УДК 81’25
DOI https://doi.org/10.32782/2710-4656/2024.1.1/38

Єлісєєва С. В.
Одеський державний університет внутрішніх справ

ЛЕКСИЧНІ ОСОБЛИВОСТІ ТА СПОСОБИ ПЕРЕКЛАДУ ДИСКУРСУ «ТЕМНИХ РИНКІВ» ДАРКНЕТУ

Стаття присвячена вивченню особливостей дискурсу «темних ринків» даркнету та способів перекладу лексики, яка використовується в «темної мережі». Звертається увага на поняття «кіберпростору» та «кіберзлочинності», надається пояснення структури та аналізуються особливості використання кіберпростору, який розглядається як окрема сфера життєдіяльності людини. Цілі його використання можуть бути різними, у тому числі з метою скоєння злочинів. Суть незаконних дій у кіберсфері відображається поняттям «кіберзлочину». В Інтернеті були створені окремі певні сайти, які недоступні для громадського пошуку і звичайних громадських браузерів, які стали мати назву Даркнет, від англ. darknet, darkweb – «темна мережа». Системна організація лексики кіберпростору, а саме даркнету, її вивчення та знаходження відповідних способів її перекладу є дуже важливим питанням в аспекті боротьби з кіберзлочінністю, найважливіше за все яку складає незаконна торгівля в темних мережах. Мова даркнету описує поза правові відносини та дії людей, яка є специфічною, має специфічний набір мовних засобів (слів та граматичних засобів) загальновживаної мови. Вона відрізняється специфічним тематичним варіюванням, а також специфічним ситуативним відношенням щодо використання. Згадана мова постійно розвивається та створює свій власний набір лексичних одиниць, термінів, надаючи перевагу певним синтаксичним моделям. Крім вербальних, мова даркнет використовує і невербальні знаки, такі як малюнки, картинки, схеми та ін., та має тісні зв’язки з певними сферами життя, де використовуються специфічні набори мовних одиниць, мовні структури, специфічні способи використання морфології, лексики, синтаксису і організації тексту. Для перекладу контенту даркнета потрібен не тільки переклад окремих слів та виразів, але і локалізація матеріалу, де використовуються невербальні знаки. Мова даркнету включає певні терміни, переклад яких буває доволі важким через специфіку використання. До специфічної лексики даркнету належить також велика кількість абревіатур, переклад яких також є своєрідним викликом для перекладача через їх контекстуальність та специфіку сфери використання. Переклад у сфері кіберзлочинів є своєрідним викликом для перекладача, так як має певні особливості та труднощі. Для цього потрібно залучати професіональних перекладачів, які мають досвід роботи в сфері правоохоронної діяльності та комп’ютерних технологій.

Ключові слова: *кіберпростір, кіберзлочінність, «темна мережа», даркнет, темні вебринки, лексика, переклад, торгівля, послуги, терміни, абревіатура, дискурс.*

Постановка проблеми. На теперешній час все більше набуває важливості захист національних інтересів країни на міжнародному рівні. У зв’язку з швидким розвитком комп’ютерної індустрії стало можливим використання можливостей мережі Інтернет з метою надання різних видів послуг, у тому числі незаконних, що є загрозою як для економічної так і для інформаційної безпеки країни. Тому актуальним є питання розробки ефективних методів боротьби з кіберзлочинністю, які на данному етапі знаходяться в стані становлення і потребують удосконалення.

Для розробки і вдосконалення методів боротьби з кіберзлочінністю необхідно читко і ясно розуміти весь контент прихованих темних мереж інтернету. Для цього потрібно залучати професіональних перекладачів, які мають досвід роботи в сфері правоохоронної діяльності та комп’ютерних технологій. Переклад у сфері кіберзлочинів є своєрідним викликом для перекладача, т.к. має певні особливості та труднощі.

Аналіз останніх досліджень і публікацій. Щоб зазначити останні дослідження в сфері лексики кіберпростору, варто коротко торкнутися її особливостей. Говорячи про кіберпростір та даркнет, про який піде мова в статті, можна сказати, що в цієї сфері формується своя особова специфічна мова, яку використовують користувачі з метою здійснення незаконних операцій або будь-яких незаконних дій за допомогою «темної мережі» Інтер-

нет. Тобто мова даркнету насичена термінологією та абревіатурами, а також загальновживаною лексикою з різноманітних сфер життя, якщо говорити про темні ринки даркнету. Комп'ютерну термінологію та термінологію киберпростору вивчали такі науковці, як Т.Р. Кияк, В.И. Карабан, А.Б. Сарієва, О.В. Гаврилова, І.Б. Ментинська, О.О. Пучков, А.Я. Гладун, І.Я. Субач, К.О. Хала, О.В. Шванова, І.В. Діордіца та багато інших вчених. Але ще залишаються питання щодо способів перекладу деякої специфічної сучасної лексики даркнету, а саме термінології та абревіатур, які використовуються на «темних ринках» мережі Інтернет.

Постановка завдання. Метою статті є висвітлення поняття кіберпростору та кіберзлочінності, даркнету та його «темних ринків», опис та аналіз лексики вказаних ринків і способів її перекладу.

Виклад основного матеріалу. Говорячи про переклад в сфері кіберзлочінності, спочатку необхідно розглянути питання кіберпростору в цілому та кіберзлочіну. Кіберпростір – це середовище, створене організованою сукупністю інформаційних процесів на підставі об'єднаних загальними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем і управління ними [1].

На теперішній час кіберпростір має досить багато визначень. Але при всьому різноманітті визначень, основна увага звертається не на технології, а на діяльність людей, які використовують ці технології [2]. Кіберпростір має матеріальну та нематеріальну складові. До матеріальної складової належать, наприклад, засоби зв'язку, такі як мобільні телефони, рації та інше, засоби обчислювальної техніки, матеріальні складові телекомунікаційних мереж, написання алгоритмів і кодів та інше. До нематеріальної складової кіберпростору належать: інформація, процеси зчитування кодів, процеси передачі інформації між користувачами та інше. Люди створили кіберпростір для своїх власних потреб і задоволення, призначивши його для себе і зробивши його зручним для себе [3].

Кіберпростір можна розглядати як окрему сферу життєдіяльності людини. Можна сказати, що кіберпростір – це простір для інформаційних об'єктів і подій. Можливі приклади об'єктів у кіберпросторі включають в себе такі елементи, як веб-сайт, веб-сторінка, аккаунт на форумі, електронний лист, відеоролик та інші. Щодо подій у цьому просторі, можна вказати на такі явища, як діалог в чаті, обговорення на форумах та блогах, поява нової статті, створення та припинення існування нових сайтів, хакерські атаки на веб-ресурси та інше.

Для всіх цих подій і об'єктів неможливо точно визначити їх приналежність до конкретної країни або сервера. Наприклад, один веб-сайт може розташовуватися на кількох серверах, але в кіберпросторі він може сприйматися як єдиний об'єкт. Крім того, деякі об'єкти у кіберпросторі можуть існувати не фізично на серверах, а бути генерованими "на льоту" при запиті користувача. Зазвичай, фізична структура веб-сайту на сервері відрізняється від логічної структури, яку сприймає відвідувач через кіберпростір.

Досліджуючи кіберпростір як окремий простір для функціонування людини, доцільно звернутися до аналізу чинників, які його формують, впливають на поведінку осіб, визначають характер їхніх дій, а також мають вплив на комунікацію як у самому кіберпросторі, так і в реальному житті.

Можливості та переваги використання кіберпростору майже необмежені. Цілі його використання можуть бути різними, наприклад, для роботи, у навчанні, для розваг та задоволення соціальних потреб, під час встановлення соціальних контактів. Майже будь-яка людська потреба може бути задоволена через або за допомогою комп'ютера та Інтернету. Задоволення потреби може відбуватися у дуже короткий проміжок часу з малими витратами та можливістю анонімності. Кіберпростір дозволяє ігнорувати будь-які соціальні заборони [4].

Вчені з колишнього радянського простору широко використовують такі терміни, як «комп'ютерні злочини», «злочини в сфері комп'ютерної інформації», «злочини, пов'язані з використанням комп'ютерів», «злочини, пов'язані з використанням інформаційних технологій», «кіберзлочин» і т. д. Більшість з цих термінів вказують на порушення, які можуть виходити за межі онлайн простору. У значній мірі суть незаконних дій у кіберсфері відображається поняттям кіберзлочину. Кіберзлочин може бути описаний як протиправне втручання в роботу комп'ютерів, програм, мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні дії, вчинені за допомогою комп'ютерів, мереж та програм [5].

Сучасний Інтернет умовно ділять на три рівні, різницю між якими пояснюють за допомогою метафори айсберга:

1. Clearnet – це вершина: поверхнева, видима та доступна для широкої аудиторії, якою микористуємося щодня і яка містить лише невелику частину всіх мереж та послуг.

2. Deepnet – це частина інтернету, яка знаходиться «під водою» і яку можна знайти тільки занурившись глибше. Тут зберігаються вебре-

сурси, які захищені за допомогою паролів та інших засобів. Це включає серверні системи вебсайтів, портали для онлайн-банкінгу та інші служби, які не є доступними для широкої публіки.

3. Darknet – остання частина айсберга, «темна мережа», доступна за допомогою спеціалізованого програмного забезпечення, найпоширенішим з яких є Tor (TheOnionRouter) [6].

В Інтернеті були створені окремі певні сайти, які недоступні для громадського пошуку і звичайних громадських браузерів, які стали мати назву Даркнет, від англ. darknet, darkweb – «темна мережа». Тут інформація обмінюється в умовах строгої анонімності, створюючи своєрідне підпілля у світі онлайн-комунікацій. На відміну від звичайної частини інтернету, яка відкрита для кожного користувача, даркнет вимагає спеціальних інструментів і знань для навігації.

Своє походження Даркнет бере ще з часів кінця 60-х років, коли була запущена комп'ютерна мережа ARPANET, яка отримувала фінансування від військових і яка стала основою для сучасного Інтернету. Не всі користувачі хотіли співпрацювати з урядами. Намагаючись уникнути контролю, вони використовували адреси, які не були включені в списки мереж.

Початкові форми тіньового Інтернету з'явилися в студентських середовищах, де, за інформацією журналіста Джона Маркоффа, в 70-х роках відбувся перший нелегальний онлайн-продаж марихуани.

У 80-х роках стандартизація протоколів Інтернету посилила проблему збереження конфіденційних даних. Почали з'являтися «сховища даних», тобто сервери, розташовані в країнах з більш лояльним законодавством. Важливим кроком у розвитку даркнету став патент на технологію Onion, який у 1998 році отримав федеральний уряд США і яка утворила основу для системи TOR.

У 2008 році з'явився браузер Tor, що забезпечував анонімність у мережі. Також тоді з'явилася криптовалюта біткоїн, яка підтримує анонімні транзакції. Це все сприяло росту цифрових чорних ринків. У 2011 році був створений Silk Road, який революціонізував тіньовий Інтернет, який провів транзакції на понад $1,2 млрд.

Для забезпечення конфіденційності користувачів даркнет використовує різноманітні технології, серед яких найбільш розповсюдженими є:

1. Tor (The Onion Router): ця система забезпечує анонімність, спрямовуючи трафік через низку добровільних серверів, які називаються вузлами.

2. I2P (Invisible Internet Project): це анонімна мережа, що дає змогу користувачам обмінюватися даними, не розкриваючи свою реальну особистість [7].

Даркнет має як законні, так і незаконні аспекти. До законнів аспектів належать, наприклад, такі, як анонімне спілкування, доступ до інформації, спілкування з людьми з усього світу. До незаконніх аспектів належать торгівля наркотиками та зброєю, поширення екстреміських та різних видів протизаконних відео матеріалів, пропонування послуг вбивств та іншого за замовленням, фрод і шахрайство, крадіжки особистих даних, фішинг, стеження та багато інших протизаконних дій [8].

Незаконне використання даркнету є серйозною проблемою, яка потребує уваги та боротьби з боку правоохоронних органів і суспільства загалом. З цією метою дуже важливо вчасно розкривати злочини, а також сприяти запобіганню створення злочинів за допомогою темних мереж. Так як міжнародною мовою є англійська, в даркнеті використовується саме ця мова. Тому для роботи з темними мережами потрібно розбиратися в певної термінології та взагалі в англійській лексиці, яка там використовується.

Системна організація лексики кіберпростору, а саме даркнету, її вивчення та знаходження відповідних способів її перекладу є дуже важливим питанням в аспекті боротьби з кіберзлочінністю, найважливіше за все яку складає незаконна торгівля в темних мережах.

В даркнеті ми можемо зустріти багато різновидів товару, який заборонений для легального продажу. Для того, щоб розібратися з особливостями перекладу лексики в цьому напрямку, спочатку потрібно систематизувати самі темні ринки та послугі, які там пропонуються. Сьогодні слідчі, які розслідують злочини в Інтернеті, мають справу з різними злочинами на різних веб-платформах. Відтоді, як з'явився вільний доступ до «темної мережі», переважно через браузер Tor, злочинна торгівля в Інтернеті значно розвинулася. В мережі можна знайти все: від контрафактної продукції, що продається в соціальних мережах, до послуг найманих вбивць, які пропонуються в даркнеті. Злочинці також різні. Це може бути безробітна мати, яка продає ліки в соціальних мережах, підліток, який пропонує фальшиві документи на нелегальних ринках у даркнеті, або організована група, що спеціалізується на торгівлі наркотиками та продає свою продукцію за віртуальні валюти. Злочинці використовують методи шифрування, пірингові додатки, соціальну інженерію та віртуальні валюти, але ця діяльність залишає цифрові відбитки, такі як IP-адреси, електронні листи,

біткоїн-гаманці або дані з відкритих джерел, які можуть бути корисними для правоохоронців. Для виявлення подібних злочинів необхідно проводити розслідування в різних онлайн-просторах: соціальних мережах, темній павутині, торгових майданчиках, веб-сайтах, блогах тощо, що потребує корректного перекладу дискурсу.

Існує делілька видів темних ринків. Прикладами темних веб-ринків можуть слугувати наступні: ASAP, AlphaBay, Monopoly, ToRReZ, Hydra.

Щодо товарів або послуг, які пропонуються на темних ринках, то до них відносяться, наприклад, торгівля наркотичними (drugs), хімічними (chemicals), психотропними засобами (psychotropic drugs) та іншими речовинами; торговля вогнепальною зброєю (firearms); відмивання грошей (money laundering); фальшиві ID посвідчення (fake IDs), фінансова інформація (financial data), матеріали дитячої сексуальної експлуатації (child sexual exploitation materials (CSEM)), вбивства на замовлення (murder as a service) та багато іншого.

Для коректного перекладу лексики подібного матеріалу велике значення має контекстуальність та ознайомленість перекладача з специфікою використання тих чи інших слів, а також розуміння неологізмів, які постійно з'являються в чатах онлайн.

Не можна сказати, що в «темній» Інтернет мережі використовується фахова мова, але це є специфічна мова, яка має специфічний набір мовних засобів (слів та граматичних засобів) загальновживаної мови. Мова даркнет відрізняється специфічним тематичним варіюванням, а також специфічним ситуативним відношенням щодо використання. Згадана мова постійно розвивається та створює свій власний набір лексичних одиниць, термінів, надаючи перевагу певним синтаксичним моделям. Можна сказати, що мова даркнет – це субмова, яка має свої лінгво-стилістичні особливості.

Крім вербальних, мова даркнет використовує і невербальні знаки, такі як малюнки, картинки, схеми та ін., та має тісні зв'язки з певними сферами життя, де використовуються специфічні набори мовних одиниць, мовні структури, специфічні способи використання морфології, лексики, синтаксису і організації тексту. Для перекладу контенту даркнета потрібен не тількі переклад окремих слів та виразів, але її локалізація матеріалу, де використовуються невербальні знаки.

У широкому значенні можна сказати, що мова даркнет описує поза правові відносини та дії людей. Так як на ринках даркнету пропонуються послугі з різних сфер діяльності, тому перекладачу потрібно бути освідченним і уважним під час перекладу необхідного матеріалу за предметним змістом, розбиратися в медичних засобах, бути знайомим з лексикою біології та хімії, сфери фінансів, знати способи перекладу військової термінології, зокрема розбиратися у видах та способах використання вогнепальної зброї, та багато іншого. Якщо перекладачу доводиться працювати з матеріалом, наданим йому правоохоронними органами для перекладу онлайн чатів даркнету, в такому випадку йому потрібно знати ще її сленг і жаргонізми, які можуть використовувати наркомани, вбивці та інші злодії та правопорушники. Тобто можна зробити висновок, що мова даркнету відноситься до кримінальної мови, оскільки вже сама мережа та її послуги є нелегальними.

Мова даркнет включає певні терміни, переклад яких буває доволі важким через специфіку використання. В теперешній час існують такі поняття як *clearnet* і *darknet,* які, відповідно, перекладаються як «чиста (прозора) мережа», тобто законна (легальна) і «темна мережа», незаконна (нелегальна). *Chainanalysis* – інструмент для аналізу трансакцій.

Такий вираз як *dead drops* «мертві точки» означає віддаленні місця, де продавець скриває товар, про які він повідомляє покупця. Слово *multisig* (скорочення від *multisignature*), яке перекладається частково калюкою, частково дослівно як «мультипідпис» і означає, що певну нелегальну транзакцію можна підтвердити лише наданням двох або більше закритих приватних ключів. *Escrow* перекладається як «умовне депанування» та означає, що ринок володіє платежем під час покупки, а після отримання товару покупець повідомляє ринок, який завершує угоду, надаючи гроші постачальнику.

Наприклад, розглянемо такі терміни, як *phishing, salami fraud, salami slicing*. *Phishing* – фішинг, представляє собою вид шахрайства, спрямований на отримання особистої інформації від користувачів, такої як номери кредитних карток, бази даних інтернет-магазинів та деталі валютних операцій. Шахраї винаходять різні схеми, щоб змусити користувачів самостійно розкривати конфіденційні дані. Наприклад, вони можуть відправляти електронні листи з пропозиціями підтвердити реєстрацію облікового запису, які містять посилання на веб-сайт в Інтернеті. Зовнішній вигляд цих повідомлень повністю копіює дизайн відомих ресурсів, щоб збільшити ймовірність успіху шахраїв. *Phishing* перекладається або калькуванням, або описовим способом для пояснення

його значення. Щодо перекладу терміну *salami slicing*, то його можна перекласти як «метод або технологія салямі», сутність якого полягає в скоєнні злочину поступово, маленькими кроками, які є непомітними. Наприклад, платежі можуть округлятися, а різниця може поступати на спеціальний рахунок злочинця. Переклад цього терміну у всіх варіантах є калькою або лексичним копіюванням.

Ще один цікавий термін, який зустрічається на ринку даркнету і має певні труднощі перекладу – це *hijacking*, який перекладається як «захоплення/викрадення браузера», переклад виконується за допомогою експлікації. Викрадач браузера – це комп'ютерна програма, яка змінює та модифікує конфігурації браузера на такі, які потрібні зловмиснику. Ціль – шпигунство, збір даних про історію веб-перегляду та пошукові запити користувача, отримання логінів та паролей, які вводяться вручну.

Такий термін, як *drop catching* перекладається експлікацією як «перехоплення домену». Іноді реєстранти відмовляються від свого доменного імені з різних причин. Коли доменне ім'я припиняється, воно стає доступним для реєстрації новим реєстрантом через певний період часу (наприклад, через чотири місяці для доменів в зоні «.eu»). Негайна реєстрація такого доменного імені називається «перехопленням» (drop catching). Ці домени є привабливими для злочинців, оскільки популярність попереднього веб-сайту в домені може привернути інтернет-трафік на їхні незаконні товари та послуги. *Peer-to-peer networks* перекладається як «однорангові мережі», що позначають торгові майданчики, які існують у однорангових мережах, тобто вони не зберігаються в одному місці, а спільно використовуються різними комп'ютерами в різних місцях. Розглянуті терміни відносяться скоріш до технік, які дозволяють скоювати певні злочини в комп'ютерної мережі.

Щодо сфер, пропонованих на ринках даркнету, розглянемо, наприклад, відмивання грошей онлайн (*online money laundering*) (дослівний переклад). Тут використовуються декілька термінів, пов'язаних з цією діяльністю. Такі терміни, як *mixers* і *tumblers* перекладаються калькою «міксери/змішувачі і тумблери», і позначають методи, які використовуються для приховування коштів і яки ускладнюють відстеження транзакцій для правоохоронних органів. Змішувачі використовуються для поділу грошей на дрібні суми і змішування їх з грошима, що належать іншим особам. Потім гроші надсилаються на адреси одержувачів у випадковому порядку, що практично унеможливлює відстеження одержувача грошей, які надходять з адреси, що цікавить слідство. Термін *chain hopping* перекладається як «стрибки по ланцюжку» і означає переключення між різними криптовалютами, часто в швидкій послідовності, щоб втратити трекери, або використовувати певні криптовалюти «конфіденційної монети». Термін *money mule* перекладається калькуванням як «грошовий мул» (інколи ще називають *smurfer* – смурфер) і позначає людину, яка переказує гроші, отримані незаконним шляхом, наприклад, шляхом крадіжки чи шахрайства. Грошові мули переказують кошти особисто через кур'єрську службу або в електронному вигляді від імені інших. Зазвичай за послуги мулу платять невеликою частиною перерахованих грошей [9]. В цілому, аналізуючи терміни, які використовуються в даркнеті можна сказати, що вони доволі образні та метафоричні.

До іншої категорії термінології належать назви будь-яких наркотичних та хімічних препаратів. Наприклад *opioids* – опіоіди, (перекладається калькою/ метод транслітерації), препарати, здатні викликати ейфорію та ті, які приводять до залежності та абстинентного синдрому. *Drug paraphernalia* – наркотичні засоби, спосіб перекладу – заміна частини мови та диференціація значення. *Dissociatives* – диссоціативи (переклад калькою/метод транслітерації), психоактивні речовини, що порушують сприйняття зовнішнього світу та призводять до порушення нормальної роботи свідомості [10]. *Crystal meth shards* перекладається як «уламки кристалів метамфетаміну» (дослівний переклад з використанням транспозиції). В цієї назві зустрічаєтьтся скорочення *meth* від повної форми *methamphetamine* (метамфетамін) – переклад методом транслітерації.

До специфічної лексики даркнету належить також велика кількість абревіатур, переклад яких також є своєрідним викликом для перекладача через їх контекстуальність та специфіку сфери використання. Розглянемо декілька прикладів. Наприклад, абревіатура *RCs (Research Chemicals)* перекладається як психостимулятори, де використовується експлікація як спосіб перекладу. Абревіатура *MDMA (3,4-Methylenedioxy methamphetamine)* – це метилендіоксиметамфетамін (перекладзадопомогоютранслітерації), іншими словами це екстазі або «клубний наркотик» (переклад способом експлікації або описовий спосіб).

Говорячи про безкоштовні програмні засоби анонімізації варто згадати такий як *PGP encryption* – це засіб шифрування, повна форма абревіатури якого є *Pretty Good Privacy*, що перекладається як «досить хороша конфіденційність».

Тут використовується дослівний спосіб перекладу. Абревіатура, яка зустрічається майже на всіх темних ринках даркнету – це *CSEM (Child Sexual Exploitation Materials)*, яка перекладається як «матеріали сексуальної експлуатації дітей». Абревіатура *DD (Direct Deal)* перекладається як «пряма угода» і означає що покупець надсилає гроші безпосередньо постачальнику, надаючи постачальнику контроль над грошима замість ринку. Така угода зазвичай використовується, коли постачальник має добру репутацію. Абревіатура *FE (Finalise Early)* перекладається як «завершення попередньої операції» і означає, що покупець передає платіж постачальнику, а потім покупець просто чекає на товар. Така угода надзвичайно ризикована для покупця. На деяких ринках користувачам пропонується зареєструватися та розв'язати *CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)* – повністю автоматизований публічний тест Тьюринга для розрізнення комп'ютерів і людей) – це один з різновидів заходів безпеки, відомий як автентифікація «виклик-відповідь» [11].

Ще одна цікава абревіатура в даркнеті – це *DDoS (Distributed Denial of Service)*, яка перекладається як «розподілена атака типу «відмова в обслуговуванні»». При DDoS-атаці обсяг масових запитів на сервер перевищує допустимий, що призводить до перевантаження інформаційної системи надлишковим числом запитів, що блокує обробку звернень і робить сервер недоступним для інших користувачів. При перекладі цієї абревіатури поряд з дослівним перекладом використовується експлікація.

Така абревіатура як *PGP (*Pretty Good Privacy) перекладається як «Достатньо надійна конфіденційність» (спосіб перекладу – диференціація значення) і означає програмне забезпечення для шифрування, розроблене для забезпечення конфіденційності, безпеки та автентифікації систем комунікації в режимі онлайн [12]. Абревіатура *ACS (Automated Cards Shops)* перекладається як «автоматизовані магазини карток» (переклад за допомогою транспозиції), де покупець вибирає кредитну картку, яку хоче купити, відповідно до заданих полів (банки, ідентифікаційний номер (*BIN – bank identification number*), місто, штат, поштовий індекс, країна, дата народження, банк, ціна тощо) без безпосереднього спілкування з продавцем. *CVV (Card Verification Value)* перекладається як «код автентифікації картки платіжної системи Visa» (описовий переклад або експлікація).

Висновки. Аналізуючи вищенаведену інформацію, можна зробити висновки, що у рамках кіберпростору даркнета формується мова, яка властива лише даному простору. Кіберпростір даркнету чине вплив на поведінку людей, впливає на комунікацію всередені кіберпростору і в реальному житті. Дискурс даркнету представляє собою систему, що відкрита для взаємодії усередині «темної мережі» та формується через взаємодію різних текстів на одну тему за певними тематиками. Сутність дискурсу виявляється не у відокремленому тексті, а в складній взаємодії багатьох текстів. Можна вважати, що дискурсивність даркнету – це сукупність текстів, що об'єднані спільною тематикою. У дискурсі простежується кілька перспектив в одному тексті, оскільки користувачі включають інші види дискурсу або дискурси інших мовців у свої висловлювання. Щодо способів перекладу лексики, то використовуються такі способи, як дослівний преклад (найчастіш це стосується перекладу хімічних речовин та інших наркотичних засобів), де також в основному застосовується метод транслітерації, експлікація, тобто описовий переклад, калька та диференціація значення. Всі ці способи перекладу можуть варіюватися відповідно контекстуальним значенням слів та можуть бути змішаними у випадку перекладу словосполучень, де найчастіше використовується описовий переклад. Описовий переклад також може бути використаним при перекладі абревіатур. Важливо, щоб при перекладі зберігалося та передавалося внутрішнє значення терміну. В сфері кіберпростору даркнету прослідкується дуже швидка динаміка поповнення галузі новими лексичними одиницями, тому перекладачам необхідно постійно вивчати термінологію та іншу специфічну лексику, яка з'являється в даркнеті, а саме на платформах «темних рикнів».

Список літератури:

1. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ : НІСД, 2014. 328 с. С. 315

2. Бурячок В.Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В.Л. Бурячок, Р.В. Киричок, П.М. Складаний. К., 2018. 320 с.

3. Б. О. Рогожук. Структурно-семантичні особливості лексики кіберпростору в сучасній англійській та українській мовах. *Вісник студентського наукового товариства ДонНУ імені Василя Стуса*, Том 1 № 14 (2022) / Філологія.

4. Музичук А. Психологічні особливості використання кіберпростору. / Волинський національний університет імені Лесі Українки. URL: https://www.inforum.in.ua/conferences/28/95/747 (дата звернення: 7.02.24)

5. Мельник С.В., Тихомиров О.О., Лєнков О.С. До проблеми формування понятійно-термінологічного апарату кібербезпеки. URL: https://tihomalaw.at.ua/publ/kibernetichna_bezpeka/do_problemi_formuvannja_ponjatijno_terminologichnogo_aparatu_kiberbezpeki/2-1-0-5 (дата звернення: 7.02.24)

6. OSINT Investigations. URL: https://mtg-bi.com/blog/darkweb-vs-deepweb (дата звернення: 11.02.24)

7. Online trade in Illicit Goods and services. URL: https://www.cepol.europa.eu/training-education/online-trade-illicit-goods-services (дата звернення: 11.02.24)

8. Розбираємося, що таке даркнет. URL: https://foxminded.ua/shcho-take-darknet/ (дата звернення: 14.02.24)

9. Money mull. URL: https://en.wikipedia.org/wiki/Money_mule (дата звернення (14.02.24)

10. Стійкий галюциногенний розлад сприйняття. URL: https://uk.wikipedia.org/wiki/ (дата звернення: 14.02.24)

11. Що таке CAPTCHA. URL: https://www.google.com/search?q=CAPTCHA&oq=CAPTCHA&aqs=chrome..69i57j0i512l6j69i60.2863j0j7&sourceid=chrome&ie=UTF-8 (дата звернення: 15.02.24)

12. PGP. URL: https://uk.wikipedia.org/wiki/PGP (дата звернення: 21.02.24)

Yelisieieva S. V. LEXICAL FEATURES AND METHODS OF THE "DARK MARKETS" DISCOURSE TRANSLATION ON THE DARKNET

The article deals with studying features of the darknet "dark markets" discourse and ways of the "dark web" vocabulary translation. Attention is drawn to the concepts of "cyberspace" and "cybercrime", the structure and the features of the cyberspace use are explained and analyzed, that is considered as a separate sphere of human activity. The purposes of its use may be different, including the purpose of committing crimes. The essence of illegal actions in the cyber sphere is reflected in the concept of "cybercrime". Special sites were created on the Internet that were inaccessible to public search and regular public browsers, which became known as the Darknet, from English "darknet, darkweb" – "dark network". The systematic organization of the vocabulary of cyberspace, namely the darknet, its study and finding appropriate methods and translations is a very important issue in the aspect of combating cybercrime, the most important of which is illegal trade in dark networks. The language of the darknet describes non-legal relations and actions of people, which is specific and has a specific set of linguistic means (words and grammatical means) of the common language. It is distinguished by specific thematic variations, as well as a specific situational attitude to use. The language of speech mentioned above is constantly evolving and creating its own set of lexical units, terms, preferring certain syntactic models. In addition to verbal language, the darknet also uses non-verbal signs, such as drawings, pictures, diagrams, etc., and has close connections with certain areas of life, where specific sets of linguistic units, language structures, and specific ways of using morphology, vocabulary, and syntax and text organization are used. Translation of darknet content requires not only the translation of individual words and expressions, but also the localization of material that uses non-verbal signs. The language of the darknet includes certain terms, the translation of which can be quite difficult due to the specifics of use. The specific darknet vocabulary also includes many abbreviations, the translation of which is also a challenge for the translator because of their contextuality and specific scope of use. Translation in the field of cybercrime is a specific challenge for a translator, as it has some features and difficulties. In order to do it, you need to involve professional translators with experience in the field of law enforcement and computer technology.

Key words: *cyberspace, cybercrime, dark web, darknet, dark web markets, vocabulary, translation, trade, services, terms, abbreviation, discourse.*