КІБЕРЗЛОЧИННІСТЬ У СФЕРІ ЕЛЕКТРОННОЇ ТОРГІВЛІ ЯК ПРОЯВ КРИМІНАЛЬНОГО ПРОФЕСІОНАЛІЗМУ

МАКАРЕНКО Наталія Костянтинівна - доктор юридичних наук, доцент, професор кафедри кримінології та кримінально-виконавчого права Національної академії внутрішніх справ

orcid.org/0000-0001-7354-5122

ЛУЦЕНКО Юрій Васильович - доктор юридичних наук, професор

orcid.org/0000-0002-8731-2941

УДК 343.9

DOI 10.32782/LAW.UA.2023.3.9

У статті досліджуються питання, які стосуються кіберзлочинності у сфері електронної торгівлі як прояв кримінального професіоналізму, також звертається увага на кримінологічні проблеми професійної кіберзлочинності в Україні. Досліджується розвиток технологій, за допомогою яких почали активно вчинятися не лише злочини у сфері електронної торгівлі, а й суспільно небезпечні діяння, які раніше вважалися традиційними.

У роботі здійснено аналіз ознак кримінального професіоналізму кіберзлочинів. Пропонується типологія кіберзлочинців за рівнем їх кримінального професіоналізму.

У ході дослідження сформувалася теза, що сьогодні виділяються нові характеристики кіберзлочинців у сфері електронної торгівлі, що потребує сучасних підходів до вивчення сутності кримінального професіоналізму кіберзлочинців.

Ключові слова: кібербезпека/кіберзлочинність, особа кіберзлочинця, типологія кіберзлочинців, протидія кіберзлочинності, кримінальний професіоналізм, злочинні угруповання, професійна злочинність, диверсія у сфері комп'ютерної інформації, комп'ютерне шпигунство, електронна торгівля, шахрайство, запобігання шахрайству, шахрайство у сфері електронної торгівлі, причини та умови злочинності

Постановка проблеми

Історія людської цивілізації свідчить, що будь-який розвиток й прогрес, який приносив людству нові цивілізаційні блага та можливості, завжди супроводжувався негативними явищами. Сучасна масова цифровізація та стрімкий розвиток комп'ютерних технологій, які значно спростили життя людині, не стали винятком.

Майже всі фахівці з кібербезпеки визнають, що кіберзлочини, у тому числі у сфері електронної торгівлі, є сьогодні одними з динамічніших груп суспільно небезпечних діянь, які завдяки технологіям є відносно безпечними для діяльності різноманітних злочинних угруповань та відкривають нові «горизонти», у тому числі й для професійної злочинності. Вже сьогодні нікого не дивує існування Інтернет-мереж, за допомогою яких злочинці фактично створили чорний ринок для збуту наркотиків, зброї, крадених товарів та інших шахрайських дій [4].

Останнім часом, у зв'язку із ситуацією, яка склалася з коронавірусною хворобою у минулих роках, подальшою швидкою діджиталізацією бізнесу вторгненням рф в Україну, буде посилюватися й кримінальний тренд – кіберзлочинність та шахрайство у сфері електронної торгівлі [10, с. 79–84].

Аналіз останніх досліджень і публікацій

Серед науковців, які в тій чи іншій мірі зверталися до цієї проблематики, слід назвати О. М. Бандурку, В. В. Голіну, С. М. Гусарова, Б. М. Головкіна, О. М. Джужу, М. В. Корнієнка, О. М. Костенка, О. М. Литвинова, Є. С. Назимка, А. В. Тарасюка, В. І. Шакуна, О. Н. Ярмиша та ін. Окремі питання про-

блематики розглядалися в роботах Ю. М. Батуріна, П. Д. Біленчука, М. С. Вертузаєва, В. Б. Вехова, В. О. Голубева та інших фахівців з кібербезпеки.

Метою статті є дослідження питань, які стосуються кіберзлочинності у сфері електронної торгівлі, та з'ясування, яким чином кіберзлочинність впливає на розвиток суспільних правовідносин у світлі сучасних викликів сьогодення.

Виклад основного матеріалу

Зростання науково-технічного прогресу обумовлює негативні тенденції розвитку злочинного світу, приводить до появи нових форм і видів злочинних посягань. Сьогодні під впливом використання сучасних інноваційних технологій виникла і набирає стрімкого розвитку нова загроза міжнародному правопорядку. Сучасні етапи науково-технологічного розвитку світового співтовариства нерозривно пов'язані з упровадженням передових технологій. Сьогодні в нашій країні створені належні передумови переходу до суспільства нової генерації, що базується на інноваційних технологіях, наскрізній цифровізації виробництва, інформаційних і телекомунікаційних розробках, які забезпечують актуальність і достовірність інформації [16, с. 5; 11, с. 70].

Комп'ютерні системи містять у собі новітні, більш досконалі можливості для невідомих раніше правопорушень, а також для вчинення традиційних злочинів, але нетрадиційними засобами. Слід констатувати, що відбулося різке набуття кіберзлочинцями кримінального професіоналізму, про що свідчить збільшення кількості зухвалих за задумом і кваліфікованих за виконанням злочинів.

На відміну від традиційних видів злочинів, історія яких налічує століття, кіберзлочинність, так само як і шахрайство у сфері електронної торгівлі, є явищем новітньої, цифрової доби. Сама природа мережі Інтернет сприяє вчиненню кіберзлочинів. Такі її властивості, як глобальність, трансграничність, анонімність користувачів, їх широка аудиторія слугують кіберзлочинцям на всіх етапах вчинення шахрайських дій та інших злочинів, а також дозволяють ефективно уникати кримінального переслідування правоохоронними органами.

Сьогодні в науці відсутній єдиний підхід щодо поняття «кіберзлочинність». Так, під кіберзлочинністю Б. М. Головкін розуміє сукупність злочинів, що вчиняються у віртуальному просторі за допомогою комп'ютерних систем або через використання комп'ютерних мереж та інших засобів доступу до віртуального простору, у межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [5, с. 34].

В. М. Болгов вважає, що кіберзлочини – це сукупність передбачених чинним законодавством кримінально караних, суспільно небезпечних діянь (дій чи бездіяльності), що посягають на право захисту від несанкціонованого поширення та використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію [3, с. 132].

Попри відсутність єдиного підходу до розуміння кіберзлочинності, зазначимо, що це явище властиве всім країнам, які в силу свого наукового прогресу вступили у період широкої цифровізації своєї діяльності. Про це свідчить прийняття у листопаді 2001 року країнами Європейського Союзу Конвенції Ради Європи про кіберзлочинність, у якій виділяються наступні групи кіберзлочинів:

злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему);

злочини, пов'язані з використанням комп'ютера як засобу вчинення злочинів, а саме – для маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерні підроблення);

злочини, пов'язані з контентом (змістом даних);

злочини, пов'язані з електронною торгівлею;

злочини, пов'язані з порушенням авторського права і суміжних прав;

акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж [15].

Виходячи з вищенаведеного, виокремлюють такі ознаки кіберзлочинності: неправомірне використання комп'ютерних технологій та віртуального простору (перш за все електронна торгівля); транскордонність; зміна кількісних та якісних показників кіберзлочинності, зокрема різке підвищення кримінального професіоналізму та високої мобільності злочинців; інтелектуальний характер та активна динаміка використання розвитку і поширення високих технологій; рівень кіберзлочинності тісно пов'язаний з економічним рівнем розвитку суспільства в різних державах та регіонах; кібернетичні загрози швидкозмінні та високотехнологічні; високий рівень латентності; залежність географії поширення від фактору урбанізації; активними учасниками (співучасниками) кіберзлочинів є різного роду шахраї, здирники, рекетири, терористи, сутенери, педофіли, торговці людьми, зброєю, наркотиками; наявність стійкої тенденції до організованості, груповий характер вчинення кіберзлочинів [8, с. 173–175; 2, с. 235–239; 9, с. 12–18; 5, с. 103–114].

Серед вищевказаних ознак сучасної кіберзлочинності особливе місце займає кримінальний професіоналізм, наявність якого свідчить, що кіберзлочинність фактично відтворює всі етапи розвитку професійної злочинності та перетворилася на кримінальну професію.

На теперішній час можна виділити чотири етапи в розвитку кіберзлочинності:

I етап – поява кіберзлочинності та субкультури хакерів;

II етап – розповсюдження кіберзлочинності, поява спеціалізацій кіберзлочинності й національних груп хакерів;

III етап – набуття організованих форм і транснаціонального характеру у всіх сферах кіберзлочинності.

IV етап – використання у військово-політичних цілях з метою дестабілізації ситуації в країні [6].

Як відомо, професія є складним поняттям соціального статусу та соціальної ролі особистості, є видом трудової діяльності, що вимагає певної підготовки, та, як правило, є джерелом існування [12, с. 241]. З цього визначення випливають три ознаки професії: вид діяльності, підготовка, отримання матеріального доходу.

Професія як вид діяльності людини має і соціальний зміст. Її носіями є конкретні люди, які формують мікросередовище, виробляють професійну лексику та етику поведінки. Вищевикладене передбачає й четверту ознаку професії – зв'язок індивіда із соціально-професійним середовищем.

Кіберзлочинність має той самий набір ознак та характеристик, що й будь-яка професія. Відмінність лише в тому, що особа, яка володіє певними професійними навичками, при заняттi легальною діяльністю використовує свої сили і знання для досягнення позитивної мети як для себе особисто, так і для суспільства й держави загалом. Кіберзлочинець, займаючись нелегальною, соціально шкідливою діяльністю, спрямовує зусилля для досягнення лише власної позитивної мети, яка є різко негативною для інших громадян, суспільства і держави.

Таким чином, мова може йти про кримінальний професіоналізм кіберзлочинця. У зв'язку з цим, А. Ф. Зелінський важливою ознакою злочинця-професіонала вважав те, що останній займається професійно саме злочинною діяльністю. Злочинну діяльність він трактує як протизаконну діяльність особи, яка має відповідні вміння, навички, прийоми та засоби, і вважає цю діяльність своїм основним заняттям, яке є головним чи додатковим джерелом доходів [7, с. 165].

О. І. Нікітенко розглядає злочинну діяльність злочинців-професіоналів у двох аспектах: 1) як високий рівень виконання злочинних операцій, що забезпечує досягнення практично всіх встановлених цілей; 2) як спосіб існування за рахунок результатів злочинної діяльності [13, с. 240–246].

Обов'язковою ознакою кримінального професіоналізму є стійкість злочинної діяльності та кримінальна спеціалізація, яка характеризує неодноразове (систематичне) вчинення однорідних (тотожних) злочинів, яке спрямовано на задоволення певних потреб особи, виробляє в неї певну звичку

та переходить з часом у норму поведінки з чіткою установкою на обрану нею діяльність [12, с. 231].

Серед кіберзлочинців існує поділ злочинних ролей. Вони переважно дотримуються обраної спеціалізації, оскільки перехід до іншої сфери злочинності вимагає нових навичок та досвіду [12, с. 239].

Так, різновидом шахрайства в банківській системі є кардінг – незаконні фінансові операції з використанням платіжної картки або її реквізитів, що не ініційовані або не підтверджені її держателем. Реквізити платіжних карт, як правило, беруть зі зламаних серверів Інтернет-магазинів, платіжних та розрахункових систем, а також з персональних комп'ютерів (безпосередньо чи через програми віддаленого доступу, так звані «трояни»).

У сфері електронної комерції та господарської діяльності, фішинг – виманювання у користувачів Інтернету їх логінів та паролів до електронних гаманців, сервісів онлайн аукціонів, переказування або обміну валюти, тощо. Шахраї найчастіше змушують користувачів самостійно розкрити конфіденційні дані – наприклад, посилаючи електронні листи із пропозиціями, підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в Інтернеті, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів.

Фішинг буває кількох видів:

СМС-фішинг, коли потенційна жертва шахраїв отримує повідомлення про те, що її кредитну картку заблокував банк, а для розблокування необхідно надати реквізити, або ж про те, що власник картки отримав виграш, але потрібно заплатити за його доставку. Варіантів СМС-повідомлень безліч, тому потрібно бути особливо уважними, якщо ви отримуєте повідомлення.

Інтернет-фішинг, коли шахраї створюють фішингові (підроблені) сторінки, які імітують офіційні сторінки банків, платіжних сервісів, Інтернет-магазинів тощо.

Вішинг – вид кіберзлочинів, у якому в повідомленнях міститься прохання зателефонувати на певний міський номер, а при розмові запитуються конфіденційні дані власника картки.

Скімінг – копіювання даних платіжної картки за допомогою спеціального пристрою (скімера). Зазвичай відбувається під час здійснення карткових операцій із банкоматами. Для отримання даних злочинці використовують мінікамери або змінні клавіатури.

Онлайн-шахрайство – фальшиві Інтернет-аукціони, інтернет-магазини, сайти й телекомунікаційні засоби зв'язку.

Мальваре – створення та поширення вірусів і шкідливого програмного забезпечення.

Серед комп'ютерних злочинів існують злочини і проти державної безпеки, серед яких необхідно виділити такі суспільно небезпечні діяння, як неправомірний доступ до державної таємниці на машинному носії та диверсію у сфері комп'ютерної інформації, комп'ютерне шпигунство [11, с. 72].

Наступною ознакою кримінального професіоналізму є специфічні особисті якості, знання, вміння та навички злочинця. Необхідно відмітити, що в кіберзлочинність втягнуто широке коло осіб – від висококваліфікованих фахівців до дилетантів. Злочинці мають різний соціальний статус та різний рівень освіти. Тому вивчення особистісної складової кримінального професіоналізму неможливе без вивчення особистих якостей кіберзлочинців.

Для кіберзлочинця кримінальний професіоналізм має особисту раціональність. Кіберзлочини, зважаючи на їхню відносну безкарність, а також високу прибутковість, є досить привабливим видом діяльності. Ризики під час вчинення кіберзлочинів схожі на ризики під час здійснення легальної трудової діяльності (виробничий травматизм, монотонність, стреси тощо).

Однією з головних умов зростання та «привабливості» професійної кіберзлочинності є той факт, що Інтернет дає практично 100-відсоткову конфіденційність знаходження користувача в мережі. Існують добре відомі кіберзлочинцям програмні та технічні засоби, призначені для збереження анонімності. Також існують й доступні способи отримання доступу до комп'ютера на правах конфіденційності, наприклад – Інтернет-кафе.

Кіберзлочинці для вчинення кіберзлочинів повинні мати технічні знання та кваліфікацію. Діапазон рівня спеціальної професійної освіти кіберзлочинців достатньо широкий – від мінімальних знань користувача

комп'ютера до висококваліфікованих фахівців: 52% з них мали спеціальну підготовку в галузі автоматизованої обробки інформації, 97% були працівниками установ і організацій, які використовували комп'ютерні системи, мережі та інформаційні технології у своїх виробничих процесах, а 30% мали безпосереднє відношення до експлуатації засобів комп'ютерної техніки.

В окремих випадках особи, які вчинили кіберзлочини, взагалі не мали комп'ютерної освіти і спеціально технічного досвіду. Зокрема, дуже часто шахрайські дії з банківськими картками вчиняються злочинцями, які не мають високої технічної підготовки і механічно виконують певний алгоритм дій. Удосконалення схеми кіберзлочину створить для них значні труднощі. Щодо кіберзлочинців, які мають високу технічну підготовку для вдосконалення схем кіберзлочинів, ступінь суспільної небезпеки їхньої злочинної діяльності значно зростає.

Для більшості кіберзлочинців особливе значення має те, що маючи відповідні технічні знання, вони не домоглися або не захотіли домогтися визнання в суспільстві і вирішили використати свій талант у кримінальних цілях. Тобто жага до професійного визнання змусила їх піти на вчинення злочинів.

Наступною особливістю, що ідентифікує кримінальний професіоналізм кіберзлочинців, є кримінальні вміння. Кримінальне вміння – це здатність, заснована на набутих знаннях та навичках, здійснювати кримінальну діяльність – складну модель поведінки з високою якістю та необхідним кількісним результатом [12, с. 252].

Говорячи про причини та умови злочинності з урахуванням сучасних викликів та загроз необхідно зазначити, що під причинами злочинності в сучасній Україні розуміється система негативних соціально-психологічних явищ, пов'язаних із суперечностями суспільства і держави, що породжують злочинність.

Під умовами злочинності прийнято розуміти систему негативних економічних, соціальних, психологічних, організаційних, правових явищ, пов'язаних із суперечностями суспільства і держави, що створюють можливість формування причин і дії злочинності.

Причини й умови злочинності в основному зводяться до чотирьох підсистем – економічні причини й умови, причини та умови кримінальної агресивності, причини та умови кримінальної необережності і правові причини та умови [14].

Оцінюючи кримінальні вміння кіберзлочинця крізь призму відповідності його навичкам, а також складності виконуваних завдань, слід зазначити, що кіберзлочинність дозволяє максимально скоротити термін від задуму до злочинного результату, що також говорить про її суспільну небезпеку.

Система кримінальних умінь кіберзлочинців базується переважно на технічних знаннях. Крім цього, система включає актуальні та специфічні знання, до яких належать уявлення про основи кримінального, кримінального процесуального та іншого законодавства, знання стратегії й тактики діяльності правоохоронних органів, систем безпеки, психологічних та віктимологічних особливостей особистості взагалі, а також окремих категорій потерпілих та іншу необхідну інформацію [12, с. 262].

До актуальних для конкретної ситуації вмінь й навичок відносяться такі, які в цій конкретній ситуації дозволяють найбільш ефективно та успішно вчинити кіберзлочин у тому числі у сфері електронної торгівлі. Зокрема, основними характеристиками особи кіберзлочинця є оригінальність мислення й поведінки, обережність, уважність. Такі особи зосереджують увагу на розумінні, передбаченні та управлінні процесами. Це є основою їх компетенції й професійної майстерності. До того ж, вони відзначаються уважністю та пильністю, їхні дії витончені, хитрі, супроводжуються відмінним маскуванням [2].

Кримінальний професіоналізм кіберзлочинців не завжди переслідує отримання прибутку від злочинної діяльності. У деяких випадках результат може переслідувати інші цілі (помста, набуття чи зміцнення авторитету, дискредитація, політичні цілі тощо).

Можна помітити, що в системі цінностей кіберзлочинців лідирують індивідуальні або групові егоїстичні орієнтації. На перше місце ставиться особисте матеріальне благополуччя, прояв свого «Я», створення власних найбільш комфортних умов або груповий

інтерес (наприклад, нічим не обмежене вчинення кіберзлочинів й загальнодоступність комп'ютерних технологій з безроздільним використанням комп'ютерної інформації призводить до об'єднання кіберзлочинців у стійкі злочинні угруповання, що мають іноді транснаціональний характер).

Необхідно відзначити, що у кіберзлочинців склалася й своя субкультура, з'явився свій жаргон – «сленг», зрозумілий лише вузькому колу злочинців.

За ознакою відповідного рівня кримінального професіоналізму кіберзлочинців можна розподілити за типами:

тип кіберзлочинця-початківця (середній матеріальний достаток, можливість володіти комп'ютерними пристроями (одним або більше); вік – від вісімнадцяти до тридцяти років; переважно особи чоловічої статі з технічною освітою (в окремих випадках – незакінчена); діяльність – або професійна діяльність, пов'язана з інформаційними, електронними торгівлями та комп'ютерними технологіями (фахівці комп'ютерних фірм, адміністратори баз даних тощо), або відсутність постійної роботи);

стійкий тип кіберзлочинця (середній і вищий за середній матеріальний достаток, наявність глибоких знань у сфері інформаційних технологій, мереж, інших досягнень цифрового суспільства; вік – від двадцяти до двадцяти п'яти років; переважно чоловіча стать з тенденцією прояву активності осіб жіночої статі (5%); освіта – переважно вища технічна або аналогічна, наявність можливості володіти інноваційними комп'ютерними системами, пристроями, комп'ютерними розробками);

професійний тип (високий рівень матеріальної забезпеченості; вік – старше двадцяти п'яти років; переважно особи чоловічої статі; освіта – вища технічна, наявність професійних знань, навичок, умінь у сфері інформаційних технологій, мереж, інших досягнень цифрового суспільства на високому рівні, постійне вдосконалення навичок у сфері застосування засобів для вчинення кіберзлочинів, у тому числі розроблених особисто);

особи, які раніше вчиняли злочини, «перекваліфікувалися» на кіберзлочинців через широкі можливості кіберпростору, а також представники організованої злочинності, здатні об'єднати осіб, які мають спеціальні знання для вчинення кіберзлочинів.

Висновки

Це дослідження дало можливість окреслити наявні проблеми та сформувати вектор нових наукових досліджень у питаннях, які стосуються шахрайства у сфері електронної торгівлі.

Аналіз наявних проблем, які існують у сфері кіберзлочинності, є відносно новим напрямом боротьби зі злочинністю, що, у свою чергу, дозволяє виділити такі його ознаки:

1) кіберзлочинність є раціонально привабливим кримінальним промислом;

2) кіберзлочинність дозволяє досягти професійного визнання у злочинних колах;

3) кіберзлочинність дозволяє максимально скоротити термін від задуму до злочинного результату.

Враховуючи високий рівень латентності злочинів цього виду, можна спрогнозувати подальше зростання професійної кіберзлочинності у сфері електронної торгівлі, що вказує на необхідність розроблення нових більш ефективних заходів протидії цьому явищу сьогодення.

Література

1. Біленчук П. Д., Обіход Т. В. Кібербезпека і засоби запобігання та протидії кіберзлочинності й кібертероризму. *Часопис Київського університету права*. 2018. № 3. С. 235–239.

2. Біленчук П., Малій М. Кіберсвіт у новому тисячолітті. Хто вони: кіберзлочинці, кібершахраї, кібертерористи? URL: https://lexinform.com.ua/dumka-eksperta/kibersvit-u-novomu-tysyacholitti-hto-vony-kiberzlochyntsi-kibershahrayi-kiberterorysty/ (Дата звернення: 17.06.2023).

3. Болгов В., Гадіон Н., Гладун О. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій: науково-практичний посібник. Київ: Національна академія прокуратури України, 2015. 202 с.

4. Газізова Ю. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових

злочинів. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606 (Дата звернення: 20.05.2023).

5. Голіна В. В., Головкін Б. М. Кримінологія: Загальна та Особлива частини. Навчальний посібник. Харків: Право, 2014. 284 с.

6. Дзюндзюк В. Б., Дзюндзюк Б. В. Поява і розвиток кіберзлочинності. *Державне будівництво.* 2013. № 1. URL: http://nbuv.gov.ua/UJRN/DeBu_2013_1_3 (Дата звернення: 17.06.2023).

7. Зелінський А. Ф. Кримінология: навч. посіб. Харків: Рубікон, 2000. 240 с.

8. Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. *Актуальні проблеми вітчизняної юриспруденції.* 2016. № 3. С. 172–177.

9. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ: автореф. дис. … канд. юрид. наук. Харків, 2016. 19 с.

10. Луценко Ю. В., Арешонков В. В. Вплив організованої злочинності на світову безпекову політику, що викликана пандемією Covid-19. *Наукові записки Інституту законодавства Верховної Ради України*, 2022. № 1, С. 78–86.

11. Луценко Ю. В., Денисенко М. М. Протидія злочинності в умовах воєнного стану: теоретико-правові проблеми. *Прикарпатський юридичний вісник.* 2022. Випуск 3(44). С. 70–75.

12. Макаренко Н. К. Запобігання професійній злочинності в Україні: монографія. Київ: Нац. акад. внутр. справ, 2021. 455 с.

13. Нікітенко О. І. Кримінально-правова політика України в боротьбі з організованою і професійною злочинністю. *Кримінальна правова політика держави: теоретичні та практичні аспекти проблеми*: матеріали Міжнар. наук. конф. (Донецьк, 17–18 листоп. 2006 р.). Донецьк: Донецький юрид. ін-т Луганського держ. ун-ту внутр справ, 2006. С. 240–246.

14. Причини й умови злочинності в Україні. URL: http://lib-net.com/content/9264_Prichini_i_ymovi_zlochinnosti_v_Ykraini.html (Дата звернення: 20.06.2023).

15. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 вересня 2005 року № 2824-IV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text (Дата звернення: 17.06.2023).

16. Тарасюк А. В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи: монографія. Київ; Одеса: Фенікс, 2020. 404 с.

Makarenko N. – Doctor of Law, Assistant Professor, Professor of Department of Criminology and Criminal Enforcement Law National Academy of Internal Affairs

Lutsenko Yu. – Doctor of Law, professor

CYBERCRIME IN THE SPHERE OF ELECTRONIC TRADE AS A MANIFESTATION OF CRIMINAL PROFESSIONALISM

The article examines issues related to cybercrime in the field of electronic commerce as a manifestation of criminal professionalism, and also draws attention to criminological problems of professional cybercrime in Ukraine. The development of technologies with the help of which not only crimes in the field of electronic commerce, but also socially dangerous actions, which were previously considered traditional, began to be actively committed, is being studied.

The paper analyzes the signs of criminal professionalism of cybercrimes. A typology of cyber criminals is proposed according to the level of their criminal professionalism.

In the course of the research, a thesis was formed that today new characteristics of cybercriminals are emerging in the field of electronic commerce, which requires modern approaches to studying the essence of the criminal professionalism of cybercriminals.

Key words: *cyber security/cybercrime, identity of the cybercriminal, typology of cybercriminals, combating cybercrime, criminal professionalism, criminal groups, professional crime, computer information sabotage, computer espionage, e-commerce, fraud, fraud prevention, e-commerce fraud, causes and conditions of crime*