УДК 343.98

ВЕЙЦ А.М., *доктор філософії,* старший помічник начальника відділу забезпечення якості освітньої діяльності та вищої освіти військової академії.
ORCID: https://orcid.org/0000-0002-7454-1534.

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ, ВЧИНЕНИХ У ВІЙСЬКОВОМУ СЕРЕДОВИЩІ

Анотація. *У статті досліджуються особливості розслідування кіберзлочинів, вчинених у військовому середовищі. Наголошується на загрозі злочинності у військовому кіберпросторі як основному чиннику негативного впливу на об'єкти критичної інформаційної інфраструктури, передусім системи управління державою, об'єктів життєзабезпечення, електроенергетики, транспорту, ядерної і хімічної промисловості, банківської сфери тощо. Виокремлено й проаналізовано чинники, які ускладнюють процес досудового розслідування, зокрема обмежені можливості фіксації обстановки вчинення кіберзлочину та слідової картини, існування ризику для особистої безпеки слідчого, представників правоохоронних органів під час проведення слідчих (розшукових) дій на території ведення активних бойових дій, наявність спеціального суб'єкта кримінального правопорушення, а також можлива протидія з боку командирів військових підрозділів у випадках неналежного виконання ними службових обов'язків, що стало умовою вчинення кримінального правопорушення їх підлеглим. Окрема увага приділена пошуку варіантів вирішення даних проблемних питань, в результаті чого сформульовано власні пропозиції щодо покращення якості розслідувань кримінальних правопорушень у військовому середовищі, вчинених у кіберпросторі. Висвітлюються перспективи подальших досліджень у вказаному напрямку, які включають продовження розробки методики і стандартів для проведення слідчих (розшукових) дій з урахуванням специфіки військового кіберпростору, прогнозування наслідків імплементації міжнародного досвіду, зокрема країн-членів НАТО, у вітчизняні криміналістичні технології, а також вдосконалення технологічних інновацій для покращення якості розслідувань кримінальних правопорушень у військовому середовищі, вчинених у кіберпросторі.*

Ключові слова: *кіберзлочинність, військове середовище, досудове розслідування, цифрові сліди, штучний інтелект, кібербезпека.*

Summary*. The article examines the peculiarities of investigating cybercrimes committed in a military environment. It emphasizes the threat of criminal activity in the military cyberspace as a major factor negatively impacting critical information infrastructure, particularly state governance systems, essential services, energy, transportation, nuclear and chemical industries, and the banking sector. The article identifies and analyzes factors that complicate the pre-trial investigation process, including limited capabilities for documenting the scene of the cybercrime and the evidence collected, the risk to the personal safety of investigators and law enforcement representatives during investigative activities in areas of active hostilities, the presence of a specialized entity committing the criminal offense, and potential resistance from military unit commanders in cases of improper execution of their duties that facilitated the commission of the crime by their subordinates. Special attention is given to finding solutions to these problematic issues, resulting in the formulation of proposals aimed at improving the quality of investigations into criminal offenses in military settings committed in cyberspace. The article outlines the prospects for further research in this area, which include the continued development of methodologies and standards for conducting investigative activities considering the specifics of military cyberspace, forecasting the implications of implementing international practices, particularly from NATO member countries, into domestic*

forensic technologies, as well as enhancing technological innovations to improve the quality of investigations into criminal offenses in military environments committed in cyberspace.

Keywords: *cybercrime, military environment, pre-trial investigation, digital footprints, artificial intelligence, cybersecurity.*

Постановка проблеми. В реаліях сьогодення кіберзлочинність стала однією з найсерйозніших загроз для національної безпеки, оскільки здатна негативно впливати на більшість функцій держави, включаючи її обороноздатність. Здійснюючи протидію військам країни-агресора, яка розпочала повномасштабне вторгнення на територію України в 2022 році, Збройні Сили дедалі частіше стають об'єктами атак із використанням електронно-обчислювальних систем і комп'ютерних мереж, а це, в свою чергу, наражає на небезпеку не тільки військову, а й цивільну інфраструктуру. Надзвичайно актуальною загрозою на сьогодні є розвідувально-підривна діяльність у кіберпросторі проти України, яка пов'язана з проведенням спецслужбами іноземних держав, насамперед РФ, розвідувальної діяльності з метою викрадення інформації та підривних акцій з порушення штатного режиму функціонування об'єктів критичної інформаційної інфраструктури, передусім систем управління державою, об'єктів життєзабезпечення, електроенергетики, транспорту, ядерної і хімічної промисловості, банківської сфери [1, с. 105]. Правоохоронці стикаються з непоодинокими випадками залучення до подібної деструктивної діяльності осіб, які знаходяться безпосередньо на території нашої держави та з тих чи інших мотивів вчиняють кіберзлочини. Особливо небезпечних рис набуває ситуація, коли злочинцями виявляються службові особи або такі, які здійснюють професійну діяльність, пов'язану з наданням публічних послуг, або навіть військові посадові особи.

Процес досудового розслідування вчинених у кіберпросторі кримінальних правопорушень саме у військовому середовищі ускладняється низкою чинників, пов'язаних зі специфікою проходження військової служби: конфіденційністю переважної більшості даних у зв'язку з наявністю грифу "Для службового користування", "Таємно", "Цілком таємно", динамічністю обстановки в операційних зонах, складністю збору й аналізу цифрових доказів в умовах бойових дій тощо. Незважаючи на те, що законами України передбачено механізми й алгоритми проведення досудового розслідування кіберзлочинів, брак уніфікованих стандартів і протоколів, які б регламентували слідчі дії, коли йдеться про комп'ютерні злочини у військовому середовищі, на нашу думку, знижує ефективність правоохоронних органів, призводить до втрати так званих "віртуальних", або "комп'ютерно-технічних слідів" [2, с. 305]. Отже, існує потреба в розробці нових підходів до розслідування кіберзлочинів, які враховують специфіку військового середовища, технологічні інновації та досвід бойових дій на території нашої держави.

Результати аналізу наукових публікацій. На сьогодні проблематика досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі, розглядається у працях як зарубіжних, так і вітчизняних вчених. Процес збирання, використання та застосування доказів кіберзлочинів досліджували І.О. Воронов [3], О.А. Самойленко [4], А.Ф. Волобуєв [5], Б.М. Головкін, О.І. Денькович, В.В. Луцик, Д.М. Цехан [6], М.О. Кравцова [7]. Аналіз впровадження інноваційних засобів досудового розслідування кіберзлочинів є предметом уваги таких науковців, як В.А. Коршенко [8], В.М. Шевчук [9], А.С. Колодіна, Т.С. Федорова [10], І.М. Осика, А.О. Калюжна, О.А. Матвієнко [11] тощо.

Однак у науковому дискурсі залишаються недостатньо вивченими особливості досудового розслідування кримінальних правопорушень, вчинених у військовому кіберсередовищі.

Метою статті є визначення особливостей розслідування кіберзлочинів, вчинених у військовому середовищі, з акцентом на виявленні чинників, що ускладнюють цей процес, та розробці нових алгоритмів і підходів, які забезпечать ефективність розслідувань у контексті сучасних технологічних викликів та специфіки військової служби.

Виклад основного матеріалу. З кожним роком кількість кримінальних правопорушень, пов'язаних з незаконним втручанням або використанням електронно-обчислювальних систем і комп'ютерних мереж, невпинно зростає. Характеризуючи ознаки кіберзлочинів, Б.М. Головкін, О.І. Денькович, В.В. Луцик і Д.М. Цехан слушно зауважують, що найбільш істотним з проявів "…кримінально протиправної поведінки, які належать до кіберзлочинів, є те, що у процесі їх вчинення задіяні інформаційні (комп'ютерні) системи… Тобто у процесі вчинення (скоєння) кіберзлочину злочинець використовує особливі можливості, властивості, якими наділені інформаційні (комп'ютерні) системи для реалізації свого кримінально протиправного умислу" [6, с. 30]. Стрімкий технологічний прогрес, як наслідок, призводить до того, що зловмисники постійно нарощують свої фахові знання та навички маскування злочинних дій у кіберпросторі, вдосконалюючи з цією метою багаточисленні бекдори, анонімайзери, VPN- або TOR-мережі, експлойти, інструменти для фішингу тощо.

Станом на сьогодні, після прийняття Верховною Радою Закону України "Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану" [12], кримінальна відповідальність за вчинення кіберзлочинів у вітчизняному законодавстві передбачена розділом XVI Кримінального кодексу України, який включає в себе статті:

361 – *Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж;*

361^1 – *Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут;*

362 – *Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї;*

363 – *Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється";*

363^1 – *Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку)*,

а також частиною четвертою статті 190 – *Шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки*

та статтею 258^5 Кримінального кодексу України *(Фінансування тероризму)* – у разі використання комп'ютерних технологій.

Крім того, деякі кримінальні правопорушення у кіберпросторі залежно від елементів їхнього складу можуть бути кваліфіковані за сукупністю з іншими статтями КК України. Повномасштабне вторгнення на територію України, розпочате рф у 2022

році, наклало свій відбиток на ситуацію в державі з кібербезпекою: під час дії правового режиму воєнного стану кримінальні правопорушення, вчинені у кіберпросторі, створюють додаткову загрозу національним інтересам, оскільки можуть бути направлені на дестабілізацію внутрішньої ситуації, пошкодження об'єктів критичної інфраструктури, формування підґрунтя для проведення розвідувальних операцій на користь країни-агресора тощо.

Окрему категорію складають кіберзлочини, вчинені у військовому середовищі. Їхня специфіка обумовлена багатьма факторами, серед яких: конфіденційність даних, доступних військовослужбовцям, робота з державною таємницею, використання спеціалізованого програмного забезпечення та вимоги до наявності відповідних технічних знань, вплив стресових умов на особовий склад тощо. В сукупності з агресією рф, що виражається не тільки у застосуванні збройної сили на болі бою, а й у використанні комп'ютерних інструментів проти нашої держави, це робить військове середовище вразливим до злочинних дій, пов'язаних зокрема із використанням електронно-обчислювальних систем і комп'ютерних мереж.

В сучасних реаліях перед правоохоронними органами, залученими до проведення досудових розслідувань кіберзлочинів, вчинених у військовому середовищі, постає низка проблемних питань:

1. ***Фіксація обстановки вчинення кіберзлочину та слідової картини.*** Так, якщо обстановкою вчинення даного кримінального правопорушення виступає безпосередньо кіберпростір [6, с. 98], сліди становлять будь-які інформаційні зміни у даному середовищі. Отже, слідчому необхідно отримати доступ до предмету вчинення злочину або іншої електронно-обчислювальної машини, комп'ютерної мережі, в якій відбилися сліди злочину, що може бути ускладнено обмеженням доступу до таких машин і мереж, особливо в умовах дії правового режиму воєнного стану. Крім того, сучасні технології та засоби дозволяють зловмисникам приховано вносити зміни в сліди злочину як до його виявлення, так і безпосередньо під час досудового розслідування.

2. ***Існування ризику для особистої безпеки слідчого, представників правоохоронних органів під час проведення слідчих (розшукових) дій на території ведення активних бойових дій.*** Враховуючи, що в зонах активних бойових дій збір інформації часто обмежений через небезпеку, відсутність доступу та логістичні проблеми [13, с. 295], ефективність досудових розслідувань кіберзлочинів, які вимагають безпосередньої присутності правоохоронців у зонах збройного конфлікту, може суттєво знижуватися. В даному контексті, на нашу думку, слід зауважити, що негативну роль відіграє відсутність в Україні повноцінної системи військової юстиції, яка включала б спеціалізований орган досудового розслідування з окремим департаментом контррозвідувального захисту інтересів держави у сфері інформаційної безпеки у його складі, укомплектований військовослужбовцями, спеціалізовану військову прокуратуру та спеціалізовані військові суди. Запровадження такої системи розширило б можливості удосконалення досудового розслідування в умовах воєнного стану, на даний момент зведеного до прийняття Закону України "Про внесення змін до Кримінального процесуального кодексу України щодо удосконалення порядку здійснення кримінального провадження в умовах воєнного стану" [14].

3. ***Наявність спеціального суб'єкта кримінального правопорушення.*** В деяких випадках кіберзлочини у військовому середовищі можуть вчинятися службовими особами або такими, які здійснюють професійну діяльність, пов'язану з наданням публічних послуг. Найскладнішою вважаємо слідчу ситуацію, коли зловмисником виявляється військова посадова особа. Наявність у таких злочинців глибоких фахових

знань, безперешкодного доступу до службових електронно-обчислювальних систем і комп'ютерних мереж, систем оперативного управління тощо, а в деяких випадках і бойового імунітету, – надає їм змогу приховано втручатися в кіберпростір, знищувати фізичні та цифрові сліди. В даному контексті погоджуємось із твердженням Б.М. Головкіна, О.І. Денькович, В.В. Луцика та Д.М. Цехана про те, що "можливість оперативно змінювати зміст сайту, фізичне розташування серверів на території інших держав, використання анонімних програмних пакетів є факторами, які суттєво ускладнюють можливість фіксації цифрової інформації. Особливої гостроти ця проблема набуває у зв'язку з тим, що встановлення факту такого порушення є чи не найвагомішою складовою процесу доказування у відповідних провадженнях" [6, с. 134-135].

4. ***Можлива протидія з боку командирів військових підрозділів у випадках неналежного виконання ними службових обов'язків, що стало умовою вчинення кримінального правопорушення їх підлеглим*** [15, с. 217]. Як слушно зазначає О.С. Тарасенко, даний фактор в умовах воєнних дій може мати негативний характер, а тому "…суттєво ускладнює проведення процесуальних дій та вимагає свого врахування" [15, с. 216]. Така протидія може виражатися в ухиленні від процесуальних дій, що полягають у проведенні досліджень і необхідних судових експертиз, забезпеченні збереженості отриманих комп'ютерних даних, включаючи дані про рух інформації, які були згенеровані і збережені за допомогою комп'ютерної системи [16, с. 28], та навіть затриманні підозрюваного. Розслідування кримінальних правопорушень, вчинених у кіберпросторі військовими посадовими особами, вимагає особливого теоретико-правового забезпечення, з урахуванням усіх можливих факторів негативного впливу на хід розслідування, яке на сьогоднішній день є недостатнім та потребує суттєвого удосконалення.

На думку А.Ф. Волобуєва, для успішної боротьби зі злочинами, де комп'ютер використовується як їхнє знаряддя, зокрема, необхідно здійснити "…розробку методик розслідування злочинів, пов'язаних з використанням комп'ютерної техніки, а також розвиток експертизи електронних засобів та програмного забезпечення… як один із пріоритетних напрямків розвитку наукових досліджень у криміналістиці та судовій експертизі" [5, с. 70].

В.С. Давиденко підкреслює, що "розслідування кримінальних правопорушень у військовому середовищі – складний та багатогранний процес, який у межах дослідження предмета доказування у кримінальному провадженні вимагає встановлення й аналізу низки обставин і їх джерел" [17, с. 105-106]. До того ж, "протидія правопорушенням у кіберпросторі та активна кібероборона під час воєнного стану вимагає нових підходів та методів, удосконалення чинного законодавства у зазначеній сфері та дослідження проблемних питань діяльності правоохоронних органів щодо розслідування кіберзлочинів та протидії кібероперацій держави-агресора" – пише М.В. Гуцалюк [18, с. 109].

Підтримуючи бачення вищезазначених вчених, вважаємо за доцільне зауважити, що під час досудового розслідування кіберзлочинів, вчинених у військовому середовищі, не завжди можуть бути застосовані в повному обсязі традиційні методики розслідування злочинів саме через специфічні ознаки вказаного середовища. Аргументом на користь даного твердження є й те, що згідно Єдиного звіту про кримінальні правопорушення за січень-грудень 2023 року, оприлюдненого Офісом Генерального прокурора, за вказаний період зареєстровано 3841 кримінальне правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, з них направлено

проваджень до суду – 2455, у яких на кінець звітного періоду рішення про закінчення або зупинення провадження не прийнято – 1274 [19]. Воєнні реалії сьогодення й аналіз слідчо-судової практики дають змогу зробити припущення, що певна кількість цих кримінальних правопорушень була вчинена у військовому середовищі.

Отже, наступним кроком після визначення специфічних проблемних питань, що виникають на етапі досудового розслідування досліджуваної категорії кіберзлочинів, вбачається необхідність пошуку варіантів їхнього вирішення. Розглянувши різні підходи, описані як у зарубіжних, так і у вітчизняних наукових доробках, а також врахувавши аспекти правового режиму воєнного стану, що триває в Україні з 2022 року, ми сформулювали власні пропозиції щодо покращення якості розслідувань кримінальних правопорушень у військовому середовищі, вчинених у кіберпросторі.

По-перше, здається раціональним відновлення повноцінної системи військової юстиції, умовними "трьома китами" якої є: військова поліція, до функцій одного зі структурних підрозділів якої повинен належати контррозвідувальний захист інтересів держави у сфері інформаційної безпеки та здійснення оперативно-розшукових заходів у цій сфері; військова прокуратура та військові суди. На даний момент досудове розслідування, підтримання державного обвинувачення та винесення судових рішень, що стосуються Збройних Сил, здійснюється виключно цивільними особами, які часто не мають відповідної підготовки, а також не можуть і не повинні виконувати визначені законом обов'язки з ризиком для життя в бойових умовах, тоді як укомплектування таких структур особами зі статусом військовослужбовців у тому числі сприятиме всебічному розкриттю обставин кримінальних правопорушень, вчинених у військовому кіберсередовищі. Досліджуючи організацію діяльності системи військової юстиції у державах-членах НАТО, П.П. Богуцький доходить висновку, що в цих державах визнаним "…є підхід щодо унеможливлення якісної діяльності у системі військової юстиції цивільних інституційних утворень, а також щодо обов'язковості забезпечення належного рівня військової підготовки слідчих, прокурорів… суддів" [20, с. 218]. В контексті реалізації стратегічного курсу євроатлантичної інтеграції О.В. Шамара справедливо зазначає, що "утворення системи органів Військової юстиції України – це шлях, який відповідатиме реалізації положень Стратегії національної безпеки України, у тому числі у сфері зміцнення особливого партнерства з НАТО та набуття повноправного членства в Організації Північноатлантичного договору, в частині взаємосумісності Збройних Сил України та інших складових сектору безпеки і оборони з відповідними структурами держав Альянсу…" [21, с. 245]. Окрім того, військова кібербезпека передбачає по суті комплекс унікальних процесів і рішень задля захисту мереж, пристроїв і систем військового призначення від несанкціонованого доступу, які є відмінними від засобів, використовуваних з тією самою метою в цивільній сфері. Високий рівень технічного забезпечення вчинення злочинів у кіберпросторі та конспірації злочинцем такої діяльності актуалізують необхідність залучення суб'єкта спеціальних знань у процес їх розслідування [4, с. 281]. Відсутність у слідчого специфічних знань, відповідного досвіду та рівня розуміння таких процесів є передумовою до формування несприятливої слідчої ситуації.

По-друге, важливою складовою вдосконалення системи розкриття комп'ютерних злочинів, вчинених у військовому середовищі, є впровадження в процес досудового розслідування та судової експертизи інноваційних, високоінтенсивних технологій, адаптованих до завдань, які стоятимуть перед слідчими департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки майбутнього органу досудового розслідування. Сучасна криміналістика вже

використовує технології біометричної ідентифікації для впорядкування автоматизованої системи кримінальної реєстрації, проведення судових фоноскопічних експертиз, судових молекулярно-генетичних експертиз тощо, і у слідчо-судовій практиці можна прослідкувати чітке підтвердження ефективності даних технологій у контексті розслідування кримінальних правопорушень у військовому середовищі. Однак, враховуючи властивості кіберпростору та його обстановку, необхідно зазначити, що для ефективного розслідування саме таких злочинів дедалі важливішим стає використання засобів штучного інтелекту. Створення нових програм на основі методів штучного інтелекту й адаптація вже існуючих теоретично дозволить більш точно фіксувати обстановку вчинення злочину шляхом:

1) аналізу та інтерпретації великого обсягу даних, що міститься в предметі вчинення злочину або іншій електронно-обчислювальній машині, комп'ютерній мережі, в якій відбилися сліди злочину;

2) моніторингу підозрілих маніпуляцій в комп'ютерній мережі, електронно-обчислювальній системі безпосередньо в зоні збройного конфлікту, а також так званого "пасивного моніторингу" для виявлення загроз вказаного типу;

3) узагальнення й аналізу розвідувальних даних, які можуть свідчити про підготовку до вчинення кримінального правопорушення у кіберпросторі;

4) створення предиктивних моделей з метою прогнозування розвитку подій та настання певних результатів кіберзлочину у військовому середовищі.

"На основі сказаного можна стверджувати, що штучний інтелект здатен: сприяти підвищенню ефективності розслідувань; знизити кількість помилок та зайвих витрат часу і зусиль; надати допомогу у аналізі великих обсягів інформації і, як наслідок, виявляти можливі зв'язки між різними фактами, що можуть мати ключове значення для розслідування злочинів" [22, с. 152].

По-третє, необхідно чітко уніфікувати питання, що стосуються правового визначення, кваліфікації, алгоритмів слідчих (розшукових) дій, типових слідчих ситуацій при розслідуванні комп'ютерних злочинів, вчинених у військовому середовищі.

Підкреслює це В.В. Федюк, зазначаючи, що нормативна регламентація кримінальної відповідальності за кібершпигунство в Україні передбачена загальним складом кримінального правопорушення, передбаченого ст. 114 КК України.

Проте актуальним залишається питання визначення цього діяння, зважаючи на специфіку сфери "кібер", оскільки, як вже з'ясовано, ця сфера є дуже широкою.

Стратегія кібербезпеки України 2021 р. надає чи не єдине легальне визначення кібершпигунства, як організованих та спонсорованих урядами інших держав кібератак, що пов'язані з викраденням у політичних, економічних або військових цілях чутливої інформації [23, с. 261].

Аналогічну ситуацію ми можемо бачити і з низкою інших суспільно небезпечних діянь, за які передбачена кримінальна відповідальність і які пов'язані з неправомірним втручанням або використанням електронно-обчислювальних систем і комп'ютерних мереж у військовому середовищі. Важливим аспектом в цьому напрямку, на нашу думку, стане вивчення досвіду бойових дій, розпочатих в Україні після повномасштабного вторгнення рф. В свою чергу, слідчо-прокурорська та судова практика органів військової юстиції, у разі їхнього відновлення на законодавчому рівні та початку реального функціонування, слугуватиме потужним підґрунтям для чіткої регламентації й уніфікації вищевказаних питань.

Висновки та перспективи подальших досліджень.

Аналіз новітніх досліджень і статистичних даних показав, що кіберзлочинність у сьогоднішніх реаліях України є однією з найвагоміших загроз, яка тільки підвищується, коли йдеться про вчинення комп'ютерних злочинів у військовому середовищі. Нерідко Збройні Сили стають об'єктами атак із використанням електронно-обчислювальних систем і комп'ютерних мереж, а це, в свою чергу, наражає на небезпеку не тільки військову, а й цивільну інфраструктуру. В слідчо-судовій практиці наявні й випадки, коли суб'єктом злочину виступає службова особа або така, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг, або навіть безпосередньо військова посадова особа, і саме в таких випадках ситуація може набувати особливо небезпечних рис.

В ході дослідження виокремлено низку проблемних питань, що постають перед правоохоронними органами, залученими до проведення досудових розслідувань кіберзлочинів, вчинених у військовому середовищі, а саме:

1. Фіксація обстановки вчинення кіберзлочину та слідової картини.
2. Існування ризику для особистої безпеки слідчого, представників правоохоронних органів під час проведення слідчих (розшукових) дій на території ведення активних бойових дій.
3. Наявність спеціального суб'єкта кримінального правопорушення.
4. Можлива протидія з боку командирів військових підрозділів у випадках неналежного виконання ними службових обов'язків, що стало умовою вчинення кримінального правопорушення їх підлеглим.

Сформульовано власні пропозиції щодо покращення якості розслідувань кримінальних правопорушень у військовому середовищі, вчинених у кіберпросторі, що передбачають: відновлення повноцінної системи військової юстиції в Україні, з відповідним законодавчим забезпеченням та наділенням необхідними повноваженнями, а також укомплектуванням її органів особами зі статусом військовослужбовців; впровадження в процес досудового розслідування та судової експертизи інноваційних, високоінтенсивних технологій, адаптованих до завдань, які стоятимуть перед вказаними органами, з урахуванням специфіки діяльності у зонах збройного конфлікту; уніфікацію питань, що стосуються правового визначення, кваліфікації, алгоритмів слідчих (розшукових) дій, типових слідчих ситуацій при розслідуванні комп'ютерних злочинів, вчинених у військовому середовищі, з використанням слідчо-прокурорської та судової практики органів військової юстиції як підґрунтя для чіткої регламентації й уніфікації вищезазначених питань.

Перспективи подальших досліджень у даній сфері полягають у продовженні розробки методик і стандартів для проведення слідчих (розшукових) дій з урахуванням специфіки військового кіберпростору, прогнозуванні наслідків імплементації міжнародного досвіду, зокрема країн-членів НАТО, у вітчизняні криміналістичні технології, а також вдосконаленні технологічних інновацій для покращення якості розслідувань кримінальних правопорушень у військовому середовищі, вчинених у кіберпросторі.

Використана література

1. Гуржій С.В. Засади інституціонально-функціонального забезпечення кібербезпеки в сучасних умовах. *Інформація і право.* № 2(37)/2021. С. 103-104. DOI: https://doi.org/10.37750/2616-6798.2021.2(37).238344.

2. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право.* 2019. № 5. С. 304-307. URL: http://pgp-journal.kiev.ua/ archive/2019/5/57.pdf

3. Воронов І.О. Криміналістичний аналіз кримінальних правопорушень у сфері використання комп'ютерів. *Юридичний бюлетень.* 2022. № 4. С. 180-186. DOI: https://doi.org/ 10.32850/LB2 414-4207.2022.24.24

4. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія. Одеса: ТЕС, 2020. 372 с.

5. Волобуєв А.Ф. Проблеми розслідування "комп'ютерних злочинів". *Вісник Університету внутрішніх справ.* 1996. № 1. С. 63-70.

6. Кіберзлочинність та електронні докази: навч. посіб. / Б.М. Головкін, О.І. Денькович, В.В. Луцик, Д.М. Цехан. Львів: ЛНУ ім. Івана Франка, 2022. 298 с. URL: https://nlu.edu.ua/wp-content/uploads/2023/09/cybercrime-and-digital-evidence.pdf

7. Кравцова М.О. Сучасний стан і напрями протидії кіберзлочинності в Україні. *Вісник кримінологічної асоціації України.* 2018. № 2 (19). С. 155-166. URL: https://dspace.univd.edu.ua/ server/api/core/bitstreams/c451d2ca-1ebe-4be3-a50d-f86ca1b0e37f/content

8. Коршенко В.А. Судова телекомунікаційна експертиза як джерело доказів під час розслідування кіберзлочинів. *National law journal: theory and practice*. 2017. № 2 (24). С. 192-194. URL: https://ibn.idsi.md/sites/ default/files/imag_file/192_194_Sudova%20telekomun%D1%96 kac%D1%96jna%20ekspertiza%20jak%20dzherelo%20dokaz%D1%96v%20p%D1%96d%20chas.pdf

9. Шевчук В.М. Криміналістичні інновації та цифрові технології у протидії сучасній злочинності: тези доповідей Всеукраїнської науково-практичної конференції *Слідча та детективна діяльність: виклики і перспективи*, м. Харків, 25 трав. 2023 р. Харків: "Юрайт", 2023. С. 148-153. URL: https://ivpz.kh.ua/wp-content/uploads/2023/10/%D0%97%D0%B1%D1%96 %D1%80%D0%BD%D0%B8%D0%BA-%D0%A1%D0%BB%D1%96%D0%B4%D1%87%D0%B0-%D1%82%D0%B0-%D0%B4%D0%B5%D1%82%D0%B5%D0%BA%D1%82%D0%B8%D0%B2% D0%BD%D0%B0-%D0%B4%D1%96%D1%8F%D0%BB%D1%8C%D0%BD%D1%96%D1%81%D 1%82%D1%8C_25.05.23.pdf#page=148

10. Колодіна А.С., Федорова Т.С. Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права*. 2022. № 1. С. 176-180. DOI: https://doi.org/10.32782/klj/2022.1.27.

11. Осика І.М., Калюжна А.О., Матвієнко О.А Використання сучасних технологій у криміналістиці в умовах воєнного стану: можливості та обмеження. *Юридичний науковий електронний журнал.* 2024. № 5. С. 469-472. DOI: https://doi.org/10.32782/2524-0374/2024-5/116.

12. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24.03.22 р. № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-IX#Text

13. Вейц А.М. Воєнна криміналістика: сучасні підходи до розслідування кримінальних правопорушень у зонах конфліктів. *Наукові інновації та передові технології*. 2024. № 9 (37). С. 289-301. DOI: https://doi.org/10.52058/2786-5274-2024-9(37)-289-301.

14. Про внесення змін до Кримінального процесуального кодексу України щодо удосконалення порядку здійснення кримінального провадження в умовах воєнного стану: Закон України від 14.04.22 р. № 2201-IX. URL: https://zakon.rada.gov.ua/laws/show/2201-20#Text

15. Тарасенко О.С. Криміналістичні особливості досудового розслідування в умовах військових дій: тези доповідей Міжнародного науково-практичного онлайн-семінару *Діяльність державних органів в умовах воєнного стану,* м. Кривий Ріг, 29 квіт. 2022 р. ДонДУВС, 2022. С. 216-218. URL: https://dnuvs.in.ua/wp-content/uploads/2022/06/zbirnyk-semina ru-29.04.2022.pdf# page=216

16. Бабакін В.М. Особливості міжнародного співробітництва при розслідуванні кіберзлочинів. *Форум права*. 2014. № 4. С. 27-30. URL: https://dspace.univd.edu.ua/server/api/core/ bitstreams/661ed915-06d3-49da-beb3-06056c249682/content

17. Давиденко В.С. Кримінальна субкультура як предмет дослідження у формуванні окремих методик розслідування військових злочинів. *Європейські перспективи*. 2013. № 5 С. 105-109. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21D BN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/evpe_2013_5 _21.pdf

18. Гуцалюк М.В. Особливості протидії кіберзлочинності під час воєнного стану. *Інформація і право*. № 3(46)/2023. С. 108-117. DOI: https://doi.org/10.37750/2616-6798.2023.3(46).287212.

19. Єдиний звіт про кримінальні правопорушення за січень-грудень 2023 року. URL: https://old.gp.gov.ua/ua/file_downloader.html?_m=fslib&_t=fsfile&_c=download&file_id=241804

20. Богуцький П.П. Система військової юстиції України: теоретико-прикладний аспект. *Інформація і право*. № 3(46)/2023. С. 215-223. DOI: https://doi.org/10.37750/2616-6798.2023.3(46).287256.

21. Шамара О.В. Відновлення військової прокуратури, як елементу системи органів військової юстиції України. *Інформація і право.* № 1(48)/2024. С. 241-250. DOI: https://doi.org/10.37750/2616-6798.2024.1(48).300832.

22. Зачек О.І., Дмитрик Ю.І., Сеник В.В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ*. 2023. № 3. С. 148-156. DOI: https://doi.org/10.32782/2311-8040/2023-3-19.

23. Федюк В.В. Кримінальна відповідальності за кібершпигунство: проблеми нормативної регламентації: тези доповідей VI Міжнародної науково-практичної конференції *Кримінально-правова охорона інформаційної безпеки*, м. Харків 12 трав. 2022 р. Харків: “Право”. С. 260-263. URL: https://ivpz.kh.ua/wp-content/uploads/2023/01/%D0%97%D0%B1%D1%96%D1%80%D0%D%D0%B8%D0%BA-%D1%82%D0%B5%D0%B7_1205_2022_%D1%81%D0%B0%D0%B9%D1%82_-1pdf#page=261

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~