DOI: https://doi.org/10.37634/efp.2022.10(1).3
УДК 343.9

Іван Григорович ***БОГАТИРЬОВ***
д.ю.н., професор, Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука; заслужений діяч науки і техніки України
ORCID: https://orcid.org/0000-0003-4001-7256
e-mail: vanbogatyrov@gmail.com

АКТУАЛЬНІ ПРОБЛЕМИ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

У статті піднято проблеми кіберзлочинності. Здійснено аналіз праць вітчизняних вчених з даної проблеми. Розкрито кібербезпеку як інноваційну систему віртуальності сучасного інформаційного простору. Показано кіберзлочинність як соціально-правове явище якісно нового типу. Акцентовано увагу на той факт, що кібербезпека в умовах військового стану в Україні набуває особливої актуальності, оскільки є інвестиційним ризиком з якісним забезпеченням антикорупційного складника у військовій сфері.

Ключові слова: *кібербезпека, кіберзлочинність, військовий стан, явище, суспільство, військова сфера*

ВСТУП

Багатогранність розвитку суспільного життя у третьому тисячолітті дуже активно позначилось на інтенсивному використанні державними і приватними установами новітніх комп'ютерних технологій, можливостей електронних мереж. Проблема кіберзлочинності стала актуальною з розвитком інформаційних технологій та передумовою швидкого, масштабного і динамічного розвитку цифрового суспільства.

Саме вони сьогодні вимагають від нас системи знань і здібностей до логічного мислення, здатності аналізувати та досліджувати отриману інформацію, реалізація якої дозволить країні бути матеріально-технічно спроможною конкурувати з іншими країнами.

Тому не дивно, що з динамічністю розвитку суспільства появою нових системних форм організації суспільних відносин (соціальні мережі, віртуальна реальність, блокчейн тощо) з'являється новий вид високотехнологічної злочинності – кіберзлочинність, яка виступає складною і відносно новою сферою діяльності правоохоронних органів.

Отже, кіберзлочинність – це проблема, з якою зіштовхнулась планета у XXI ст. та яка обіцяє зростати та поглинати дедалі більше коштів. Незважаючи на заходи, що їх вживають окремі особи, фірми, а також держава, кіберзлочинність продовжує свою діяльність, збільшуючи прибутки порушників і зменшуючи вміст кишень пересічних громадян.

Специфіка цього виду злочинності полягає у тому, що готування та скоєння таких злочинів здійснюється майже не відходячи від «робочого місця», злочини є доступними; оскільки комп'ютерна техніка повсякчас дешевшає, злочини можна скоювати з будь-якої точки земної кулі, у будь-якому населеному пункті, а об'єкти злочинних посягань можуть знаходитись за тисячі кілометрів від злочинця.

Все це створює певні перепони для правоохоронних органів у тому, щоб виявити, зафіксувати і вилучити кримінально значущу інформацію під час виконання слідчих дій для використання її як речового доказу. І найголовніше, що про це знають і кіберзлочинці, а тому їхня поведінка нахабна та протиправна.

Отже, розглядаючи кіберзлочинність в Україні, слід звернути увагу на той факт, що перші кроки світова спільнота здійснила у сфері запобігання кіберзлочинності, ухваливши Конвенцію Ради Європи про кіберзлочинність у 2001 р., яку Україна ратифікувала у 2005 р.. Відповідно до положень цієї Конвенції [1], кіберзлочинність – це сукупність злочинів, поєднаних у такі групи:

– кримінальні правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем;

– кримінальні правопорушення, безпосередньо пов'язані з використанням комп'ютера як засобу скоєння злочину;

– кримінальні правопорушення, пов'язані зі змістом даних (інформації), розміщеної в комп'ютерних системах;

– кримінальні правопорушення, пов'язані з порушенням авторських і суміжних прав, а також акти расизму та ксенофобії, вчинені за допомогою комп'ютерних систем.

Важливого значення у системі запобігання кіберзлочинності набуває законодавче закріплення поняття «кіберзлочин» – прийняття Верховною Радою Закону «Про основні засади кібербезпеки України» №2163-VIII від 05.10.2017. Зокрема, у ст. 1 подано таке визначення: «кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України» [2].

А це зі свого боку створило певні умови зміцнення тісних зв'язків між кіберзлочинністю та організованою злочинністю. До речі, Інтернетом користуються всі, зокрема й окремі злочинні групи, але останні створюють сектори тіньового ринку, з поділом праці між злочинними групами і цілими майданчиками, для торгівлі програмним забезпеченням для вчинення злочинів, продажу інформації тощо.

МЕТА статті – фрагментарне дослідження кіберзлочинності, зумовлене актуальністю наукових пошуків у цій сфері та висвітлення його результатів для широ-

кого загалу.

МЕТОДИ ДОСЛІДЖЕННЯ

Проблемі кіберзлочинності та її запобіганню приділяли увагу, як вітчизняні так і зарубіжні вчені серед яких: А. Богатирьов, П. Біленчук, Р. Грищук, Є. Скулиш, Т. Обіход, М. Довбиш, Л. Харченко, В. Ліпкан, О. Логінов, Ю. Лісовська, А. Марущак, В. Цимбалюк, Є. Користін, В. Бутузов, В. Василевич та ін.

Дане дослідження базується на працях вітчизняних і зарубіжних вчених, а також на матеріалах періодичних видань, статистичних збірників. У дослідженні використано методи аналізу і синтезу, порівняння та узагальнення, а також низку інших методів.

РЕЗУЛЬТАТИ

Поділяючи позицію вітчизняних вчених П.Б. Біленчука та Т.В. Обіход про те, що реалізація стратегії кібербезпеки України здійснюється на підставі національного оборонного безпекового економіко інтелектуального потенціалу з використанням механізму державно-приватного партнерства [3, с. 238], ми робимо узагальнення про те, що кібербезпека – це гарантія концептуальної основи цивілізаційного розвитку освіти, науки і практики у третьому тисячолітті, це збереження від кібератак злочинців економічного, соціального та людського потенціалу.

Здійснений науковою школою «Інтелект» аналіз вітчизняних і міжнародних документів, які забезпечують правове регулювання використання інформаційних технологій показав, що кіберзлочинність – відносно нове соціально-правове явище, яке виникло у світі з появою нових інформаційних технологій, мета якого отримати бажану необхідну для злочинців інформацію, яка зберігається на носіях комп'ютера у будь-якому вигляді та вміщує дані про сфери людської діяльності.

До того ж використання комп'ютерних мереж у різних державних і недержавних сферах передбачають відомості, що зберігаються у пам'яті будь-якого фізичного чи віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, оброблення й передачі, а тому створюють всі передумови виникнення кіберзлочинності.

Вітчизняний вчений М. Довбиш вважає, що проблема кіберзлочинності набула глобального масштабу, а збитки від діяльності кібершахраїв сягнули десятків мільярдів доларів. Для протистояння кібершахраям у світі створюються спеціальні підрозділи та структури. Їх повноваження безупинно розширюються, а технічні можливості посилюються, наприклад, Європейський центр боротьби з кіберзлочинністю, який запрацював на початку 2013 р. [4].

До речі, як зауважує Ю. Лісовська, в сучасних умовах інформаційного світу проблема кіберзлочинності тісно пов'язана з кібербезпекою, оскільки саме вона посідає особливе місце в наукових дослідженнях, які активізуються з кожним роком, враховуючи надвисокі темпи розвитку суспільних відносин в електронній сфері [5, с. 4].

Інший вітчизняний вчений Є. Скулиш вважає, що на сьогодні немає єдиного розуміння стосовно обсягу протиправних посягань, які можуть розцінюватися як кіберзлочини, а також є проблема з відмежуванням кіберзлочинності як принципово нового виду злочинної діяльності від злочинів, які традиційно вчиняються з використанням комп'ютерних технологій. Особливо проблематичними в цьому плані є такі ознаки, як об'єкт та предмет кіберзлочинів, які, являючи собою характерні риси загального поняття "кіберзлочинність", безпосередньо окреслюють сферу застосування тієї чи іншої кримінально-правової норми [6, с. 47].

Вітчизняний вчений Р. Грищук у монографічному дослідженні «Основи кібернетичної безпеки» зазначав, що кардинальна зміна форм та способів збройного протистояння внаслідок повсюдного поширення надбань високих технологій, суттєво вплинула на виконання завдань за призначенням силовими та спеціальними структурами будь-якої розвиненої держави світу.

Водночас, як пише дослідник, Україна прагне увійти до кола держав з розвиненою економікою, а тому активно впроваджує в усіх сферах технологічні інновації, які окрім усіх інших позитивних аспектів створюють передумови для виникнення нових й нетипових на сьогодні для силових та спеціальних структур держави викликів й загроз безпеці.

Наприклад, комп'ютеризація економічної, військової, соціальної та інших сфер породжує такі нові виклики та загрози для силових та спеціальних структур держави: для Служби безпеки України – проблему боротьби з кібертероризмом; для Міністерства внутрішніх справ України – проблему боротьби з кіберзлочинністю; для Міністерства оборони України – проблему забезпечення кібероборони держави; для Державної служби спеціального зв'язку та захисту інформації України – проблему кіберзахисту державних інформаційних ресурсів тощо [7, с. 555].

От чому вітчизняні і зарубіжні вчені стали єдині в тому, що кіберзлочинність, вийшовши за межі національних кордонів, перетворилися на транснаціональне явище та глобальну загрозу людству. А стрімкість фінансової глобалізації, формування глобальної фінансової системи та ускладнення світової фінансової архітектури поруч із розвитком інформаційно-комунікаційних технологій зумовили виведення на провідні позиції у міжнародному вимірі кіберзлочинності таку її форму, як легалізація кримінальних доходів.

На відміну від «традиційного» відмивання доходів, для здійснення якого використовується банківська система, кібервідмивання засновано на використанні різних видів операцій та постачальників фінансових послуг – від банківських переказів, внесення чи зняття готівки, використання електронних грошей до «грошових мулів» і послуг з переказу грошей.

Головні механізми легалізації злочинних доходів вимагають від злочинців швидкого й ефективного проведення їх легалізації. Причому, з огляду на специфіку кіберзлочинності, організатори та виконавці схем переважно є освіченими та технічно грамотними, відповідно, і методи, які ними використовуються під час легалізації отриманих коштів, можуть також бути досить складними та нестандартними.

Інформація чи гроші викрадаються через Інтернет, що надає додаткові можливості для переказу коштів з рахунків фізичних або юридичних осіб на рахунки зловмисників, насамперед за допомогою вірусних програм для зчитування паролів і конфіденційної

інформації.

Віруси, вражаючи комп'ютерні системи, копіюють паролі, ключі, зберігають скриншоти, пов'язані з фінансовою чи іншою важливою інформацією, та передають дані кіберзлочинцям. Небезпечним винаходом є програми, здатні впливати на роботу та спричиняти збій у функціонуванні стратегічних об'єктів, телекомунікаційних мереж чи банківської інфраструктури.

Кіберзлочини здійснюються за рахунок інноваційних підходів і проведення високоінтелектуальних операцій, застосування нестандартних рішень і урізноманітнення методів. Організація злочинних груп є високоструктурованою та вирізняється вузькою спеціалізацією ролей і обов'язків. Водночас складнішим і витонченішим стає доступ до інформації, що реалізується на підпільних ринках. Серед причин стрімкого зростання кіберзлочинності варто виділити:

– прибутковість, оскільки доходи, які отримують кіберзлочинці за декілька секунд чи хвилин, можуть перевищувати мільйони доларів. Тому на сьогодні кіберзлочинність – проблема номер один у світі;

– відсутність великого ризику, оскільки психологічний аспект злочину припускає наявність деяких засобів стримування. У віртуальному світі злочинці не можуть бачити своїх жертв, чи то окремі люди, чи то цілі організації, які вони вибрали для атаки. Грабувати тих, кого ти не бачиш, до кого не можеш дотягтися рукою, набагато легше;

– суспільну небезпечність кіберзлочинів їх поширеність. Саме ці злочини останніми роками набули загрозливих масштабів і диктують необхідність формування адекватної відповіді з боку держави. Отже, кіберзлочинність сьогодні становить загрозу не тільки національній безпеці окремої держави, а й загрожує людству загалом, саме тому зазначеній проблемі приділяється серйозна увага в багатьох державах.

Окремо варто виділити проблему кіберзлочинності в місцях несвободи Державної кримінально-виконавчої служби (далі ДКВС) України в умовах війни, оскільки серед домінуючих причин та умов вчинення такої злочинності є: корупційний складник або службова недбалість персоналу виправної колонії ДКВС України, яка призводить до несанкціонованого доступу засуджених до автоматичних систем місць несвободи; незаконне використання засудженими у місцях несвободи Інтернету; вчинення шахрайських дій з метою отримання грошових коштів [8, с. 90] тощо.

Отже, беззаперечним є той факт, що інформаційні технології з кожним днем дедалі більше інтегруються в людське життя. Як наслідок, люди відчули можливості державних установ надавати їм послуги набагато швидше, ніж це було раніше. До того ж мільйони людей у своєму житті використовують новітні інформаційні технології. До речі, Інтернет сьогодні є одним із складників повсякденного життя людей.

Водночас, як зауважують кримінологи, у контексті використання інформаційних технологій є і негативні її сторони. Зокрема, несанкціоноване втручання в роботу комп'ютерних і телекомунікаційних мереж, виготовлення та розповсюдження шкідливого програмного забезпечення, атаки на об'єкти критичної інфраструктури дозволило кіберзлочинцям використовувати їх у власних інтересах, здійснювати незаконне втручання у політичні процеси розвитку країни та особисте життя громадян.

На жаль, Україна є однією з країн, яка зараз надзвичайно гостро відчуває на собі всі так звані побічні ефекти еволюції інформаційного суспільства. Розповсюдження комп'ютерних вірусів, атаки на українські об'єкти фінансового та енергетичного секторів, викрадення інформації – це ще не повний перелік кіберзлочинів, які відомі в Україні.

На жаль, кіберзлочинність, попри зусилля правоохоронних органів, спрямованих на її запобігання, щороку не зменшується, а навпаки, постійно збільшується. Серед причин та умов кіберзлочинності слід виділити також Інтернет-шахрайство з банківськими картками в Україні. Цей вид злочину стає дедалі більш масовим негативним явищем відтоді, відколи громадяни стали активно користуватися цим платіжним інструментом.

Небезпечність піднятої вченими проблеми підтверджується не тільки збільшенням кількості крадіжок грошей у власників платіжних карток, а й фіксацією правоохоронцями нових схем афер (перехоплювачі клавіатури, спеціально розроблені вебсайти, поштові повідомлення, складені за всіма правилами соціальної інженерії тощо).

З іншого боку, самі громадяни добровільно залишають багато особистої інформації в базах даних супермаркетів, Інтернет-магазинів (наприклад, OLX, «Розетка», Leboutique, Work, Parfums, Makeup тощо), заповнюючи анкетні дані (ПІБ, місце та рік народження, номер мобільного тощо), котрі зловмисники можуть використати у корисних цілях.

Найчастіше паролі й дані платіжних карток в українців виманюють або через спеціально створені сайти (фішинг), або способом особистого спілкування шахраїв з жертвою по телефону (вішинг). З цією метою злочинці використовують сайти, призначені для переведення грошей з однієї картки на іншу, поповнення рахунку мобільних телефонів тощо.

Враховуючи, що сучасним атакам кіберзлочинів майже неможна запобігти, кримінологи радять більше зусиль спрямовувати на підготовку команд реагування на інциденти. Кіберзлочинці – це не одинаки, а добре підготовлені, мотивовані і фінансовані організації.

Вся інформація, яку ви знаєте про свою мережу і техніку, – ніщо, якщо ви не знаєте, хто вам протистоїть. Тому вам потрібно стати на місце хакера і зрозуміти, що йому цікаво у вашій компанії і як він може це отримати.

Головне порушення кібербезпеки сьогодні – це відсутність комплексного підходу (люди, системи, процеси), ігнорування питань кібербезпеки з боку CEO, зайва впевненість у безпеці.

Раніше зловмисники атакували для шантажу або заволодіння грошовими коштами, сьогодні це використання інфраструктури жертви для атаки на третіх осіб, маніпулювання виборами або техногенні катастрофи. Кібербезпека є важливим видом національної безпеки, метою якої є забезпечення основоположних прав, свобод громадян від кіберзагроз, кіберінцидентів та кіберзлочинів.

Будучи новим середовищем, кіберзлочинність впливає на соціалізацію особистості неповнолітнього, шко-

ляра чи учня профтехучилища. Хоча за даними педагогів, інтернет має великий виховний потенціал і виконує певні соціальні функції: інформаційну, комунікативну, конативну (поведінкову), розважальну (рекреаційну).

Водночас, впливаючи на формування світогляду, розвиток моральних якостей особистості неповнолітнього, Інтернет несе в собі не тільки позитивні, а й негативні наслідки. У соціальних мережах користувачам дозволено робити те, що заборонено вдома чи в школі, можна здійснювати всі свої найсміливіші та навіть небезпечні мрії.

У мережі вони виявляють велику свободу у висловлюваннях і вчинках (аж до образ, нецензурних виразів), оскільки ризик розкриття та особистої негативної оцінки ззовні мінімальний. Тут вони презентують себе з іншого боку, ніж в умовах реальних соціальних норм, грають певні ролі, які ніколи не реалізують поза мережею, сценарії ненормативної поведінки, що може призвести до деформації особистості.

Гострою залишається й проблема насилля над дітьми у кіберпросторі. Психологічну, фізичну шкоду несе в собі показ порнографічних матеріалів, сцен сексуального насильства над дітьми. Для вирішення вищезазначених проблем потрібно діяти системно і використовувати різні можливості, зокрема інформаційно-технічні.

Важливо навчити неповнолітніх відокремлювати світ віртуальної реальності від дійсності, зрозуміти значущість справжнього життя в оточуючому соціумі, навчити позитивно використовувати можливості та ресурси Інтернету, правил безпеки у кіберпросторі, формувати культуру спілкування в соціальних мережах. Потрібно також займатися просвітою батьків у цьому напрямі роботи.

На жаль, ні школа, ні профтехучилища не змогли запропонувати підліткам жодної альтернативи соціальним мережам. Нині процес використання учнями соціальних мереж школою часто ігнорується. Можна стверджувати, що в освіті соціальні мережі лише створили передумови для залучення школярів до цілеспрямованих проєктів в Інтернет-середовищі.

На завершення дослідження проблеми кіберзлочинність ми пропонуємо власний алгоритм, який дозволить кожному з нас може зробити свій внесок у сферу запобігання кіберзлочинності, дотримуючись простих правил, серед яких:

– створення власноруч надійних паролів і періодичне їх змінювання;

– своєчасне використання та оновлення антивірусних програм забезпечення роботи комп’ютера;

– робота з комп'ютером у режимі користувача. Цією порадою, за дослідженням кримінологів, нехтують найчастіше. Якщо після встановлення операційної системи ви продовжуєте для зручності використовувати комп'ютер в режимі «адміністратор», цим створюєте додаткові ризики зараження комп'ютера вірусами, які пропустила антивірусна система;

– під час використання комп’ютера здійснюйте обережність у разі спроби підвищити власну анонімність. Окремі користувачі, намагаючись залишити якнайменше слідів свого перебування в мережі Інтернет, застосовують анонімайзери, безкоштовні проксі-сервери або програмні додатки типу TOR;

– завжди контролюйте інформацію, яку розміщуєте на власній сторінці у соціальній мережі. Надлишкова відкритість щонайперше може бути використана у підготовці протиправних дій стосовно вас;

– візьміть за правило не відкривати посилання, що надходять вам у повідомленнях на сторінці. Краще копіюйте їх і вставляйте у пошукову сторінку браузера як текст.

ВИСНОВКИ

Отже, дослідження кіберзлочинності в епоху нового інформаційного розвитку суспільства є фундаментальною основою кримінологічної науки і дозволяє нам стверджувати, що саме феномен кіберзлочинності з’явився у третьому тисячолітті завдяки системній цілісності й водночас багатогранності суспільного життя з об’єктивною необхідністю використанням сучасних інформаційних технологій (Інтернет, комп’ютер, електронні мережі тощо).

Здійснений аналіз вітчизняних і міжнародних документів у сфері запобігання кіберзлочинності показав, що позитивні наслідки запобігання кіберзлочинності можуть мати місце лише за умови співробітництва та великої уваги до цього питання з боку світового співтовариства. Річ у тім, що саме злочини у віртуальному просторі носять транснаціональний характер, спричиняють неабиякі збитки морального та матеріального характеру, становлять загрозу національній та світовій кібербезпеці.

Здійснено аналіз праць вітчизняних вчених з цієї проблеми. Зазначено, що багатогранність розвитку суспільного життя у третьому тисячолітті дуже активно позначилось на інтенсивному використанні державними і приватними установами новітніх комп’ютерних технологій, можливостей електронних мереж.

Доведено, що проблема кіберзлочинності стала актуальною з розвитком інформаційних технологій та передумовою швидкого, масштабного і динамічного розвитку цифрового суспільства.

Запобігання кіберзлочинності в Україні – це насамперед створення власноручного захисту шляхом введення в комп’ютер свого паролю і періодичність його змінювати; по-друге, своєчасне оновлення антивірусних програм; по третє, роботу з комп'ютером має здійснюватися тільки у режимі користувача. На жаль, цією порадою, за дослідженням кримінологів, нехтують найчастіше, тим самим створюючи додаткові ризики зараження комп'ютера вірусами тощо.

Список використаних джерел

1. Конвенція про кіберзлочинність. *Офіційний вісник України*. 2007. № 65. Ст. 2535. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

2. Про основні засади кібербезпеки України: Закон України від 05.10.2017 № 2163-УТТТ. URL: http://zakon2.rada.gov.ua/laws/show/2163-19

3. Біленчук П.Д., Обіход Т.В. Кібербезпека і засоби запобігання та протидії кіберзлочинності й кібертероризмі. *Часопис*

Київського університету права. 2018. № 3. С. 235-239.

4. Довбиш М. Кіберзлочинність в Україні. URL: https://www.science-community.org/ru/node/16132

5. Лісовська Ю.П. Кібербезпека: ризики та заходи. Київ: Видавничий дім «Кондор», 2019. 272 с.

6. Скулиш Є.Д. Теоретико-методологічні засади визначення об'єкта та предмета кіберзлочинів. *Правова інформатика*. 2014. № 2. С. 47–53.

7. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: монографія. Житомир: ЖНАЕУ, 2016. 636 с.

8. Богатирьов А.І. Проблема кіберзлочинності в місцях несвободи Міністерства юстиції України. *Кібербезпека в Україні: правові та організаційні питання*: матеріали всеукр. наук.-практ. конф. (Одеса, 17 листопада 2017 р.). Одеса: ОДУВС, 2017. С. 90–92.

References

1. Convention on cybercrime. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (in Ukrainian).

2. Law of Ukraine on basic principles of cybersecurity of Ukraine №2163-УТТТ (2017, October 05). URL: http://zakon2.rada.gov.ua/laws/show/2163-19 (in Ukrainian).

3. Bilenchuk P.D., Obihod T.V. Cybersecurity and means of preventing and countering cybercrime and cyberterrorism. *Law Review of Kyiv University of Law*. 2018. № 3. pp. 235-239. (in Ukrainian).

4. Dovbysh M. Cybercrime in Ukraine. URL: https://www.science-community.org/ru/node/16132 (in Ukrainian).

5. Lisovska Yu.P. Cybersecurity: risks and measures. Kyiv, 2019. 272 p. (in Ukrainian).

6. Skulysh Y.D. Theoretical and methodological foundations for determining the object and subject of cybercrime. *Legal Informatics*. 2014. № 2. pp. 47–53. (in Ukrainian).

7. Hryshchuk R.V., Danyk Yu.H. Fundamentals of cyber security. Zhytomyr, 2016. 636 p. (in Ukrainian).

8. Bohatyrov A.I. The problem of cybercrime in places of non-freedom of the Ministry of Justice of Ukraine. *Cybersecurity in Ukraine: legal and organizational issues:* materials of the Ukrainian scientific and practical conference (Odesa, November 17, 2017). Odesa, 2017. pp. 90–92. (in Ukrainian).

Ivan BOHATYROV
Doctor of Legal Sciences, Professor, Academician Stepan Demianchuk International University of Economics and Humanities; Honored Worker of Science and Technology of Ukraine
ORCID: https://orcid.org/0000-0003-4001-7256
e-mail: vanbogatyrov@gmail.com

CURRENT PROBLEMS OF CYBERCRIME PREVENTION IN UKRAINE

The problems of cybercrime were explored in the article. The analysis of the works of Ukrainian scientists on this problem is carried out. Cybersecurity is revealed as an innovative system of virtuality of the modern information space. Cybercrime is shown as a social and legal phenomenon of a qualitatively new type, attention is focused on the fact that cybersecurity under martial law in Ukraine is becoming particularly relevant, since it is an investment risk with high - quality support for the anti-corruption component in the military sphere.

It is proved that the problem of cybercrime has become relevant with the development of information technologies and a prerequisite for the rapid, large-scale and dynamic development of the digital society. Today these things require from us a system of knowledge and abilities for logical thinking, the ability for analyzing and investigating the received information, the implementation of which will allow the country to be financially and technically able to compete with other countries.

Therefore, it is not surprising that with the dynamic development of society, the emergence of new systemic forms of organizing public relations (social networks, virtual reality, blockchain, etc.), a new type of high – tech crime appears-cybercrime, which is a complex and relatively new field of law enforcement activities.

Thus, cybercrime is a problem that faced planets in the Twenty-First Century and promises to grow and absorb more and more funds. Despite measures taken by individuals, firms, and the state, cybercrime continues to operate, increasing the profits of violators and reducing the contents of the pockets of ordinary citizens.

All these factors create certain obstacles for law enforcement agencies to identify, record and seize criminally significant information when performing investigative actions for use as material evidence. And the most important thing is that cybercriminals also know about this, so their behavior is brazen and illegal.

It is concluded that cybercrime in Ukraine is primarily the creation of personal protection by entering your password into the computer and changing it periodically; secondly, timely updating of antivirus programs; thirdly, work with the computer should be carried out only in user mode. Unfortunately, this position, according to criminologists' research, is most often neglected, thereby creating additional risks of infecting your computer with viruses.

Keywords: *cybersecurity, cybercrime, martial law, phenomenon, society, military sphere*