

ІНСТРУКЦІЯ ДЛЯ ВИКРИВАЧІВ: ЯК СЕБЕ УБЕЗПЕЧИТИ

*Підготовлено в рамках проекту «Боротьба з корупцією:
залучення журналістів та викривачів до платформи Хабардокс»,
за підтримки Фонду сприяння демократії Посольства США в Україні.
Погляди авторів не обов'язково збігаються з
офіційною позицією уряду США.*

Викривач – герой, а не «стукач»

В Україні корупція – використання особою наданих їй службових повноважень і пов'язаних із цим можливостей задля отримання неправомірної вигоди – є проблемою номер один.

Усі зусилля держави побороти корупцію будуть марними, якщо громадяни стоятимуть осторонь і сповідуватимуть звичай «моя хата скраю». Вкорінена в суспільстві думка, що інформувати про злочини, зокрема корупційні, означає доносити, «стукати», має поступитися західним традиціям, де верховенство права – передусім. Викривати хабарників і корупціонерів – це почесно і гідно. Саме викривачі корупції та інших зловживань влади, такі як Едвард Сноуден, стають людьми, здатними змінити світ.

Викривач – це особа, яка розголошує інформацію про зловживання владою, корупційні правопорушення, нецільове використання бюджетних коштів, розкрадання державного або комунального майна, порушення прав людини, дії чи бездіяльність органів влади та їх посадових осіб, що становлять небезпеку для здоров'я, життя людини, довкілля тощо. Викривач може скористатись інформацією про корупційні злочини кількома способами:

1. **Надіслати правоохоронним органам.** Цей спосіб теоретично має бути більш ефективним з погляду перевірки наданої інформації та притягнення порушника до відповідальності. Водночас в умовах високого рівня корумпованості та політизованості правоохоронних органів він може мати прямо протилежний ефект.
2. **Надіслати ЗМІ.** Цей спосіб ґрунтується на тому, що оприлюднення інформації про корупцію створює суспільний тиск на органи влади та правоохоронні органи, позбавляючи їх можливості ігнорувати або замовчувати факти корупції. Водночас варто розуміти, що авторитетні ЗМІ не публікуватимуть інформацію без її ретельної перевірки. На цьому спеціалізуються деякі журналісти-розслідувачі.

Хто викриває корупцію – ризикує

В Україні – найбільш корумпованій країні Європи – викривання корупційних фактів є вкрай важливою, але дуже ризиковою справою. На жаль, ви можете стати об'єктом тиску, погроз і навіть небезпечних дій з боку корупціонерів, які не хочуть, щоб ви розкривали докази корупційних схем. Залякування, звільнення з роботи, судові позови, кримінальне переслідування і фізична розправа – це ризики оприлюднення правди, яка так потрібна суспільству. Тому викривати хабарників і корупціонерів необхідно, але робити це треба максимально обережно.

Без доказів корупцію не подолати

Повідомлення про корупцію без доказів корупційних дій не мають сенсу, бо довести справу до кінця за відсутності доказової бази неможливо. Якщо ви знаєте про факти корупції і хочете, щоб винних було покарано, то правоохоронним органам або журналістам-розслідувачам потрібно надати не просто інформацію, а докази цих фактів. Зазвичай такими доказами є документи в електронному та паперовому вигляді, фотографії, аудіо- та відеозаписи.

Будь-які докази краще зберігати та передавати в електронному вигляді. Так ви маєте більше можливостей убезпечити себе. З іншого боку, так простіше перевірити достовірність наданих доказів, аніж у випадку з паперовими копіями. Тому навіть якщо ви маєте документи або фотографії у паперовому вигляді чи аудіо- або відеозаписи в аналоговому форматі на фізичному носії (наприклад, на касеті чи компакт-диску), варто перевести їх в електронний вигляд – відсканувати або оцифрувати – і передавати вже в такому форматі.

Передаючи докази, передусім будьте обережними

Під час передачі важливої інформації, що потенційно може становити загрозу, найбільш небезпечним є сам момент передачі. Якщо це відбувається під час зустрічі, то за вами можуть стежити або впізнати в майбутньому. Утім, варто розуміти, що передача інформації в електронному вигляді, через електронну пошту або файлообмінник, може бути так само небезпечною, якщо її здійснювати у відкритому інтернеті.

Для спеціаліста не складно зламати вашу електронну пошту або профіль у соціальній мережі чи відстежити вашу IP-адресу. Таким чином, у разі недотримання правил цифрової безпеки, передача небезпечної інформації в інтернеті робить вас абсолютно незахищеним від зовнішнього втручання, а отже, вразливим до тиску, погроз або помсти.

Оберіть для роботи безпечний браузер – Tor

Tor (The Onion Router) – це інтернет-браузер, який забезпечує анонімність і захист користувачів від стороннього моніторингу. З погляду користувача, це такий самий браузер, як і звичні для всіх Internet Explorer, Google Chrome, Opera, Firefox тощо, отже, його використання не потребує жодних спеціальних знань і навичок. Суттєва відмінність полягає в тому, що він набагато безпечніший для роботи.

Tor спрямовує ваш інтернет-трафік через мережу серверів, які приховують IP-адресу користувача. Таким чином стає практично неможливим відстежити, що саме ви робили в інтернеті, які сайти відвідували, які файли завантажували. Встановлення та використання браузера Tor безплатне.

Для завантаження Tor потрібно перейти на його офіційну веб-сторінку www.torproject.org.

Tor Browser for Windows

Version 5.0.3 - Windows 8, 7, Vista, and XP

Everything you need to safely browse the Internet.

[Learn more »](#)



DOWNLOAD
Tor Browser

Not Using Windows?
Download for [Mac](#) or [GNU/Linux](#)

(sig) What's This?

English ▾



Під час завантаження ви можете обрати мову інтерфейса. Завантаживши Tor, встановіть його в себе на комп'ютері. Після встановлення ви можете використовувати його для роботи в інтернеті замість незахищених браузерів.

Захищений браузер усіх питань не вирішує

Браузер Tor забезпечує вам високий рівень анонімності та безпеки під час користування інтернетом. Однак для безпечної передачі інформації про факти корупції цього може бути недостатньо, адже виникає потреба в захищеному каналі зв'язку між викривачем та отримувачем інформації, наприклад – журналістом-розслідувачем.

Для задоволення цієї потреби та убезпечення діяльності викривачів і журналістів-розслідувачів в Україні Талліннський технічний університет спільно з Українським інститутом публічної політики розробили й запустили спеціальний анонімізатор повідомлень про корупцію – Хабардокс.

хабардокс

ГОЛОВНА БЕЗПЕКА ІНФОРМАТОРАМ РОЗСЛІДУВАЧАМ БЛОГ

анонімізатор повідомлень

хабардокс

захист викривачів

НАДАТИ ДОКАЗИ
КОРУПЦІЇ



Хабардокс гарантує: вас не розшифрують

Хабардокс – це захищений веб-сайт, за допомогою якого викривачі, що хочуть оприлюднити докази корупції, можуть зв'язатися з провідними журналістами-розслідувачами України та передати їм інформацію за допомогою захищеного та анонімного каналу зв'язку.

Ніхто, навіть журналіст-адресат вашого повідомлення, не зможе відстежити, від кого та з якої IP-адреси воно надіслано. З іншого боку, ніхто, крім самого журналіста, якому ви надіслали повідомлення, не знатиме, що саме містилося в ньому, – ані керівництво ЗМІ, ані інтернет-провайдер чи IT-спеціаліст. Водночас ви зможете не просто надіслати журналісту повідомлення, а й додати до нього файли, що містять докази корупційних злочинів, а також отримати відповідь і продовжити спілкування, без втрати анонімності та високого рівня захисту інформації.

Ваші повідомлення зможе отримати та прочитати тільки журналіст-розслідувач, якого оберете ви самі. І навіть якщо його комп'ютер буде викрадено чи конфісковано, то побачити ваші повідомлення буде неможливо, адже кожен журналіст, який є користувачем Хабардокс, має окремий електронний ключ. Ви також отримаєте свій електронний ключ, що дасть вам змогу перевіряти стан опрацювання наданої вами інформації та отримувати повідомлення від журналіста.

Хабардокс приховує вашу IP-адресу, а також шифрує інформацію, що передається, у спосіб, який практично унеможлиблює її розшифрування. За рівнем складності шифрування Хабардокс відповідає найвищим міжнародним стандартам – це набагато надійніше за будь-який поштовий сервер чи файлообмінник. Сервери, на яких зберігаються дані Хабардокс, розташовано поза межами України, так само як і технічне адміністрування цієї платформи, тому українські органи влади чи окремі особи позбавлені можливості отримати фізичний доступ до цієї інформації.

Детальніше з особливостями функціонування платформи Хабардокс і переліком українських журналістів-розслідувачів, які є її користувачами, можна на її публічній веб-сторінці <http://www.xabardocs.org/>.

Передати інформацію за допомогою Хабардокс дуже просто.

Крок 1. Встановіть браузер Tor.

Пропустіть перший крок, якщо ви вже встановили цей браузер.

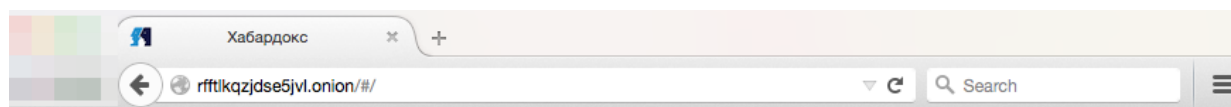
Крок 2. Зайдіть на захищену сторінку Хабардокс.

Відкрийте браузер Tor і введіть адресу захищеної сторінки Хабардокс <http://rfftlkqzjd-se5jvl.onion>.



Крок 3. Почніть надавати свідчення на головній сторінці.

Натисніть посилання «Надати свідчення».



Вітаємо на захищеній сторінці
Хабардокс!

Тут безпечно і анонімно викривають корупційні дії.

Ви інформатор?



Надати свідчення

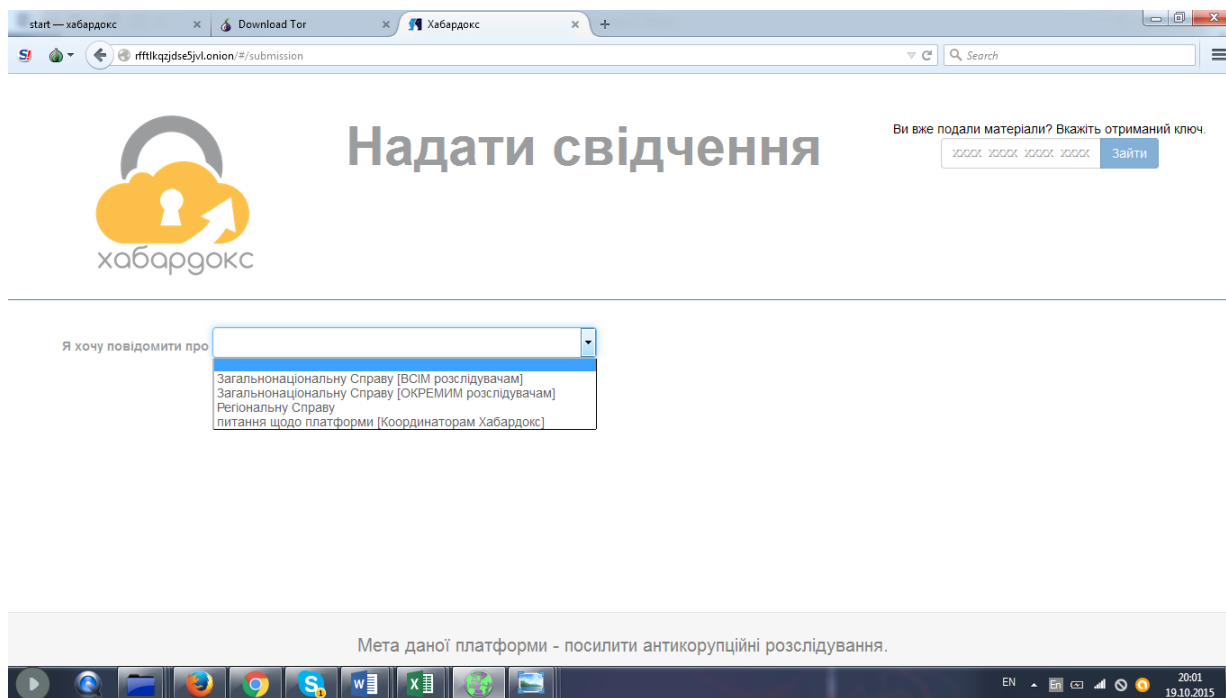
Ви вже подали матеріали? Вкажіть отриманий ключ.

XXXX XXXX XXXX XXXX

Зайти

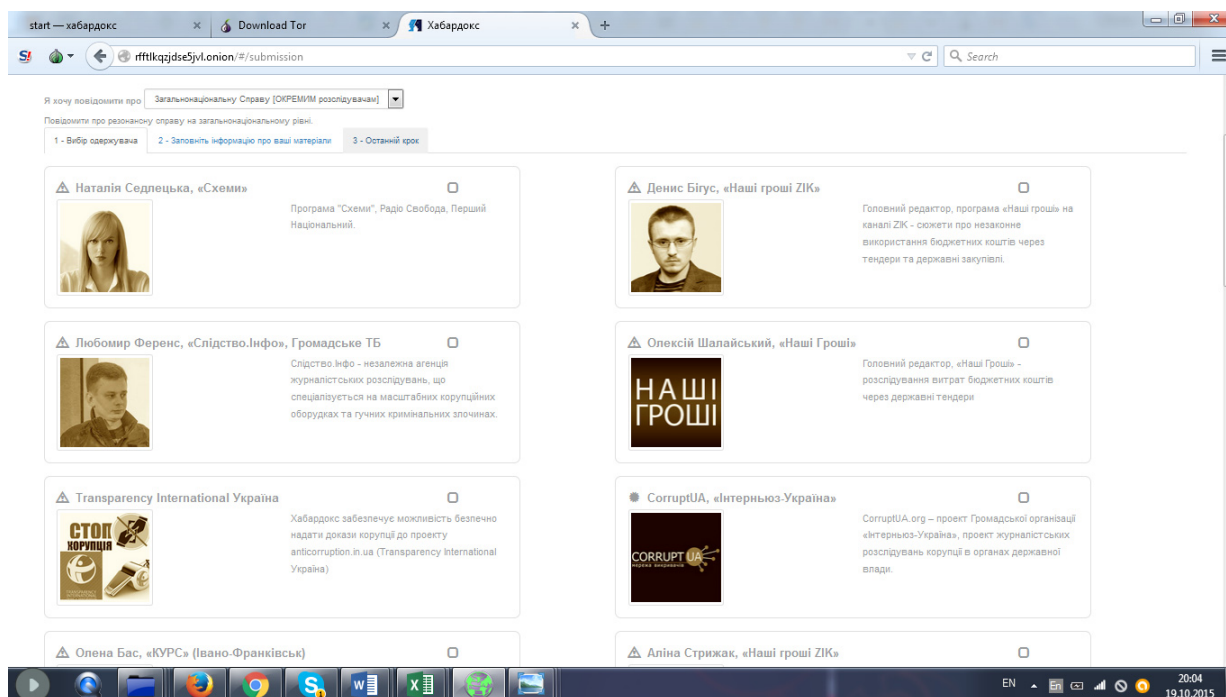
Крок 4. **Оберіть, кого саме з абонентів стосується ваша інформація.**

Оберіть характеристику вашої інформації та потрібну вам групу абонентів за допомогою спливаючого меню.



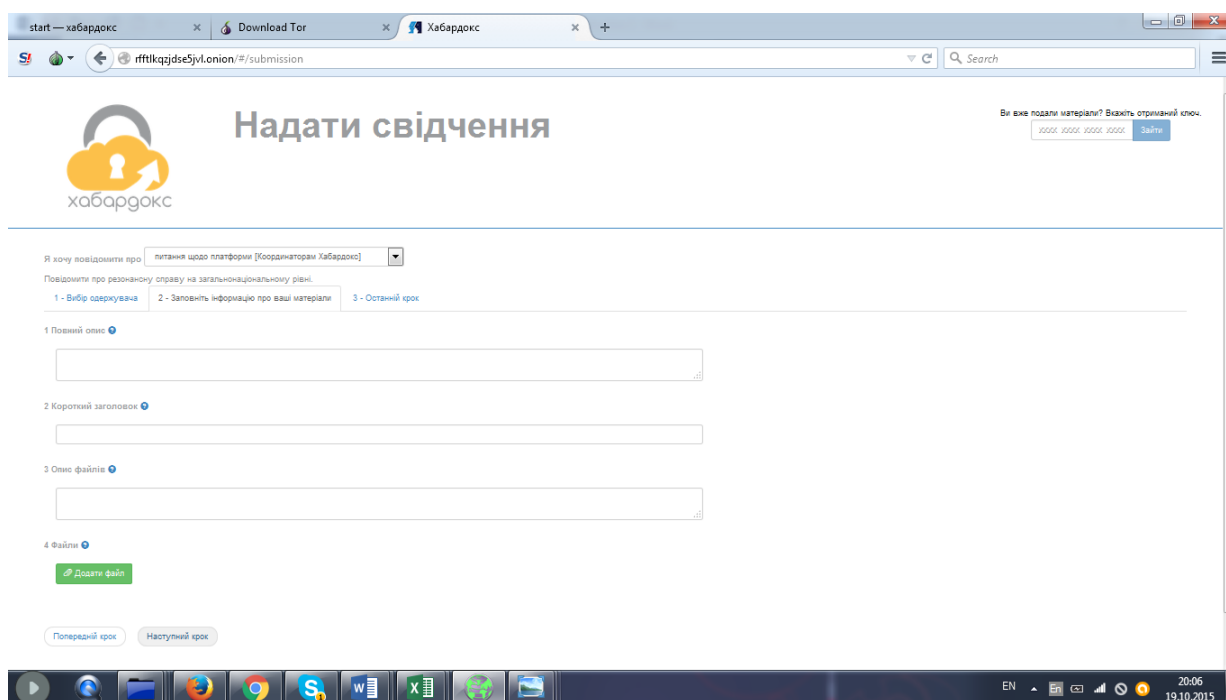
Крок 5. **Оберіть адресата вашого повідомлення.**

З переліку журналістів-розслідувачів, які є користувачами Хабардокс, оберіть того, кому довіряєте найбільше, або того, хто спеціалізується на тематиці, найбільш близькій до вашої інформації (наприклад, державні закупівлі, зловживання владою тощо).



Крок 6. Надайте свідчення.

Завантажте матеріали-докази (вордівські файли, відскановані документи, аудіо- чи відеозаписи) та, за потреби, додайте до них невеличкий опис з поясненням.



Зверніть увагу! Переконайтеся, що ви випадково не переслали інформацію, що містить ваші персональні дані, або таку, що може дати змогу вас ідентифікувати.

Вітаємо! Ви стали викривачем і зробили свій внесок у боротьбу з корупцією.

Якщо інформація та докази, які ви надали, відповідають дійсності, то ця справа може стати предметом журналістського розслідування, результати якого будуть опубліковані у ЗМІ і, ймовірно, призведуть до розкриття корупційного злочину та покарання винних.

Під час збору та передачі інформації про корупцію пам'ятайте про правила цифрової безпеки:

1. Використовуйте захищений інтернет-браузер Tor для будь-яких дій в інтернеті, які ви хочете зберегти у таємниці.
2. Не зберігайте інформацію, що може становити небезпеку, на вашому комп'ютері. Перенесіть її на фізичний носій (компакт-диск, флешка чи карта пам'яті) та зберігайте його у надійному місці, бажано поза вашим помешканням і місцем роботи.
3. Якщо ви вже передали докази та не хочете більше їх зберігати, знищіть фізичний носій цієї інформації таким чином, щоб він був непридатний до подальшого використання або ремонту.
4. Не пересилайте матеріали з комп'ютера, наданого вашим роботодавцем, а також з вашого помешкання чи офісу. Для цього краще скористатися місцем із відкритим WiFi-доступом до інтернету, наприклад, кафе. Варто уникати камер спостереження.
5. Не роздруковуйте документи, що становлять небезпеку, на принтері, розміщеному у вас вдома або в офісі.