# 8.2. Рівні мережі Вебу

Глобальну мережу умовно можна розподілити на три рівні (рис.1):

**Поверхневий або видимий (Surface Web).** Сюди відносять загальнодоступні, відкриті веб-ресурси. Це сайти, які можна відвідати за стандартним посиланням і знайти в пошукових системах.

**Глибокий (Deep Web).** Містить контент, який не потрапляє в пошукові системи. Вміст приватних хмарних сховищ, корпоративних мереж і різних закритих баз даних - все це глибокий інтернет. Найчастіше доступ до таких ресурсів захищений логіном і паролем.

**Темний (Dark Web), тіньова мережа (Darknet).** Це збірна назва комп'ютерних мереж, призначених для анонімної передачі інформації. Там є сервіси для торгівлі, спілкування та обміну контентом, але їх не можна відкрити через стандартний браузер або знайти в звичайній пошуковій системі.

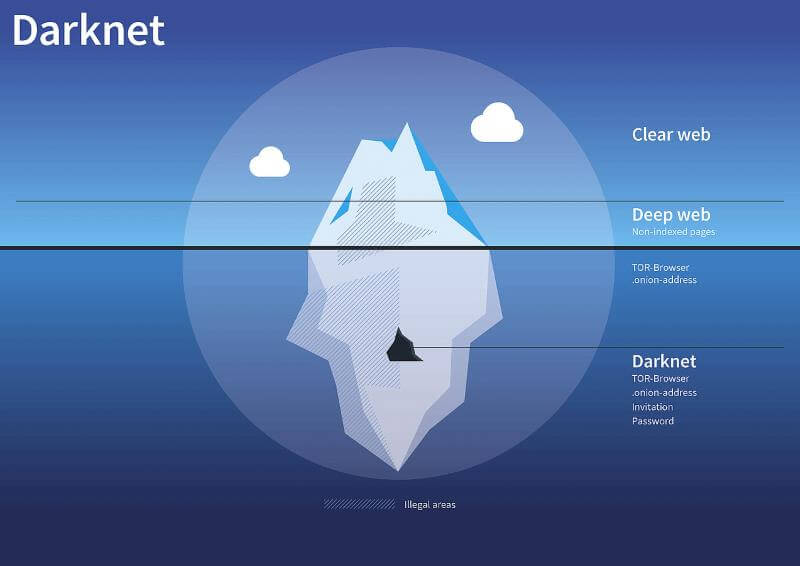


Рис.1. Рівні Інтернету

## Surface Web і Deep Web

Для наочності можна уявити Інтернет як велике місто, в якому є відкриті громадські простори - вулиці, бульвари, парки. Вони нанесені на карту, по ним можна пройтися і легко знайти потрібну будівлю.

В Інтернеті такі «громадські» місця називаються Surface Web (видима мережа). Це веб-сторінки, документи, мультимедійні файли, веб-додатки та інші матеріали, які спокійно індексують пошукові боти. Ці ресурси може знайти та переглянути будь-який користувач - безкоштовно, без реєстрації та без встановлення спеціальних програм.

Окрім громадських, в місті є приватні зони, куди без пропуску, квитка або запрошення потрапити не можна. Це можуть бути бізнес-центри, закриті клуби, кінотеатри, будинки і квартири жителів, внутрішні дворики. В Мережі теж є маса подібних місць, в які не заглядають пошукові боти - разом такі простори називаються Deep Web (глибока або невидима мережа). Сюди в першу чергу відносяться всі сторінки в Інтернеті, які не можна відкрити без виконання певних умов.

Deep Web це прихований інтернет. Це весь контент, який не індексується в пошукових системах, тому не може бути легко доступним. Він також представляє більшу частину мережі.

Сюди відноситься приватні сервери та сторінки, певні служби передачі платежів або файли, які зберігаються у хмарі. В цьому випадку немає загрози безпеці, немає контенту, який може бути незаконним чи проблематичним. Це вся частина Інтернету, до якої не можна отримати доступ через пошукові системи.

Цей невидимий Інтернет становить понад 90% від загальної кількості. Важко підрахувати точно, але, він містить весь контент, який зберігається у хмарних сервісах: академічні бази даних, медичні звіти, урядові звіти, репозиторії організацій.

Якщо щось відкрити можна, а знайти - не можна, то це теж Deep Web. Наприклад, якщо користувач зазначив в профілі соцмережі, що хоче приховати його від пошуковиків? Навіть якщо пошуковий бот на нього якимось чином вийде, він змушений буде його проігнорувати. Не зможе пошуковик обробити і контент, який генерується прямо в момент відкривання сторінки і залежить від того, хто саме її відкриває. Наприклад, персоналізовані пропозиції на сайті інтернет-магазину - щоб їх побачити, треба бути користувачем з певними цифровими даними, а боту їх не покажуть.

Також, до Deep Web відноситься весь контент, на який немає жодного посилання з видимої мережі. Пошуковий робот просто не дізнається про існування такого контенту, адже він знаходить нові сторінки, переходячи по посиланнях з вже проіндексованих сторінок.

Основна частина Deep Web - це багато безпечних веб-сторінок і документів, якими користується більшість користувачів, але з певних причин приховані від сторонніх очей.

## Darknet і Dark Web

Як в місті, так і в Інтернеті усамітнення шукають не тільки добропорядні громадяни, а й ті, хто хоче приховати свою не зовсім легальну діяльність. У місті темні справи зазвичай провертають в нетрях і кримінальних кублах. Для них вибирають місця, куди просто так не заблукаєш та їх не відзначають на загальнодоступних картах. Адреси та явки кожного кубла відомі лише обмеженому колу осіб. Хоча звичайні люди знають, що десь вони точно існують.

Приблизно так само працюють Darknet (темні або тіньові мережі) - конспіративні мережі різних «угруповань». Вузли кожного окремо взятого даркнету - сервери, комп'ютери, роутери - невидимі не лише для пошуковиків, але і для більшості браузерів, оскільки для передачі даних всередині таких мереж використовуються нестандартні протоколи. Звичайному користувачеві увійти туди не допоможуть ні прямі посилання, ні паролі.

Разом даркнети складають Dark Web (темний веб) - ту частину Deep Web, яка вважається притулком темних особистостей: торговців наркотиками і зброєю, здирників, продавців крадених даних тощо. Багато хто знає, що Dark Web існує, але не всі розуміють, як туди потрапити.

Втім, конспірація буває потрібна не тільки хакерам і посередникам в нелегальних оборудках. Дисиденти, борці за свободу слова або інформатори, які допомагають журналістам в розслідуваннях, можуть ховатися від переслідування в підозрілому районі, а для анонімного спілкування в Мережі користуватися Dark Web. Деякі йдуть в тіньові мережі для того, щоб захиститися від збору даних в Інтернеті. Для цього є більш доступні і безпечні інструменти, але деяким подобається радикальний підхід.

Потрапити в Даркнет можна тільки через протокол TOR. Ця мережа спеціально створювалася прихованою та анонімною, щоб ніхто не зміг встановити цензуру або обмежити діяльність учасників.

Сенс Даркнету в анонімності, але сама мережа не гарантує анонімність автоматично. Щоб її дотримуватись, одного використання TOR-браузера недостатньо. Людина може на форумі залишити певні дані про себе, які можуть розкрити її справжню особу, або завантажити троян, який стежитиме за нею. У цьому плані Даркнет такий самий, як і звичайний інтернет — чим більше користувач викладає даних про себе, тим простіше його виявити.

Зазвичай в Даркнет входять через браузер Tor, тому більшість сайтів у даркнеті перебувають у псевдодомені .onion. Псевдодомен означає, що насправді такого домену в інтернеті немає, але всередині даркнета до них можна звертатися.

Наприклад, якщо ввести адресу http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main\_Page у звичайний браузер, то виведеться помилка, тому що DNS-сервери не знають, як обробляти цей домен. А якщо ввести ту ж адресу в Tor-браузері, з'явиться вікно HiddenWiki - Вікіпедії для Даркнету (рис.2). У ній немає нічого забороненого, вона просто розповідає, куди можна піти, якщо ви вперше зайшли.

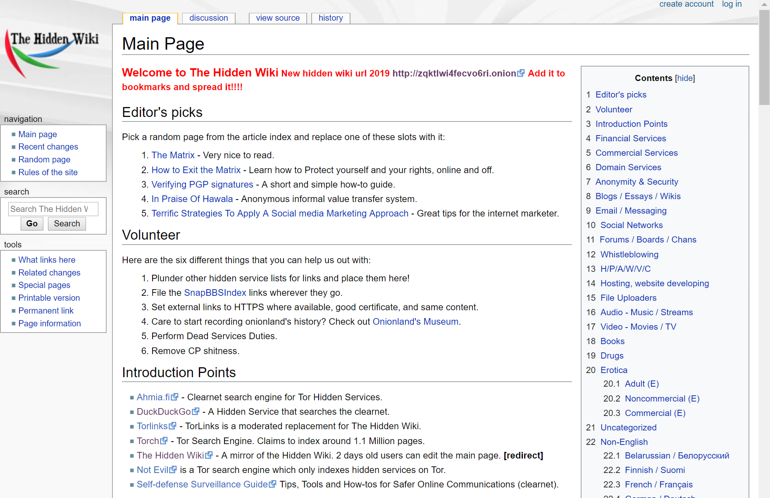


Рис.2. Інтерфейс HiddenWiki

Onion-сайти розміщують зазвичай на віртуальних хостингах, які легко завести або легко змінити, якщо це потрібно для збереження анонімності. З цієї ж причини в даркнеті не працює частина посилань, оскільки хостинги, де розміщувалися ці сайти, закрилися або переїхали на нову адресу. Тому, в даркнеті популярні каталоги посилань - спеціальні тематичні добірки сайтів, з яких вибирають потрібні користувачі. HiddenWiki - теж приклад такого каталогу.

Пошуковики там теж є, але вони працюють не так, як Google. Багато ресурсів приховано від індексації і доступні тільки за прямим посиланням. Приклади пошукових систем - TORCH і Seeks.

### Влаштування Дарнету

Даркнет можна розділити на дві частини: сайти з текстами та форумами без державної цензури та даркнет-магазини з продажу чого завгодно. Торгових сайтів багато, і вони найчастіше пропонують щось незаконне.

### Даркнет і криптовалюта

З 2014 року даркнет виріс у кілька разів завдяки біткоїну та решті криптовалют. До цього механізм оплати всередині був складний, і багатьох це зупиняло. Біткоїн зменшив поріг входу в платний даркнет і зробив його доступним майже кожному.

Тепер майже все, що відбувається всередині даркнету, оплачується криптовалютою. Є навіть окремі крипто-біржі зі спрощеною реєстрацією, щоб залишити якнайменше електронних слідів.

### Даркнет і закон

Може здатися, що даркнет ідеальне місце для злочинців. Але спецслужби також можуть зайти туди. У певному сенсі їм навіть легше: знаючи, що кілери скупчуються на одному сайті, а фінансові шахраї — на іншому. Тому, можна проводити атаки на основі соціальної інженерії, використовувати вразливість сайтів і навіть уразливість TOR.

Якщо зайти в Даркнет з з позиції «подивитися, що там і як влаштовано», то це легально. Але, якщо робити щось, що порушує закон країни, це вже підпадає під адміністративний чи кримінальний кодекс. За продаж наркотиків, купівлю зброї або за розповсюдження забороненого порно в даркнеті можна отримати кримінальне переслідування.

Головне правило даркнету - там немає жодних законів, тому ніхто не може гарантувати анонімність усередині мережі. Все, що людина там робить (як і в звичайному інтернеті), вона робить на свій страх та ризик. Якщо хтось робить щось незаконне та ненавмисно розкриє частину інформації про себе — це може бути використано проти людини. Наприклад, для шантажу чи вимагання грошей.

## Технологія Tor

TOR - це технологія, яка дозволяє з деяким успіхом приховати особистість людини в інтернеті. Розшифровується як The Onion Router - цибулинний маршрутизатор.

TOR спочатку був військовим проектом США, потім його відкрили для спонсорів, на тепер має назву Tor Project. Основна ідея цієї мережі - забезпечити анонімність і безпеку в мережі, де більшість учасників не довіряють один одному. Суть протоколу в тому, що дані проходять через кілька комп'ютерів, шифруються, у них змінюється IP-адреса і утворюється захищений канал передачі даних. Побічним результатом такої технології став даркнет - інтернет всередині інтернету.

### Принцип роботи у TOR

Під’єднання до потрібного ресурсу відбувається через кілька серверів. Зазвичай, в ланцюжку беруть участь три сервера: вхідний, проміжний і вихідний (рис.3).

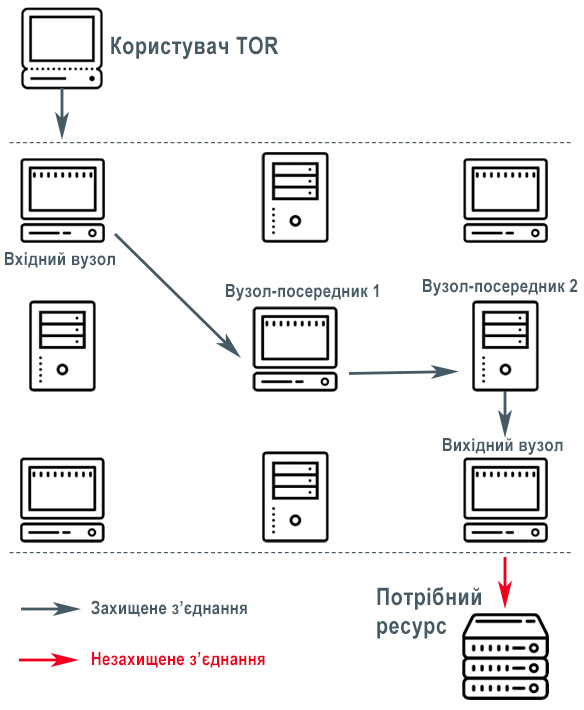


Рис.3. З’єднання в мережі TOR

Перед тим як запит або дані підуть в мережу, спеціальна програма на комп'ютері користувача шифрує їх так, щоб кожен сервер міг розшифрувати лише свою частину. Беруться вихідні дані і шифруються для вхідного вузла, потім те, що вийшло, шифрується для проміжного, і ось це все ще раз шифрується для вихідного вузла (рис.4).

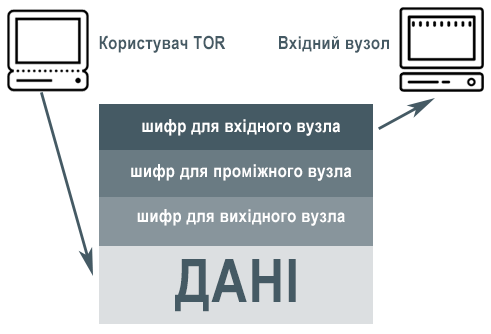


Рис.4. Шифрування даних з боку користувача

Виглядає як цибулина. Звідси і з'явилася назва «цибулинне шифрування», тому що кожен сервер знімає тільки свою частину шифру і передає дані далі по ланцюжку.

### Вузли

Перший вузол - вхідний, через нього користувач входить в мережу TOR. Зазвичай їх вибирають з тих серверів, які довели свою надійність, стабільне і швидке з'єднання. Вхідний вузол отримує «цибулину» з шифрів, розшифровує перший шар і знаходить там адресу, за якою потрібно передати цей пакет далі. Більше він не бачить нічого, оскільки дані всередині зашифровані два рази.

Другий вузол - проміжний. Робить те ж саме, що і перший: знімає свій шар шифру, дізнається, куди надсилати дані, і скеровує все ще секретні дані на вихідний вузол. Проміжні сервери найпростіші в обслуговуванні, оскільки вони просто розшифровують і передають дані. Проміжні сервери не знають, звідки прийшли дані і куди відправляться в самому кінці.

Останній вузол в ланцюжку - вихідний, він найважливіший з усіх. Справа в тому, що він знімає останній шар шифрування і надсилає дані в чистому вигляді за потрібною адресою. Саме його адресу буде видно тому сайту, на який йде запит. Саме до них прийдуть правоохоронні органи, якщо будуть розслідувати злочини, скоєні через TOR.

Від вихідного вузла запит надсилається на потрібний сайт, звідти надходить відповідь, і весь ланцюжок рухається в зворотному напрямку теж з потрійним шифруванням.

Зараз в мережі Tor передачею трафіку займаються близько 8000 маршрутизаторів. Вони розташовані по всьому світу і працюють завдяки добровольцям, які погоджуються віддати частину трафіку для цієї справи. Важливо, що у більшості вузлів немає спеціального заліза або додаткового ПЗ - всі вони працюють за допомогою ПЗ Tor, налаштованого на роботу в якості вузла.

Швидкість і анонімність мережі Tor залежить від кількості вузлів - чим більше, тим краще. І це зрозуміло, оскільки трафік одного вузла обмежений. Чим більше у мережі Tor вузлів, тим складніше відстежити користувача.

Зазвичай, для безпечного інтернет-серфінгу використовують Tor Browser - офіційний браузер від розробників цієї мережі. У ньому прописані всі налаштування, які потрібні для підключення до мережі, але для повної приватності потрібно буде самому додати частину розширень, наприклад, NoScript. Він відключає всі скрипти, через які можна обчислити справжню адресу користувача.

### Вразливості Tor

Незважаючи на потрійне шифрування, у TOR є декілька вразливостей, про які потрібно знати.

Прослуховування на вихідному вузлу. Через вихідний вузол трафік йде в мережу в чистому вигляді, тому, деякі власники таких вузлів можуть там щось прочитати. Наприклад, логін і пароль від інтернет-магазину, пошти або текст листування, якщо повідомлення не шифрується. SSL-шифрування теж не врятує, вже є програми, які його розшифровують.

### SSL-сертифікати і безпечний інтернет

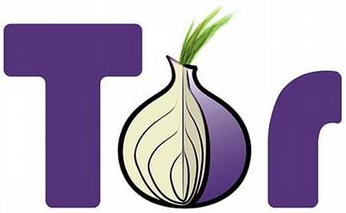
Щоб захиститися від таких витоків, слід використовувати сайти, які підтримують HTTPS-протокол: він шифрує всі дані і захищає від прослуховування. Використовувати месенджери і поштові клієнти з вбудованим шифруванням - це теж допоможе захистити повідомлення.

* **Глобальне спостереження.** Теоретично можлива ситуація, коли хтось просто спостерігає зсередини за мережею і за тим, як проходить трафік. Якщо спостерігати досить довго за тими, хто сидить на одному і тому ж каналі і не змінює ланцюжок вузлів, то можна обчислити його справжню IP-адресу. У лабораторних умовах на це йде близько двох годин.
* **Блокування провайдером.** У деяких країнах заборонено використовувати TOR, тому провайдери знаходять все вхідні вузли і блокують їх. Тому, розробники мережі придумали рішення для цих ситуацій - частину вхідних вузлів зроблено секретними і не публікуються в загальному доступі. Коли програма намагається встановити TOR-з'єднання і бачить, що вузли зі списку заблоковані, вона робить спеціальний запит і отримує адресу секретного вузла. Але цей запит провайдер теж може зробити.
* **Інформаційна гігієна.** Якщо вийти в інтернет через TOR і зайти в соцмережу під своїм логіном (або пошту, або на форум, де точно відомий власник), то ступінь анонімності різко зменшується. Фахівці зможуть встановити вашу особистість і на інших сайтах.

### Покращення безпеки TOR

Головна проблема TOR - вихідні вузли і відкритий трафік. Щоб забезпечити потрібний рівень безпеки, використовують зв'язку TOR + VPN.

## Браузер Tor і захист анонімності в Інтернеті

Браузер Tor - безкоштовна, відкрита і некомерційна програма, яка надає користувачам анонімний доступ в інтернет. Основна ідея проекту - просувати права людини, забезпечуючи вільний і безпечний доступ до Мережі. Для звичайних користувачів - це спосіб захистити себе і свій трафік не лише від влади, але і від провайдерів, власників публічних WiFi-точок і сайтів, наприклад, а також спосіб обійти блокування деяких сайтів.

Якщо стежити за користувачем або його трафіком (провайдер, урядові органи чи спецслужби), можна дізнатися, що користувач користується браузером Tor, але не те, з якою метою. Кожен раз користувач потрапляє в інтернет за допомогою випадкового комп'ютера-волонтера, а сам браузер за замовчуванням не зберігає історію його дій, тому, в інтернеті ніхто не дізнається, ким є користувач і не зможе отримати інформацію про нього.

### Відмінності між Tor і VPN

В роботі Tor забезпечується анонімність, а в роботі VPN - приватність. Тобто, Tor захищає інформацію про користувача, а VPN - дані про те, чим він займається в інтернеті. Tor краще використовувати для анонімного відвідування інтернету і спілкування. VPN більше підходить для обходу блокування і цензури в інтернеті, за умови, що анонімність для користувача не так важлива.

Через структуру шифрування даних браузер Tor уповільнює швидкість інтернет-з'єднання. Браузер не зможе захистити користувача, якщо він сам видає інформацію про себе в інтернеті (обліковий запис в соцмережах, оплата в інтернет магазині за допомогою карти) або якщо на комп'ютері користувача є віруси або програми, які стежать за його діяльністю.

Нарешті, Tor НЕ нелегальний, але його анонімністю нерідко користуються злочинці. Оскільки провайдер, швидше за все, буде знати, що користувач користується браузером Tor, він може привернути на це увагу влади.

Tor не ідеальний. Але при правильному і акуратному використанні, він може забезпечити анонімність користувача в інтернеті

Найпростішим способом для перегляду даркнету, що містить сайти Tor є використання плагіну Tor Browser (<https://addons.mozilla.org/uk/firefox/addon/tortm-browser-button/>) для браузера Mozilla Firefox.

Використання Tor Browser дозволяє приховати місце знаходження користувача, IP-адресу та інші ідентифікаційні дані від звичайних веб-сайтів. Раніше, щоб підключитися до Tor потрібні були спеціальні знання, які були складними для пересічного користувача, натепер складнощі підключення обмежуються лише установкою плагіну Tor Browser до браузера Mozilla Firefox (рис.5).

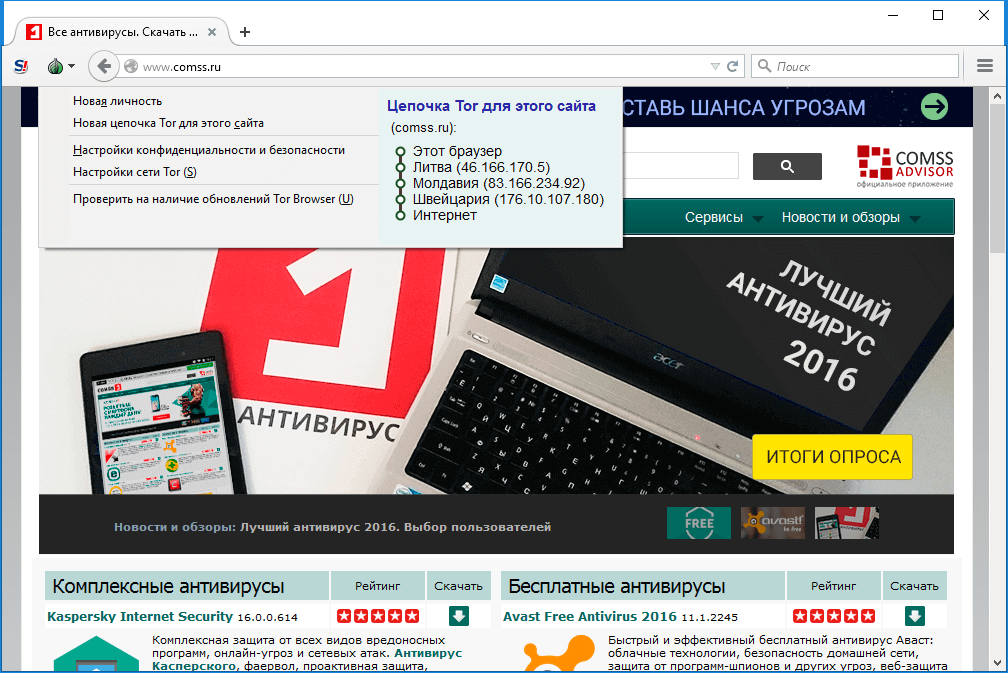


Рис.5. Плагін Tor в браузері Mozilla Firefox

Tor з'явився не тільки в результаті зусиль групи хакерів. Tor був ключовою технологією, що розроблена американською військово-морською дослідницькою лабораторією спільно з агентством передових оборонних дослідницьких проектів. Будучи некомерційним проектом, Tor отримує значні пожертви від різних федеральних суб'єктів, зокрема від національного наукового фонду США. На сайті проекту є окрема сторінка зі списком прикладів легітимного використання Tor, наприклад, політичними дисидентами в країнах з жорстким контролем над інтернетом і звичайними громадянами, які піклуються про конфіденційність в мережі.

Tor НЕ буде зашифровувати дані користувача - для цього потрібно використовувати віртуальну приватну мережу VPN. Tor скеровує трафік через серію проміжних мережних вузлів. Цей підхід значно ускладнює спроби відстеження з боку урядових чи спецслужб. Використання Tor забезпечує якісно новий рівень приватності, значно більший, ніж при застосуванні режиму приватного перегляду в звичайному браузері. При використанні режиму приватного перегляду в звичайних браузерах, по закінченні сесії видаляється кеш та історія переглядів. Режим приватного перегляду не приховує реальну IP-адресу від відвідуваних веб-сайтів, хоча запобігає спробам стеження через куки.

Підключення до мережі Tor вимагає більше дій, ніж установка браузера і перехід до сайтів. Спочатку потрібно отримати код підтримки, але Tor Browser значно спрощує цей процес. Файли доступні для ОС Windows, Mac і Linux. Проект Tor рекомендує встановлювати браузер на переносний USB-носій для більшої анонімності і портативності. Для цього на флешці потрібно виділити 80 мегабайт.

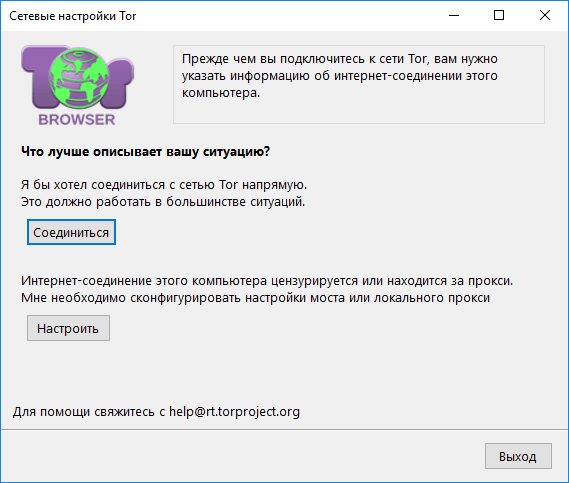


Рис.6. Мережні налаштування мережі Tor

Перед тим, як користуватися анонімним з'єднанням, потрібно повідомити Tor детальну інформацію про Інтернет-підключення. Якщо підключення цензорується або знаходиться за проксі, потрібно вибрати окрему опцію, в іншому випадку можна підключитися до мережі Tor безпосередньо. Після підключення до мережі Tor, браузер завантажується, і можна побачити сторінку проекту Tor (рис.7).

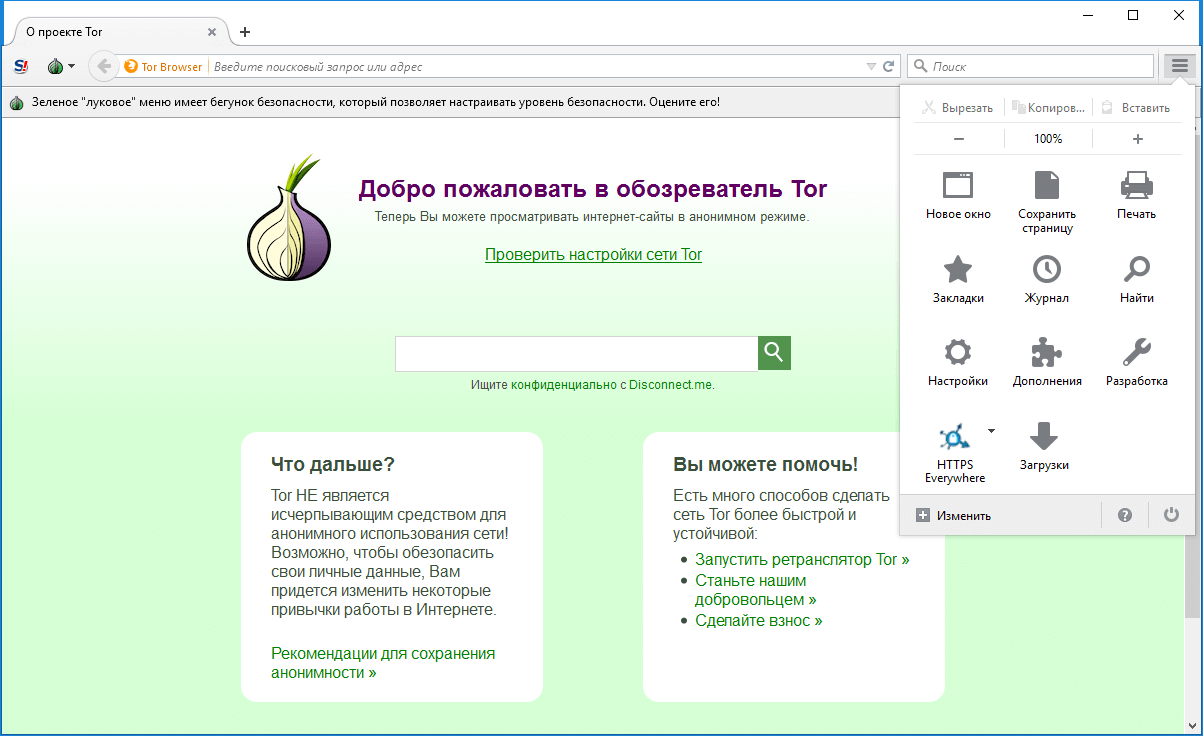


Рис.7. Домашня сторінка браузера Tor

На домашній сторінці браузера міститься заклик до фінансової підтримки проекту, пошуковий рядок анонімної системи Disconnect.me і посилання для перевірки налаштувань мережі Tor. При натисканні на посилання завантажується сторінка, яка повідомляє про успішний перехід на анонімне з'єднання. Рекомендується виконувати цю перевірку. Показана IP-адреса – жодним чином не пов'язана з фактичною IP-адресою, це адреса мережного вузла Tor.

Інтерфейс браузера практично не відрізняється від Firefox, за винятком кількох встановлених плагінів. Розширення NoScript, що часто використовується в Firefox, встановлено і може застосовуватися для блокування різних скриптів та іншого, що не відноситься до HTML контенту. Зелена кнопка із зображенням цибулини ліворуч адресного рядка є плагіном Torbutton. Кнопка дозволяє побачити налаштування мережі Tor, а також використаний ланцюжок серверів Tor перед доступом до даркнету.

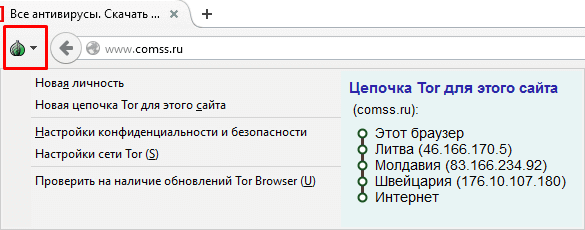


Рис.8. Ланцюг з’єднань Tor

Якщо користувача не влаштовує поточний ланцюжок, можна запросити новий, або для поточної сесії, або для поточного сайту. Це одна з найбільш затребуваних особливостей браузера.

Tor Browser значно спрощує користування існуючими інструментами безпеки та приватності. Наприклад, NoScript складний в налаштуванні і може викликати проблеми з працездатністю сайтів. Однак, панель налаштувань конфіденційності та безпеки, що викликається після натискання Torbutton, представляє лише необхідні налаштування. На низькому рівні всі функції браузера включені. На високому рівні безпеки, всі скрипти JavaScript і деякі зображення блокуються. Це дозволяє налаштувати необхідний рівень безпеки без детального налаштування окремих опцій у вікнах конфігурації (рис.9).

Чому потрібно відключати JavaScript при використанні Tor Browser? Шпигуни можуть зламати JavaScript за допомогою шкідливих скриптів і розкрити особу користувача в Tor. Якщо реальна IP-адреса буде розкрита, інтернет-провайдер зможе повідомити відповідні служби про це, якщо запідозрить здійснення нелегальної онлайн-активності.

Однак не потрібно повністю вимикати JavaScript, адже в такому випадку багато сайтів не будуть працювати: контент не буде завантажуватися або його неможливо буде використовувати.

Можна вибирати, на яких сайтах вимикати JavaScript. Якщо сторінки не заслуговують довіри, JavaScript відключають, щоб не ставити під загрозу безпеку. Для надійних сайтів на кшталт Google чи Reddit можна залишити модуль включеним.

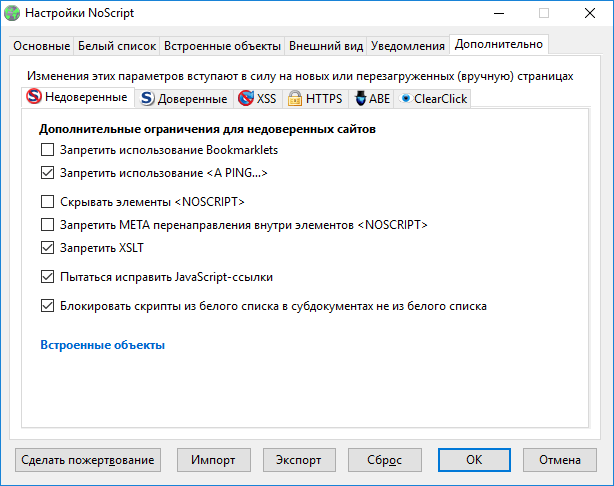


Рис.9. Відключення підтримки JavaScript

Все, що користувач робить в браузері, тестується на анонімність: при спробі перемкнути браузер в повноекранний режим з'являється повідомлення "Відкриття браузера на максимальну величину може дозволити веб-сайтам визначити роздільність вашого монітора. Ми рекомендуємо залишати вікно браузера в первісному вигляді ".

Сайт проекту Tor повідомляє, що використання виключно Tor не гарантує повної анонімності, користувачі повинні дотримуватись правил безпечної перегляду: не використовувати BitTorrent, не встановлювати додаткові розширення, не відкривати документи чи мультимедійні файли, будучи підключеним до мережі. Рекомендації відвідувати лише захищені протоколом HTTPS сайти втратила актуальність завдяки вбудованому плагіну HTTPS Everywhere.

Багато сайтів запитують введення CAPTCHA при використанні браузера Tor. Це пов'язано з тим, що замасковані адреси виглядають підозріло для служб безпеки.

Можна використовувати Tor для анонімного перегляду звичайних сайтів, але існує ціла мережа прихованих сайтів, які взагалі не з'являються в публічному Інтернеті і є видимими лише за допомогою підключення Tor. Якщо використовувати стандартну пошукову систему, наприклад, анонімну Disconnect.me, можна побачити тільки стандартні сайти.

Конфіденційність можна покращити, якщо використовувати анонімні пошукові системи:

* DuckDuckGo (https://duckduckgo.com/)
* Startpage.com (<https://www.startpage.com/>)
* Ahmia (<https://ahmia.fi/>)
* Sinbad Search

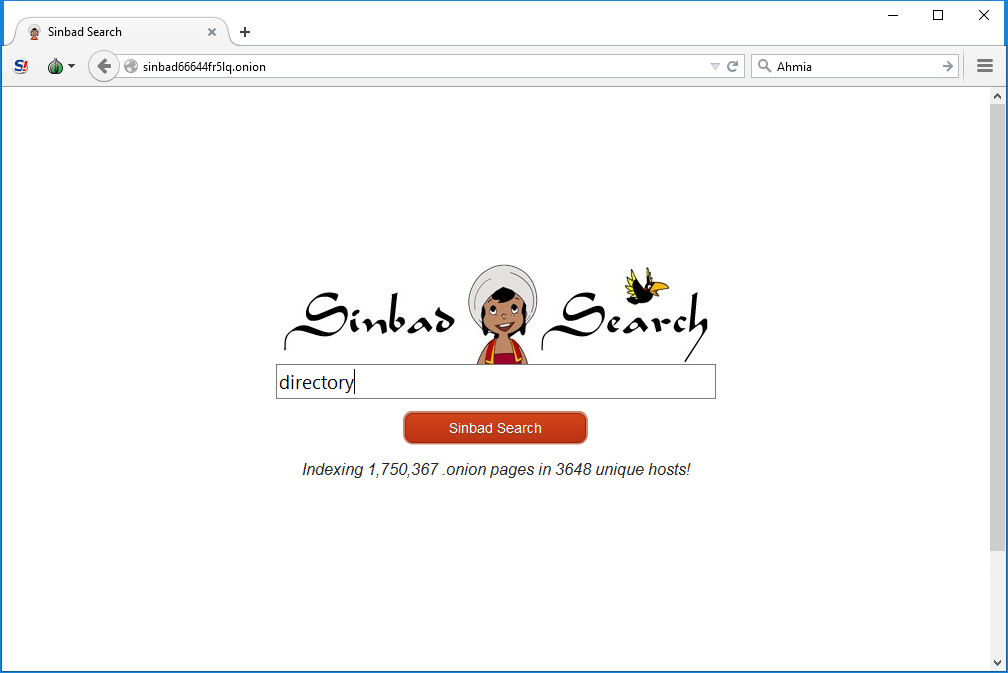


Рис.10. Пошукова система Sinbad Search

Адреси прихованих сайтів Tor закінчуються на .onion, а перед цим використовується 16 букв і цифр. Можна знайти директорії прихованих сайтів в категоріях, які дуже нагадують стару версію Yahoo.

Є також директорія Tor Links, яка містить інші категорії. Тут можна знайти велику кількість чатів і дошок оголошень, аудіофайли, зламані гри, фінансові сервіси, наприклад, анонімний клієнт біткоїна, і навіть Tor-версію Facebook.

Багато сайтів onion працюють дуже повільно або взагалі непрацездатні, оскільки ними не займаються великі компанії. Часто доводиться натискати посилання onion, щоб побачити повідомлення "Не вдається підключитися". Sinbad виводить червоний маркер "офлайн при останній спробі", що означає, що сайт може не функціонувати.

Швидкість завантаження веб-сторінки в Tor, як правило, значно повільніше, ніж при серфінгу зі стандартним підключенням. Неможливо визначити точно, наскільки зменшиться швидкість завантаження при використанні Tor, оскільки ця величина залежить від великої кількості факторів і завжди буде різною через використання різного ланцюжка серверів при кожному новому підключенні. Час завантаження може мінятися кожен раз для кожної сесії браузера (рис.11).

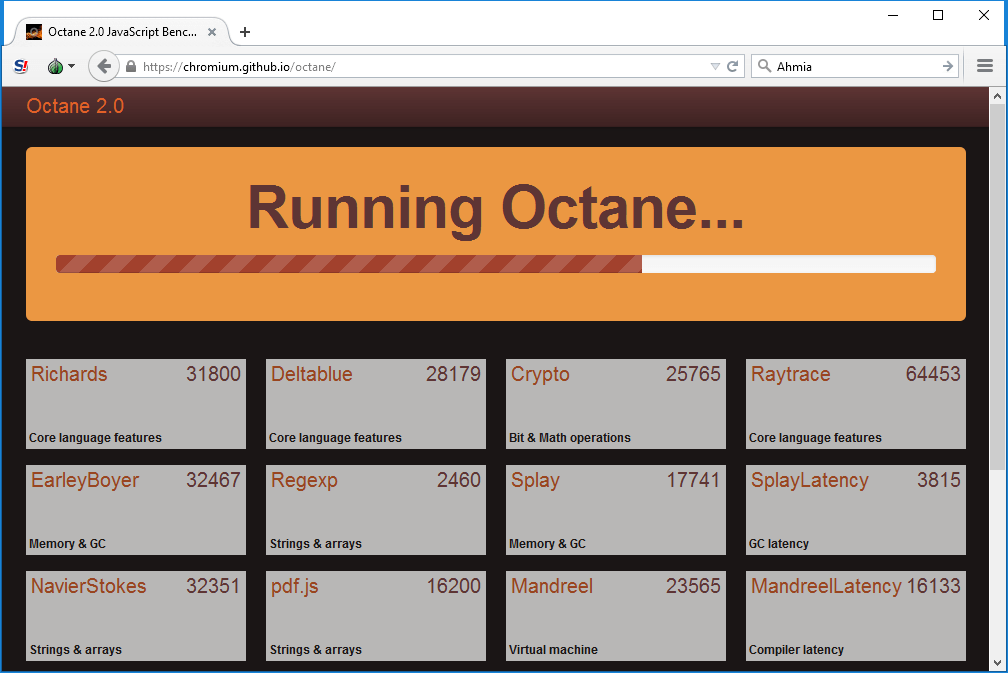


Рис. Завантаження ресурсу через мережу Tor

Tor стає необхідним інструментом за часів практично повної відсутності приватності в Інтернеті. Продукт дозволяє відвідувати сайти з упевненістю того, що певні сервіси не дивляться за кожним кроком, наприклад поява відповідної реклами.

Звичайно, за анонімність в Tor Browser буде падіння швидкості роботи на час для детальної настройки конфіденційності та безпеки.

#### Переваги

* Просте підключення до анонімної мережі Tor.
* Простий інтерфейс для складних інструментів безпеки.
* Простота налаштування.
* Сумісний з сучасними стандартами, функціонально насичений браузер.
* Вбудовані інструменти конфіденційності.

#### Недоліки

* Падіння швидкості завантаження сторінок.
* Ускладнений пошук сайтів на рідній мові.
* Плагін NoScript та інші інструмент приватності можуть викликати труднощі у початківців.

## Контрольні запитання

1. Перелічити основні рівні мережі Інтернет.
2. Які ресурси можна віднести до рівня DeepWeb?
3. Які ресурси знаходяться в DarkWeb?
4. Що таке Onion-сайти? Як можна до них доступитися?
5. Особливості технології Tor

## Літературні джерела

1. Deep web, dark web, darknet и surface web <https://www.kaspersky.ru/blog/deep-web-dark-web-darknet-surface-web-difference/30044/>
2. Що таке даркнет <https://thecode.media/darknet/>
3. Захист від хакерів и спецслужб <https://www.dw.com/ru/zashhita-ot-hakerov-i-specsluzhb-brauzer-tor-stanovitsja-vse-bezopasnee/a-58051150>
4. Використання Tor Browser <https://ru.wizcase.com/blog/руководство-tor-browser/>
5. Що таке TOR <https://thecode.media/tor/>
6. Як працює Tor <https://habr.com/ru/post/357128/>
7. Tor браузер <https://vps.ua/blog/how-to-use-tor-browser/>
8. Огляд Tor Browser <https://www.comss.ru/page.php?id=2860>
9. Tor захищає анонімність в Інтернеті <https://www.currenttime.tv/a/chto-takoe-tor/31169166.html>
10. DarkNet – які загрози живуть в тіні <https://stakhanovets.ru/blog/darknet-kakie-ugrozy-zhivut-v-teni-chast-1/>