ISSN 1995-6134

УДК 343.3

К.В. ЮРТАЄВА,
канд. юрид. наук, Харківський національний університет внутрішніх справ
ORCID: http://orcid.org/0000-0002-6096-2020
ResearcherID: http://www.researcherid.com/rid/D-1818-2016

ПРОБЛЕМИ КРИМІНАЛІЗАЦІЇ НЕЗАКОННОГО ВИКОРИСТАННЯ КОМП'ЮТЕРНИХ ПАРОЛІВ, КОДІВ ДОСТУПУ АБО ПОДІБНИХ ДАНИХ, ЯКІ НАДАЮТЬ ДОСТУП ДО КОМП'ЮТЕРНИХ СИСТЕМ АБО ЇХ ЧАСТИН

Ключові слова: *кіберзлочин, зловживання пристроями, комп'ютерний пароль, код доступу, кваліфікація злочинів, криміналізація*

Вироблення адекватних заходів протидії кіберзлочинності (комп'ютерній злочинності) є однією з найбільш актуальних проблеми сучасної системи кримінальної юстиції. Складність поставленого завдання обумовлюється низкою об'єктивних факторів, пов'язаних зі специфікою зазначених злочинів:

– транскордонний характер комп'ютерних злочинів;

– неузгодженість юрисдикційних аспектів протидії кіберзлочинності (наявність позитивних і негативних конфліктів кримінальних юрисдикцій);

– специфічні властивості комп'ютерної інформації як предмета злочину;

– постійне вдосконалення злочинних засобів та методів вчинення кіберзлочинів;

– орієнтація кримінального і кримінального процесуального законодавства на традиційні моделі вчинення та поширення злочинності;

– складність та суперечливість процесу кримінально-правової кваліфікації комп'ютерних злочинів;

– недоліки кримінального процесуального законодавства щодо отримання, фіксації та дослідження електронних доказів тощо.

Практика доводить, що класична правова доктрина часто не має ефективних засобів для вирішення зазначених завдань. У результаті цього в межах традиційних наукових знань почали виокремлювати окремі підгалузі, націлені на вивчення та розробку специфічних заходів протидії кіберзлочинності. Так, наприклад, у межах криміналістики в останні роки виокремилася форензика – прикладна наука, пов'язана з особливостями розслідування злочинів, пов'язаних з комп'ютерною інформацією, збиранням та дослідженням електронних доказів. У межах кримінології отримала розвиток кіберкримінологія, напрям кримінологічних досліджень детермінації злочинів, що вчиняються у кіберпросторі, та їх впливу на фізичний простір, і кібервіктимологія, що вивчає форми он-лайн віктимізації, її впливу на жертв злочинів та зворотної реакції суспільства і систем. Два останні терміни (Cyber Criminology і Cyber Victimology) увів у науковий вжиток відомий індійський дослідник комп'ютерної злочинності Д. Каруппаннан у 2007 р. і 2015 р. відповідно [1]. Таким чином, парадигми фізичного світу далеко не завжди пристосовані до діянь, що вчиняються у віртуальному просторі та кіберпросторі, як інституційному втіленні Інтернету. Відповідно, протидія комп'ютерним злочинам вимагає відхід від традиційних моделей протидії злочинності, в тому числі й перегляд чинних норм про кримінальну відповідальність за кіберзлочини. Одним із актуальних аспектів окресленої проблеми є вдосконалення законодавства України про кримінальну відповідальність стосовно незаконного використання комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин. Тому метою статті є аналіз норм чинного КК України щодо закріплення відповідальності за незаконного використання комп'ютерних паролів, кодів доступу або подібних даних, які нада-

ISSN 1995-6134

ють доступ до комп'ютерних систем або їх частин.

Питанням кримінальної відповідальності та кваліфікації кіберзлочинів приділено досить значну увагу в дослідженнях вітчизняних науковців. Як відомо, злочини, пов'язані з використанням комп'ютерних технологій, отримали своє закріплення у різних розділах Особливої частини КК України, відповідно питання їх кваліфікації тим чи іншим чином порушується під час розгляду різних за об'єктами суспільно небезпечних діянь: злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, злочинів проти власності, злочинів у сфері господарської діяльності, злочинів проти виборчих, трудових та інших особистих прав і свобод людини і громадянина, злочинів проти авторитету органів державної влади тощо. Так, питань кваліфікації кіберзлочинів торкалися у своїх дослідженнях Д.С. Азаров, А.А. Васильєв, О.П. Горпинюк, О.О. Дудоров, М.В. Карчевський, Д.Ю. Кондратов, В.В. Кузнецов, А.А. Музика, Є.В. Лащук, М.І. Мельник, П.І. Орлов, С.О. Орлов, Д.В. Пашнєв, М.В. Плугатир, О.Е. Радутний, Н.А. Розенфельд, М.І. Хавронюк та багато інших науковців. Незважаючи на значну кількість досліджень за вказаною тематикою, недостатньо дослідженим залишається питання криміналізації незаконного використання комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин.

На теперішній час Кримінальний кодекс України (далі – КК України) не містить окремих норм щодо кримінальної відповідальності за незаконне використання комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин, проте питання щодо передбачення такої норми ставилося як в науці, так і на рівні окремих законодавчих ініціатив. Уперше питання про встановлення вказаної кримінально-правової заборони було порушено у зв'язку з підписанням Україною Конвенції Ради Європи про кіберзлочинність 2001 р. (далі – Конвенція). Слід зазначити, що зазначена міжнародна угода, хоча й ініційована країнами-членами Ради Європи із самого початку замислювалася як універсальний інструмент протидії кіберзлочинності. Під час її підписання до Конвенції долучилися чотири країни, які не є членами Ради Європи, – Канада, Японія, Південно-Африканська Республіка та Сполучені Штати Америки. На сьогоднішній день Конвенцію про кіберзлочинність 2001 р. підписали та ратифікували 12 країн, що не входять до Ради Європи. Ратифікуючи вказану міжнародну угоду, Верховна Рада України скористалася правом, передбаченим ст.19 Віденської конвенції про право міжнародних договорів 1969 р., та частково обмежила дію певних положень договору щодо нашої держави. Так, зокрема, у Законі України «Про ратифікацію Конвенції про кіберзлочинність» зазначено, що Україна зокрема залишає за собою право частково не застосовувати п.1 ст.6 Конвенції щодо встановлення кримінальної відповідальності за зловживання пристроями [2]. Так, п. а.1 ст.6 Конвенції передбачає встановлення відповідальності щодо виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином пристроїв, включаючи комп'ютерні програми, створені або адаптовані, в першу чергу, з метою вчинення будь-якого зі злочинів, перерахованих у ст.ст.2–5 Конвенції (незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему), та комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі зазначених злочинів. Відповідно до ч.3 ст.6 Конвенції сторони можуть залишити за собою право не застосовувати п.1 ст.6, за умови, що таке застереження не стосується продажу, розповсюдження або надання для використання іншим чином комп'ютерних паролів, кодів

ISSN 1995-6134

доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи [3]. Цією можливістю і скористалася Україна, обмеживши свої зобов'язання встановленням відповідальності лише за продаж, розповсюдження або надання для використання іншим чином зазначених предметів.

Аналізуючи відповідність і повноту реалізації Україною своїх міжнародних зобов'язань стосовно встановлення кримінальної відповідальності за незаконне використання комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин, а саме за їх продаж, розповсюдження або надання для використання іншим чином, приходимо до висновку, що фахівці по-різному оцінюють реалізацію вимог Конвенції у цій частині. У висновку на законопроект «Про ратифікацію Конвенції про кіберзлочинність» М.І. Хавронюк і Ю.М. Матєров пропонували утриматися від зробленого Україною застереження щодо встановлення кримінальної відповідальності за зловживання пристроями, оскільки, на їх думку, вимоги Конвенції у цій частині вже частково реалізовані через встановлення кримінальної відповідальності в ст.361-1, ст.200 і ч.3 ст.190 КК України [4]. Ю.Ю. Орлов вважає, що у кримінальному законодавстві України враховано всі вимоги Конвенції. Аналізуючи відповідність окремих положень Конвенції нормам КК України, він зазначає, що протизаконному використанню пристроїв і комп'ютерних програм, передбаченому ст.6 Конвенції, відповідають ст.ст.361-1, 362, 363 КК України [5, с.6]. М.В. Карчевський більш докладно окреслює вказану проблему, зазначаючи, що національне кримінальне законодавство прямо не передбачає відповідальність за навмисний продаж, розповсюдження або надання для використання іншим чином вказаних предметів, і визнає необхідність проведення подальших досліджень у вказаному питанні. Утім дослідник зауважує, що, на його думку, наявних у чинному кримінальному законодавстві засобів кримінально-правової охорони від посягань, що вчиняються у співучасті, а також засобів протидії попередній злочинній діяльності, цілком достатньо для виконання вимог Конвенції. Так, зазначає М.В. Карчевський, враховуючи, що конститутивною ознакою навмисного продажу, розповсюдження або надання для використання іншим чином комп'ютерних паролів, кодів доступу або подібних даних є мета подальшого вчинення злочинів, зазначені діяння слід визнати пособництвом у вчиненні відповідних злочинів [6, с.72–73]. Таким чином, у наукових дослідженнях відсутня консолідована позиція з аналізованого питання. Експертні висновки часто носять занадто загальний характер, без надання цьому питанню глибинного аналізу, чітких та зрозумілих практичних рекомендацій щодо притягнення до відповідальності за незаконне використання комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин.

Проведення власного аналізу відповідності закріплення положень Конвенції щодо встановлення у чинному КК України відповідальності за продаж, розповсюдження або надання для використання іншим чином комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин, враховуючи наукові доробки інших дослідників та законотворчу практику, дозволяє сформулювати наступні висновки. У цілому, погоджуючись з М.В. Карчевським, слід визнати, що чинний КК України безпосередньо не передбачає відповідальність за незаконне використання комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин. Дійсно, теоретично можна притягнути особу до відповідальності за розповсюдження коду доступу до комп'ютерної системи, враховуючи чинні положення про пособництво, передбачені ч.5 ст.27 КК України, однак, вбачається, що таке сприяння має бути здійснено у відношенні конкретної

ISSN 1995-6134

особи щодо конкретного злочину. Відповідно до загальних положень теорії кримінально-правової кваліфікації співучасть завжди має бути конкретною, стосуватися злочину, який повинен бути виконаний у той чи інший час, в тому чи іншому місці, полягати у вчиненні обумовлених співучасниками діянь тощо [7, с.215]. Крім того, має бути доведено усвідомлення особи хоча б у загальних рисах, що розповсюдження або продаж комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин, є частиною конкретного комп'ютерного злочину та сприяє його вчиненню. Враховуючи вищевикладене, вбачається, що незаконне, без права на це розповсюдження конфіденційної інформації як-от комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин, є самостійною, ізольованою діяльністю особи, яка зазвичай спрямована на невизначене та не персоніфіковане коло осіб. Умисел особи зазвичай обмежуються збутом (розповсюдженням) зазначених предметів з отримання матеріальної винагороди або без такої, тому подібну діяльність вбачається недоцільним розглядати як співучасть у вчиненні інших комп'ютерних злочинів.

Окремо слід розглянути випадки, коли особа будь-яким чином без право на це умисно отримує комп'ютерний пароль, код доступу або подібні дані, які надають доступ до комп'ютерної системи або її частини, для подальшого незаконного їх використання самостійно, без залучення інших осіб. Так, наприклад, розповсюдженими є схеми отримання логінів або паролів користувачів за допомогою фішингу (англ. phishing, походить від fishing – риболовля, виманювання), виду комп'ютерного шахрайства, метою якого є отримання доступу до конфіденційної інформації користувачів (логінів і паролів для виводу грошей на рахунок, для доступу до електронної скриньки або акаунту у соціальних мережах тощо). Найбільш розповсюдженими видами фішингу можна визнати: 1) масову розсилку від імені якогось банку або сервісу з проханням надіслати у відповідь особисті данні, тому це необхідно для перевірки безпеки або чогось ще; 2) підробку сайту-оригінала – зазвичай фішинг-шахраї підробляють лише одну сторінку – сторінку логіну та паролю. Для заманювання жертв на вказані сайти також використовується масова розсилка електронних повідомлень з проханням перейти на сайт [8, с.229–230]. За способом вчинення також виокремюють голосовий фішинг – вішинг і фішинг за допомогою SMS-повідомлень – смішінг. Кількісні показники фішингових атак вражають: у 2016 р. їх загальна кількість склала 1220523, що на 65 % більше, ніж аналогічний показник за 2015 р. [9, с.5]. Вбачається, що незаконне отримання комп'ютерних паролів, кодів доступу або подібних даних, за наявності необхідних підстав можна кваліфікувати як готування до вчинення комп'ютерного злочину. Проте, у деяких випадках притягнення до кримінальної відповідальності стає неможливим, наприклад, за готування до злочину, передбаченого ст.163 КК України, оскільки останній є злочином невеликої тяжкості, готування до яких не тягне за собою кримінальної відповідальності. Крім того, умисел на вчинення подальших комп'ютерних злочинів не завжди можливо довести. Утім, слід зазначити, що фішинг-шахраї часто збирають та накопичують конфіденційну інформацію з метою передачі (збуту) іншим особам, що знову повертає нас до вже аналізованих проблем співучасті у вчиненні побідних злочинних діянь. Вищевикладене дозволяє зробити висновок, що КК України на теперішній час не передбачає ефективних можливостей притягнення до кримінальної відповідальності за дії, пов'язані з незаконним використання комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин. Враховуючи негативну динаміку розповсюдження суспільно небезпечних діянь, пов'язаних з протиправними

ISSN 1995-6134

діями з комп'ютерними паролями, кодами доступу або подібними даними, вбачається цілком доречним та своєчасним передбачення кримінальної відповідальності за вказані незаконні діяння.

Спроби внести відповідні зміни до КК України декілька разів мали місце у вітчизняній законотворчості. У першу чергу слід відмітити законопроект «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України щодо відповідальності за злочини у сфері комп'ютерної інформації» № 3039-1 від 12.03.2004 р., в якому пропонувалося доповнити Розділ XVI Особливої частини КК України ст.363-4 «Незаконне розповсюдження даних, які призначені для отримання незаконного доступу до комп'ютерної системи чи телекомунікаційної мережі» [10]. Зазначимо, що цей законопроект був зареєстрований ще до ратифікації Україною Конвенції про кіберзлочинність 2001 р. У 2014 р. був зареєстрований законопроект № 1272, спрямований на посилення відповідальності за незаконні дії з платіжними інструментами, яким було запропоновано доповнити КК України ст.200-2 «Фішинг» [11]. Частково підтримуємо критику вказаного законопроекту щодо недоречності введення у кримінальне законодавство таких неправових понять, як скіммінг, скіммінгові пристрої, фішинг, однак категорично не погоджуємося з тим, що фішинг (у тому числі у формулюванні, наданому в законопроекті) вже охоплюється ст.ст.361 і 361-1 КК України [12], адже вчинення подібних дій часто відбувається без втручання у роботу електронно-обчислювальний машин і комп'ютерних мереж. У той же час вбачається більш правильним передбачення загальної норми щодо незаконного використання комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин, а не тільки у банківській сфері.

Аналіз іноземного досвіду засвідчує тенденцію на користь встановлення кримінальної відповідальності за діяння пов'язані з незаконним заволодінням та використанням комп'ютерних паролів, кодів доступу та подібних даних, які надають доступ до комп'ютерних систем або їх частин. Наприклад, у Директиві Європейського Союзу щодо атак проти інформаційних систем від 12.08.2013 р. зазначено, що члени Європейського Союзу мають передбачити кримінальну відповідальність за умисне виготовлення, продаж, придбання для використання, розповсюдження або надання для використання іншим чином комп'ютерних паролів, кодів доступу та подібних даних, які надають доступ до комп'ютерної системи або її частини, хоча б у випадках, коли ці діяння не є малозначними [13]. У різних формах з певними термінологічними та змістовими особливостями відповідальність за вказані діяння передбачені в ст.285 КК Грузії [14], ст.216 КК Естонської Республіки [15], ст.260-4 КК Республіки Молдови [16], ст. 46 Антикорупційного закону Румунії [17], § 1028A(6) Титулу 18 США [18]. В іноземній правовій літературі подібні діяння також часто розглядаються як частину більш широкого новітнього виду злочинності – крадіжки особистості, або приватності (identity theft) [19].

Дослідження міжнародно-правових зобов'язань України щодо протидії кіберзлочинності, світового досвіду криміналізації подібних питань, їх суспільної небезпечності та поширеності, призводить до висновку про необхідності передбачення кримінальної відповідальності за незаконне заволодіння та використанням комп'ютерних паролів, кодів доступу та подібних даних, які надають доступ до комп'ютерних систем або їх частин. На нашу думку, зазначена норма повинна мати загальний характер щодо кіберзлочинів, передбачених у різних розділах КК України, та має бути поміщена до Розділ XVI Особливої частини КК України. Внесення зазначених змін до законодавства України про кримінальну відповідальність відкриє нові перспективи протидії злочинам в інформаційній сфері та значно знизить можливості порушників

ISSN 1995-6134

уникнути кримінальної відповідальності, скориставшись недосконалістю вітчизняного правових норм. Подальшого дослідження потребують питання, пов'язані з кримінально-правовою протидією незаконному використання конфіденційних даних та втручанню у приватність, вчинених з використанням комп'ютерних технологій.

ЛІТЕРАТУРА

1. Jaishankar K., Ph.D. Indian Criminologist with an International Outlook. URL: http://www.jaishankar.org/ (дата звернення: 01.06.2017).
2. Про ратифікацію Конвенції про кіберзлочинність : Закон України № 2824-IV від 07.09.2005. URL: http://zakon3.rada.gov.ua/laws/show/2824-15 (дата звернення: 01.06.2017).
3. Конвенція про кіберзлочинність 2001 р. URL: http://zakon3.rada.gov.ua/laws/show/994_575 (дата звернення: 01.06.2017).
4. Висновок на проект Закону України «Про ратифікацію Конвенції про кіберзлочинність» № 0261 від 30.05.2005. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=24623 (дата звернення: 01.06.2017).
5. Орлов Ю. Ю. Реалізація вимог міжнародної Конвенції про кіберзлочинність у законодавстві України // Науковий вісник Нац. акад. внутр. справ. 2011. № 6. С. 3–9.
6. Карчевський М. В. Питання оптимізації зобов'язань, зумовлених ратифікацією Конвенції про кіберзлочинність // Бюлетень Міністерства юстиції України. 2012. № 3. С. 70–80.
7. Навроцький В. О. Основи кримінально-правової кваліфікації : навч. посібник. К., 2006. 704 с.
8. Сабадаш В. П. Фішинг як найбільш розповсюджений вид шахрайства в Інтернеті // Університетські наукові записки. 2006. № 1 (17). С. 228–233.
9. Phishing Attack Trends Report - 4Q 2016. Released Feb 23, 2017. URL: http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf (дата звернення: 01.06.2017).
10. Проект Закону України «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України щодо відповідальності за злочини у сфері комп'ютерної інформації» № 3039-1 від 12.03.2004. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=14303 (дата звернення: 01.06.2017).
11. Проект Закону України «Про внесення змін до Кримінального кодексу України (щодо посилення відповідальності за незаконні дії з платіжними інструментами, обладнанням для їх підробки, системами дистанційного обслуговування та іншими засобами доступу до банківських рахунків)» від 05.12.2014 № 1272. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=52730 (дата звернення: 01.06.2017).
12. Висновок на проект Закону України «Про внесення змін до Кримінального кодексу України (щодо посилення відповідальності за незаконні дії з платіжними інструментами та іншими засобами доступу до банківських рахунків)» від 05.12.2014 № 1272. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=52730 (дата звернення: 01.06.2017).
13. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32013L0040&from=EN (дата звернення: 01.06.2017).
14. Уголовный кодекс Грузии от 22.07.1999 г. URL: https://matsne.gov.ge/ka/document/download/16426/143/ru/pdf (дата звернення: 01.06.2017).
15. Penal Code of the Republic of Estonia. URL: https://www.unodc.org/res/cld/document/estonia-criminal-code-as-amended-2013_html/Estonia_Criminal_Code_as_amended_2013.pdf (дата звернення: 01.06.2017).
16. Уголовный кодекс Республики Молдова от 18.04.2002 г. URL: http://lex.justice.md/ru/331268/ (дата звернення: 01.06.2017).

ISSN 1995-6134

17. Anti-corruption law 161/2003 of Romania. URL: http://www.legi-internet.ro/en/romanian-itc-legislation-and-articles/criminalitate-informatica/romanian-cybercrime-law.html (дата звернення: 01.06.2017).

18. Title 18 USC. Crimes and Criminal Procedure. URL: http://uscode.house.gov/view.xhtml;jsessionid=4BC8860933A1E8ABD588A9CE013988B7?req=granuleid%3AUSC-prelim-title18&saved=%7CKHRpdGxlOjE4IHNlY3Rpb246MTAzMCBlZGl0aW9uOnByZWxpbSk%3D%7C%7C%7C0%7Cfalse%7Cprelim&edition=prelim (дата звернення: 01.06.2017).

19. Identity Theft and Related Crimes. An Overview of Minnesota Criminal Law. URL: http://www.house.leg.state.mn.us/hrd/pubs/idtheft.pdf (дата звернення: 01.06.2017).

Юртаєва К. В. Проблеми криміналізації незаконного використання комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин // Форум права: електрон. наук. фахове вид. 2017. № 3. С. 221–227. URL: http://nbuv.gov.ua/j-pdf/FP_index.htm_2017_3_39.pdf

Розглянуто питання закріплення кримінальної відповідальності за незаконне використання комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних системи або їх частини, в КК України. Визначено недоліки норм щодо кримінальної відповідальності за кіберзлочини. Запропоновано внесення змін до законодавства України про кримінальну відповідальність з метою вдосконалення кримінально-правової протидії кіберзлочинності.

***

Юртаева К.В. Проблемы криминализации незаконного использования компьютерных паролей, кодов доступа или подобных данных, которые предоставляют доступ к компьютерным системам или их частям

Рассмотрены вопросы закрепления уголовной ответственности за незаконное использование компьютерных паролей, кодов доступа или подобных данных, которые предоставляют доступ к компьютерным системам или их частям, в УК Украины. Определены недостатки норм об уголовной ответственности за киберпреступления. Предложено внесение изменений в законодательство Украины об уголовной ответственности с целью совершенствования уголовно-правового противодействия киберпреступности.

***

Yurtayeva K.V. Problems of Establishing Criminal Liability for Illegal Use of Computer Passwords, Access Codes, or Similar Data by Which the Whole Or Any Part of a Computer System is Capable of Being Accessed

The article is devoted to an issue of establishing criminal liability for illegal use of computer passwords, access codes, or similar data by which the whole or any part of a computer system is capable of being accessed in the Criminal Code of Ukraine. It defines drawbacks of the norms on criminal liability for cybercrime. It proposes amendments to Ukrainian criminal legislature for enhancing counteraction measures for cybercrime.