Література:

1. Сімейне право України : Підручн. / За ред. Гопанчука В. С. – К. : Істина, 2002. – 304 с.
2. Румянцева-Козовник А.В. Правові аспекти усиновлення іноземцями дітей, які є громадянами України / А. В. Румянцева-Козовник // Наше право № 6. – 2014. – С. 71-72
3. Скоробогач О. В. Міжнародно-правові стандарти усиновлення іноземцями дітей, які є громадянами України / О.В. Скоробогач // Право і безпека. – 2013. - № 1 (48). – С. 201-205.
4. Кухар А. О. Актуальні питання удосконалення інституту міжнародного усиновлення / А. О. Кухар // Держава і право. Юридичні і політичні науки. – 2010. – Вип. 48. – С. 407.
5. Погорецька Н.В. Міжнародне усиновлення : проблемні питання / Н.В. Погорецька // Форум права. – 2011. – № 3. – С. 612, 613. [Електронний ресурс] – Режим доступу: http:// archive.nbuv.gov.ua / e-journals/FP/2011-3/11pnvupp.pdf.
6. Cantwe11 N., Lammerantl, Martinez-Mora L. Assessment of the Adoption Sistem in Ukraine. – Geneva ISS, October 2005. – P. 119. – [Електронний ресурс]. – Режим доступу: https://www.osce.org/ukraine/75897?download=true.

УДК 343.3

Мазуренко Світлана Вікторівна
канд. юрид. наук, доцент,
доцент кафедри права інтелектуальної власності
та корпоративного права
Національного університету
"Одеська юридична академія"

ЗАГАЛЬНІ ЗАСАДИ КІБЕРЗЛОЧИННОСТІ ЯК СУСПІЛЬНОГО ТА ПОЛІТИКО-ПРАВОВОГО ЯВИЩА

В статті розглянуто поняття «кіберзлочинність» та її види як соціально-небезпечне явище на різних етапах технічного прогресу, починаючи з середини двадцятого століття; охарактеризовані наслідки даної злочинної діяльності та методи боротьби з нею в Україні та інших країнах світу.

Ключові слова: кіберзлочинність, Інтернет, кібершахрайство, комп'ютерний злочин, піратство.

В статье рассмотрено понятие «киберпреступность» и ее виды как социально-опасное явление на разных этапах технического прогресса, начиная с середины двадцатого столетия; охарактеризованы последствии данной преступной деятельности и методы борьбы с ней в Украине и других странах мира.

Ключевые слова: киберпреступность, Интернет, компьютерное преступление, пиратство, кибермошенничество, пиратство.

The concept of "cybercrime" and its types as a socially dangerous phenomenon at various stages of technological progress, beginning in the middle of the twentieth century, has been fully considered. Characterized by the consequences of this criminal activity and methods of combating it in Ukraine and other countries of the world.

Key words: cybercrime, the Internet, computer crime, piracy, cyber fraud.

Термін «кіберзлочинність» часто вживається поряд з терміном «комп'ютерна злочинність», як зазначає Буров О. [1], причому нерідко ці поняття використовуються як синоніми. Дійсно, ці терміни дуже близькі один одному, але все-таки, на мій погляд, не синонімічні. Поняття «кіберзлочинність» (в англомовному варіанті - cybercrime) ширше, ніж «комп'ютерна злочинність» (computer crime), і більш точно відображає природу такого явища, як злочинність в інформаційному просторі. Так, Оксфордський тлумачний словник визначає приставку «cyber-» як компонент складного слова. Її значення - що уналежнюється до інформаційних технологій, мережі Інтернет, віртуальної реальності. Практично таке ж визначення дає Кембриджський словник. Таким чином, «cybercrime» - це злочинність, пов'язана як з використанням комп'ютерів, так і з використанням інформаційних технологій і глобальних мереж.

У той же час термін «computer crime» в основному відноситься до злочинів, скоюваних проти комп'ютерів або комп'ютерних даних.

Термін «комп'ютерна злочинність» вже за своїм смисловим навантаженням, і зводить суть явища до злочинів, скоєних за допомогою комп'ютера. У теперішній же час з розвитком інформаційних технологій саме поняття «комп'ютер» стає розмитим. Наприклад, сьогодні практично всі мобільні телефони мають доступ в мережу Інтернет. З розвитком 3G мереж мобільні телефони здатні підключатися до глобальної мережі за технологією HSPDA (мережа четвертого покоління) або UMTS (мережа третього покоління), що за швидкістю ненабагато поступається можливостям підключення до мережі Інтернет за допомогою звичайного комп'ютера, а в перспективі і перевищує їх.

На шляху поділу термінів «кіберзлочинність» і «комп'ютерна злочинність» й використанню саме першого терміна слід звернутися до міжнародного права. Рада Європи в листопаді 2001 року прийняла Конвенцію про кіберзлочинність [2], вживши саме термін «cybercrime», а не «computer crime». Кіберзлочинність - це злочинність у так званому кіберпросторі. Автори «модельного закону» про кіберзлочинність Міжнародного Союзу Електрозв'язку (2009 р.) визначають кіберпростір як «фізичний і не фізичний простір, створений і (або) сформований таким чином: комп'ютери, комп'ютерні системи, мережі, їхні комп'ютерні програми, комп'ютерні дані, дані контенту, рух даних, і користувачі». В даний час офіційне визначення кіберпростору на міжнародному рівні відсутнє, втім, як і визначення кіберзлочинності.

Згідно з положеннями Конвенції та Додаткового протоколу [3] предметами відповідних злочинів є: ціла комп'ютерна система або її частина (ст. 2 Конвенції); комп'ютерні дані, які не призначені для публічного користування, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить у собі такі комп'ютерні дані (ст. 4 Конвенції); комп'ютерна інформація (ст. 4 Конвенції); пристрої, у тому числі комп'ютерні програми, створені або

адаптовані з метою вчинення злочину (підпункт «і» пункту «а», пункт «b» ч. 1 ст. 6 Конвенції); комп'ютерні паролі, коди доступу або подібні дані, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи (підпункт «іі» пункту «а», пункт «b» ч. 1 ст.6 Конвенції); комп'ютерні дані (ст. 7, пункт «а» ст. 8 Конвенції); порнографічний матеріал (частина перша ст. 9 Конвенції); об'єкти авторського права і суміжних прав (ст. 10 Конвенції); расистський чи ксенофобський матеріал, доступ до якого може бути здійснений за допомогою комп'ютерної системи (ст. 3 Додаткового протоколу); дані, які містять погрози з расистських або ксенофобських мотивів, передані через комп'ютерну систему (ст. 4 Додаткового протоколу); інформація публічного характеру, яка містить образу осіб з расистських або ксенофобних мотивів (ст. 5 Додаткового протоколу); матеріал, який заперечує, значно мінімізує, схвалює чи виправдовує дії, які є геноцидом або злочинами проти людства, котрий розповсюджений через комп'ютерні системи або доступ до якого може бути здійснений через такі (ст. 6 Додаткового протоколу) [4].

У 2013 р. Управління ООН з наркотиків і злочинності в опублікованому звіті «Всебічне дослідження проблеми кіберзлочинності та відповідь заходів з боку держав - членів, міжнародного співтовариства і приватного сектора» [5] відзначає, що поняття «кіберзлочинність» залежить від контексту і мети вживання цього терміна. При цьому, як наголошується в тому ж документі, що хоча основне "ядро" цього терміна представляють злочини проти конфіденційності, цілісності та доступності даних, крім цього досить обмеженого списку комп'ютерних злочинів, в поняття «кіберзлочинність» включаються будь-які дії, спрямовані на нелегальне вилучення прибутку, контент-злочини, та інші протизаконні діяння в кіберпросторі. При цьому, як відзначають автори звіту, у створенні якогось універсального визначення кіберзлочинності немає необхідності, так як, наприклад, з метою міжнародного співробітництва в розслідуванні злочинів набагато важливіше гармонізувати норми, що відносяться до збору та поданням електронних доказів. Ця необхідність не обмежується якимось

штучним терміном «кіберзлочинів», оскільки на електронних носіях і в електронних комунікаціях може міститися інформація, що відноситься до будь-якого виду злочинів, скоєних як у кіберпросторі, так і поза ним.

Автори цієї роботи дотримуються точки зору про те, що поняття кіберзлочинності як сукупності злочинів поширюється на всі види злочинів, скоєних в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть виступати (бути) предметом (метою) злочинних посягань, середовищем, в якій відбуваються правопорушення і засобом або знаряддям злочину. Таким чином, кіберзлочинність може бути визначена як сукупність злочинів, скоєних в кіберпросторі за допомогою комп'ютерних систем чи комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж, і проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [6].

Стрімке зростання кількості кібератак на державні ресурси й загальне збільшення кіберзлочинів обумовлює необхідність упорядкування проблеми на міжнародному рівні. Так, резолюції чи рішення з даного питання ухвалювали країни «великої вісімки», Організація Об'єднаних Націй, Міжнародний союз електрозв'язку, Рада Європи й інші об'єднання та організації. Водночас досі єдиним дієвим міжнародно-правовим документом є Конвенція про кіберзлочинність [7]. І хоча кількість країн-підписантів постійно збільшується (станом на 2014 рік їх було вже 43), однак не всі її ратифікували. Однією з причин відмови від ратифікації стало те, що згідно з положенням Конвенції будь-яка зі сторін має право отримувати доступ до комп'ютерних даних (ресурсів), розташованих у мережах загального користування іншої сторони, не повідомляючи її про це. Кіберпростір як новий вимір геополітичного суперництва ставить під сумнів дотримання принципу суверенності держав. Низка країн висловлює ідею розроблення універсального документа, що мав би забезпечити збереження класичного розуміння суверенітету в нову цифрову епоху. Зокрема, Росія послідовно підтримує ідею прийняття

Конвенції про забезпечення міжнародної інформаційної безпеки (КЗМІБ) [8].

Серед найбільш уразливих до кіберзлочинів сфер суспільного життя - фінансовий сектор економіки, а саме банки та їх послуги. Найбільш поширеними злочинами в банківській сфері є шахрайство з використанням платіжних карток та їх реквізитів і шахрайство з використанням дистанційного банківського обслуговування (система «клієнт-банк»). Середній показник таких злочинів у країнах Європейського союзу складає 0,06–0,08%, в Україні у 2011–2012 рр. кількість подібних злочинів сягала 0, 045% всіх операцій із платіжними картками. І хоча фахівці розглядають ці показники як показники злагодженої роботи правоохоронців і банків у протидії кіберзлочинності, проте не слід забувати, що в Україні більшість громадян після кризи 2009 р. не довіряють свої кошти фінансовим установам, дуже багато людей не залишають на пластикових картках навіть заробітну плату, яку їм перераховують на спеціальних рахунок.

За 2012 р. в Україні зафіксовано 139 випадків шахрайства з використанням системи «клієнт банк» на загальну суму 116 млн. грн, проте 75% цих коштів було повернуто постраждалим особам. У цілому за офіційними даними Нацбанку України загальна кількість шахрайських операцій за минулий рік збільшилась на 47%, а сума збитків на 20%. На 2012 р. 40% від загальної кількості українських банків постраждали від кібернетичних злочинів. На початку 2013 р. було виявлено 14 кіберзлочинів на загальну суму близько 20 млн. грн, із яких було повернуто 88%. Згідно даним Нацбанку України у 2011 р. число протиправних операцій із платіжними картками в українських банках зросло до 7,6 тис. порівняно з 2,9 тис. за 2010 р., а обсяг неправомірного списання коштів збільшився майже в півтора рази і досяг 9,1 млн. грн.

Слід зазначити, що ці кіберзлочини можуть учинятися як хакерами, які не мають жодного відношення до банку, так і співробітниками банків, які мають доступ до персональних даних клієнтів. Так звані інсайдери досить часто зливають конфіденційну інформацію шахраям, отримуючи за це частку від

награбованих коштів. Наразі це поширена проблема серед великих структур не тільки державних, де заробітна плата не досить велика, а й великих холдингів, компаній, які оперуються великими базами з персональними даними. Тому мають значення не тільки засоби захисту від зовнішнього втручання в банківські системи, а також моніторинг обігу даних, які використовуються всередині великих установ і підприємств, що, на жаль, не так поширено на українському ринку фінансових послуг [9].

Кіберзлочинність - явище за своєю природою транскордонне. Тому аналіз кіберзлочинності або його різновиду - комп'ютерної злочинності - у рамках однієї країни чи групи країн, безумовно, цінний, але навряд чи здатний дати уявлення про справжні масштаби і про розмах цього явища. Глобальність і транскордонність комп'ютерних і телекомунікаційних мереж, можливість маніпуляцій злочинця з ідентичністю (тобто використання чужих імен, адрес, паролів і т.п.) створює ситуації, коли злочинець знаходиться на одному континенті, злочин безпосередньо вчиняється на іншому, а наслідки злочину наступають на третьому. Більше того, в останні кілька років у зв'язку з появою і поширенням ботнетів - мереж інфікованих комп'ютерів, які проводять атаки незалежно від користувачів, ситуація ускладнилася ще більше: злочинець, сотні атакуючих комп'ютерів і потерпілий від злочину можуть перебувати на території більш ніж двох або трьох держав.

В даний час не існує ні релевантної статистики, що відбиває реальну картину стану кіберзлочинності, ні надійних методів збору таких даних. І справа не тільки у відсутності однаковості національного кримінального законодавства країн у сфері боротьби з кіберзлочинністю і різної практики його застосування, відмінностях у формуванні кримінальної статистики та особливості правоохоронної системи. Так, до цих пір неясно, до якої міри достовірна статистика про економічні втрати в результаті кіберзлочинності. Є думка, наприклад, що дохід від кіберзлочинів значно перевищив дохід від інших злочинів, включаючи торгівлю наркотиками. За останніми даними, наведеними в липні 2013 р. [10] в спільному аналізі

американського Центру стратегічних і міжнародних досліджень та компанії McAfee, щорічні втрати світової економіки від кіберзлочинів досягли вже 500 мільярдів доларів. Щоб уявити собі масштаби і обороти цього кримінального бізнесу, досить навести деякі приклади. Віртуальні шахраї, заволодівши через Мережу номерами більш ніж мільйона банківських карт - громадян США, одночасно зробили розкрадання в 130 банкоматах в 49 містах Америки. При цьому вся операція зайняла не більше 30 хвилин, а розмір прибутку злочинців склав близько 9 млн. доларів, які потім були переведені на рахунки в різні держави, в основному в пострадянському просторі. У 2010 р. ФБР висунуло звинувачення проти 37 жителів Росії, України та інших східноєвропейських країн, підозрюваних у використання комп'ютерного вірусу для злому американських банківських рахунків. Найбільша частина кіберзлочинності залишається за рамками статистики – тому можна говорити, що в офіційну статистику потрапляє лише десять, у кращому випадку двадцять відсотків скоєних діянь.

Структура кіберзлочинності розрізняється помітно в різних країнах залежно , передусім , від характеру і ступеня розвитку інформаційних технологій , поширення мережі Інтернет , використання електронних сервісів та електронної комерції і т.п. Структура кіберзлочинності, наприклад, в США, виглядає наступним чином. За даними одного з досліджень, 44% склали крадіжки грошей з електронних рахунків, 16% - пошкодження програмного забезпечення, стільки ж - викрадення секретної інформації, 12% - фальсифікація інформації, 10% - замовлення послуг за чужий рахунок. Проблема кіберзлочинності також має різні наслідки і структуру для розвинених країн і країн, що розвиваються. Так, наприклад, якщо проблема СПАМ (незаконних масових розсилок електронною поштою) для розвинених держав небезпечна в основному через вірусних програм, які розсилаються разом зі СПАМом, то в країнах, що розвиваються проблемою є також пропускна здатність телекомунікаційних мереж, які не можуть витримати подібного навантаження. Структура і динаміка кіберзлочинності, а також її масштаби залежать також від

культури кібербезпеки користувачів в окремій державі, що також має різні аспекти залежно від ступеня розвитку економіки тієї чи іншої країни.

Загрози в інформаційному просторі змінюються з розвитком технологій. Наприклад, у 2008 році серед десяти найбільш небезпечних загроз, що відзначаються фахівцями були: мережі ботів; «цілеспрямовані атаки на урядові сайти, приватні підприємства, і кінцевих користувачів; фінансове шахрайство, потерпілими від якого є банки, приватні підприємства і кінцеві користувачі; шахрайство з посвідченням особи; спам і крадіжка персональних даних; шпигунство - економічний і в державних органах; Web-атаки; соціальні мережі; неправильне або зловмисне використання внутрішніх мережевих ресурсів; віруси і черв'яки.

У 2013 році, згідно з прогнозом фахівців McAfee, на перший план виходять загрози, пов'язані з використанням мобільного доступу в мережу Інтернет (заражені шкідливим ПЗ програми для мобільних телефонів і віруси, що блокують оновлення антивірусного ПЗ, смс-повідомлення, заражені вірусами). Крім того, серед небезпечних тенденцій відзначаються: постійний розвиток способів атак на Windows 8 і HTML5; атаки, спрямовані не так на вилучення вигоди, а на заподіяння шкоди інфраструктурі; використання шкідливого ПЗ для ботнетів, яке оновлює з'єднання навіть після того, як ботнет знищений, що дозволяє подальше поширення інфекції; розвиток аутсорсингу кібератак серед кримінальних груп та продаж ПЗ і послуг по вчиненню кіберзлочинів. Також попереджається, що політичний активізм в Інтернеті буде заміщатися екстремістськими групами, а причетність держав до кіберзлочинності збільшиться - як у плані атак, організованих на державному рівні, так і в плані можливості стати мішенню атак.

При огляді актуальних послуг і типових цін на них, існуючі на ринку кіберзлочинності, експерти виділили такі види злочинів, які становлять найбільшу суспільну небезпеку: DDoS-атаки - мережеві атаки, спрямовані на відмову в обслуговуванні; шахрайство в системах ДБО - неправомірна відправка електронних платіжних доручень з метою розкрадання

грошових коштів; спам - масова розсилка небажаних повідомлень електронної пошти; продаж трафіку - послуги з установки програм на велику кількість комп'ютерів і послуги з перенаправлення відвідувачів на певні веб-сайти (послуга відноситься до внутрішнього ринку кіберзлочинності); партнерські програми - нелегальний продаж медикаментів, продаж контрафактного ПЗ, завантажень і т.п. (послуга відноситься до внутрішнього ринку кіберзлочинності).

Сьогодні практично всі дослідники і фахівці визнають, що ситуація з кіберзлочинністю в світі поки має тенденцію до погіршення. Ще одна небезпечна тенденція - дедалі більший зв'язок між кіберзлочинністю та організованою злочинністю. Більшість кіберзлочинів вчиняється індивідуумами або невеликими злочинними групами. Однак фахівці відзначають зростаючий взаємозв'язок між кіберзлочинністю та організованою злочинністю. Можна з упевненістю сказати, що Інтернет використовується злочинними групами вже не тільки як допоміжний засіб, але і як місце і основний засіб вчинення традиційних злочинів - шахрайств, крадіжок, вимагань. За даними Європолу, тільки в ЄС, діє близько 3600 таких груп. Більш того, протягом останніх років відзначається «професіоналізація» організованої кіберзлочинності: не тільки комп'ютерні атаки стають все більш комплексними і явно вимагають участі професіоналів у їх підготовці, але і шахрайства в мережі Інтернет, крадіжка даних, відмивання грошей перетворюються на великий сектор тіньового ринку, з поділом праці між злочинними групами і цілими майданчиками для торгівлі програмним забезпеченням для вчинення злочинів, для продажу інформації, для «аутсорсингу» навичок, необхідних на тій чи іншій стадії вчинення Інтернет-злочинів.

Більш того, мережа Інтернет все частіше використовується організованими злочинними групами для відмивання грошей. Інтернет представляє величезні можливості для махінації з рахунками. Онлайн аукціони дозволяють провести переміщення грошей у зв'язку з нібито легальними поставками, розвиток електронних платежів і он-лайн банків надає безліч способів приховати рух злочинних доходів і

виробляти незаконні угоди. В даний час, однак, можливості відмивання грошей, отриманих в результаті саме кіберзлочинів, обмежені через необхідність переводити кошти, викрадені онлайн в «фізичний» світ, що в якійсь мірі стримує зростання економічних кіберзлочинів [11].

Література:

1. Буров, О. Кіберзлочинність як загроза інформаційному суспільству / О. Буров, Л. Бурова, А. Пенська // Теорія і практика інтелектуальної власності : Науково-практичний журнал. - 2008. - №3. - С. 39-40.

2. Конвенція Ради Європи «Про кіберзлочинність», прийнята 23 листопада 2001 р., ратифікована Верховною Радою України 7 вересня 2005 р. / Відомості Верховної Ради України. - 2006.

3. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, прийнятий 28 січня 2003 р., ратифікований Верховною Радою України 21 липня 2006 р./ Відомості Верховної Ради України. – 2007.

4. Андрушко, П. Використання модельних норм Конвенції Ради Європи "Про кіберзлочинність" та Додаткового протоколу до неї у нормотворчому процесі в Україні : теоретичні проблеми реалізації / П. Андрушко, Н. Розенфельд // Право України* : Юрид. журн. - 2007. - № 12. - С. 65.

5. Comprehensive Study on Cybercrime [Електронний ресурс] // UNODC. – 2013. – Режим доступу до ресурсу: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

6. Політова А. С. Кіберзлочини: проблема визначення [Електронний ресурс] / А. С. Політова // Х: ХНУВС. – 2013. – Режим доступу до ресурсу: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/180/Aktual_p1tan_rozsl_kiberzloch_2013.pdf?sequence=1&isAllowed=y.

7. Конвенція Ради Європи «Про кіберзлочинність», прийнята 23 листопада 2001 р., ратифікована Верховною Радою України 7 вересня 2005 р. / Відомості Верховної Ради України. - 2006.

8. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва [Електронний ресурс] / Д. В. Дубов // К: НІСД. – 2014. – Режим доступу до ресурсу: http://www.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf.

9. Буров, О. Кіберзлочинність як загроза інформаційному суспільству / О. Буров, Л. Бурова, А. Пенська // Теорія і практика інтелектуальної власності : Науково-практичний журнал. - 2008. - №3. - С. 43.

10. Рассолов, И.М. Киберпреступность: понятие, основные черты, формы проявления / И.М. Рассолов// Юридический мир. - 2008. - № 2. - С. 44-46.

11. Клочко А. М. Проблеми питання транснаціональної кіберзлочинності [Електронний ресурс] / А. М. Клочко // Х: ХНУВС. – 2013. – Режим доступу до ресурсу:http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/180/Aktual_p1tan_rozsl_kiberzloch_2013.pdf?sequence=1&isAllowed=y.

УДК 347.965.42

Малєнко Ольга Валеріївна
асистент кафедри приватного права,
адвокат,
Чернівецький національний університет
імені Юрія Федьковича

УЧАСТЬ АДВОКАТА В ПРОЦЕДУРІ МЕДІАЦІЇ, ЯК НОВИЙ НАПРЯМОК В АДВОКАТСЬКІЙ ДІЯЛЬНОСТІ

Стаття присвячена дослідженню особливостей участі адвоката у процедурі посередництва у якості медіатора. Розглянуто та проаналізовано ознаки за якими можливо визначити специфіку діяльності адвоката-медіатора. Виявлено переваги і недоліки у наданні медіативної допомоги адвокатом-медіатором.

Ключові слова: адвокат, медіатор, адвокат-медіатор, адвокатська діяльність, медіація.

Статья посвящена исследованию особенностей участия адвоката в процедуре посредничества в качестве медиатора.. Установлены и проанализированы признаки по которым можно определить специфику деятельности адвоката-медиатора.