УДК 343.34

АКТУАЛЬНІ ПИТАННЯ ВДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Ольга КОСИЦЯ,
кандидат юридичних наук,
викладач кафедри адміністративного, господарського
права та фінансово-економічної безпеки
Сумського державного університету

SUMMARY

The article deals with the research of normative legal acts that regulate organizational principles of counteraction to cybercrime in Ukraine, examination of problem questions that require further scientific understanding and solving the legislative and practical levels. The author outlines the advisability of adopting a special law that would define the principles of cybersecurity in the country, a national system for combating cybercrime and also pays particular attention to the harmonization of the normative documents in the field of cybersecurity and information security. For giving the system a legislation over about criminal responsibility must be brought to only formulations of disposition and characterizing signs of the articles of Criminal Code of Ukraine, that envisage responsibility for crimes that it may be to accomplish with the use of the computer systems and of informative communication networks.

Key words: cybercrime, counteraction to crime, cyberpolice, cybersecurity, information security.

АНОТАЦІЯ

Статтю присвячено дослідженню нормативно-правових актів, які регламентують організаційні засади протидії кіберзлочинності в Україні, висвітленню актуальних і проблемних питань, які потребують подальшого наукового осмислення та вирішення на законодавчому і практичному рівнях. Окреслено доцільність прийняття окремого закону, який би визначав засади кібербезпеки в державі, національну систему протидії кіберправопорушенням. Крім того окрему увагу варто приділяти гармонізації нормативних документів у сфері забезпечення кібербезпеки та інформаційної безпеки. З метою систематизації законодавство про кримінальну відповідальність необхідно привести до єдиних формулювань диспозиції та кваліфікуючих ознак статей Кримінального кодексу України, які передбачають відповідальність за злочини, які можливо вчинити з використанням комп'ютерних систем та інформаційно-комунікаційних мереж.

Ключові слова: кіберзлочинність, протидія правопорушенням, кіберполіція, кібербезпека, інформаційна безпека.

Постановка проблеми. Проблема розробки законодавства, яке б регламентувало сферу боротьби з кіберзлочинністю, та організаційно-правовий статус суб'єктів, які б протидіяли цьому негативному та руйнівному явищу, є актуальною сьогодні як ніколи раніше. Впровадження ефективного механізму правового регулювання протидії правопорушенням у кіберпросторі – це пріоритетне та першочергове завдання не лише України, але й усієї світової спільноти.

Актуальність дослідження зумовлена, насамперед, тим, що поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення персональних даних, незаконних фінансових операцій, крадіжок і шахрайства в мережі Інтернет. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави [1]. Як справедливо зазначає І.М. Рассолов, із першого дня існування всесвітнього віртуального простору в нього стали проникати різні правопорушники, зокрема й злісні злочинці. З'являються нові форми і види злочинних посягань у сфері високих технологій. Злочинці все частіше застосовують системний підхід до планування своїх дій, використовують сучасні технології та спеціальні засоби, створюють нові системи конспірації. Наразі комп'ютерна злочинність перетворилася в кримінальну сферу, в якій діють шахраї, зломщики-хакери, рекетири, педофіли, сутенери, торговці людьми і наркотиками й багато інших порушників законів [2]. На шляху просування до безпечного функціонування суб'єктів у національному та світовому інформаційному просторі вкрай важливим є системний підхід до пошуку ефективних управлінських рішень. Серед актуальних напрямів наукових досліджень забезпечення інформаційної безпеки України сьогодні необхідно виділити формування гармонійного понятійно-термінологічного апарату сфери безпеки кіберпростору і визначення специфіки протидії кіберзлочинності в системі державної діяльності із забезпечення інформаційної безпеки [3, с. 78].

Створення вітчизняної нормативно-правової та термінологічної бази у сфері протидії кіберправопорушенням, гармонізації нормативних документів у сфері забезпечення кібербезпеки та інформаційної безпеки, захисту інформації, відповідальності за кіберзлочини, відповідно до міжнародних стандартів і стандартів ЄС та НАТО, є пріоритетним напрямом забезпечення національної безпеки України.

Аналіз останніх досліджень і публікацій. Для дослідження обраної теми використано роботи науковців різних галузей знань. Організаційно-правові основи протидії кіберправопорушенням як самостійної сфери наукових досліджень та елемента інформаційної безпеки досліджують фахівці в галузі адміністративного й інформаційного права: О.А. Безуглий, В.М. Брижко, В.Д. Гавловський, І.В. Діордіца, Д.А. Клубань, В.А. Ліпкан, І.М. Рассолов, О.О. Тихомиров, Г.В. Форос, В.П. Шеломенцев та ін. Особливості організації протидії кіберзлочинності є предметом вивчення таких науковців, як В.М. Бутузов, С.В. Демедюк, О.Є. Користін, М.О. Кравцова, В.О. Кудінов, В.В. Марков, О.В. Орлов, С.М. Рогозін, В.М. Смаглюк, В.Г. Хахановський, В.С. Цимбалюк, О.О. Юхно, Д.А. Ястребов та ін. Відсутність у науковців і законодавців єдиного підходу до національної системи суб'єктів забезпечення кібербезпеки, напрямів протидії кіберзлочинності,

поняття кіберзлочину та відповідальності за їх вчинення зумовлює проведення нових наукових досліджень.

Метою статті є дослідження сучасного стану нормативного та організаційного забезпечення протидії кіберзлочинності, висвітлення актуальних питань та пропозицій із вдосконалення законодавства у вказаній сфері.

Виклад основного матеріалу. Передумовами боротьби з кіберзлочинністю в сучасних державах, на думку вчених [4, с. 85–86], є:

1) існування нормативно-правової бази, яка застосовується на національному рівні й сумісна з міжнародними структурами;

2) наявність судових структур і поліцейських сил, що володіють відповідними ресурсами і кваліфікацією для роботи на національному рівні та співпраці з міжнародною мережею з метою боротьби з транснаціональною кіберзлочинністю. Г.В. Форос, своєю чергою, виділяє три напрями діяльності з протидії кіберзлочинності: попередження кіберзлочинів, загальна організація боротьби з кіберзлочинністю та правоохоронна діяльність, спрямована саме на виявлення, припинення та розкриття кіберзлочинів, застосування заходів кримінальної відповідальності й покарання стосовно осіб, які вчинили кіберзлочин [5, с. 168].

Протидія кіберзлочинності здійснюється на національному та міжнародному рівнях, за допомогою нормативного врегулювання, організаційного та технічного забезпечення. На виконання умов Угоди про асоціацію, ратифікованої Конвенції Ради Європи про кіберзлочинність [12], Стратегії Національної безпеки в державі (2015 р.) [7], розроблено та прийнято Стратегію кібербезпеки України (2016 р.) [1], План заходів на 2016 рік з реалізації Стратегії кібербезпеки України (2016 р.) [8], Доктрину інформаційної безпеки (2017 р.) [9], Рішення РНБО «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» (2017 р.) [10], створено Національний координаційний центр кібербезпеки (2016 р.) [11].

Угодою про асоціацію між Україною та Європейським Союзом [6], ратифікованою Законом України від 16 вересня 2014 року № 1678-VII, передбачено, що сторони Угоди співробітничають у попередженні та боротьбі з кримінальною та незаконною організованою чи іншою діяльністю та спрямовані на вирішення низки ключових проблем, однією з яких є кіберзлочинність. Стратегія Національної безпеки України закріплює пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів наступні: розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам та їх нейтралізації; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого в Російській Федерації; реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав – членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки та оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки [7].

Особливої уваги заслуговує документ «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» [10]. Для оперативної та ефективної протидії кіберзлочинності суттєвим питанням є розробка та внесення в установленому порядку на розгляд Верховної Ради України законопроектів щодо імплементації положень Конвенції про кіберзлочинність, ратифікованої Законом України від 07 вересня 2005 року № 2824-IV [12], передбачивши, зокрема:

1) надання правоохоронним органам повноважень щодо внесення обов'язкових до виконання приписів власникам комп'ютерних даних (операторам і провайдерам телекомунікацій, іншим юридичним і фізичним особам) про термінове фіксування та зберігання комп'ютерних даних, необхідних для розкриття злочину, на строк до 90 днів із можливістю продовження такого строку до 3-х років, а також унормування порядку внесення зазначених приписів;

2) установлення вимог щодо надання операторам і провайдерам телекомунікацій на вимогу правоохоронних органів інформації, необхідної для ідентифікації постачальників послуг і маршруту, яким було передано інформацію;

3) запровадження блокування (обмеження) за рішенням суду операторами та провайдерами телекомунікацій визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу);

4) запровадження дієвого механізму використання в кримінальному процесі доказів в електронній формі, зібраних у процесі здійснення оперативно-розшукової діяльності.

Крім того, в умовах виникнення нових загроз національній і міжнародній безпеці, повсякденного зростання кількості та потужності кібератак на державні й фінансові установи, вмотивованих інтересами окремих держав, груп та осіб, постала необхідність затвердити протокол спільних дій суб'єктів забезпечення кібербезпеки, власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час виявлення, попередження, припинення кібератак і кіберінцидентів, а також при усуненні їхніх наслідків.

Так, аналіз прийнятої у 2016 році Стратегії кібербезпеки України [1] свідчить, що інституціональний механізм системи забезпечення кібербезпеки становлять Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи. Координуючу та контролюючу функцію у сфері забезпечення інформаційної та кібербезпеки відповідно до Конституції України та у встановленому законом порядку виконує Рада національної безпеки і оборони України (далі – РНБО) [1, 9].

Основними суб'єктами з попередження, виявлення, припинення та розкриття злочинів, які вчиняються у кіберпросторі; розслідування кіберінцидентів і кібератак щодо державних електронних інформаційних ресурсів; забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі є Служба безпеки України та Національна поліція України. Суттєвих позитивних результатів у сфері протидії кіберзлочинності може бути досягнуто за умови взаємодії основних суб'єктів з попередження, виявлення, припинення та розкриття злочинів, які вчиняються у кіберпросторі, а також, безумовно, взаємодії та координації діяльності всіх підрозділів кримінальної поліції при виявленні ними правопорушень у сфері інформаційної безпеки та інших правопорушень, вчинених із використанням комп'ютерної системи та інформаційно-комунікаційних

мереж. Основним завданням Департаменту кіберполіції Національної поліції України є безпосередня участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

С.В. Демедюк і В.В. Марков зазначають, що в процесі реформування кримінальної поліції Національної поліції України необхідно вирішити наступні завдання: створити механізм координації та взаємодії діяльності кіберполіції з іншими підрозділами Національної поліції та правоохоронними органами держави; вдосконалити та модернізувати професійну підготовку фахівців у вищих навчальних закладах і науково-дослідних установах МВС з метою отримання висококваліфікованих спеціалістів, здатних виконувати свої професійні обов'язки в умовах нового етапу розвитку органів внутрішніх справ та у сфері протидії сучасним високотехнологічним кіберзлочинам; упровадити в діяльність Національної поліції України функціонування програмно-технічних комплексів (терміналів) зворотного зв'язку для прийому звернень та заяв про кіберзлочини, що дозволить у режимі реального часу здійснювати оперативне реагування для їх запобігання, припинення або розкриття; передбачити участь фахівців кіберполіції у формуванні та реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також іншим кримінальним правопорушенням [13, с. 92].

Вважаємо, що протидії кіберзлочинності також сприятиме розробка спеціального Закону про боротьбу з кіберзлочинністю. Так, заслуговує на увагу Проект Закону «Про основні засади забезпечення кібербезпеки України» № 2126а від 19 червня 2015 р. [14], спрямований на правове регулювання та розбудову захищеного інформаційного простору держави, прогресивного розвитку ІТ-сфери, як рушійної сили становлення безпекового цифрового суспільства та цифрової економіки України, які є невід'ємними умовами входження в європейський інформаційний простір. Суттєвою перевагою та досягненням законопроекту є закріплення понятійного апарату, а саме таких понять, як кібератака, кібербезпека, кіберзагроза, кіберпростір, кіберзлочин та інші, визначення суб'єктів національної системи кібербезпеки та їх завдань.

Вказаний законопроект викликав інтерес та критику з боку науковців і практиків. Одним із суттєвих недоліків документу є те, що встановлені завдання суб'єктів національної системи кібербезпеки не узгоджуються з базовими чинними законодавчими актами, які регулюють діяльність таких органів, залишається невизначеним, хто буде відповідати за забезпечення кібербезпеки в інших сегментах, зокрема: органів державної влади та державного управління, економіки, судової системи, приватного сектору. Згідно з висновком Інтернет-асоціації України, виходячи зі змісту статті 9 проекту Закону, залишається невизначеним, який державний орган у повному обсязі матиме повноваження щодо формування державної політики задля забезпечення кібербезпеки України [15]. Крім того, в проекті Закону «Про основні засади забезпечення кібербезпеки України» [14] запропоновано визначення суб'єктів забезпечення кібербезпеки постійної готовності: державні органи або їх підрозділи, що входять до складу національної системи кібербезпеки, сили та засоби яких спеціально виділені для перебування в постійній готовності до реагування на кіберзагрози та оперативного виконання завдань забезпечення кібербезпеки.

Відповідно до положень ст. 8 проекту національну систему кібербезпеки складають РНБО, Міністерство оборони України, Генеральний штаб Збройних Сил України Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Міністерство внутрішніх справ (на відміну від Національної поліції України як зазначено в прийнятій Стратегії [1]), розвідувальні органи. Один із суб'єктів національної системи кібербезпеки, визначений Стратегією кібербезпеки [1] – Національний банк України – в законопроекті не вказується. У цілому позитивно оцінюючи проаналізований законопроект, доцільним є приведення його у відповідність до прийнятих стратегічних документів.

Окрему увагу слід приділити також такому напряму протидії кіберзлочинності, як застосування заходів кримінальної відповідальності та покарання осіб, які вчинили кіберзлочини. Наявність у Кримінальному кодексі України [16] шести статей про правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (Розділ XVI КК України), окремих статей (наприклад, ст. 200 «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення», частини третьої ст. 190 «Шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки») і видів злочину, в яких комп'ютерні продукти визначені як засіб злочину (ст.ст. 163, 176, 177), на сьогодні вже замало.

З метою забезпечення системності законодавство про кримінальну відповідальність необхідно привести до єдиних формулювань диспозиції та кваліфікуючих ознак статей Кримінального кодексу України, що передбачають відповідальність за злочини, які можливо вчинити з використанням інформаційно-комунікаційних мереж.

Поряд із прийняттям Закону України «Про основні засади забезпечення кібербезпеки України» або в рамках закону пропонуємо внести до Кримінального кодексу України зміни і доповнення, зокрема доповнити статті: Крадіжка (ст. 185), Вимагання (ст. 189), Порушення недоторканності приватного життя (ст. 182) наступною кваліфікуючою ознакою: з несанкціонованим доступом до комп'ютерної системи та інформаційно-комунікаційних мереж, у тому числі в мережі Інтернет, а статті «Ввезення, виготовлення, збут і розповсюдження порнографічних предметів» (ст. 301), «Сприяння вчиненню терористичного акту (ст. 258-4)», «Створення терористичної групи чи терористичної організації» (ст. 258-3), «Публічні заклики до вчинення терористичного акту» (ст. 258-2) – через комп'ютерну систему або інформаційно-телекомунікаційну мережу, в мережі Інтернет.

Висновки. На підставі вищевикладеного сформульовано такі положення:

– в національне правове поле вкрай необхідним є введення та визначення таких понять, кіберпростір, кібертероризм, кіберекстремизм, кібервійни, кіберзлочин, кіберзлочинність, та комплексно – які правопорушення є кіберзлочинами;

– не дивлячись на те, що необхідний комплекс організаційно-правових і технічних заходів протидії кіберзлочинності ще буде створений, його розробка має відбуватися з активним запозиченням досвіду високорозвинених країн, ІТ-спеціалістів, аналітичних і статистичних даних підрозділів із боротьби з тероризмом та екстремізмом

в органах безпеки, підрозділів Національної поліції з протидії, виявлення та розслідування правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку на основі міжнародного співробітництва спеціальних підрозділів компетентних органів;

– виконання рішення РНБО (п. 6.): «Національній поліції України разом зі Службою безпеки України вжити невідкладних заходів щодо забезпечення повного та об'єктивного розслідування кібератак на інформаційно-телекомунікаційні системи фінансового сектору держави» [10] можливо за умови вдосконалення взаємодії між Національною поліцією України та Службою безпеки України, а саме нормативного врегулювання порядку спільного використання цілодобової контактної мережі для надання невідкладної допомоги під час розслідування кіберзлочинів;

– у системі органів Національної поліції раціональним і неминучим є створення організованої системи взаємодії та координації з метою надання допомоги під час розслідування злочинів, учинених у мережі Інтернет або через комп'ютерну систему чи інформаційно-телекомунікаційну мережу.

Список використаної літератури:

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс] : Указ ПУ від 15 берез. 2016 р. № 96/2016 // Офіц. сайт Верховної Ради України. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/96/2016.

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

3. Тихомиров О.О. Протидія кіберзлочинності як складова державного забезпечення інформаційної безпеки / О.О. Тихомиров // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф. (Київ, 22 берез. 2011 р.). – Київ : Вид-во НА СБ України, 2011. – Ч. 2. – С. 78–82.

4. В поисках кибердоверия / Д-р Хамадун И. Туре Генеральный секретарь Международного союза электросвязи и Постоянная группа по мониторингу информационной безопасности Всемирной федерации ученых. – 2014. – 174 с. – [Электронный ресурс]. – Режим доступа : https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.02-1-2014-PDF-R.pdf.

5. Форос Г.В. Правове регулювання протидії кіберзлочинам / Г.В. Форос// Правова держава. – 2016. – № 24.– С. 164–169.

6. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [Електронний ресурс] : Угода від 27 черв. 2014 р. // Офіц. сайт Верховної Ради України. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/984_011/paran2820#n2820.

7. Про рішення Ради національної безпеки і оборони України від 06 травня 2015 року «Про Стратегію національної безпеки України» [Електронний ресурс] : Указ Президента України від 26 трав. 2015 р. № 287/2015 // Офіц. сайт Верховної Ради України. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/287/2015.

8. Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України [Електронний ресурс] : Розпорядження КМ України від 24 черв. № 440-р // Офіц. сайт Верховної Ради України. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/440-2016-%D1%80.

9. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки» [Електронний ресурс] : Указ Президент України від 25 лют. 2017 р. № 47/2017 // Офіц. сайт Верховної Ради України. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/47/2017.

10. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» [Електронний ресурс] : Указ Президента України від 13 лют. 2017 р. № 32/2017 // Офіц. сайт Верховної Ради України. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/32/2017.

11. Про Національний координаційний центр кібербезпеки : Указ Президента України від 07 черв. 2016 р. № 242/2016 [Електронний ресурс] // Офіц. сайт Верховної Ради України. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/242/2016.

12. Конвенція про кіберзлочинність (ратифіковано із застереженнями і заявами Законом № 2824-IV від 07 верес. 2005 р.) [Електронний ресурс] // Офіц. сайт Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua.

13. Демедюк С.В. Кіберполіція України / С.В. Демедюк, В.В. Марков // Наше право. – 2015. – № 6. – С. 87–93.

14. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Проект Закону № 2126а від 19 чевр. 2015 р. // Офіц. сайт Верховної Ради України. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.

15. Законопроект по кибербезопасности нужно тщательно доработать / Internetua [Электронный ресурс] – Режим доступа : http://internetua.com/zakonoproekt-po-kiberbezopastnosti-nuzno-tschatelno-dorabotat.

16. Кримінальний кодекс України від 05 квіт. 2001 р. № 2341-III [Електронний ресурс] // Офіц. сайт Верховної Ради України. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2341-14.

17. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення [Електронний ресурс] / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – № 2. – С. 299–309.

18. Шеломенцев В.П. Основні проблеми побудови системи кібернетичної безпеки України [Електронний ресурс] / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2014. – № 2. – С. 183–186.

19. Орлов О.В. Організаційні та нормативно-правові засади боротьби з кіберзлочинністю / О.В. Орлов, Ю.М. Оніщенко // Державне управління: удосконалення та розвиток : електронне наукове фахове видання. – 2014. – № 5. – Режим доступу : http://www.dy.nayka.com.ua/?op=1&z=715.

20. Узденов Р.М. Новые границы киберпреступности / Р.М. Узденов // Всероссийский криминологический журнал. – 2016. – Т. 10. – № 4. – С. 649–655. – DOI : 10.17150/2500-4255.2016.10(4).649-655.