КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ / CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION (CIIP)

КІБЕРЗЛОЧИННІСТЬ ЯК ЧИННИК НЕГАТИВНОГО ВПЛИВУ НА КРИМІНОГЕННУ СИТУАЦІЮ У РЕГІОНАХ

Андрій Бабенко

Донецький юридичний інститут, Україна

БАБЕНКО Андрій Миколайович, к.ю.н.

Рік та місце народження 1974, м. Донецьк, Україна.
Освіта: Донецький інститут внутрішніх справ при Донецькому державному університеті (з 2011 року – Донецький юридичний інститут МВС України) 2000 рік.
Посада: доцент кафедри кримінального права та кримінології з 2009 року.
Наукові інтереси: аналіз, програмування та запобігання злочинності в регіонах.
Публікації: більше 30 наукових публікацій, серед яких монографія, 2 підручника, навчальний посібник, науково-практичні рекомендації, наукові статті та тези доповідей.
E-mail: **kvester@mail.ru**

Анотація. *У даній статті досліджено вплив кіберзлочинності на стан злочинності в Україні. Побудовано просторово-часову теоретичну модель криміногенної ситуації в регіонах країни. Виявлено основні сфери потенційної загрози для суспільної безпеки з боку кіберзлочинності. Отримані результати дозволяють вдосконалити інформаційне забезпечення правоохоронних органів у запобіганні злочинності та окреслюють подальші напрямки регіональних кримінологічних досліджень.*

Ключові слова: *кіберзлочинність, Інтернет - злочинність, інтенсивність злочинності, криміногенна ситуація в регіонах, рівень кримінальної вираженості, суспільна безпека.*

Вступ

Протягом останніх десятиріч в Україні простежуються загальносвітові тенденції кардинальних змін соціального середовища, які пов'язані з впровадженням нових технологій. На сьогоднішній день спостерігається формування по суті нового типу соціальної парадигми – інформаційного суспільства. Невід'ємним елементом сучасного інформаційного середовища стала всесвітня комп'ютерна мережа Інтернет, яка дала суспільству безмежні можливості з оперативної передачі, отримання, обліку та обміну будь-якою інформацією. Нові можливості, які з'явилися в результаті розвитку інформаційних технологій стали широко використовуватися представниками кримінального світу. І, як наслідок, кіберзлочинність перетворилась на чинник, який став здійснювати вагомий тиск на суспільні відносини. Це почало негативним чином впливати на криміногенну ситуацію в країні і окремих її частинах – в регіонах. З'явилися нові форми, види та способи вчинення злочинів. Традиційні злочини – торгівля людьми, наркотиками, зброєю; замовлення на вбивства; шахрайства з фінансовими ресурсами; викрадання коштів і т.д. почали вчинятися більш масштабно, – з використанням високих технологій та без ризику швидкого викриття. За таких умов вбачається вкрай **актуальним** дослідження криміногенного простору України, виявлення факторів негативного впливу на криміногенну ситуації в країні та її регіонах. Одними із таких суттєвих кримінологічних чинників вбачається розширення мережі Інтернет та зростання пов'язаної з цим процесом – кіберзлочинності (або інтернет-злочинності, що використовується нами як синоніми – А.Б.).

Аналіз існуючих досліджень

Проблемам дослідження кіберзлочинності та запобіганню їй приділяли значну увагу відомі вчені різних галузей науки. Так, І.Р. Шинкаренко [1] вивчав питання кваліфікації, розслідування та протидії злочинам у сфері використання комп'ютерної техніки. І.Ф. Хараберюш, В.Я. Мацюк, В.А. Некрасов, О.І. Хараберюш [2] висвітлили особливості протидії злочинам, що вчиняються у сфері інформаційних технологій з використанням оперативно-технічних засобів. Значним внеском у

розв'язання проблеми охорони інформаційної безпеки України кримінально-правовими засобами можна вважати роботу М.В. Карчевського [3]. У контексті класифікації кібератак важко переоцінити роботи О.Г. Корченка, Є.В. Паціри, С.О. Гнатюка, В.М. Кінзерявого, С.В. Казмірчук [4]. В галузі формування кримінально-правової політики [5, с.39-42] та використання інформаційних технологій [6, с.90-93] у протидії кіберзлочинності присвячені роботи П.Л. Фріса, Н.А. Савінова, В.А. Намоконова та ін.. Поряд з цим, сучасною наукою не досліджені особливості територіального розподілу кіберзлочинності, її вплив на загальну криміногенну ситуацію та окремі види злочинності. Відсутня комплексна узагальнена картина про криміногенний простір країни та його мінливість під впливом злочинного використання високих технологій. Саме така інформація, на наш погляд, містить важливе теоретичне та практичне значення з точки зору покращення інформаційного забезпечення, і як наслідок, підвищення ефективності роботи правоохоронних органів у запобіганні злочинності.

Метою даної роботи є дослідження впливу кіберзлочинності на стан злочинності в Україні, побудова теоретичної моделі криміногенної ситуації в регіонах країни та виявлення основних сфер потенційної загрози для суспільної безпеки з боку кіберзлочинності.

Основна частина дослідження

Свого часу відомий російський кримінолог В.А. Номоконов висунув гіпотезу про зростання загроз суспільній безпеці, пов'язаних з криміналізацією інформаційної сфери і, зокрема, Інтернету. Досліджуючи статистичні дані Російської Федерації щодо злочинів у сфері комп'ютерної інформації, вчений констатував, що вони зростають пропорційно розширенню Мережі Інтернет [6, с.90]. У цьому контексті для підвищення ефективності діяльності правоохоронних органів у запобіганні злочинності і кіберзлочинності, як невід'ємної її частини, важливого кримінологічного значення набуває перевірка цієї гіпотези в умовах України, а також виявлення закономірностей злочинності, її регіональних особливостей та визначення основних сфер потенційної загрози з боку кіберзлочинності.

Статистичні дані свідчать про те, що протягом останніх років український інформаційний простір характеризується стрімким розширенням мережі Інтернет. Проведеним нами аналізом географії поширення Інтернет користувачів, розповсюдженості кіберзлочинності та загальної злочинності на території України виявлено наявність тісних зв'язків між цими явищами, що вказує на їх взаємообумовленість. Так, за даними компанії BIGMIR-Internet найвищого поширення користувачів в мережі Інтернет зафіксовано у східних областях України. Географія Інтернет-користувачів у нашій країні має такий вигляд: м. Київ – 55%, області: Донецька – 6,98%%; Харківська – 6,16%; Одеська – 5,00%; Дніпропетровська – 4,32%; АР Крим – 2,55%; Луганська – 2,14%; Запорізька – 1,30%. В свою чергу, західні області України характеризуються низьким розповсюдженням Інтернету і такими показниками щодо його користувачів: Закарпатська – 0,65%; Тернопільська - 0,57%; Вінницька – 0,61%; Чернівецька – 0,31%; Івано-Франківська – 0,15% і т.д. [7, с.3-4]. Така географія майже повністю співпадає з географією поширеності злочинності серед регіонів України. Причому не лише Інтернет-злочинністю, а й загальною та окремими її видами [8, с.116-123; 9, с. 151-159; 10, с. 65-68].

Якщо порівняти наведені дані зі статистичними даними МВС щодо зареєстрованої злочинності у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, то неважко помітити, що найбільша кількість їх реєструється саме в регіонах з високим рівнем користувачів Інтернету – у східних та південних областях України. Так, у 2011 р. зі 130 злочинів досліджуваного виду, вчинених в Україні: у Дніпропетровській області вчинено 26 злочинів, у Донецькій – 25, у Запорізькій – 15, у Миколаївські – 11, у Луганській вчинено 8 таких фактів і т.д.. Тобто понад 65% у загальній структурі злочинів цього виду. Серед західних областей найбільша кількість злочинів цієї категорії зафіксована у Тернопільській області – 6 випадків, на другому місці опинилася Вінницька область – 3 факти, у Івано-Франківській області зафіксовано 2 злочини, у Закарпатській – 1, і у Чернівецькій – 0 [11]. Така статистика свідчить про наявність кореляції між концентрацією користувачів Інтернету в регіоні та кіберзлочинністю.

Далі ми порівняли отримані дані з територіальним розподілом злочинності у 27 регіонах України (24 області, АР Крим, м. Київ та м. Севастополь), де нами виявлені стійки закономірності щодо інтенсивності загальної злочинності, та окремих її видів, які фіксувалися у регіонах країні в період з 2001-2011 роки. Це дало нам можливість побудувати теоретичну модель криміногенної ситуації в регіонах країни [8, с.116-123; 9, с. 151-159] та порівняти географію розповсюдженості кіберзлочинності з географією Інтернет-користувачів а також порівняти ці дані з окремими видами злочинності. В ході дослідження нами зафіксовано наявність залежностей між ними. Наприклад, для сільськогосподарських західних регіонів, де зафіксовано низький рівень активності користувачів Інтернету і невелика кількість вчинюваних кіберзлочинів, були характерними *низький рівень кримінальної вираженості* загальною злочинністю (з середньою інтенсивністю злочинності від 475 до 675 злочинів на 100 тис. населення – Закарпатська, Ів. Франківська, Львівська, Рівненська, Тернопільська та Чернівецька області), та *помірний рівень кримінальної вираженості,* (з середньою інтенсивністю злочинності від 676 до 875 злочинів на 100 тис. населення – Вінницька, Волинська, Житомирська, Київська, Хмельницька, Черкаська, Чернігівська області). Регіони із помірною активністю користувачів Інтернету і значною кількістю кіберзлочинів характеризувалися

середнім рівнем кримінальної вираженості загальною злочинністю(з середньою інтенсивністю злочинності від 876 до 1075 злочини на 100 тис. населення – Кіровоградська, Миколаївська, Одеська, Полтавська, Сумська та Херсонська області). Для високоурбанізованих промислових східних та курортних південних регіонів були характерними високі рівні активності користувачів Інтернету та високі показники кіберзлочинності. В абсолютних показниках різниця у кількості вчинених кіберзлочинів між східними та західними регіонами перевищувала 10-ти – 15-ти кратні розміри. Відповідно, тут нами зафіксовані *високий* (від 1076 до 1272 злочинів на 100 тис. населення – АР Крим, Донецька, Харківська області та м. Київ) та *дуже високий* рівень кримінальної вираженості загальною злочинністю (від 1275 до 1475 злочинів на 100 тис. населення – Дніпропетровська, Запорізька, Луганська області та м. Севастополь) (Рис.1.).

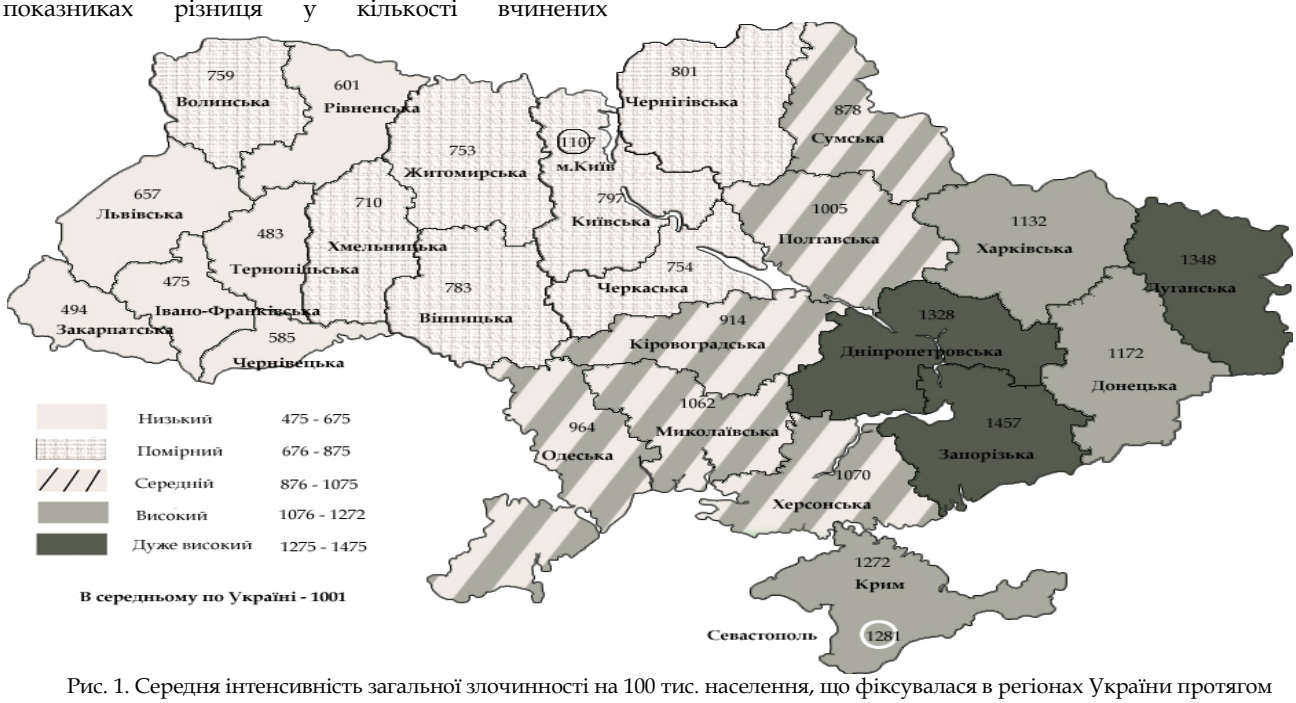

Рис. 1. Середня інтенсивність загальної злочинності на 100 тис. населення, що фіксувалася в регіонах України протягом 2001-2011 років

Наведені дані свідчать про наявність кореляційного зв'язку між рівнем злочинності, географією розповсюдженості споживачів послуг Інтернет та Інтернет-злочинністю, а отже, і про наявність взаємно обумовлюючих кримінологічно значущих зв'язків між ними.

Пояснення такої ситуації можна знайти в тому, що мережа Інтернет, будучі носієм масового постачальника інформації, перетворився у один із домінуючих інструментів інформаційно-технічного, морально-правового та психологічного впливу на населення і майже всі сфери соціального буття. Поряд з наявністю в Інтернеті великої кількості позитивної та корисної інформації, ці Мережі відрізняються перенасиченістю різного роду негативною інформацією, – порнографією, насиллям, пропагандою наркотиків та даремного часу проводження, інструкціями з виготовлення зброї, вибухівки, та психотропних речовин. В Інтернеті також можна легко знайти інформацією про послідовність вчинення протиправних дій, поради стосовно скоєння різних злочинів та уникнення відповідальності. Мережі Інтернет переповнені іграми, що пропагують насильство та масові вбивства і т.д. Нерідко з використанням мережі Інтернет вчиняються й самі злочини – торгівля людьми, шахрайства, замовлення на вбивство, продаж зброї та наркотиків. Враховуючи велику латентність Інтернет-злочинності, в цілому така ситуація негативно впливає на криміногенну ситуацію у країні.

Таким чином сучасний Інтернет - простір, характеризуючись надмірною доступністю значних інформаційних ресурсів та максимальним розширенням соціальних контактів, продукує у населення певний інформаційний світогляд, відношення до життя, оточення і закону.

Не зважаючи на те, що у Кримінальному кодексі України міститься цілий розділ, який передбачає відповідальність за вчинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, за які передбачено кримінальну відповідальність, цей фактор не утримує осіб від вчинення кіберзлочинів. Пояснення цьому може полягати з одного боку в недосконалості кримінального та процесуального законодавства, з іншого – у дефіциті висококваліфікованих фахівців, які відмовляються працювати за низьку заробітну платню, що їм пропонують у правоохоронних органах. У зв'язку з цим, злочинці завжди знаходяться на декілька кроків попереду правоохоронних органів. Останні працюють постфактум, в умовах дефіциту високо-кваліфікованих спеціалістів, недосконалого законодавства, яким вони змушені керуватися, недосконалого матеріально-технічного забезпечення і т.д.. Тоді як злочинці не дотримуються жодних

правил, нехтують законом, діють конфіденційно, в умовах неочевидності, і тільки їм відомо де, коли і яким способом буде вчинений злочин. Звідси досліджуваний вид злочинності має високий рівень латентності (не виявлених злочинів) і здійснює вагомий тиск на криміногенну ситуацію як на рівні всієї держави, так і на рівні окремих регіонів.

На думку фахівців з питань інформаційної безпеки, кіберзлочини за способом вчинення об'єднуються у такі групи:

– інформаційні – незаконні способи отримання інформації, зокрема, шляхом несанкціонованого доступу до комп'ютерів та мереж, поширення неправдивої інформації;

– фінансові – «злам» банківських систем безпеки, отримання безкоштовних послуг телефонного зв'язку, крадіжки грошей з кредитних карток, створення електронних пірамід, шахрайство під виглядом віддалених продаж або роботи тощо;

– такі, що завдають шкоду здоров'ю та загрожують життю людей (виведення з ладу медичного обладнання, «тероризування» особи і т.д.)[12, с.16].

Вказані групи не охоплюють явища, які є сприятливим середовищем для вчинення інших злочинів – пропагування насилля, розпусти, споживання наркотиків, рекламування ведення злочинного способу життя і т.д. Тобто поза сферою контролю знаходиться діяльність, що детермінує вчинення тяжких та особливо тяжких злочинів проти: життя та здоров'я особи, свободи, власності, статевої свободи та недоторканості особи тощо. У цьому сенсі, на наш погляд, кримінальне та кримінально-процесуальне законодавство потребує ретельних наукових досліджень та суттєвого вдосконалення. В цілому, слід зазначити, що кіберзлочинність в українській кримінології є малодослідженим асоціальним явищем. В жодному з сучасних вітчизняних підручників з кримінології нам не вдалося знайти узагальненої кримінологічної інформації про цей вид асоціального прояву. Така ситуація негативно впливає на підготовку фахівців для правоохоронних органів. Між тим, слід зазначити, що кіберзлочинність вже давно перетворилася на самостійний вид злочинності з особливостями кількісно-якісних показників, регіонального розподілу, детермінації, особи злочинця, що потребує вивчення і врахування під час підготовки фахівців із запобігання злочинності. Більше того, ця сукупність злочинних діянь, здатна завдавати значної шкоди будь-яким інтересам держави, суспільства та особистості. У зв'язку з цим набуває важливості групування кіберзлочинів за об'єктом завдання шкоди. Окреслимо деякі з них – найбільш значні.

Так, кіберзлочинність здатна завдавати значної шкоди *безпеці держави*. Серед злочинів цієї категорії можна виділити диверсію у сфері комп'ютерної інформації – тобто блокування, знищення, модифікація або копіювання інформації, що являє собою державну таємницю у військовій, економічній і інших галузях з метою підриву економічної безпеки, політичної стабільності та обороноздатності держави.

Наступним видом кіберзлочинів можна вважати злочини, що являють загрозу для *громадської безпеки*. Як загальновідомо, комп'ютеризація охопила практично всі сфери життєдіяльності сучасного суспільства. Комп'ютерні мережі, Інтернет, відповідна техніка, обладнання та програмне забезпечення стали невід'ємною складовою у роботі хімічної промисловості, наземного, морського та повітряного транспорту, атомної енергетики, збройних сил і т.д. Неправомірний доступ у комп'ютерне забезпечення таких галузей створює підвищену небезпеку не лише для їх діяльності, а і для громадської безпеки. Наслідком втручання у їх роботу можуть бути техногенні або екологічні катастрофи, аварійні ситуації, масове травмування чи загибель людей тощо.

Самостійну групу кіберзлочинів складають такі, що можуть посягати на *економічну безпеку*. Дана категорія злочинів об'єднує різного роду викрадання шляхом неправомірного доступу до автоматизованих систем забезпечення діяльності різних підприємств, до інформаційних ресурсів фінансових установ і т.д. До цієї категорії злочинів також можна віднести виготовлення та збут фальшивих кредитних або розрахункових карток або платіжних документів. Така діяльність здатна привести до значних фінансових втрат і навіть до знищення підприємств, краху цілих економічних галузей.

Серед кіберзлочинів значного розповсюдження набули діяння, які порушують *суспільну та особисту безпеку* у сфері забезпечення конституційних прав і свобод громадянина та людини. Широкого розповсюдження набули злочини, пов'язані зі збутом наркотичних засобів та зброї, торгівля людьми, сексуальне розбещення неповнолітніх і т.д.. Окремо хотілося б виділити діяння, що порушують тайну електронних повідомлень та спілкування, викрадання та розповсюдження об'єктів інтелектуальної власності – програмного забезпечення, кінопродукції, результатів дисертаційних досліджень, винаходів і т.д.

За результатами проведеного регіонального дослідження можна констатувати, що сучасна криміногенна ситуація та соціальна дійсність не в повній мірі контролюється правоохоронними органами, а злочинці не отримують адекватного покарання. Так, не охоплює всі форми та способи вчинення комп'ютерних злочинів кримінальне законодавство. Воно не завжди встигає за соціальним та технічним прогресом, якій дуже оперативно бере на озброєння злочинний світ. Переважна частина кіберзлочинності залишається латентними – тобто без кримінально-правового реагування. Покарання за цю групу злочинів є не адекватним їх суспільній безпеці. Навіть за виявлені та доведені злочини суди призначають покарання, які не пов'язані з позбавленням волі і ізоляцію злочинців від суспільства. Це в свою чергу породжує безкарність і є сприятливими умовами для подальшого розвитку і

удосконалення форм та способів вчинення кіберзлочинів.

Однією із суттєвих причин такого стану, на наш погляд, є недосконалість сучасної системи підготовки фахівців з протидії кіберзлочинності. Уявляється, що у контексті підвищення ефективності діяльності регіональних правоохоронних органів у запобіганні кіберзлочинності важливого значення набуває вдосконалення професійної підготовки кадрів цих органів. З цією метою є вкрай необхідним введення в систему ВНЗ спеціальних курсів з цієї проблематики. Істотному збагаченню знань про кіберзлочинність сприятиме доповнення підручників з криміналогії додатковим розділом «Кримінологічна характеристика та запобігання кіберзлочинності». В цьому розділі мають бути окреслені кримінологічні закономірності кіберзлочинності, її регіональні особливості, інформація про її причини та умови, основні тенденції та сфери потенційної загрози, дані про особу злочинця, заходи запобігання, іноземний досвід протидії.

Слід пам'ятати, що особливостями кіберзлочинності є той факт, що вчинення таких дій потребує застосування спеціальних знань, навичок роботи з комп'ютерною технікою з високотехнологічними пристроями та системами, тобто залучення додаткового інтелектуального ресурсу. Як наслідок, вона створює загрозу більш великому колу суспільних відносин ніж традиційні злочини. Отже, злочинність досліджуваного виду являє собою підвищену суспільну небезпеку і їх вчинення повинно оцінюватися суспільством більш суворо з точки зору покарання. Уявляється, що штраф або максимальне покарання у вигляді позбавлення волі строком до шести років (Розділ XVI Кримінального кодексу України) розглядається такими, що явно не відповідають ступеню їх суспільної безпеки і є недостатнім для цих злочинів. Вочевидь назріла потреба для визнання вчинення злочину з використанням електронно-обчислюваної техніки або комп'ютерних мереж і Інтернет особливо кваліфікуючою ознакою не лише за Шахрайство, передбачене ч.3 ст.190 КК України, а й за інші злочини. Такі наприклад, як окремі злочини, передбачені Розділом XIII КК України «Злочини у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інші злочини проти здоров'я населення» та Розділом IX КК «Злочини проти громадської безпеки»: контрабанда наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів (ст..305 КК України), збут наркотичних засобів, психотропних речовин або їх аналогів (ст. 307 КК України), схиляння до вживання наркотичних засобів, психотропних речовин або їх аналогів (ст..315 КК України), незаконне поводження зі зброєю, бойовими припасами або вибуховими речовинами (ст.263 КК України) та злочини з інших розділів Кримінального кодексу України. Причому ефективне вирішення питання кримінальної відповідальності за кіберзлочини може міститися у об'єднані зусиль практичних працівників і правознавців з фахівцями у галузі безпеки комп'ютерних мереж і Інтернет, програмного забезпечення та обладнання, квантової інформації і кріптології, управління інформаційною безпекою і т.д. Таке об'єднання зусиль дозволить правильно сформулювати диспозиції кримінально-правових норм. Саме таким чином у повній мірі можливо визначити всі необхідні сфери суспільних відносин та напрямки діяльності, що потребують кримінально-правового регулювання.

Висновок

1. В ході дослідження виявлені особливості територіального розподілу кіберзлочинності, встановлено її вплив на загальну криміногенну ситуацію та окремі види злочинності в регіонах. Наведено комплексну узагальнену картину про криміногенний простір країни та його мінливість під впливом злочинного використання високих технологій. Отримана інформація може мати теоретичне та практичне значення з точки зору покращення інформаційного забезпечення, і як наслідок, підвищення ефективності роботи правоохоронних органів у запобіганні злочинності в регіонах країни.

2. Доведено, що останніми роками кіберзлочинність перетворилась на фактор, який здійснює вагомий тиск на суспільні відносини. Це негативним чином впливає на криміногенну ситуацію в країні і окремих її частинах – в регіонах. З'явилися нові форми, види та способи вчинення злочинів. Традиційні злочини – торгівля людьми, наркотиками, зброєю; замовлення на вбивства; шахрайства з фінансовими ресурсами; викрадання коштів і т.д. почали вчинятися більш масштабно, – з використанням високих технологій та без ризику швидкого викриття.

3. За результатами регіонального дослідження можна констатувати, що сучасна криміногенна ситуація та соціальна дійсність не в повній мірі контролюється правоохоронними органами, а злочинці не отримують адекватного покарання. Покарання за цю групу злочинів є не адекватним їх суспільній безпеці і потребує законодавчого врегулювання у сторону збільшення строків позбавлення волі.

4. Кіберзлочинність має високий рівень латентності (не виявлених злочинів) і здійснює вагомий тиск на криміногенну ситуацію як на рівні всієї держави, так і на рівні окремих регіонів.

5. Подальше розширення мережі Інтернет та науково-технічний прогрес крім позитивних змін містить в собі потенційні загрози криміногенного характеру, які пов'язані з їх використанням представниками злочинного світу. Отже, представники різних наукових галузей та правоохоронні органи повинні об'єднати зусилля з метою зниження потенційних загроз кримінального характеру на суспільні відносини від кіберзлочинності шляхом вдосконалення кримінального законодавства.

6. З метою підвищення ефективності діяльності регіональних правоохоронних органів у запобіганні кіберзлочинності важливого значення

набуває вдосконалення професійної підготовки кадрів правоохоронних органів. З цією метою є вкрай необхідним введення в систему ВНЗ спеціальних курсів з цієї проблематики. Підручники з кримінології повинні бути доповнені додатковим розділом «Кримінологічна характеристика та запобігання кіберзлочинності». В цьому розділі мають бути окреслені кримінологічні закономірності кіберзлочинності, її регіональні особливості, інформація про її причини та умови, основні тенденції та сфери потенційної загрози, заходи запобігання, іноземний досвід протидії.

Література

[1] Преступления в сфере использования компьютерной техники: квалификация, расследование и противодействие: [монография] / [И.Р. Шинкаренко и др.]. – Донецьк: РВВ ЛДУВС, 2007. – 267 с.

[2] Хараберюш І.Ф. Використання оперативно-технічних засобів у протидії злочинам, що вчиняються у сфері нових інформаційних технологій: [монографія] / [І.Ф. Хараберюш, В.Я. Мацюк, В.А. Некрасов, О.І. Хараберюш]. – К.: КНТ, 2007. – 196 с.

[3] Карчевський М.В. Кримінально-правова охорона інформаційної безпеки України: [монографія] / М.В. Карчевский. – Луганськ, 2011. – 538 с.

[4] Корченко О.Г. Основний принцип формування класифікації кібератак/ О.Г. Корченко, Є.В. Паціра, С.О. Гнатюк, В.М. Кінзерявий, С.В. Казмірчук // Вісник Східноукраїнського національного університет ім. Володимира Даля. - № 4 (146). – ч. 1, 2010. – С. 184-193.

[5] Фріс П.Л. Кримінально-правова політика у сфері протидії кіберзлочинності в Україні: ефективність та перспективи розвитку / П.Л.Фріс, Н.А.Савінова // Боротьба з інтернет-злочинністю [матеріали міжнародної наук.-практ. конф. (м.Донецьк,12-13 червня 2013 р.)]. – Донецьк: ДЮІ МВС України, 2013. – 266 с.

[6] Намоконов В.А. Новые информационные технологии в борьбе с преступностью / В.А. Намоконов // Российский криминологический взгляд. – 2005. - № 1. – С.90-93.

[7] Глобальная статистика украинского интернета [Електронний ресурс].– Режим доступу:http://i.bigmir.net/index/UAnet_global_report_032010.pdf. – Назва з екрану.

[8] Бабенко А.М. Кримінологічна класифікація регіонів України та її значення для протидії злочинності /А.М. Бабенко // Бюлетень Міністерства юстиції України. – 2013. - № 3 (137). – С. 116-123.

[9] Бабенко А.М. Регіональний підхід в кримінології як метод вивчення злочинності /А.М. Бабенко// Проблеми правознавства та правоохоронної діяльності. – 2013. - №1 (52). – С.151-159.

[10] Бабенко А.М. Мережі Інтернет як об'єкт регіонального дослідження в контексті профілактики злочинності / А.М. Бабенко // Боротьба з інтернет-злочинністю [матеріали міжнародної наук.-практ. конф. (м. Донецьк,12-13 червня 2013 р.)]. – Донецьк: ДЮІ МВС України, 2013. – 266 с.

[11] Стан та структура злочинності в Україні (2010 – 2011 р.р.) [Електронний ресурс]. – Режим доступу: http://mvs.gov.ua/mvs/control/main/uk/publish/article/717134. – Назва з екрану.

[12] Панченко В.М. Сучасний стан та проблеми боротьби з Інтернет-злочинністю / В.М. Панченко // Боротьба з Інтернет-злочинністю [матеріали міжнародної наук.-практ. конф. (м. Донецьк,12-13 червня 2013 р.). – Донецьк: ДЮІ МВС України, 2013. – 266 с.]

УДК 343.92 (045)

Бабенко А.Н. Киберпреступность как фактор негативного влияния на криминогенную ситуацию в регионах

Аннотация. *В данной статье исследовано влияние киберпреступности на состояние преступности в Украине. Построена пространственно-временная теоретическая модель криминогенной ситуации в регионах страны. Выявлены основные сферы потенциальной угрозы для общественной безопасности со стороны кирерпреступности. Полученные результаты позволят усовершенствовать информационное обеспечение правоохранительных органов в противодействии преступности и определяют направления дальнейших региональных криминологических исследований.*

Ключевые слова: *киберпреступность, Интернет-преступность, интенсивность преступности, криминогенная ситуация в регионах, уровень криминальной пораженности, общественная безопасность.*

Babenko A.N. Cyber criminal activity as a factor of negative influence on criminogenic situation in the region

Abstract. *Influence of cyber criminal activity upon the level of criminal activity in Ukraine has been researched in the article. Areal and temporal theoretical model of criminogenic situation in the regions of Ukraine has been built. Main spheres of potential threat of cyber criminal activity for the society have been revealed. The results obtained permit to improve the informational data base for law-enforcement bodies in preventing crimes and they outline further directions of regional criminological research.*

Key words: *cyber criminal activity, Internet-criminal activity, criminogenic situation in regions, level of criminal infection, social safety.*

Отримано *4 червня 2013 року*, затверджено редколегією *19 червня 2013 року*