УДК 004.738.5:355.01
DOI: 10.31673/2412-9070.2022.051117

А. В. ЛЕМЕШКО, доктор філософії;
Є. О. НОВІЧЕНКО, студентка магістратури;
А. В. НЕДАВНІЙ, студент магістратури;
Є. С. ДУРНЄВ, студент магістратури;
А. В. СТАСЮК, студент магістратури,
Державний університет телекомунікацій, Київ

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ VPN ПІД ЧАС ВОЄННОГО СТАНУ В УКРАЇНІ

Завдяки невпинному розвитку інформаційних технологій, особливо мережі «Інтернет» та глобалізації по всій земній кулі, вдалося здійснити величезний стрибок у зростанні передавання даних та доступності інформації поміж великого кола людей.

Зараз інтернет по суті є знаменом глобального віртуального світу з безліччю безкоштовної інформації. Щодня попит на нього невпинно зростає, що також спонукає постачальників інтернет-послуг до постійного розвитку ринку та вдосконалення технологій передавання даних.

Сьогодні складно уявити світ без вільного доступу до інтернету. Але влада деяких країн світу на законодавчому рівні обмежує доступ до різних ресурсів в інтернеті, а це зі свого боку швидко нарощує попит на використання технологій та сервісів приховування фактичного місцеположення в мережі «Інтернет», зокрема VPN. Дехто використовує VPN для збільшення своєї анонімності в мережі «Інтернет» та отримання доступу до заблокованих урядом ресурсів. Хтось користується цією технологією для покращення захисту особистої інформації. Під час вибору сервісу, який надає доступ до VPN, більшість користувачів керуються якістю послуг та ціною на них.

Потреба у VPN-сервісах після початку повномасштабного російського вторгнення в Україну зросла в кілька разів. Попит значно збільшився через блокування українських медіаресурсів на тимчасово окупованих територіях та появу ІТ-армії України.

Технологія VPN захищена за всіма сучасними стандартами. Шифрування даних, автентифікація джерела, перевірка хеша — це все невід'ємна частина цієї технології, що забезпечує конфіденційність даних, які передаються в інтернеті. Загалом, все це допомагає підвищити рівень захищеності особистих даних користувачів.

Через блокування українських ресурсів, глушіння операторів зв'язку та знищення їхньої інфраструктури громадяни України, котрі залишаються на тимчасово окупованих територіях, здебільшого мають доступ тільки до російського медіапростору. Проте за допомогою VPN-сервісів вони можуть отримати доступ до українського медіапростору.

Ключові слова: інформаційні технології; VPN; попит; сервіси; інтернет; користувачі; доступ; інформація.

ВСТУП

Постановка проблеми. Після окупації українських територій загарбники всіма способами намагаються відгородити наших громадян від усього цивілізованого світу. Блокування стільникового зв'язку та інтернету, насильне приєднання мережної інфраструктури українських провайдерів зв'язку до російської інтернет-мережі — це лише деякі з таких способів. Змінивши український канал зв'язку на російський, окупанти мають можливість фільтрувати весь інтернет-трафік, що, зі свого боку, дає їм змогу блокувати доступ до будь-яких міжнародних та українських вебресурсів. Щоб здобути доступ до заблокованих ресурсів та збільшити свою анонімність під час перегляду того чи іншого вебресурсу, українці повинні використовувати VPN-сервіси.

Аналіз останніх досліджень і публікацій. Британський кореспондент газети «The New York Times» Адам Сатаріано у своїй публікації «How Russia Took Over Ukraine's Internet in Occupied Territories» надав статистику зміни маршрутизації трафіку в Херсоні з моменту окупації, щодо зростання попиту на використання технології VPN [1].

Також дослідження провідних VPN показало, що з початку повномасштабного вторгнення рф в Україну потреба в застосуванні технології VPN на росії значно збільшилась (майже на 1092%) порівняно зі статистикою до 24 лютого 2022 року (рис. 1). Імовірно це спричинено з блокуванням медіаресурсів та соціальних мереж, наприклад Twitter і Facebook.

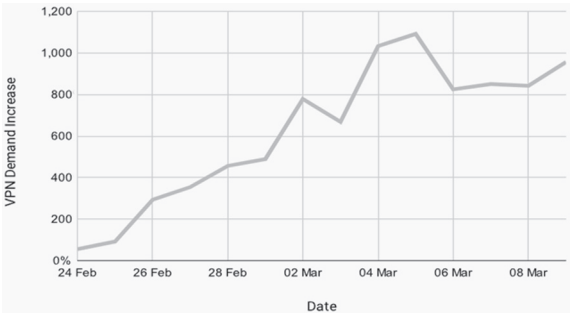

Рис. 1. Діаграма зростання попиту на VPN у рф

В Україні на тимчасово окупованих рф територіях доступ до українського контенту також заблоковано, що є вагомою причиною використання українцями VPN. Тому попит на VPN в Україні зріс на 609%, що вище за середньодобовий показник на початок лютого [2].

Формування мети статті. Метою роботи є дослідження функцій технології VPN та способи її використання. Об'єкт — технологія VPN, способи її застосування в Україні та в сучасному світі загалом. Предмет — Virtual Private Network.

ОСНОВНА ЧАСТИНА

VPN — це віртуальна приватна мережа, тобто тип вебслужби, яка дає змогу користувачам приховувати активність у мережі, особистість і фізичне розташування пристрою, з якого здійснюється підімкнення під час роботи в мережі.

Для доступу в інтернет VPN створює приватне мережне з'єднання між пристроєм і віддаленим сервером, що належить постачальнику інтернет-послуг. Це цифрове підімкнення або тунель для підвищення безпеки шифрує дані користувача. Він також приховує IP-адресу користувача, щоб ніхто інший не зміг його відстежити. А отже, робота в інтернеті стає безпечною, надійною та анонімною.

Постачальники послуг інтернету (ISP) реєструють та відстежують історію відвідувань через IP-адресу пристрою користувача. Цю інформацію потенційно можна продати стороннім рекламодавцям, передати уряду або залишити вразливою перед порушенням безпеки. Завдяки маршрутизації даних через зашифрований point-to-point тунель на віддалений VPN-сервер є можливість приховати IP-адресу користувача, виконавши всі запити в інтернеті через IP-адресу VPN-сервера. Підімкнення VPN перенаправляє пакети даних від комп'ютера користувача до іншого віддаленого сервера, перш ніж надсилати їх третім особам в інтернеті.

Принципи роботи та протоколи VPN

До основних принципів технології VPN належать:

♦ ***тунелювання*** — віртуальна приватна мережа переважно створює безпечний тунель передавання даних між ПК користувача та іншим VPN-сервером. Під час під'єднання до інтернету VPN-сервер стає джерелом усіх даних. Тобто дані, відправлені від одного користувача до іншого, спочатку проходять через VPN-сервер, який їх шифрує та приховує IP-адресу джерела, виконуючи запит від себе, а згодом користувацькі дані передаються до отримувача;

♦ ***шифрування*** — це процес кодування інформації з метою запобігання несанкціонованому доступу. Технологія VPN використовує протоколи шифрування для забезпечення конфіденційності даних.

Державна служба спеціального зв'язку та захисту інформації України радить вибрати VPN з шифрування військового класу, наприклад AES-256, та з використанням протоколів безпеки, зокрема OpenVPN, L2TP, IKEv2, WireGuard тощо [6].

Розглянемо далі основні VPN-протоколи.

1. *IPsec*. У терміні «IPsec» «IP» означає «інтернет-протокол», а «sec» — «безпечний». IPSec — це стандарт, який охоплює три протоколи, кожен з яких має свій функціонал, що забезпечує безпеку передавання даних із протоколів IP. До них належать такі протоколи: AH (відповідає за автентифікацію джерела і перевірку цілісності даних), ESP (відповідає за шифрування даних, а також може виконувати функції автентифікації джерела і перевірку цілісності даних) та IKE (відповідає за узгодження роботи учасників захищеного з'єднання).

Використовуючи протокол IPSec, пристрої, між якими ініціалізується з'єднання, мають змогу вибирати алгоритм передавання даних, тип перевірки цілісності даних і тип автентифікації один одного [3].

2. *OpenVPN*. Протокол OpenVPN є кросплатформним OpenSource проєктом, а отже, його можна застосовувати майже на будь-якому пристрої абсолютно безкоштовно, через що він і став доволі популярним.

OpenVPN для забезпечення конфіденційності даних у тунелі використовує бібліотеку OpenSSL. Цей протокол гарантує безпеку, оскільки він має відкритий вихідний код та підтримує кілька стандартів шифрування, а також є універсальним і не залежить від платформи. Саме завдяки відкритості коду, будь-хто може на свій лад змінити чи виправити OpenVPN відповідно до своїх уподобань [4].

Нарешті, варто згадати, що OpenVPN має кілька плагінів і сценаріїв сторонніх розробників для покращення функціональності його брандмауерів [5].

3. *WireGuard*. WireGuard — протокол тунелювання, який використовує криптографію, тому є одним із найбезпечніших протоколів VPN. Порівнюючи з OpenVPN, WireGuard має простий код, а отже, він менш схильний до помилок і неправильного налагодження, оскільки має не таке складне налаштування.

4. *L2TP (IPsec)*. L2TP (Layer 2 Tunnel Protocol) — це протокол VPN, який не застосовує шифрування, а співпрацює з протоколом шифрування IPsec.

Принцип роботи протокола L2TP/IPsec такий: він не гарантує шифрування чи конфіденційність даних, тому покладається на протокол шифрування, який він пропускає в тунелі для забезпечення конфіденційності. Таким протоколом шифрування даних виступає IPsec. Протокол IPsec розміщено «поверх» L2TP, щоб мати бажану функцію безпеки.

IPsec у поєднанні з L2TP забезпечує такі переваги для протоколу тунелювання VPN:

- автентифікацію через EAP або локальні облікові записи користувачів для клієнтів віртуальної приватної мережі;
- автентифікацію повідомлень і перевірку цілісності, які гарантують, що повідомлення не були підроблені та що джерело є автентичним;
- можливість для інтернет-провайдерів отримати шифрування та дешифрування за допомогою симетричних сеансових ключів для підімкнення до VPN;
- взаємну автентифікацію, яка гарантує, що шлюз IPsec дійсно спілкується зі справжнім клієнтом L2TP/IPsec, а не зі зловмисником, котрий маскується під нього [10].

5. *EoIP*. Протокол EoIP (Ethernet over IP) — це тунель рівня каналу даних (L2) на мережному рівні (L3). Через цей тунель дані передаються на рівні кадру Ethernet. EoIP забезпечує прозоре мережне середовище, яке емулює пряме з'єднання Ethernet між мережами. Усі MAC-адреси видимі, і за допомогою цього типу тунелю можна з'єднати дві локальні мережі L2 через інтернет. Тунель EoIP може працювати через IPIP, PPTP та будь-яке інше з'єднання, здатне передавати IP-пакети. Через нього можна надсилати будь-який трафік, крім IP, зокрема ARP, DHCP, PPPoE, IPv6 тощо.

Протокол EoIP розроблено компанією MikroTik, тому є сумісність із ними і роутерами Linux, які вміють працювати з EoIP [11].

6. *GRE*. Generic Routing Encapsulation — це протокол для інкапсуляції пакетів даних, які використовують один протокол маршрутизації всередині пакетів іншого протоколу.

GRE — це спосіб завантаження одного типу пакета в інший тип пакета, аби перший пакет мав змогу перетнути мережу, яку він зазвичай не зміг би здолати. Тобто, це так само, як один тип транспортного засобу (наприклад, автомобіль) завантажується на інший тип транспортного засобу (паром), щоб перетнути місцевість, яку інакше не зміг би подолати [14].

VPN-сервіс Tor

Сьогодні найбільш надійним VPN-сервісом уважається Tor Browser.

***Tor* (*The Onion Router*)** — це величезна за масштабом автономна мережа, що анонімізує весь вебтрафік, який курсує через неї, для забезпечення приватного вебсерфінгу та анонімності в інтернеті.

Технологія Tor приховує IP-адресу користувача та активність в інтернеті завдяки перенаправленню всього вебтрафіку через величезну мережу різних пов'язаних між собою маршрутизаторів, пристроїв та серверів.

Tor за допомогою спеціального методу шифрування, розробленого ВМС США для захисту комунікацій американської розвідки, анонімізує трафік усередині своєї мережі. Технологія Tor являє собою OpenSource платформу конфіденційності. Але в деяких країнах його заборонено, наприклад у Китаї — через його популярність в DarkNet.

Tor анонімно передає зашифровані дані через три рівні міжнародних проксі-серверів, які утворюють схему Tor (рис. 2):

1) *вузол входу/охорони*: спочатку Tor Browser випадковим чином під'єднується до загальновідомого вузла входу. Вузол шлюзу передає свої дані в схему Tor;

2) *проміжні вузли*: користувацькі дані повністю зашифровані. Потім Tor надсилається через низку вузлів, які розшифровують дані шар за шаром. Щоб забезпечити анонімність, кожен проміжний вузол знає лише ідентичність попереднього та наступного проміжних вузлів;

3) *вихідний вузол*: після видалення останнього рівня шифрування розшифровані дані залишають мережу Tor через вихідний вузол і досягають кінцевого пункту призначення на сервері.

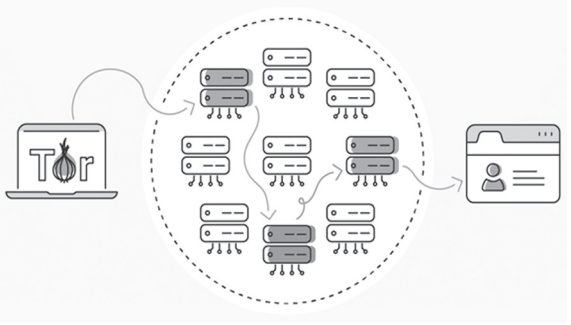

Рис. 2. Браузер Tor надсилає вебтрафік через вхідний вузол, середній вузол і вихідний вузол для шифрування та дешифрування трафіку

Після того, як дані були захищені кількома рівнями шифрування, трафік передається через низку мережних вузлів. Кожен вузол може розшифрувати тільки свою частину даних.

Вагомою відмінністю є те, що мережею VPN-сервісів керує окремий центральний постачальник послуг, а мережа Tor децентралізована та створена виключно ресурсами так званих «волонтерів» [9].

Використання VPN-сервісів на окупованих територіях

Українцям, які перебувають на тимчасово окупованій території, рекомендується використовувати такі VPN-сервіси:

1. ***ExpressVPN***. Цей VPN-сервіс посідає перше місце в більшості рейтингів. Його зареєстровано на Британських Віргінських островах, тому він не підпадає під юрисдикцію урядів США та Європи й не передає дані користувачів до поліції за запитом.

2. ***VPN Unlimited***. Нацполіція України рекомендує цей сервіс, а також такі великі ресурси, як Engadget і vpnMentor. Країна реєстрації — США. Компанія обіцяє захист конфіденційності своїх користувачів, тому не зберігає інформацію про використані сервери, зміст здобутих даних, історію браузера та загальний час з'єднання.

3. ***TunnelBear***. Цей сервіс підтримує українців під час війни. Після російського вторгнення він запропонував українцям 100 ГБ інтернет-трафіку безплатно.

4. ***NordVPN***. VPN-сервіс компанії Nord Security, що працює в галузі кібербезпеки. Має позитивні відгуки провідних технологічних видань світу. Країна реєстрації — Панама.

5. ***ClearVPN***. Під час війни ClearVPN став безплатним для українців, тож кожен може завантажити його собі, щоб безпечно користуватися мережею [7].

Уникнення VPN-блокування

Компанія FS GROUP, яка є вендором продуктів інформаційної безпеки, створила поради для обходу VPN-блокування.

1. Використання різних VPN-сервісів. Популярні VPN-сервісів можуть піддаватися блокуванню з боку рф, але заблокувати всі VPN неможливо. Тому краще мати встановлені різні VPN-сервіси на користувацьких пристроях.

2. Установлення приватного VPN-сервера. Користувач може створити особистий VPN зі своєю IP-адресою, яку не буде заблоковано. Проте такий користувацький VPN-сервер не дає стандартних гарантій безпеки, як під час роботи з платними VPN.

3. Використання інших VPN-протоколів. Сучасні VPN роблять з урахуванням набору з різних протоколів. Деякі з них беруть за основу конфіденційність і безпеку користувача, інші призначені для забезпечення швидкої роботи. Залежно від того, яку програму VPN встановлює користувач, він може змінити протокол, перейшовши на панель налаштувань і вибравши потрібний VPN-протокол. Найкращі VPN-протоколи: WireGuard, OpenVPN, L2tp/IPsec, iKev2.

4. Налаштування браузера для уникнення блокування. Використовуйте спеціальні VPN-розширення для браузера.

Українцям, які перебувають на тимчасово окупованій території та в разі перетину лінії розмежування, необхідно регулярно очищати історію браузера та месенджерів, видаляти соціальні мережі, які можуть видати проукраїнську позицію особи та створити проблеми під час спілкування з окупантами.

VPN-програма також може привернути увагу окупанта, тому краще її видалити. Але якщо потрібно залишити цей застосунок на телефоні, його слід приховати. На Android-смартфонах користувач може використати функцію «приховати програму», якщо версія операційної системи пристрою це підтримує. Також можна встановити сторонній лаунчер, наприклад Nova Launcher, і змінити дизайн іконки будь-якої програми. Це дає можливість замаскувати VPN та будь-яку іншу програму, наприклад під калькулятор [8].

ВИСНОВКИ

Україна продовжує боротися з російською інформаційною монополією, яка є одним із ключових факторів російського панування. До блокування російських вебсайтів уже було заборонено деякі російські фільми та серіали. Обидва кроки є дуже суперечливими з юридичного та етичного погляду. Проте, маючи юридичні недоліки, вони створюють факти на місцях. Наприклад, такі кроки стимулюють внутрішнє українське аудіовізуальне виробництво: вперше за часи незалежності Україна дійсно почала виробляти власний контент, фільми чи серіали, а не споживати російський (часто ідеологічно токсичний) продукт.

Розроблені поради для уникнення блокування українських ресурсів допоможуть людям на тимчасово окупованих територіях підтримувати зв'язок з рідними та бути добре обізнаним в правдивих новинах.

Спочатку завжди важко звикнути до чогось нового. Але водночас ці кроки спонукають українців шукати альтернативи. І це не може не позначитися на суспільно-політичному житті країни.

Список використаної літератури

1. ***Як Росія*** *захопила український Інтернет на окупованих територіях [Електронний ресурс]. URL:*

https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html?fbclid=IwAR3X5hLRrVnsROrLN-tf4TTjB5NZNeUOCvrGyyzfCeaMiphFlsSXyOY5DA0 (дата звернення: 09.08.2022).

2. ***Використання*** *VPN в Росії та Україні стрімко зросло [Електронний ресурс]. URL:*

https://tech.co/news/vpn-usage-russia-ukraine (дата звернення: 10.03.2022).

*3. **Що таке** IPsec? Як працює IPsec VPN? [Електронний ресурс]. URL:*

https://www.cloudflare.com/learning/network-layer/what-is-ipsec/

*4. **Що таке** OpenVPN? [Електронний ресурс]. URL:*

https://openvpn.net/faq/what-is-openvpn/

*5. **Що таке** OpenVPN? Як це працює та коли його використовувати у 2022 році [Електронний ресурс]. URL:*

https://www.allthingssecured.com/vpn/faq/what-is-openvpn/ (дата звернення: 07.02.2022).

*6. **Держспецзв'язку:** Що таке VPN, і як ним безпечно користуватись [Електронний ресурс]. URL:*

https://www.kmu.gov.ua/news/derzhspeczvyazku-shcho-take-vpn-i-yak-nim-bezpechno-koristuvatis (дата звернення: 27.05.2022).

*7. **Для тих**, хто в окупації: підбірка безпечних VPN-сервісів для користування інтернетом [Електронний ресурс]. URL:*

https://henichesk.city/articles/219181/dlya-tih-hto-v-okupacii-pidbirka-bezpechnih-vpn-servisiv-dlya-koristuvannya-internetom#:~:text=ExpressVPN,користувачів%20до%20поліції%20за%20запитом (дата звернення: 16.06.2022).

*8. **Обхід** блокування. Як працює VPN на окупованій території [Електронний ресурс]. URL:*

https://v-variant.com.ua/article/vpn-v-okupatsii/ (дата звернення: 04.08.2022).

*9. **Браузер** Dark Web: що таке Tor, чи безпечний він і як ним користуватися [Електронний ресурс]. URL:*

https://www.avast.com/c-tor-dark-web-browser (дата звернення: 04.08.2022).

*10. **Що таке** L2TP/IPSEC? [Електронний ресурс]. URL:*

https://www.websiterating.com/vpn/glossary/what-is-l2tp-ipsec/

*11. **Налаштування** тунелів IPIP, GRE та EoIP [Електронний ресурс]. URL:*

https://help.keenetic.com/hc/en-us/articles/115002715029-Setting-up-IPIP-GRE-and-EoIP-tunne

*12. **Що таке** тунелювання GRE? Як працює протокол GRE [Електронний ресурс]. URL:*

https://www.cloudflare.com/learning/network-layer/what-is-gre-tunneling/

A. V. Lemeshko, Ye. O. Novichenko, A. V. Nedavnii, Ye. S. Durniev, A. V. Stasiuk

USE OF VPN TECHNOLOGY DURING MARITAL STATE IN UKRAINE

Thanks to the continuous development of information technologies, especially the Internet and globalization, it was possible to make a huge leap in the development of data transmission and the availability of information among a large number of people.

Now the Internet is the banner of a global virtual world with a lot of free information. The demand for it is constantly growing every day, which in turn encourages Internet service providers to constantly develop the market and improve data transmission technologies.

Today it is difficult to imagine a world without free access to the Internet. But the authorities of some countries of the world at the legislative level limit access to various resources on the Internet, and this, in turn, quickly increases the demand for the use of technologies and services for hiding the actual location on the Internet, such as VPN. Some use VPNs to increase their anonymity on the Internet and gain access to government-blocked resources. Some use this technology to improve the protection of personal information. When choosing a service that provides access to a VPN, most users are guided by the quality of services and their price.

The need for VPN services has grown several times since the beginning of the full-scale Russian invasion of Ukraine. Demand has increased due to the blocking of Ukrainian media resources in the temporarily occupied territories and the appearance of the Ukrainian IT army.

VPN technology is protected by all modern standards. Data encryption, source authentication, hash verification are all an integral part of this technology, which in turn ensures the confidentiality of data transmitted on the Internet. In general, all this helps to increase the level of security of users' personal data.

Citizens of Ukraine, who remain in the temporarily occupied territories, to a greater extent, have access only to the Russian media space, due to the fact that Ukrainian resources are blocked, and communication operators are «jammed» and their infrastructure is destroyed. With the help of VPN services, they can get access to the Ukrainian media space.

Keywords: information technologies; VPN; demand; services; Internet; users; access; information.