# 10.1. Рівні служби Web

В Інтернеті співіснують різні рівні служби Веб, які відрізняються за доступністю та вмістом (рис.1).

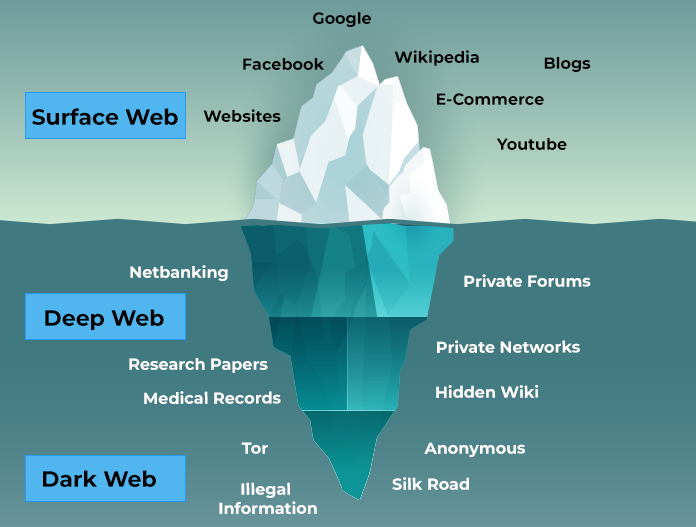


Рис.1. Рівні Інтернету

**Поверхневий або видимий (Surface Web).** Відноситься до видимої та легкодоступної частини Інтернету, яку можна індексувати та здійснювати пошук звичайними пошуковими системами. Він містить загальнодоступні сайти та веб-додатки, до яких можна отримати доступ без спеціальних інструментів чи дозволів. Прикладами Surface Web є загальнодоступні сайти.

**Глибокий (Deep Web).** Відноситься до частини Інтернету, яка не індексується пошуковими системами та не є легкодоступною для широкої громадськості. До глибокого вебу можна віднести веб-сторінки, які вимагають аутентифікації, наприклад приватні облікові записи електронної пошти, портали онлайн-банкінгу, вміст приватних хмарних сховищ, корпоративних мереж і різних закритих баз даних. Deep Web асоціюється з приватною або конфіденційною інформацією, яка не призначена для загального використання, доступ до якої захищений логіном і паролем.

**Темний (Dark Web), тіньова мережа (Darknet).** Невелика частина Deep Web, яка навмисно прихована та потребує спеціального програмного забезпечення для доступу, наприклад, браузер Tor (The Onion Router),. Він відомий своїми функціями анонімності та шифрування, що ускладнює відстеження користувачів та їхню діяльність.

Dark Web часто асоціюється з незаконною діяльністю, такою як продаж наркотиків, зброї, викрадених даних, хакерських послуг та інших незаконних товарів і послуг. Однак важливо зазначити, що не всі дії в Dark Web є незаконними, і існують законні випадки використання анонімного спілкування та конфіденційності.

Важливо розуміти, що доступ і участь у незаконній діяльності в Dark Web суперечить закону в багатьох юрисдикціях. Під час користування Інтернетом завжди рекомендується дотримуватись законів і правил країни проживання.

## 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: бази даних, медичні звіти, урядові звіти, репозиторії організацій.

Якщо щось відкрити можна, а знайти - не можна, то це теж Deep Web. Наприклад, пошуковик не зможе обробити 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). В ній немає нічого забороненого, вона просто розповідає, куди можна піти, якщо ви вперше зайшли.

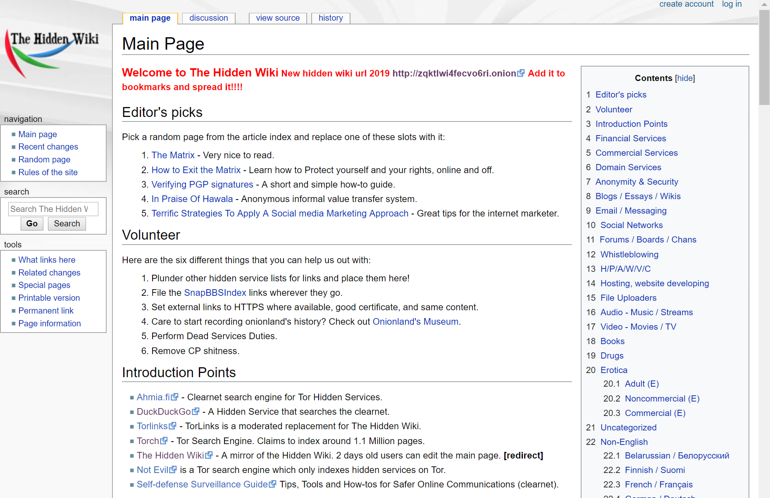


Рис.2. Інтерфейс HiddenWiki

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-каталоги.

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 Даркнету

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.

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

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 вразливість технології 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 всередині мережі. Все, що людина там робить (як і в звичайному інтернеті), вона робить на свій страх та ризик. Якщо хтось робить щось незаконне (шантаж чи вимагання грошей) та ненавмисно розкриє частину інформації про себе — це може бути використано проти нього.

## Технологія Tor

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

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.

Основна ідея - 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.

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

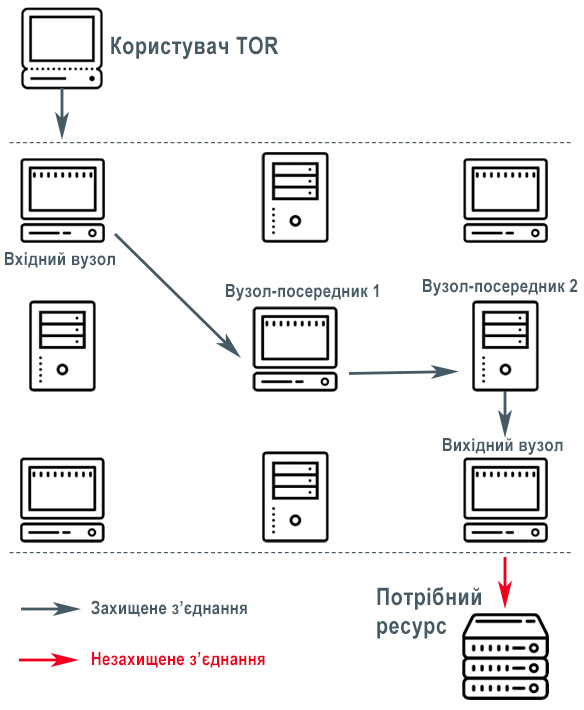


Рис.3. З’єднання в мережі TOR

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).

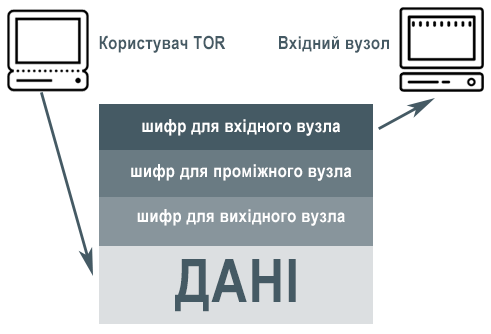


Рис.4. Шифрування даних з боку користувача

Виглядає як цибулина. Звідси і з'явилася назва «цибулинне шифрування», оскільки кожен сервер знімає лише 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 свою частину і передають дані. Проміжні сервери не знають, звідки прийшли дані і куди відправляться в самому кінці.

Останній вузол в ланцюжку - вихідний, він найважливіший зі всіх. 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.

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.

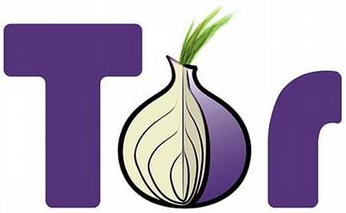
Зазвичай, для безпечного інтернет-серфінгу використовують Tor Browser - офіційний браузер від розробників цієї мережі. У ньому прописані всі налаштування, які потрібні для підключення до мережі, але для повної приватності потрібно буде самому додати частину розширень, наприклад, NoScript. Він відключає 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. 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. Розробники мережі придумали рішення для цих ситуацій - частина вхідних вузлів є 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.

## 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 (рис.5).

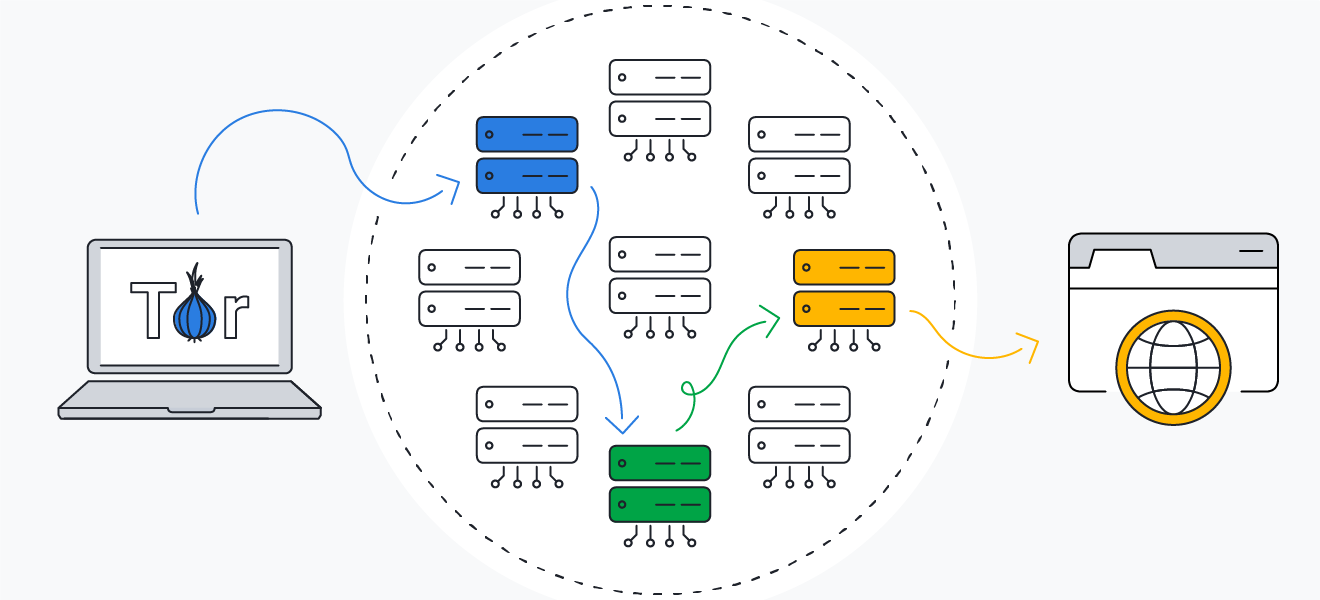


Рис.5. Обхід блокування сайтів браузером Tor

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 замовченням не зберігає історію його дій, тому, в інтернеті ніхто не дізнається, ким є користувач і не зможе отримати інформацію про нього.

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.6).

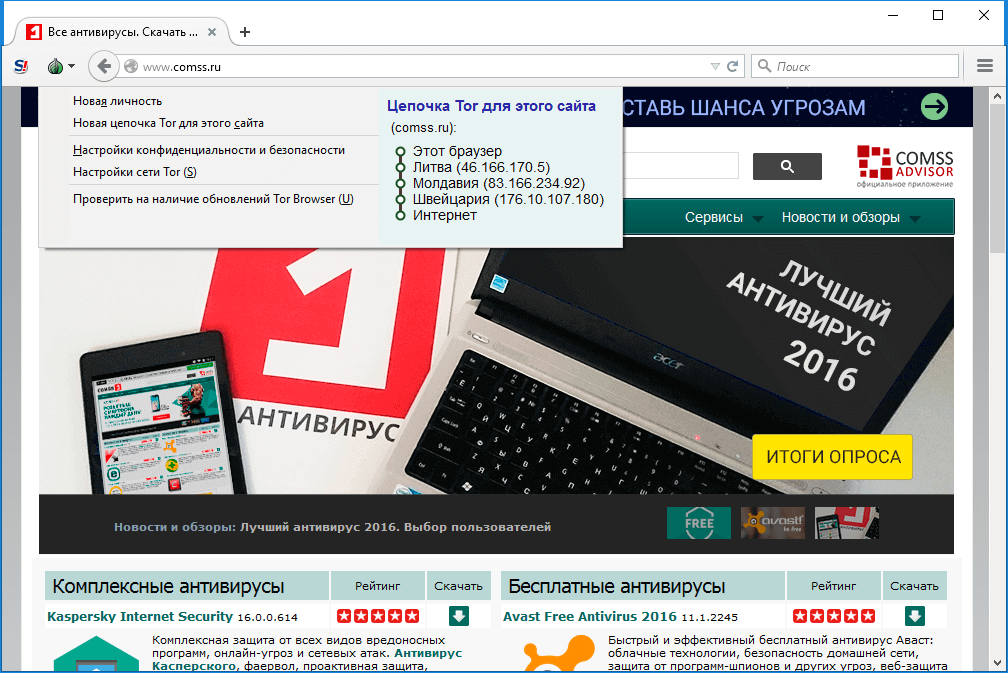


Рис.6. Плагін Tor в браузері Mozilla Firefox

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.

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.
6. Які послуги надає браузер Tor