

УДК 004.021

DOI: <https://doi.org/10.53920/ITS-2022-2-3>

Андрій Вікторович ЛЕМЕШКО,

д-р філософії, доц.,
Державний університет телекомунікацій
ORCID ID: 0000-0001-8003-3168

Єлизавета Олександрівна НОВІЧЕНКО,

студентка,
Державний університет телекомунікацій
ORCID ID: 0000-0002-4354-4513

Андрій Володимирович НЕДАВНІЙ,

студент
Державний університет телекомунікацій
ORCID ID: 0000-0002-4383-8933

БЕЗПЕКА ДАНИХ В УКРАЇНІ ЗА ДОПОМОГОЮ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ VPN

Початок XXI століття анонсував собою глобалізацію в усьому світі та швидкий розвиток інформаційних технологій, а саме мережі Інтернет, що в свою чергу допомогло зробити великий стрибок у розвитку передачі даних та доступності інформації серед великого кола людей.

Сьогодні Інтернет знаменує собою глобальний віртуальний світ з безліччю безкоштовної інформації та даних. Попит на нього зростає щодня, що спонукає постачальників інтернет послуг на постійний розвиток ринку.

На сьогоднішній день важко уявити світ без вільного доступу до Інтернету. На жаль, уряди деяких країн на законодавчому рівні обмежують доступ до тих чи інших ресурсів, що, в свою чергу, збільшує попит на розвиток та використання VPN технологій та сервісів. Деякі користувачі використовують VPN для анонімності в мережі Інтернет та отримання доступу до заблокованих ресурсів. Інші - користуються данною технологією для захисту особистої інформації. Під час вибору VPN-сервісу деякі користувачі керуються якістю послуг, які будуть надаватись, а інші - їх вартістю. Власники VPN-сервісів постійно вдосконалюють якість своєї послуг та впроваджують нові технології.

Попит на VPN-сервіси, після початку повномасштабного російського вторгнення, в Україні виріс в рази - не тільки за рахунок блокування українських медіа ресурсів, а й за рахунок появи IT-армії України. Завдяки чому деякі VPN-сервіси почали безкоштовно надавати доступ українцям до своїх серверів.

VPN має декілька рівнів захисту такі як: шифрування даних, аутентифікація джерела даних, перевірка хешу, що в свою чергу забезпечує конфіденційність передаваних даних в Інтернеті. В сумісності, це все допомагає підвищити рівень захисту особистих даних користувачів.

Громадяни України, котрі залишаються на тимчасово окупованих територіях, в більшій мірі, мають доступ тільки до російського медіа простору, за рахунок того, що український ресурси блокуються, а операторів зв'язку «глушать» та знищується їх інфраструктура. За допомогою VPN-сервісів вони можуть отримати доступ до українського медіапростору.

Ключові слова: інформаційні технології, VPN, попит, сервіси, Інтернет, користувачі, доступ, інформація.

Andrii LEMESHKO

Doctor of Philosophy, Associate Professor
State University of Telecommunications
ORCID ID: 0000-0001-8003-3168

Yelyzaveta NOVICHENKO

Student
State University of Telecommunications
ORCID ID: 0000-0002-4354-4513

Andriy NEDAVNIY

Student
State University of Telecommunications
ORCID ID: 0000-0002-4383-8933

DATA SECURITY IN UKRAINE USING VPN TECHNOLOGY

The beginning of the 21st century heralded globalization worldwide and the rapid development of information technologies, namely the Internet, which in turn helped to make a big leap in the development of data transmission and the availability of information among a large number of people.

Today, the Internet represents a global virtual world with a wealth of free information and data. The demand for it is growing every day, which encourages Internet service providers to constantly develop the market.

Today, it is difficult to imagine a world without free access to the Internet. Unfortunately, the governments of some countries at the legislative level limit access to certain resources, which, in turn, increases the demand for the development and use of VPN technologies and services. Some users use VPN for anonymity on the Internet and access to blocked resources. Others use this technology to protect personal information. When choosing a VPN service, some users are guided by the quality of the services that will be provided, while others are guided by their cost. Owners of VPN services constantly improve the quality of their services and introduce new technologies.

The demand for VPN services, after the beginning of the full-scale Russian invasion, in Ukraine has grown many times - not only due to the blocking of Ukrainian media resources, but also due to the appearance of the IT army of Ukraine. As a result, some VPN services began to provide Ukrainians with free access to their servers.

VPN has several levels of protection, such as: data encryption, data source authentication, hash verification, which in turn ensures the confidentiality of transmitted data on the Internet. In compatibility, all this helps to increase the level of protection of personal data of users.

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.

***Key words:* information technologies, VPN, demand, services, Internet, users, access, information.**

Постановка проблеми. Загарбники намагаються усіляко відгородити людей на окупованих територіях від цивілізованого світу. Один зі способів – блокування зв'язку та інтернету.

Окупанти на тимчасово захоплених територіях намагаються приєднати українців до російських інтернет-мереж, де стоїть обладнання для фільтрації інтернет-трафіку, що дозволило заблокувати безліч українських та міжнародних веб ресурсів. Щоб уникнути слідкування та обійти обмеження, українським корис-

тувачам, яких під'єднали до російських мереж, необхідно використовувати VPN-сервіси.

VPN (Virtual Private Network) – це віртуальна приватна мережа, яка забезпечує шифрування трафіку між клієнтом та VPN-сервером і зміну IP-адреси. При підключенні до VPN створюється захищений канал між комп'ютером користувача і VPN-сервером. Дані в ньому надійно зашифровані: інтернет-провайдер не дізнається локації користувача та веб-ресурсів, які він відвідував. Оновлена IP-адреса зазвичай створюється з іншого міста або країни.

VPN-сервіси дозволяють користуватися ресурсами, доступ до яких заборонено за географічним принципом або на підставі рішень органів влади. Завдяки VPN можна вільно відвідувати заблоковані сайти, достатньо лише вибрати та завантажити додаток на свій комп'ютер або мобільний пристрій

Мета статті – дослідження роботи технології VPN, а також основні її принципи. Представити причини використання даної технології. Розглянути типи та протоколи VPN.

Завданнями даної роботи:

- створити поради, які допоможуть обійти блокування VPN та безпечно користуватися месенджерами на окупованих територіях України;
- визначити основні структурні елементи зовнішньоекономічної стратегії держави, зосереджуючи увагу на інноваційній діяльності, для визначення основних принципів розвитку інноваційних процесів та проблем інвестиційної привабливості України.

Виклад основного матеріалу. VPN – віртуальна приватна мережа, що являє собою тип веб-служби, яка дозволяє користувачам приховувати активність у мережі, особистість і розташування під час роботи в мережі.

Зазвичай для доступу в Інтернет комп'ютер створює загальнодоступне з'єднання з постачальником інтернет-послуг. VPN створює приватне з'єднання між комп'ютером і віддаленим сервером, що належить постачальнику VPN. Це цифрове підключення або тунель шифрує дані користувача, щоб ніхто інший не міг їх побачити. Він також маскує IP-адресу користувача, щоб ніхто інший не міг його відстежити. В результаті робота в Інтернеті стає безпечнішою, надійнішою та анонімною [1].

По самому визначенню VPN-підключення:

1. віртуальне тому, що в процесі підключення не задіяні фізичні кабелі;
2. приватний, тому що через це підключення ніхто інший не може бачити дані користувача чи дії в Інтернеті;
3. мережеве, тому що кілька пристроїв — комп'ютер користувача і VPN-служба — працюють разом, щоб підтримувати встановлений зв'язок.

Головні причини використання VPN

1. Захист даних.

Конфідентційні дані, такі як робочі листи, платіжна інформація та позначки розташування, постійно передаються в Інтернеті. Цю інформацію можна відстежити та легко використовувати, особливо в загальнодоступній мережі, де будь-хто, хто має доступ до мережі, потенційно може отримати доступ до особистих даних. Підключення VPN перетворює дані на код і робить їх нечитаними для всіх, хто не має ключа шифрування. Він приховує активність у мережі, щоб ніхто інший не міг її побачити.

2. Робота з дому.

Сьогодні віддалена робота поширена як ніколи. За допомогою VPN віддалені працівники можуть отримати доступ до ресурсів компанії через приватне з'єднання з будь-якого місця, якщо вони можуть виходити в Інтернет. Це дає співробітникам велику гнучкість, а також гарантує, що дані компанії залишаться захищеними та безпечними навіть у загальнодоступній мережі Wi-Fi.

3. Отримання доступ до регіонального вмісту або транслявання його з будь-якого місця.

Деякі сайти та служби обмежують свій медіаконтент залежно від географічного положення, що означає, що може не бути доступу до певних видів контенту. VPN маскує або підробляє розташування локального сервера, щоб він виглядав так, ніби він знаходиться в іншому місці, наприклад, в іншій країні.

4. Обхід блокування та спостереження.

У деяких регіонах доступ до певних сайтів або служб може бути недоступним через урядові обмеження, цензуру або стеження. Спуфінг розташування дає користувачам можливість обходити брандмауери, переглядати заблоковані веб-сайти і вільно переміщатися в мережі.

5. Заборонити відстеження з боку Інтернет-провайдера та сторонніх осіб.

Постачальники послуг Інтернету (ISP) реєструють та відстежують історію відвідувань через унікальну IP-адресу вашого пристрою. Ця інформація потенційно може бути продана стороннім рекламодавцям, передана уряду або залишена вразливою перед порушенням безпеки. Шляхом маршрутизації на віддалений VPN-сервер замість серверів інтернет-провайдера VPN маскує IP-адресу користувача, запобігає відстеженню постачальником інтернет-послуг та зберігає конфіденційність особистих даних [2].

Типи VPN

Існує чотири основні типи VPN:

1. VPN-брандмауер оснащений як брандмауером, так і можливостями VPN. Цей тип використовує захист, що надається брандмауерами, для обмеження доступу до внутрішньої мережі та забезпечує переведення адрес, автентифікацію користувача, аварійні сигнали та протоколювання.

2. Апаратна VPN забезпечує високу пропускну здатність мережі, а також покращує продуктивність та надійність, але є дорогою.

3. Програмний VPN забезпечує гнучкість з погляду управління трафіком. Це найкраще, коли кінцеві точки не контролюються однією стороною і при використанні різних брандмауерів та маршрутизаторів.

4. Безпечний рівень сокету (SSL) VPN дозволяє користувачам підключатися до VPN-пристроїв за допомогою веб-браузера. SSL використовується для шифрування трафіку між веб-браузером та пристроєм VPN.

Протоколи VPN

Протоколи тунелювання VPN пропонують різні функції та рівні безпеки, і для кожного з них є переваги та недоліки. Існує п'ять основних протоколів тунелювання VPN:

1. SSTP використовує протокол HTTPS для передачі трафіку через брандмауери та веб-проксі, які можуть блокувати інші протоколи. SSTP надає механізм перенесення трафіку протоколу «точка-точка» (PPP) каналом SSL. Використання PPP дозволяє підтримувати надійні методи автентифікації, а SSL забезпечує безпеку на рівні транспорту з розширеним узгодженням ключів, перевіркою шифрування та цілісності.

2. PPTP дозволяє зашифрувати багатопротокольний трафік і обернути його в заголовок, який буде надіслано через мережу інтернет-протоколу (IP). PPTP можна використовувати для віддаленого доступу та VPN-з'єднань «точка-точка». При використанні інтернету PPTP-сервер є VPN-сервером з підтримкою PPTP з одним інтерфейсом в інтернеті та другим інтерфейсом корпоративної інтрамережі. PPTP використовує з'єднання протоколу керування передачею для керування тунелями та інкапсуляції загальної маршрутизації для перенесення кадрів PPP для тунельованих даних.

3. L2TP дозволяє зашифрувати багато-протокольний трафік, а потім використовувати будь-який носій, що підтримує доставку даних PPP, наприклад IP або асинхронний режим передачі. L2TP – це комбінація PPTP та Layer 2 Forwarding (L2F). L2TP представляє найкращі функції PPTP та L2F. На відміну від PPTP, L2TP покладається на IP безпеку (IPsec) у транспортному режимі для служб шифрування. Комбінація L2TP та IPsec відома як L2TP/IPsec. Обидва L2TP та IPsec повинні підтримуватись як клієнтом VPN, так і VPN-сервером. L2TP/IPsec – ідеальна передова таємність.

4. OpenVPN – це програмна програма з відкритим вихідним кодом, яка реалізує методи VPN для створення безпечних з'єднань «точка-точка» або «сайт-сайт» у маршрутизованих або мостових конфігураціях та засобах віддаленого доступу. Він використовує власний протокол безпеки, який використовує SSL/TLS для обміну ключами. OpenVPN дозволяє одноранговим вузлам аутентифікувати один одного за допомогою секретного ключа, сертифіката або імені користувача та пароля. Більшість провайдерів VPN, які використовують OpenVPN, використовують пряму таємність.

5. IKEv2 – це протокол на основі протоколу IPSec, який використовується у Windows 7 та вище. IKEv2 – це стандарт наступного покоління для безпечного обміну ключами між однорангові VPN-пристроями. IKEv2 особливо корисний в автоматичному відновленні VPN-з'єднання, коли користувачі тимчасово втрачають свої з'єднання.

Отже, розглянувши VPN-протоколи, можна порівняти їх за наявністю таких критеріїв, як: багатопротокольне тунелювання, підтримка аутентифікації та шифрування, управління потоком

даних у тунелі, управління правами користувачів, сфера використання, перспективи розвитку. Дане порівняння представлено в таблиці 1 [3].

Таблиця 1. Порівняльні характеристики протоколів VPN

Критерії	Протоколи			
	L2F	L2TP	IPSec	SSL/TSL
Багатопротокольне тунелювання	Так	Так	Так	Ні
Підтримка аутентифікації та шифрування	Відсутнє	Слабке	Присутнє	Дуже надійне
Управління потоком даних у тунелі	Ні	Ні	Так	Так
Управління правами користувачів	Ні	Ні	Ні	Так
Сфера використання	Віддалений доступ через провайдера	Віддалений доступ через провайдера	Для реалізації особистого рішення	Для реалізації особистого рішення
Перспективи розвитку	Слабкі	Існують	Сильні	Сильні

VPN шифрування військового рівня

Шифрування відіграло велику роль протягом тисячоліть. З розвитком сучасних технологій він залишався в авангарді інновацій, постійно розвиваючись. Хоча шифрування змінювалося формою і розвивалося протягом історії, воно завжди працювало однаково. Щоб працювати, шифрування потребує безпечного ключа, який розшифрує та шифрує. Без ключа, здатного розшифрувати зашифрований текст чи алгоритм, шифрування залишиться.

В онлайн-спілкуванні користувачі можуть застосовувати програмне забезпечення для шифрування, щоб захистити свої особисті дані від будь-кого, хто може захотіти заволодіти ними. Використовуючи математичний алгоритм, шифрування шифрує дані

в такий спосіб, що можна розшифрувати лише з допомогою певного ключа. Існує безліч типів шифрування, кожен із яких забезпечує певний рівень безпеки. В даний час найнадійнішим і найчастіше використовуваним шифруванням є AES, також відомий як Advanced Encryption Standard. Він пропонує ключ шифрування розміром до 256 біт, шифрування, яке може протистояти практично будь-якій хакерській атаці.

Як впливає з назви, VPN-шифрування військового рівня – це стандартне шифрування, яке використовується військовими установами. Це найвище доступне шифрування AES. Оскільки військові установи часто діють непомітно, вони зазвичай використовують найкращі доступні протоколи безпеки, щоб гарантувати, що кожна частина інформації залишиться прихованою та зашифрованою.

У зв'язку з цим, коли VPN-сервіс, такий як ZoogVPN пропонує своїм клієнтам стандарт шифрування VPN військового рівня, це означає, що вони надають їм найбезпечніший і надійніший протокол шифрування, доступний в даний час. Користувачі можуть бути повністю впевнені у надійності та безпеці сервісу.

Через те, що це дуже просунута і складна технологія шифрування, не багато VPN-сервісів можуть собі це дозволити. Саме тому більшість VPN-сервісів використовують звичайне чи, у деяких випадках, розширене шифрування. Це все ще досить безпечно та надійно, але набагато слабше, ніж шифрування VPN військового рівня. В ідеалі при виборі VPN-сервісу користувачі повинні шукати той, який пропонує максимально можливі стандарти шифрування.

VPN-шифрування військового рівня — це найкраще, що можна купити за гроші прямо зараз. Він може протистояти практично будь-якій спробі вторгнення. Це пов'язано з тим, що у нього багато рівнів безпеки, тому щоразу, коли хакер порушує один із рівнів, система автоматично закриває його точку входу, і йому доводиться шукати інший вхід. У той самий час, коли система розпізнає порушення, вона починає відстеження самого хакера як контрзаходи. Цей тип шифрування – найкращий спосіб запобігти та зупинити будь-які потенційні порушення безпеки. Щоб відповісти на питання, наскільки безпечно шифрування VPN військового рівня, це надзвичайно безпечно, і цього є більш ніж достатньо для захисту кожного онлайн-користувача. Хоча більшість онлайн-користувачів навіть не замислюються про цей аспект свого VPN-сервісу [6].

Рекомендовані VPN-сервіси для жителів тимчасово окупованої території

1. ExpressVPN;

Цей VPN-сервіс займає перше місце у більшості рейтингів. Його рекомендують різні технологічні видання, наприклад, The Verge. Він зареєстрований на Британських Віргінських островах, тому не підпадає під юрисдикцію урядів США та Європи й не передає дані користувачів до поліції за запитом.

ExpressVPN використовує алгоритм AES (Advanced Encryption Standard) з 256-бітним ключем, також відомий як AES-256. Ця технологія схвалена урядом США і використовується фахівцями з безпеки у всьому світі для шифрування секретної інформації.

Недоліком є ціна: пакет на місяць коштує \$9,9, але ви можете зекономити, придбавши пакет одразу на пів року або рік.

2. VPN Unlimited;

Цей сервіс рекомендує Нацполіція України й такі великі ресурси як Engadget і vpnMentor. Країна реєстрації – США.

Компанія обіцяє захист конфіденційності своїх користувачів, тому не зберігає інформацію про використані сервери, зміст отриманих даних, історію браузера та загальний час з'єднання.

Сервіс VPN Unlimited переказує на допомогу українській армії 30% від своїх доходів і спочатку запропонував українцям безоплатне використання VPN-сервісу на рік. Проте зараз роздачу промокодів на безплатне користування тимчасово припинили.

3. TunnelBear;

Ще один VPN-сервіс, який радить Нацполіція та консультанти з цифрових технологій. Місце його реєстрації – Канада. За замовчуванням використовує надійний алгоритм AES 256. Також має захист від блокування VPN за допомогою технології GhostBear. Таким чином використання VPN буде складніше виявити державним органам, організаціям й інтернет-провайдерам.

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

4. NordVPN;

VPN-сервіс і флагманський продукт компанії Nord Security, що працює в галузі кібербезпеки й підтримується Литовським стартап акселератором. Отримав хороші відгуки провідних технологічних видань світу. Країна реєстрації – Панама.

Протокол шифрування та безпека – NordLynx, OpenVPN, IKEv2. Шифрування AES-256. Приватний DNS, подвійне шифрування даних і підтримка Onion, блокування реклами та шкідливих програм, Kill-Switch.

Коштує цей VPN від \$4,13 на місяць.

5. ClearVPN.

Це VPN від української компанії MacPaw, який став цьогорічним переможцем Global Infosec Award у сфері кібербезпеки.

Попри легкий у використанні функціонал, над проєктом працювали професіонали кібербезпеки. Всі дані користувачів захищені сучасними протоколами, AES-256 шифруванням і додатковою функцією Kill Switch. Розробники гарантують швидке з'єднання та безпеку. Також застосунок має no-logs політику, яка забороняє збирати будь-яку інформацію щодо дій користувача: від IP-адреси до запитів.

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

У Держспецзв'язку зазначають, що краще обрати VPN, в якому є шифрування військового класу (наприклад, AES-256), асортимент протоколів безпеки (OpenVPN, L2TP, IKEv2, WireGuard та інші), захист від витоків через DNS, технологія TrustedServer, яка видаляє всі ваші дані при кожному перезапуску, та функцію автоматичного аварійного відключення [4].

Підтримка зв'язку на окупованих територіях України

На тимчасово окупованих територіях росіяни перевіряють телефони, вимикають зв'язок та обмежують можливість читати українські новини.

На сьогодні до переліку тимчасово окупованих територій частково входять: Донецька, Харківська, Луганська, Запорізька, Херсонська області та АР Крим.

На них окупаційна влада направила інтернет-трафік через Росію – так вони хочуть запровадити цензуру, обмежити мешканцям регіону доступ до українських і світових джерел інформації та тримати людей у тотальній невідомості.

При затриманні чи перевірці документів перевіряються фотографії, читається листування, інтернет переходить під тотальний контроль.

Поради як налагодити зв'язок і убезпечити користування смартфоном та інтернетом:

1. Очищайте телефон. Щоб не спровокувати ворога, видаліть всі листування, фотографії, історію браузера та історію дзвінків. Застосуйте вбудований функціонал додатків, що забезпечують конфіденційність (приватні вкладки браузера, що не зберігають історію, секретні чати із таймером видалення повідомлень).

2. Використовуйте блокування. Можна встановити графічний пароль або спеціальний код. Відключіть функції розблокування обличчям та відбитком пальця – так стороннім буде складніше увійти до важливих програм.

3. Зберігайте копії всіх важливих документів на хмарі або у прихованих папках та альбомах.

4. Використовуйте секретні чати та надсилайте повідомлення, що зникають через деякий час. Фотографуйте через месенджери, не зберігайте ці фотографії на телефоні.

5. Налаштуйте свій смартфон у режим віддаленого управління. У сучасних моделях смартфонів є можливість віддаленого стирання всіх даних на вашому телефоні (для цього необхідно знати пароль до хмарного облікового запису телефону (Google Account, Apple ID, Samsung Account)).

6. Використовуйте VPN.

Сенс роботи VPN – перенаправляти інтернет-з'єднання через сервери в різних точках земної кулі з метою приховати вашу реальну IP-адресу і тим самим обійти блокування.

Обхід VPN-блокування на окупованих територіях

Поради для обходу VPN-блокування:

1. Використовуйте різні VPN-сервіси. Зазвичай блокують IP-адреси найпопулярніших VPN. Але всі доступні VPN заблокувати неможливо.

2. Встановіть свій приватний VPN-сервер. Це означає, що у вас буде своя IP-адреса VPN, яку не буде заблоковано. Щоб його створити, не потрібно бути IT-експертом. В інтернеті є багато статей та посібників зі створення користувацьких VPN-серверів. Але в такому випадку ви не отримуєте стандартних гарантій безпеки, як під час роботи з платними VPN.

3. Використовуйте інший протокол VPN. Сучасні VPN роблять з урахуванням набору з різних протоколів. Деякі з них ставлять в 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 необхідний VPN-протокол. Найкращі VPN-протоколи: WireGuard, OpenVPN, L2tp/IPsec, IKEv2.

4. Налаштуйте свій браузер для обходу блокування. Використовуйте спеціальні VPN-розширення для браузера.

Приховування VPN-програми

Велика ймовірність, що при контакті з окупаційними військами, наприклад у разі перетину лінії розмежування, вони вимагатимуть ваш смартфон на перевірку. Завжди вчасно очищуйте історію браузера та месенджерів. Видаляйте соціальні мережі, які можуть видати вашу проукраїнську позицію та створити вам проблеми під час спілкування з окупантами. Не забувайте також видаляти фотографії та файли (наприклад, завантаження програм VPN). Але намагайтеся, щоб телефон не виглядав підозріло чистим, залиште мем, фотографії сім'ї, нейтральну соцмережу, один очищений месенджер.

Якщо у вас є можливість, видаліть програму VPN, оскільки вона може привернути увагу окупанта. Якщо вам потрібно залишити його на телефоні, є кілька способів приховати його.

На Android-смартфонах ви можете користуватися функцією «приховати програму», якщо ваша версія операційної системи це підтримує. Ви також можете встановити сторонній лаунчер, наприклад Nova Launcher і змінити дизайн іконки будь-якої програми. Так ви зможете замаскувати VPN та будь-яку іншу програму, наприклад, під калькулятор [5].

Висновки та пропозиції. В умовах війни російські війська можуть блокувати доступ до українських державних сайтів та ЗМІ на тимчасово окупованих територіях України. Громадянам України важливо отримувати інформацію про евакуацію, рекомендації державних органів та роботу волонтерів. Якщо користувач знаходиться на території, де сили окупантів блокують доступ до життєво важливих джерел інформації, йому знадобляться засоби обходу блокування сайтів – технологія VPN.

Розроблені поради необхідно використовувати для жителів тимчасово окупованої території України для забезпечення безпеки свої даних, а також для доступу до правдивої інформації.

ЛІТЕРАТУРА

1. Чи є безпечний VPN [Електронний ресурс]. Режим доступу: <https://azure.microsoft.com/ru-ru/resources/cloud-computing-dictionary/what-is-a-vpn/#what-is-a-vpn>.

2. Використання технології vpn для забезпечення інформаційної безпеки [Електронний ресурс]. Режим доступу: <https://cyberleninka.ru/article/n/ispolzovanie-tehnologii-vpn-dlya-obespecheniya-informatsionnoy-bezopasnosti>.

3. Для тих, хто в окупації: підбірка безпечних VPN-сервісів для користування інтернетом [Електронний ресурс]. Режим доступу: <https://henichesk.city/articles/219181/dlya-tih-hto-v-okupacii-pidbirka-bezpechnih-vpn-servisiv-dlya-koristuvannya-internetom>.

4. Держспецзв'язку: Що таке VPN, і як ним безпечно користуватись [Електронний ресурс]. Режим доступу: <https://www.kmu.gov.ua/news/derzhspetsvvyazku-shcho-take-vpn-i-yak-nim-bezpechno-koristuvatis>.

5. VPN, Tor та спілкування у месенджерах. Як підтримувати зв'язок на окупованих територіях. Детальна інструкція [Електронний ресурс]. Режим доступу: <https://forbes.ua/innovations/vpn-tor-ta-spilkuвання-u-messendzherakh-yak-pidtrimuvati-zvyazok-na-okupovanikh-teritoriyakh-detalna-instruksiya-10082022-7616>.

6. Що таке VPN-шифрування військового рівня? [Електронний ресурс]. Режим доступу: <https://zoogvpn.com/military-grade-vpn-encryption/>.

REFERENCES

1. Is VPN secure [Electronic resource]. Access mode: <https://azure.microsoft.com/ru-ru/resources/cloud-computing-dictionary/what-is-a-vpn/#what-is-a-vpn>.

2. Using vpn technology to ensure information security [Electronic resource]. Access mode: <https://cyberleninka.ru/article/n/ispolzovanie-tehnologii-vpn-dlya-obespecheniya-informatsionnoy-bezopasnosti>.

3. For those who are under occupation: a selection of safe VPN services for using the Internet [Electronic resource]. Access mode: <https://henichesk.city/articles/219181/dlya-tih-hto-v-okupacii-pidbirka-bezpechnih-vpn-servisiv-dlya-koristuvannya-internetom>.

4. State Communications: What is a VPN and how to use it safely [Electronic resource]. Access mode: <https://www.kmu.gov.ua/news/derzhspeczvyazku-shcho-take-vpn-i-yak-nim-bezpechno-koristuvatis>.

5. VPN, Tor and communication in messengers. How to maintain communication in the occupied territories. Detailed instructions [Electronic resource]. Access mode: <https://forbes.ua/innovations/vpn-tor-ta-spilkuvannya-u-messendzherakh-yak-pidtrimuvati-zvyazok-na-okupovanikh-teritoriyakh-detalna-instruktsiya-10082022-7616>.

6. What is military-grade VPN encryption? [Electronic resource]. Access mode: <https://zoogvpn.com/military-grade-vpn-encryption/>.

СТАТТЯ НАДІЙШЛА ДО РЕДАКЦІЇ 02.12.2022