні пакети на основі перевірки IP-адрес і номерів портів. Мережеві екрани експертного

рівня також виконують функції шлюзу сеансового рівня, визначаючи, чи відносяться пакети до відповідного сеансу. І, нарешті, брандмауери експертного рівня беруть на себе функції шлюзу прикладного рівня, оцінюючи вміст кожного пакета у відповідності з політикою безпеки, виробленої в конкретній організації.

Зручність firewall полягає також у можливості вести журнал мережевих підключень, що дасть повну картину використання Інтернет трафіку. Після перегляду журналу, спеціаліст або сам користувач зможе побачити всі запити, що надійшли з мережі або виходять від комп'ютера, і при необхідності дізнатися, з якої адреси була здійснена хакерська атака або підозріла мережева активність.

Мережевий екран не може запобігти вірусам, які поширюються електронною поштою та фішинговому шахрайству.

5.3.6. Бездротові мережі Wi-Fi (wireless fidelity, бездротова точність / відданість). При роботі з громадськими Wi-Fi мережами на ПК, планшетах чи смартфонах доцільно дотримуватися наступних правил.

1) Не обмінюйтесь конфіденційною інформацією. Намагайтеся не використовувати відкритий Wi-Fi для перегляду електронної пошти, входу в облікові записи, здійснення операцій в онлайн-банкінгу, відправки документів чи будь-яких інших конфіденційних даних. Усі важливі операції варто здійснювати з дому, або будь-якої іншої довіреної точки доступу, яку захищено складним та унікальним паролем та брандмауером.

2) вибирайте мережу вручну. Переконайтеся, що ваш пристрій налаштовано на вибір Wi-Fi вручну, а не на автоматичне підключення. Якщо ви вже використовували певну точку доступу раніше, ваш пристрій може автоматично підключитися до неї. Саме тому для відкритих Wi-Fi варто використовувати функцію «Забути мережу» – це дозволить уникнути непомітного для користувача підключення до Інтернету.

3) використовуйте VPN.

4) використовуйте додаткові інструменти захисту. Наприклад, Tor, VPN та DoNotTrack.

5) Увімкніть двофакторну аутентифікацію для всіх облікових записів, де це можливо. Цей крок додає ще один рівень безпеки, тому, якщо навіть зловмисники матимуть логін та пароль, дані користувача будуть захищені від несанкціонованого доступу.

6) Завершуйте активні сеанси в облікових записах. Спеціалісти рекомендують під час доступу до відкритих Wi-Fi завжди виходити з акаунтів, щоб уникнути їх компрометації. Крім цього, використовуйте функцію «Переглянути активні сеанси», яка доступна у більшості месенджерів та Інтернет-спільнот. Вона дозволяє перевірити де, коли та з яких пристроїв здійснювався вхід до вашого облікового запису.

7) вимикайте підключення до Інтернету, якщо він не використовується. Якщо ви вже виконали всі необхідні дії в Інтернеті та підключення до відкритого Wi-Fi вам більше не потрібне, просто вимкніть його. Це забезпечить захист від несанкціонованого доступу зловмисників. Чим довше ви будете підключені до відкритої мережі, тим більша імовірність того, що кіберзлочинці намагатимуться отримати доступ до ваших даних.

При розгортанні домашньої мережі Wi-Fi варто дотримуватися наступних порад.

1) Встановіть унікальний пароль для вашого облікового запису адміністратора Wi-Fi та маршрутизатора. Не залишайте маршрутизатор з паролями Wi-Fi та адміністратора, які встановлені за замовчуванням. Хакери постійно намагаються прорватися на пристрої, використовуючи ці загальновідомі облікові дані. Також корисно регулярно змінювати пароль.

2) Постійно оновлюйте прошивку. Маршрутизатор з автоматичними оновленнями – найкращий варіант, але потрібно переконатися, що ви їх включили.

3) Створіть гостьову мережу. Гостьова мережа достатньо ізольована від домашньої локальної мережі, відвідувачі отримують доступ до Інтернету без

можливості потрапити у ваші приватні дані. ви можете додатково приховати домашній Wi-Fi SSID, підключивши до домашньої мережі лише надійні пристрої та періодично перевіряючи наявність нових підключених пристроїв, щоб запобігти несанкціонованому доступу.

4) вимкнути функції WPS та UPnP. Деякі маршрутизатори Wi-Fi мають кнопку сполучення (кнопку WPS) для полегшення з'єднання, оскільки вона дозволяє уникнути вводу паролю, щоб додати нові пристрої до мережі. Але цю функцію можна використати для отримання доступу до вашої домашньої мережі. UPnP (Universal Plug and Play) призначена для полегшення підключення пристроїв без складної конфігурації – таких як смарт-телевізори. Але деякі шкідливі програми спрямовані на UPnP, щоб отримати доступ до вашої домашньої мережі.

5) Встановлення MAC-фільтрів. Щоб зробити вашу мережу ще більш безпечною, ви можете встановити режим фільтрації MAC-адрес – дозволити підключатися лише домашнім гаджетам. MAC-адресу кожного пристрою з мережним адаптером можна подивитися в його налаштуваннях. Також в розділі MAC-фільтрів вашого маршрутизатора можна заборонити доступ певних пристроїв. Це стане в нагоді, якщо ви, наприклад, давали тимчасовий доступ гостю або сусідові, але далі не хочете, щоб він використовував вашу мережу.

6) Оберіть безпечний маршрутизатор. Підчас розгортання мережі Wi-Fi ви можете стикнутися з декількома варіантами безпеки роутера. Нижче наведено список протоколів, які ранжовані за ступенем безпеки (вгорі – найбезпечніші):

WPA3,

WPA2 Enterprise,

WPA2 Personal WPA + AES,

WPA + TKIP,

WEP,

Open Network (no security implemented).

Системи, які все ще використовують WEP, не є безпечними. Для покращення функцій WEP у 2003 році було створено протокол Wi-Fi Protected Access або WPA. Цей покращений протокол, як і раніше, мав відносно низьку безпеку, але його легше було налаштувати. WPA, на відміну від WEP, використовує протокол Temporary Key Integrity Protocol (TKIP) для безпечнішого шифрування. Оскільки Wi-Fi Alliance зробив перехід із WEP на більш просунутий протокол WPA, вони мали зберегти деякі елементи WEP, щоб старі пристрої все ще були сумісні. На жаль, це означає, що такі вразливості, як функція налаштування WiFi Protected, яку можна зламати відносно легко, ще присутні в оновленій версії WPA.

Роком пізніше, в 2004 році, стала доступна нова версія протоколу Wi-Fi Protected Access 2. WPA2 має більш високий рівень безпеки, а також він простіше налаштовується в порівнянні з попередніми версіями. Основна відмінність WPA2 полягає в тому, що він використовує покращений стандарт шифрування Advanced Encryption Standard (AES) замість TKIP. Єдина помітна вразливість WPA2 полягає в тому, що за умови отримання доступу до мережі, зловмисник може атакувати інші пристрої, підключені до цієї мережі.