УДК 343.9.01
DOI 10.33244/2617-4154.1(5).2021.184-191

А. Р. Єдгаров,
Університет ДФС України
e-mail: galynadid@gmail.com
ORCID ID 0000-0003-2076-1651

ОКРЕМІ КРИМІНОЛОГІЧНІ АСПЕКТИ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ

У статті зазначається, що проблеми запобігання кіберзлочинності значною мірою дещо складно виявити через глобальний масштаб інформаційних мереж. Вказується, що у випадку ефективності вжитих зусиль заважають ті самі проблеми, які притаманні будь-якому комерційному проєкту міжнародного рівня. Зазначено, що виникають і додаткові складнощі, пов'язані за участю структур приватного сектору, в багатьох країнах законодавство з цього питання або зовсім відсутнє, або має обмежений характер. У багатьох випадках, навіть якщо керівництво країни рішуче налаштовано на боротьбу з кіберзлочинністю, у держави немає необхідних технічних можливостей для розробки потрібного законодавства або механізмів його реалізації у разі, якщо таке законодавство вже існує. Вказується, що в умовах відсутності необхідної нормативно-правової бази та технічних можливостей для її реалізації злочинці можуть увійти в Інтернет анонімно, користуючись мережею на території слаборозвиненої держави, і безкарно здійснювати кримінальні правопорушення із-за кордону, тож кіберзлочинність є розповсюдженим явищем, і відчувати себе захищеним від таких кримінальних правопорушень практично неможливо. Межі кіберпростору є безмежними, хакери мають досить розвинені навички, щоб залишитися в ньому інкогніто, і тому це створює проблеми під час розслідування таких кримінальних правопорушень.

Підсумовується, що правове регулювання діяльності в українському сегменті глобальної інформаційно-телекомунікаційної мережі «Інтернет», характеризується низькою правовою культурою і багатьма проявами режиму безвідповідальності.

Ключові слова: *кіберзлочинність, кримінальне правопорушення, запобігання, кримінальна відповідальність, інтернет-мережа.*

А. Р. Едгаров. Отдельные криминологические аспекты предупреждения киберпреступности

В данной статье отмечается, что проблемы предупреждения киберпреступности в значительной степени несколько сложно из-за глобального масштаб информационных сетей. Указывается, что в случае эффективности принятых усилий мешают те же проблемы, которые присущи любому коммерческому проекту международного уровня. Отмечено, что возникают и дополнительные сложности, связанные с участием структур частного сектора, во многих странах законодательство по этому вопросу или совсем отсутствует, либо имеет очень ограниченный характер. Во многих случаях, даже если руководство страны решительно настроено на борьбу с

киберпреступностью, у государства нет необходимых технических возможностей для разработки нужного законодательства или механизмов его реализации в случае, если такое законодательство уже существует. Суммируется, что правовое регулирование деятельности в украинском сегменте глобальной информационно-телекоммуникационной сети «Интернет», характеризуется низкой правовой культурой и многими проявлениями безответственности.

Ключевые слова: *киберпреступность, уголовное преступление, предепреждение, уголовная ответственность, интернет сеть.*

На сьогодні у сучасному правовому полі такі терміни, як «кіберзлочинність», «хакери», «комп'ютерний злом», «крадіжка машинного часу» перестали бути екзотичними для юристів. Проблеми запобігання кримінальним правопорушенням у сфері використання комп'ютерних технологій активно обговорюються науковцями, досить швидко розвивається практика застосування відповідних норм законодавства про кримінальну відповідальність.

Нині комп'ютерні кримінальні правопорушення є однією з активних груп суспільно небезпечних посягань. Достатньо швидко зростають показники поширення цих кримінальних правопорушень, а також постійно зростає їх суспільна небезпечність. Така ситуація зумовлюється прискореним розвитком сучасних технологій в ІТ-сфері, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки. Варто зауважити, що українське законодавство приділяє значну увагу цим питанням. Так, Кримінальний кодекс України передбачає самостійний розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж»; двічі положення цього розділу змінювалися і доповнювалися, що свідчить про актуальність використання сучасних технологій у суспільстві.

Історією неодноразово повчались, що розвиток і прогрес, які приносять людям нові блага та можливості, на жаль, завжди супроводжуються негативними явищами. Індустріалізація дала нам масове виробництво товарів, але вона ж поклала початок варварському винищенню природи і класовій нерівності. Боротьба за національні та соціальні права зробила аксіомою принципи рівності і справедливості, але часто призводить до кровопролиття і негативних проявів патерналізму [1].

Історія кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку має давні корені. Про кримінальні правопорушення цієї категорії згадувалося ще 5680 року до нашої ери у літописах єгипетських мудреців про так званих «Чорних отруйників», які згодовували своїм жертвам розтерті в порошок рахункові палички, щось на зразок прообразу сучасного персонального комп'ютера. В історичному ракурсі вони зародились в Америці 1945 року, коли була створена перша ЕОМ (комп'ютер), яка використовувалась для розшифровування німецьких військових кодів, а згодом і для іншої діяльності. Термін «кіберзлочинність» з'явився в американській доктрині на початку 60-х рр. минулого століття, коли були виявлені перші випадки кримінальних правопорушень, здійснених із використанням комп'ютерів. Саме тоді з'явилися перші «хакери», ними були студенти Масачусетського технологічного інституту, які маніпулювали з програмами нового університетського комп'ютера [2, с. 294].

Електронно-обчислювальні машини (далі – ЕОМ) набули широкого застосування як серед працівників правоохоронних органів, так і серед учених, хоча спочатку для цього не було ні кримінологічних, ні правових підстав [3, с. 17]. Після цього 1966 р. зафіксовано перший випадок використання ЕОМ як інструмента під час пограбування банку в Міннесоті. Першою ж людиною, що застосувала ЕОМ для вчинення податкового кримінального правопорушення на суму 620 тис. доларів і постала за це перед американським судом 1969 р., був Альфонсо Конфессоре. Подальша історія «комп'ютерних» кримінальних правопорушень відмічена такими найбільш «яскравими» подіями: кінець 70-х – пограбування «Секьюріті пасифік банк» (10,2 млн доларів); 1979 р. – комп'ютерне розкрадання у Вільнюсі (78 584 крб); 1984 р. – повідомлення про перший у світі «комп'ютерний вірус»; 1985 р. – виведення з ладу за допомогою «вірусу» електронної системи голосування в конгресі США; 1986–1988 рр. – поява першого «комп'ютерного вірусу» в СРСР; 1989 р. – блокування американським студентом 6000 ЕОМ Пентагону; 1990 р. – міжнародний з'їзд комп'ютерних «піратів» у Голландії з демонстрацією можливості необмеженого втручання в системи ЕОМ; 1991 р. – розкрадання коштів Зовнішекономбанку на суму в 125,5 тис. доларів; 1992 р. – умисне порушення роботи АСОВІ реакторів Ігналінської АЕС; 1993 р. – електронне шахрайство в Центробанку Росії (68 млрд крб); 1995 р. – спроба російського громадянина пограбувати Сіті-банк на суму 2,8 млн доларів [4, с. 133].

Враховуючи технічну незахищеність нашої держави, забезпечення інформаційної безпеки в Україні є однією з найважливіших функцій держави, адже добробут нації залежить від інформаційної складової. На сьогодні стан криміногенної ситуації вимагає розробки та впровадження заходів для протидії кримінальним правопорушенням щодо посягання на об'єкти у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку. Внаслідок соціально-економічних проблем Україна суттєво відстає у розвитку від країн-учасниць Конвенції про кіберзлочинність. Кібервійни, кібертероризм, кібершпигунство стали звичними, тому злочинність в інформаційній сфері є суттєвою загрозою національній безпеці у сфері економіки. Зареєстрований масив злочинних посягань в аналізованій сфері свідчить про суттєве зростання рівня цих злочинів за останні роки і має такі показники: 2013 року було обліковано 595 злочинів, 2014 року – 443, 2015 року – 598, 2016 року – 865, 2017 року – 2 573, 2018 року – 2 301 злочин [5].

До питання кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку зверталося чимало провідних вітчизняних і зарубіжних учених. Серед них, зокрема: Д. С. Азаров, Ю. М. Батурин, П. Д. Біленчук, А. С. Білоусов, В. М. Бутузов, А. Г. Волевоз, О. В. Демешко, І. В. Європіна, М. В. Карчевський, С. А. Кузьміна, О. В. Мазоліна, К. В. Манжула, В. М. Машкова, С. С. Мірошниченко, А. А. Музика, М. В. Рудика, В. П. Шеломенцева, М. П. Бікмурзіна, Т. В. Корнякова, В. В. Кузнецова, Є. В. Лащук, Є. І. Литвинов, Ю. М. Онищенко, П. І. Орлова, С. О. Орлов, О. Е. Радутний, Н. А. Розенфельд, В. С. Романюк, О. В. Смаглюк, Л. В. Сорока, В. С. Цимбалюк, С. В. Шапочка, Н. С. Юзікова, І. О. Юрченко, К. В. Юртаєва та інші [6]. Проте залишається чимало організаційно-правових питань, які потребують наукового дослідження та обґрунтування.

Так, відповідно до Стратегії кібербезпеки України, затвердженої Указом Президента України від 5 березня 2016 року № 96/2016, передбачається створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Однак цей документ хоча і називається стратегією, проте визначені в ньому основні засади кібербезпеки у світовій практиці не зовсім вважаються стратегічними. Варто додати, що основним атрибутом у закордонних стратегіях передбачається перелік конкретних проєктів забезпечення кібербезпеки з кінцевим терміном їх реалізації, виділеним фінансуванням і, що найголовніше, конкретними відповідальними. У нас це нагадує здебільшого концепцію – напрями, куди треба рухатися зі своїми тактиками дій, власним, а не державним фінансуванням і без будь-якої відповідальності [7].

Аналізуючи статистичні дані щодо кіберзлочинності, варто виділити попередні висновки: кількісні показники не є значними для постановки нагальної потреби в з'ясуванні, але, аналізуючи різні наукові дослідження, потрібно зазначити, що рівень латентності кіберзлочинності сягає близько 95 %, що дозволяє віднести їх до категорії високолатентних. Серед факторів їх латентності виділено три основні групи: 1) фактори, що обумовлюють природну латентність, внаслідок яких про вчинений кіберзлочин відомо лише самому винному; 2) фактори, пов'язані з негативною поведінкою жертви (очевидців) злочину та їх незверненням до правоохоронних органів, неповідомленням про факт вчинення злочину; 3) фактори, пов'язані з недоліками роботи правоохоронних органів у частині реагування на звернення та повідомлення про кримінальні правопорушення у сфері використання комп'ютерних технологій [8].

Також можна погодитися з думкою окремих науковців, що найбільш вагомою проблемою сучасного світу, яка виникає разом із стрімким розвитком інформаційних технологій та глобальної мережі Інтернет, є поява нових видів кримінальних правопорушень, зокрема кібертероризм. Кібертероризм на сьогодні розуміють як суспільно небезпечну діяльність, що свідомо здійснюється в кіберпросторі або з використанням його технічних можливостей, окремими особами чи організованими групами з терористичною метою та реалізується ними через заздалегідь сплановані й політично вмотивовані кібератаки з використанням сучасних технологій [9, с. 57].

Окремі аспекти явища кібертероризму неодноразово були предметом дослідження у роботах таких зарубіжних та вітчизняних учених, як М. Делягіна, А. Фороса, Д. Деннінга, В. Ліпкана, І. Міхеєва, К. Герасименка та інших. Саме їх внески мають вагоме значення в подальшому висвітленні проблеми. Основною відмінною рисою кібертероризму від інших видів віртуальних злочинів є безпосередній вплив на суспільство з метою його залякування, паралізації волі членів соціуму, поширенню панічних настроїв, почуття незахищеності. Це досягається шляхом тиражування інформації про загрози насильства, підтримці стану постійного страху з метою досягнення певних політичних чи інших цілей, примусу до певних дій, а також привернення уваги до самої терористичної організації. Кінцевою метою кібернетичної атаки терориста є не тільки демонстрація своїх технічних можливостей, але і спроба за допомогою їх впливати на політичну владу в країні. Зростання інформаційних технологій дає терористам можливість отримати істотний прибуток за відносно низьким ризиком. Вони можуть фінансувати свою діяльність без використання силових нападів або грабежів банків, які збільшили б ризик виявлення. Для кібертероризму характерно і те, що всі відомі сьогодні хакерські групи й окремі особи не прагнуть афішувати свої дані та виступають виключно під псевдонімом. При цьому

потрібно відрізняти хакера-терориста від простого хакера, комп'ютерного хулігана або комп'ютерного злодія, який діє в корисливих або хуліганських цілях. Найефективнішою зброєю у боротьбі з цим злочином залишається законодавство, яке потребує постійного вдосконалення. Якщо свідчити про міжнародні правові акти в цій сфері, то першим і основним документом, в якому йдеться про боротьбу з кіберзлочинністю, є Європейська конвенція 2001 року. У Конвенції Ради Європи згадується чотири типи комп'ютерних злочинів, а саме: незаконний доступ; незаконний перехват; втручання в дані; втручання в систему. Згідно з цим документом засобами кібертероризму є: комп'ютерна система, комп'ютерні дані, послуги ІКТ та дані трафіку [10, с. 146]. Кібертероризм як основна складова кіберзлочинності посідає не останнє місце й серед ряду загроз національній безпеці та інтересам України. За даними соціологічних опитувань, на його поширення нині активно впливають: високий потенціал і професійний рівень українських програмістів, послугами яких охоче користуються навіть такі флагмани програмної індустрії, як «Майкрософт»; здатність молоді швидко опановувати технічні новинки, про які ще вчора вони не мали жодного уявлення. При цьому до основних чинників, що формують джерела таких загроз, вітчизняні експерти відносять: недостатню увагу з боку державних органів до проблем інформатизації; відсутність належної державної фінансової підтримки фундаментальних і прикладних вітчизняних досліджень у сфері запобігання та боротьби з кіберзлочинністю відставання вітчизняного законодавства в інформаційній галузі від розвинених країн світу в умовах спільного існування у єдиному інформаційному просторі; відсутність ефективної політики безпеки комп'ютерних мереж і необхідних програмно технічних засобів для обмеження доступу до конфіденційної інформації в базах даних; розширення можливостей для негативного інформаційного впливу на людину, суспільство та державу за допомогою нових комп'ютерно-телекомунікаційних засобів і технологій, що постійно розвиваються; перехоплення електронної пошти, паролів і файлів за допомогою легкодоступних для зацікавлених користувачів програмно-технічних засобів [9, с. 60–61].

Загроза, яка виходить від кібертероризму, досить велика, а в деяких випадках вона може мати незворотній характер. Сучасному суспільству ще тільки належить виробити ефективну систему протидії і боротьби з цим сучасним інформаційним злом. Отже, упродовж тривалого періоду часу благоустрій суспільства й економічна стабільність ґрунтувались на надійній роботі мереж передачі інформації та обчислювальних сервісів. Проте з появою кібертероризму цей процес значно ускладнився внаслідок постійних кібератак на комп'ютерні системи. В Україні на сьогодні не розроблено конкретного нормативно-правового акта, що регулює такий вид злочинності, як кібертероризм, тому виникає потреба у вдосконаленні та доповненні вже існуючого законодавства шляхом переймання досвіду інших країн, а також розробки законів, що відповідають міжнародним стандартам, встановлених у відповідних конвенціях та договорах. Також дієвим напрямом у вирішенні проблеми протидії кіберзлочинності нині є міжнародне співробітництво правоохоронних органів у сфері інформаційної безпеки на основі узгодження національного та міжнародного законодавства, основні засади щодо кібертероризму та його протидії [11].

Якщо свідчити про правове регулювання діяльності в українському сегменті глобальної інформаційно-телекомунікаційної мережі «Інтернет», то за багато років слабкого правового режиму виникла середа з досить низькою правовою культурою і багатьма проявами режиму безвідповідальності. З розвитком інформаційних технологій стали

розроблятися інструменти для шпигунства з використанням як спеціалізованих пристроїв, так і програмного забезпечення. На відміну від класичних методів розвідки і шпигунства, нові технології внесли в них суттєві коригування. Сьогодні іноді неможливо встановити, хто саме розробив певне програмне забезпечення для проведення розвідувальних дій у сфері високих технологій. Розробниками подібного спеціалізованого програмного забезпечення можуть бути як приватні особи, так і підприємства різної форми власності, з різними джерелами фінансування. Нерідко особи, які розробили програмне забезпечення, не є тими особами, які його використовують для здійснення кібершпіонажу. Це ускладнює, а іноді унеможливлює ідентифікацію осіб, які здійснюють кібершпіонаж, і як результат – їх залучення до встановленої форми відповідальності. Подібна практика призводить до того, що зацікавлені особи найчастіше самостійно вишукують методи протидії проявам кібершпіонажу в кожному конкретному випадку. Останні включають у себе класичні методи підвищення інформаційної захищеності об'єктів, а також спеціальні методи розвідки для забезпечення ефективної протидії кіберзлочинності [12, с. 88].

Це унеможливлює якісно використовувати навіть ті механізми запобігання кіберпосяганням які існують у державі та розробляти і проваджувати нові.

Висновки. Враховуючи вищезазначене, варто погодитись, що на сьогодні складно, а іноді і неможливо, визначити ту особу, яка здійснює кіберпосягання та можливості притягнути таку особу до кримінальної відповідальності. Такий стан речей призводить до того, що особи які зазнали кіберпосягань досить часто самостійно намагаються запобігти будь яким проявам кібератак. Це можуть бути як класичні методи підвищення інформаційної захищеності об'єктів посягання, а можуть використовуватися і спеціальні методи збирання інформації для ефективного запобігання кіберзлочинності. Але, нажаль, такий самозахист також не врегульовано законодавством та потребує наукового дослідження і обгрунтування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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

2. Ричка Д. О. Історичні аспекти кіберзлочинності. *Сучасний стан і перспективи розвитку держави і права:* матеріали VII Міжнародної наукової конференції студентів, аспірантів та молодих вчених. Дніпропетровськ, 2015. С. 293–295.

3. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. Москва: ООО Издательство «Юрлитинформ», 2002. 496 с.

4. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій. *Вісник Академії адвокатури України*. 2010. № 3. С. 129–136.

5. Єдиний звіт про кримінальні правопорушення по державі / Офіційний сайт Генеральної прокуратури України. URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=104402 (дата звернення 04.12.2019).

6. Ричка Д. О. Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: дис. … канд. юрид. наук: 12.00.03. К., 2019. 220 с. URL: http://www.nusta.edu.ua/wp-content/uploads/2016/11/Dis-% D0%B0.pdf

7. Стратегія кібербезпеки України, затверджена Указом Президента України від 5 березня 2016 року № 96. URL: http://zakon2.rada.gov.ua/laws/show/96/2016

8. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ. *Науковий Вісник Харківського Національного університету внутрішніх справ.* 2016. 36.

9. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с.

10. Лисиченко Г. В., Забулонов Ю. Л., Хміль Г. А. Природний, техногенний та екологічний ризики: аналіз, оцінка, управління. *Наукова думка*, 2008.

11. Кібербезпека в Україні: правові та організаційні питання: матеріали Міжн. наук. практ. конф., м. Одеса, 22 листопада 2019 р. Одеса: ОДУВС, 2019. 108 с. URL: http://eportfolio.kubg.edu.ua/data/conference/5087/document.pdf

12. Галушкин А. А. Кибершпионаж – угроза современному обществу. *Вестник МГОУ. Серия: Юриспруденция.* 2015. № 2. С. 87–91.

REFERENCES

1. Mykyta Dovbysh. Kiberzlochynnist v Ukraini. URL : https://www.science-community.org/uk/node/16132.

2. Rychka D. O. Istorychni aspekty kiberzlochynnosti. Materialy VII Mizhnarodnoi naukovoi konferentsii studentiv, aspirantiv ta molodykh vchenykh «Suchasnyi stan i perspektyvy rozvytku derzhavy i prava». Dnipropetrovsk, 2015. S. 293–295.

3. Volevodz A. H. Protyvodeistvye kompiuternым prestuplenyiam: pravovыe osnovы mezhdunarodnoho sotrudnychestva Moskva: OOO Yzdatelstvo «Iurlytynform», 2002. 496 s.

4. Yevropina I. V. Vydy protypravnykh diian u sferi novitnikh informatsiinykh tekhnolohii. *Visnyk Akademii advokatury Ukrainy*. 2010. Chyslo 3. S. 129–136.

5. Iedynyi zvit pro kryminalni pravoporushennia po derzhavi : ofitsiinyi sait Heneralnoi prokuratury Ukrainy. URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=104402 (data zvernennia 04.12.2019).

6. Rychka D. O. Osoblyvosti kryminalno-pravovoi kvalifikatsii zlochyniv u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh i merezh elektrozviazku dys. … kand. yuryd. nauk: 12.00.03 / Rychka Denys Olehovych. K., 2019. 220 s. URL: http://www.nusta.edu.ua/wp-content/uploads/2016/11/Dis-% D0%B0.pdf

7. Stratehiia kiberbezpeky Ukrainy zatverdzhena Ukazom Prezydenta Ukrainy vid 5 bereznia 2016 roku № 96. URL: http://zakon2.rada.gov.ua/laws/show/96/2016.

8. Kravtsova, M. O. (2016). Kiberzlochynnist: kryminolohichna kharakterystyka ta zapobihannia orhanamy vnutrishnikh sprav. *Naukovyi Visnyk Kharkivskoho Natsionalnoho universytetu vnutrishnikh sprav* (1), 36.

9. Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt: pidruchnyk / [V. L. Buriachok, V. B. Tolubko, V. O. Khoroshko, S. V. Toliupa]; za zah. red. d-ra tekhn. nauk, profesora V. B. Tolubka. K.: DUT, 2015. 288 s.

10. H.V. Lysychenko, Yu. L. Zabulonov, H. A. Khmil Pryrodnyi, tekhnohennyi ta ekolohichnyi ryzyky: analiz, otsinka, upravlinnia. *Naukova dumka*, 2008.

11. Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia: materialy mizhn. nauk. prakt. konf., m. Odesa, 22 lystopada 2019 r. Odesa : ODUVS, 2019. 108 s. URL: http://eportfolio.kubg.edu.ua/data/conference/5087/document.pdf

12. Halushkyn A. A. Kybershpyonazh – uhroza sovremennomu obshchestvu. *Vestnyk MHOU*. Seryia: Yurysprudentsyia. 2015. № 2. S. 87–91.

A. R. Yedharov. Some criminological aspects of cybercrime prevention

In this article marked, that problems of prevention of cybercrime largely some difficult from the global scale of informative networks. Specified, that the same problems mix in case of efficiency of the used efforts, what inherent to any commercial project of international level. It is marked that the additional complications related to participation of structures of private sector are, in many countries legislation through this question or it is quite absent, or has a very limit character. In many cases, even if guidance of country is resolutely adjusted on a fight against a cybercrime, the state does not have necessary economic feasibilities for development of necessary legislation or mechanisms of his realization in case if such legislation exists already.

Specified, that in the conditions of absence of necessary normatively-legal base and economic feasibilities for her realization, criminals can enter the Internet anonymously, using a network on territory of the poorly developed state and with impunity to carry out criminal offences from abroad, therefore a cybercrime is the widespread phenomenon and to feel protected it is practically impossible from such criminal offences. Limits of cyberspace are boundless, hackers have sufficiently development of skill, to remain in him incognito and that is why it creates problems at investigation of such criminal offences. Summarized, that legal adjusting of activity in the Ukrainian segment of global information and telecommunication network the «Internet», is characterized a subzero legal culture and many displays of the mode of irresponsibility.

It is noted that the most effective weapon in the fight against this crime is legislation that needs constant improvement. If we talk about international legal acts in this area, the first and main document that deals with the fight against cybercrime is the European Convention. Problems of prevention of criminal offenses in the field of computer technology are actively discussed by scientists, the practice of applying the relevant provisions of the law on criminal liability is developing rapidly.

Key words: *cybercrime, criminal offence, prevention, criminal responsibility, internet network.*

Стаття надійшла до редколегії 26 лютого 2021 року