Вішинг є серйозною загрозою для користувачів інтернету, але з правильними заходами захисту можна уникнути попадання у пастку шахраїв. Освіта та свідоме використання інтернет-ресурсів є ключовими в боротьбі з цією формою кіберзлочинності.

***Панченко Євгеній Вікторович***
*начальник 4-го управління Департаменту кіберполіції Національної поліції України, старший науковий співробітник аналітичного відділу (Центр кримінальної аналітики) Національної академії внутрішніх справ*

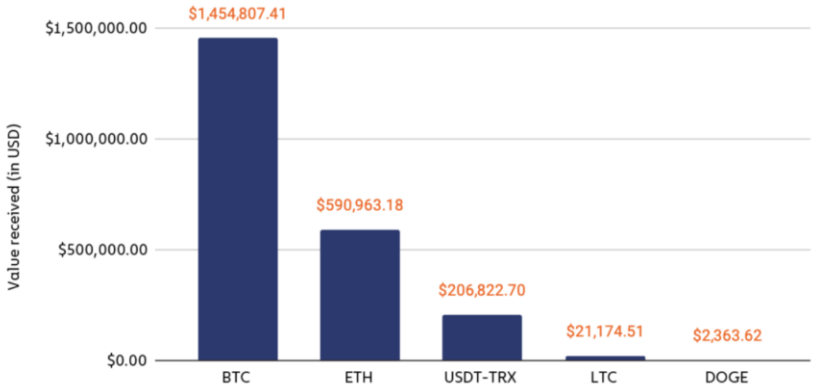
***Овсянюк Дмитро Іванович***
*начальник аналітичного відділу (Центр кримінальної аналітики) Національної академії внутрішніх справ*

## АНАЛІЗ КЛАСТЕРІВ ТА АДРЕС ГАМАНЦІВ ВІРТУАЛЬНИХ АКТИВІВ (КРИПТОВАЛЮТИ) ДЛЯ ЗБОРУ КОШТІВ НА ДОПОМОГУ РОСІЙСЬКІЙ АРМІЇ ТА ІНШИМ НЗФ

Повномасштабна війна в Україні триває більше двох років, рішучі та результативні зусилля українських військових перегорнули сторінку історії, наповнивши її перемогами та звільнивши велику частину територій України (Київську, Чернігівську, Сумську, Миколаївську, Харківську області та частину Херсонської області), що в свою чергу зосередило епіцентр активних бойових дій на Донецьку, Луганську та частину окупованої Запорізької, Херсонської області та АРК Крим, де російські війська супроводжуючись різними незаконними збройними формуваннями, зокрема ПВК «Вагнер» і підбадьорюючись пропагандою російських дезінформаційних кампаній продовжують свою агресію проти України.

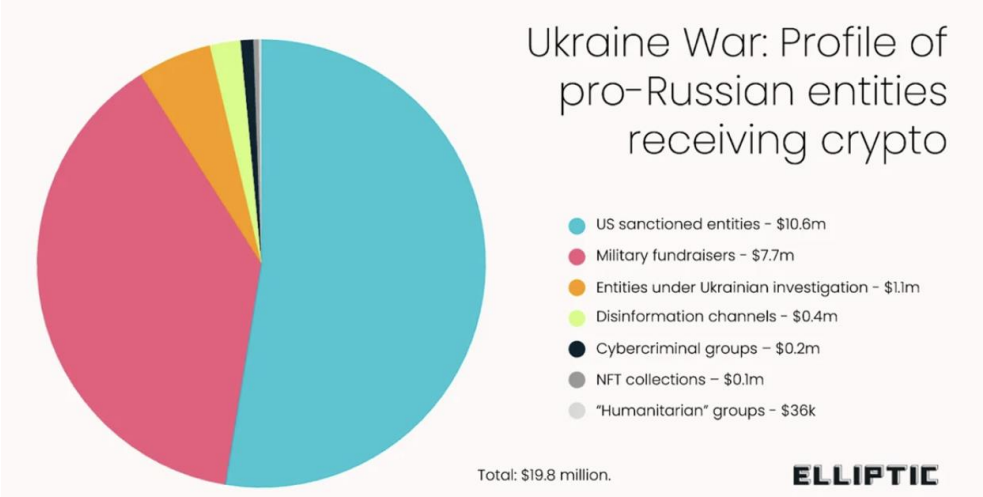
В той же час, з публікацій української розвідки та міжнародних партнерів стає зрозуміло, що існує велика кількість невирішених питань всередині російської армії, що супроводжується неякісним забезпеченням, зменшенням постачань, відсутністю системних підходів до організації зв’язку та навчання тощо. Ряд російських волонтерських груп та їхніх прихильників намагаються виправити ситуацію, в тому числі використовуючи соціальні мережі, зокрема Telegram та VK для збору коштів на військові закупівлі, розвиток БПЛА та радіозв’язку тощо, збираючи пожертви, у тому числі у віртуальних активах (криптовалюті) на закупівлю товарів та компонентів.

Як відомо, більшість криптовалют мають публічні блокчейни, що можуть бути використані для аналізу руху коштів, які надіслані чи відправлені з тієї чи іншої адреси [1]. За даними найвідомішої компанії з аналізу блокчейн «Chainalysis», з початку такими зборами займалися більше 54 організацій, які загалом отримали понад 2,2 мільйона доларів США у криптовалюті, переважно у вигляді Bitcoin та Ether. Також ними отримано значну кількість Tether, Litecoin та Dogecoin [2].




*Статистичні дані щодо збору коштів на підтримку рф*

Тим часом, представники компанії «Eliptic», що також має досвід у аналізі блокчейнів пишуть про 4,2 мільйона доларів, які зібрали росіяни на допомогу своїй армії та іншим незаконним збройним формуванням, що приймають участь у війні проти України. Ця цифра підрахована після накладення санкцій країнами членами НАТО, але до цього моменту цифра з неідентифікованих кластерів наближалася до 20 мільйонів доларів США, заявляють «Eliptic». Багато з цих платежів, ймовірно, є пожертвами, але деякі з них також можуть бути внутрішніми платежами залученим до зборів та створення дезінформації людям. Хоча ця цифра все ще може здатися невеликою порівняно зі зборами, які здійснюються Україною, трохи більше половини цих коштів пов'язані з суб'єктами, на яких поширюються санкції Сполучених Штатів Америки, що підкреслює постійні ризики для легальних сервісів віртуальних активів [5].




*Статистичні дані щодо джерел збору коштів на підтримку рф*

Серед тих, хто потрапив під санкції, є низка осіб, груп і неформальних мереж, які перейшли на криптовалюту з різних причин. Наприклад незаконне збройне формування ПВК «Вагнер», що отримало санкції від США, а також їх інформаційний канал підтримки «Оперативна група «Русич» – для них криптовалюта є джерелом збору коштів на додаток до кампанії пожертвувань у фіатній валюті. Воєнізоване угруповання «Русич», пов'язане з ПВК «Вагнер», серед суб'єктів, що потрапили під санкції OFAC (OFAC – Управління по контролю за іноземними активами Міністерства фінансів США), зібрало сотні тисяч доларів пожертв у криптовалюті. Адреси для пожертвувань були поширені через численні акаунти в соціальних мережах.

Для інших криптовалюта використовується більше як заохочення [3]. Високопосадовці так званої «Донецької народної республіки», серед яких є колишні організатори криптовалютних фінансових пірамід та особи, що потрапили під санкції, стверджують, що оплачують криптовалютою інформацію про позиції українських військових.

Під час нашого дослідження встановлено, що криптовалютні пожертви, надіслані цим організаціям, використовувалися на різні потреби - від фінансування проросійських пропагандистських сайтів до закупівлі військових товарів, таких як дрони, зброя, бронежилети, засоби зв'язку та інші засоби забезпечення.

Акаунти, які підтримують незаконні збройні формування, а також російську армію, часто публікують фотографії придбаного обладнання та опис того, як будуть використані майбутні пожертви. Ось один з таких дописів (переклад з російської): нам залишилося зібрати всього 150 тисяч рублів на безпілотник, який зможе привозити «подарунки» на позиції наших українських «друзів». Сподіваємося, що нам вдасться зняти його на відео і порадувати вас цікавими кадрами [4]. Оскільки один рубль коштує менше ніж 0,011 долари США, компоненти, необхідні для побудови БПЛА обійшлися цій групі лише у 3 400 доларів США (це було загальною ціллю збору). Отже, хоча багато організацій, які здійснювали збори, досягли лише чотиризначної цифри за рахунок збору коштів у криптовалюті, ці кошти все одно можуть зробити значний внесок у підвищення ефективності цих формувань.

Шляхом аналізу кампаній зі збору коштів, ми виявили низку підсанкційних осіб, які сприяли збору пожертв у криптовалюті на підтримку війни Росії в Україні. Олександр Жучковський, громадянин Росії, внесений до списку OFAC, використовував соціальні мережі для збору пожертв на користь терористичного угруповання «Російський імперський рух». Жучковський також підтримував проект «Террікон», який збирає пожертви у криптовалюті для підтримки НЗФ на Донбасі. На своєму сайті Terricon прямо вказував, що використовує криптовалюту у зв'язку з введенням санкцій, і навіть пропонував кілька NFT для збору коштів. Однак зараз сайт вже не активний, його було заблоковано [6].

Аналіз криптовалютних гаманців Terricon відображає його незаконний характер. Організація отримала приблизно 11% своїх коштів опосередковано від міксерів і відправила понад 29% своїх коштів на Bitzlato – біржу зі штаб-квартирою в Москві, яка сприяла відмиванню криптовалют на суму близько 1 мільярда доларів з 2019 року.


*На зображенні джерело та кінцевий кластер надісланих коштів на гаманці проекту Terricon*

Ми також виявили інші підсанкційні акаунти, пов'язані з благодійними рахунками для збору коштів на військових рф. Дописи з проросійського військового блогу «Рыбарь», який в тому числі збирає координати розташування українських військових, публікує недостовірну інформацію про російський наступ, були поширені широким колом проросійських акаунтів у соціальних мережах, включно з «Союзом добровольців Донбасу», на який OFAC наклав санкції 28 червня 2022 року.

Кілька операторів акаунтів у соціальних мережах вказали, що пожертви, надіслані їм, будуть безпосередньо спрямовані на користь «Донецької народної міліції» та «Луганської народної міліції», які в свою чергу пов'язані з «Народним ополченням Донбасу» - організацією, на яку 19 грудня 2014 року накладено санкції OFAC.

Переходячи до безпосередньо джерел походження фінансування кластерів зі збору коштів на допомогу армії рф, хотілось би акцентувати увагу, на те від кого надходять кошти, враховуючи, що увесь цивілізований світ маркує та позначає ці кластери як незаконні, а ті хто надсилає кошти стає спонсором російського тероризму. Найвірогідніше, і це помітно з результатів аналізу, що більша частина коштів вже мають незаконний характер, зокрема не тільки підсанкційний, але й пов'язаний з діяльністю нарко-шопів, послугами та товарами в дарк-нет, вірусами-вимагачами тощо.

Серед типових кампаній зі збору коштів на підтримку росії «Русич», «Катя-Валя», «Записки Ветерана» отримали найбільшу частину коштів саме від Дарк-нет маркетів, санкційних організацій, незаконних криптобірж та афілійованих з росією хакерських угруповань, в тому числі, які використовують та поширюють віруси вимагачі. На зображенні видно, що умовно не пов'язані за сферою діяльності незаконні кластери переплітаються і мають зв'язок з кластерами для допомоги російським військовим. Це не викликає подиву, адже саме така допомога незаконним збройним формуванням може безперешкодно здійснюватися без ризику втратити кошти, адже легітимні операції зазвичай блокуються у разі сумнівності джерела походження коштів.

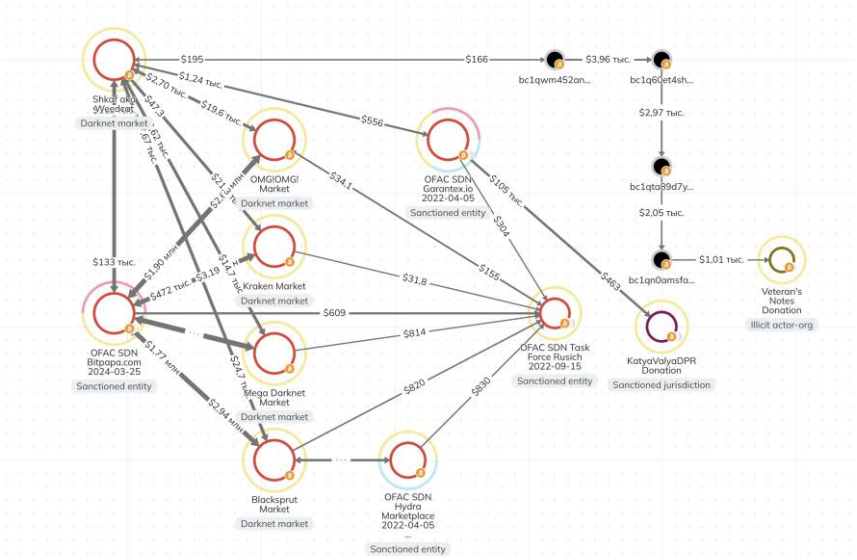



*Схема руху коштів з незаконних кластерів, які фінансують терористичні угруповання та армію росії у війні проти України*

Головною метою цього дослідження є бажання показати, що у повномасштабній війні, яка розпочата росією проти України, росіяни задіюють усі можливі джерела фінансування, у тому числі ті, що здійснюють негативний вплив на увесь світ (віруси вимагачі, дарк-нет маркетплейси, нарко-шопи), а отже і боротьба з НЗФ та особами, які збирають кошти з використанням віртуальних активів має бути комплексною, не лише на полі військових дій.

Усі наявні ресурси правоохоронних органів цивілізованого світу мають приділити увагу потокам коштів, які йдуть на фінансування росії та НЗФ, що приймають участь у війні проти України, адже рівень їх підтримки залежить на пряму від незаконних дій, що вчиняє злочинний елемент у середині країн Європейського союзу, Сполучених Штатів Америки та інших країнах. Усі ці факти можливо дослідити шляхом аналізу дарк-нет, а також подальшого руху коштів у криптовалюті.

## Список використаних джерел:

1. Носов, В. В., Манжай, О. В. і Панченко, Є. В. (2022) «Аналіз етеріум-трансакцій під час попередження та розслідування кримінальних правопорушень», Право і безпека, 87(4), с. 108-124. doi: 10.32631/pb.2022.4.09.

2. Російські кампанії зі збору коштів у війні проти України [електронний ресурс] режим доступу: https://www.chainalysis.com/blog/pro-russian-crypto-donations-war-in-ukraine/

3. Прокремлівські неонацистські угрупування підбурюють до тортур та вбивств цивільного населення в Україні [електронний ресурс] режим доступу: https://www.theguardian.com/world/2022/oct/02/pro-kremlin-neo-nazi-militia-inciting-torture-murder-ukrainian-prisoners

4. Проект «Призма» та Олексій Муратов пов’язані особи з донецькими сепаратистами [електронний ресурс] режим доступу: https://behindmlm.com/companies/prizm-ponzi-and-aleksey-muratov-linked-to-donetsk-separatism/

5. Аналіз криптоплатежів на підтримку армії рф [електронний ресурс] режим доступу: https://www.elliptic.co/blog/analysis/crypto-payments-to-russian-military-fundraisers-reaches-20-million-amid-ukraine-counter-offensive-and-wagner-revolt

6. Веб-ресурс «Террікон» присвячений кампанії зі збору коштів на підтримку рф [електронний ресурс] режим доступу: https://web.archive.org/web/20220623213541/https://terricon.org.

***Поворознік Артем В’ячеславович***
*аспірант Міжнародного гуманітарного університету*

## ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ШТУЧНОГО ІНТЕЛЕКТУ У ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ

Торгівля людьми, незважаючи на сучасний стан рівня розвиту суспільства та стан захищеності прав людини, залишається однією з найбільш актуальних проблем сучасності. Аналіз довоєнних статистичних даних Національної поліції України демонструє, що левову частку узагальнених статистичних даних цього злочину становить торгівля людьми з метою сексуальної експлуатації – 53%, з яких 59% становлять жінки, 27% хлопчиків і 14% чоловіків. Враховуючи ці дані, окремо варто відзначити високу латентність, яка становить 70% цієї кримінальної категорії [1, с. 26].

У цілому торгівля людьми має багатоаспектні прояви, включаючи сексуальне рабство, примусову працю, торгівлю органами та інші форми експлуатації. Порушена проблематика є глобальною масштабною проблемою, яка вимагає комплексного підходу та інноваційних стратегій для її подолання. У цьому контексті використання різного роду інформаційних технологій та технологій на основі штучного інтелекту набуває актуальності в боротьбі з торгівлею людьми. Інноваційні підходи та інтелектуальні рішення, що базуються на аналізі даних (у тому числі даних із відкритих джерел) та автоматизації аналітичних процесів, можуть сприяти виявленню, запобіганню та розслідуванню випадків торгівлі людьми, що дозволить забезпечити ефективнішу реакцію органів правопорядку та захист прав потерпілих.

Умови сьогодення, актуалізують проблематику застосування інформаційних технологій та штучного інтелекту у протидії торгівлі людьми. Сучасні технологічні рішення, які можуть бути застосовані для попередження злочинів у сфері торгівлі людьми, виявлення їх ознак та надання допомоги жертвам мають