УДК 338.46:002+341.48

СКУЛИШ Є.Д., *доктор юридичних наук, професор,*
Заслужений юрист України,
головний науковий співробітник НДІІП НАПрН України

ПОСИЛЕННЯ ВІДПОВІДАЛЬНОСТІ В КОНТЕКСТІ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ БОРОТЬБИ ІЗ КІБЕРЗЛОЧИННІСТЮ

Анотація. *Про правове забезпечення відповідальності за злочини у сфері інформаційного права. Проаналізований закордонний досвід у сфері боротьби з кіберзлочинами.*

Ключові слова: *кіберзлочинність, інформація, комп’ютерні мережі, інформаційні технології, Інтернет.*

Аннотация. *О правовом обеспечении ответственности за преступления в сфере информационного права. Проанализирован заграничный опыт в сфере борьбы с киберпреступлениями.*

Ключевые слова: *киберпреступления, информация, компьютерные сети, информационные технологии, Интернет.*

Summary. *About the legal providing of responsibility for the crimes in the field of informational right. Foreign experience in the field of combating cyber crimes is analysed.*

Keywords: *cyber crimes, information, computer networks, information technologies, Internet.*

Постановка проблеми. Швидкість розвитку комп’ютерних технологій та інформаційних систем обумовлює більшість із сучасних соціально-економічних процесів. Інформація, виступаючи специфічним предметом людської діяльності та специфічним об’єктом суспільних відносин, вимагає й особливих методологічних підходів до врегулювання її правового режиму. А у поєднанні із комп’ютерними технологіями вона сприяє формуванню нового типу суспільства – інформаційного та постінформаційного. Більше того, поширення областей використання комп’ютерів породжує новітні форми господарської діяльності, що також вимагає відповідного нормативного забезпечення. Однак означені процеси не завжди мають позитивний ефект, оскільки знеособлення і перенесення соціально-економічних відносин у площину віртуальної реальності, внаслідок використання комп’ютерних мереж у поєднанні із розкриттям інформаційного простору завжди породжує ризики неправомірного використання інформації. Тому застосування подібного роду технологій пов’язується із підвищеними вимогами до захисту суспільних відносин. В цьому контексті на перший план виходять саме правові механізми, зокрема – кримінально-правові.

Проблематика даного дослідження обумовлюється ще й тим, що злочини в сфері інформаційного права щодо використання комп’ютерних технологій та телекомунікацій відносяться до таких, склад яких, а іноді і сам факт скоєння довести надзвичайно важко, в той час як подібні діяння можуть завдавати значної шкоди як корпоративним, так і особистим майновим і немайновим інтересам.

Питанням правового забезпечення боротьби з кіберзлочинністю і зокрема відповідальності за скоєння подібного роду злочинів присвячено багато праць як вітчизняних, так і закордонних вчених, зокрема: П.П. Андрушко, А.Г. Волеводза, П.С. Берзіна, Голубєва В.О., М.О. Довбиша, Л.П. Зверянської, О.А. Протасевича, О.В. Суслопарова, М.І. Хавронюка та ін.

Метою статті є визначення доцільності, необхідності та обґрунтування причин посилення відповідальності за скоєння кіберзлочинів.

Виклад основного матеріалу. В даний час боротьба з кіберзлочинністю є однією з найбільш актуальних проблем у всьому світі. Зростаюча кількість кіберзлочинців, постійне вдосконалення інформаційних технологій і, як наслідок, можливості злочинних нових схем створюють чергові загрози для глобальних інформаційних мереж і суспільства в цілому. Постійно з’являються повідомлення про нові факти судових розглядів у справах про кіберзлочини, і зокрема, у справах про кібершахрайство, але мало хто звертає увагу на те, що злочинці не зупиняються лише на розробці шахрайських схем.

Наприклад, за даними компанії-розробника антивірусного програмного забезпечення Mcafee, системи газового, електричного і водопостачання вже давно піддаються подібним нападам. Mcafee провела дослідження 200 IT-відділів 14 країн, що відповідають за постачання життєво важливих ресурсів, згідно з яким був зроблений висновок про те, що 80 % IT-відділів були піддані посяганням торік. Якщо лише уявити, що хакери можуть оволодіти інформаційними технологіями в області енергетики, хімічної промисловості, нафтогазових об'єктів, порушити системи водопостачання, то наслідки будуть катастрофічними для держави та суспільства в цілому [12, с. 30-37].

Як зауважує М.О. Довбиш, кіберзлочинність – це проблема, з якою зіштовхнулась планета у 21 столітті, і яка обіцяє рости та поглинати все більше коштів. Незважаючи на усі заходи, що вживають окремі особи, фірми, а також держава, кіберзлочинність продовжує свою діяльність, збільшуючи прибутки злочинців. Тому сьогодні особливо важливо переглянути існуючі заходи боротьби та активно розробляти нові, що принесуть більшу користь та надійніший захист від кіберзлочинців. Рівень кіберзлочинності в Україні останнім часом також швидко зростає. Експерти зазначають, що Україна – дуже важливий центр хакерства, поряд із Росією, Бразилією, Китаєм та меншою мірою – Індією. У цих країнах досить освічене молоде населення, високий рівень безробіття та обмежені можливості працевлаштування [9, с. 16-25].

Особливості причинного комплексу кіберзлочинності пов’язані із специфікою віртуального світу. Тут в не меншій мірі, ніж в світі реальному, потрібна гармонізація відносин. Існуюча “цифрова нерівність” породжує дефіцит і дорожчання комп’ютерної техніки та інших засобів масової комунікації в країнах і регіонах з нерозвиненою комп’ютерною інфраструктурою. Серед найбільш уразливих до кіберзлочинів сфер суспільного життя відноситься фінансовий сектор економіки, а саме банки та їх послуги. Зростання популярності Інтернет-банкінгу спонукає шахраїв вигадувати нові способи заволодіння чужими коштами. І справа не тільки в технічній стороні, а також в обізнаності та володінні масивом персональних даних клієнтів банку, які часто опиняються в руках злочинців через необачність і довірливість громадян. Найбільш поширеними злочинами в банківській сфері є шахрайство з використанням платіжних карток та їх реквізитів і шахрайство з використанням дистанційного банківського обслуговування (система “клієнт-банк”). Зі зростанням обсягів безготівкових розрахунків зростає і кількість потерпілих від кібершахраїв. За даними НБУ, обсяг неправомірно списаних коштів в 2012 році збільшився майже в півтора рази – з 6,3 млн. до 9,1 млн. грн. [10, с. 5].

Середній показник таких злочинів у країнах Європейського союзу складає 0,06 – 0,08 %, в Україні у 2011 – 2012 рр. кількість подібних злочинів сягала 0, 045 % всіх операцій із платіжними картками. І хоча фахівці розглядають ці показники як показники злагодженої роботи правоохоронців і банків у протидії кіберзлочинності, проте не слід забувати, що в Україні більшість громадян після кризи 2009 р. не довіряють свої кошти

фінансовим установам, дуже багато людей не залишають на пластикових картках навіть заробітну плату, яку їм перераховують на спеціальний рахунок.

Слід зазначити, що ці кіберзлочини можуть скоювати як хакери, які не мають жодного відношення до банку, так і співробітники банків, які мають доступ до персональних даних клієнтів. Так звані інсайдери досить часто передають конфіденційну інформацію шахраям, отримуючи за це частку незаконних прибутків від шахрайства. Наразі це поширена проблема не лише державних структур, де заробітна плата не досить велика, а й великих холдингів, компаній, які оперують змістовними базами персональних даних. Тому мають значення не тільки засоби захисту від зовнішнього втручання в банківські системи, а також моніторинг обігу даних, які використовуються всередині великих установ і підприємств, що, на жаль, не так поширено на українському ринку фінансових послуг [9, с. 16-25].

Слід зауважити, що кіберзлочинність як явище отримала широкий резонанс в контексті розробки механізмів протидії подібного роду проявам, причому скоординованої протидії багатьох країн. З цього приводу було розроблено та прийнято багато міжнародних актів, зокрема: Бухарестська декларація про міжнародне співробітництво в боротьбі з тероризмом, корупцією і транснаціональною організованою злочинністю (2006 р.), Всесвітній саміт з інформаційного суспільства та Конвенції Ради Європи “Про кіберзлочинність” від 2001 р. (далі – Конвенція РЄ). На сьогодні саме Конвенція РЄ є одним з провідних міжнародно-правових актів в сфері боротьби із кіберзлочинністю. Вона спрямована на врегулювання таких основних питань:

– кримінально-правової характеристики злочинів щодо комп’ютерної інформації;

– кримінально-процесуальних аспектів боротьби із злочинністю, направлених на забезпечення збирання доказів при розслідуванні комп’ютерних злочинів;

– міжнародної співпраці в кримінально-процесуальній діяльності, направленій на збирання доказів скоєння таких злочинів за кордоном [1].

Також Конвенція називає п’ять видів комп’ютерних злочинів:

– незаконний доступ (протиправний умисний доступ до комп’ютерної системи або її частини);

– незаконне перехоплення (протиправне умисне перехоплення не призначених для загального користування комп’ютерних даних, зовні або усередині такої системи, включаючи електромагнітні випромінювання);

– втручання в дані (протиправне пошкодження, видалення, порушення, зміна або знищення комп’ютерних даних);

– втручання в систему (серйозна протиправна перешкода функціонуванню комп’ютерної системи шляхом введення, передачі, пошкодження, видалення, порушення, зміни або знищення комп’ютерних даних);

– незаконне використання пристроїв (виробництво, продаж, придбання для використання, імпорт, оптовий продаж або інші форми надання в користування: пристроїв, включаючи комп’ютерні програми, розроблені або адаптовані для здійснення злочинів; комп’ютерних паролів, кодів доступу або інших подібних даних, за допомогою яких можна отримати доступ до комп’ютерної системи в цілому або будь-якої її частини, з метою використовувати їх для скоєння злочинів. А також заволодіння одним з предметів, що згадуються вище, з наміром використовувати його з метою скоєння злочинів) [1].

Що стосується України, то окрім ратифікації Конвенції РЄ, актуальність проблеми боротьби із кіберзлочинністю було відмічено в Указах Президента: “Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень” від 14.07.00 р. № 891 [4], “Про заходи щодо розвитку національної

складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні” від 31.07.00 р. № 928/2000 [5], “Про деякі заходи щодо захисту державних інформаційних ресурсів у мережі передачі даних” від 24.09.01 р. № 891/2001 [3]. Проте погоджуючись із загальною думкою, яка панує в науці кримінального права, що сучасний стан нормативної бази стосовно боротьби із кіберзлочинністю вимагає вдосконалення, особливо необхідне посилення відповідальності в цій сфері. Так, на сьогодні в Кримінальному кодексі України міститься Розділ XVI, який визначає відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і телекомунікацій.

Аналізуючи норми Кримінального кодексу України (далі – КК України) приходимо до висновку, що законодавець занадто диференціює відповідальність за вчинення різних злочинів (див. Таблицю).

Таблиця

Відповідальність за вчинення кіберзлочинів за КК України [2]

Стаття КК України	**Передбачена відповідальність**
Стаття 361. ч. 1.	Штраф від шестисот до тисячі неоподатковуваних мінімумів доходів громадян, або обмеження волі на строк від двох до п’яти років, або позбавлення волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи
Стаття 361. ч. 2.	Позбавлення волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.
Стаття 361-1 ч. 1.	Штраф від п’ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправні роботи на строк до двох років, або позбавлення волі на той самий строк, з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку, які є власністю винної особи.
Стаття 361-1 ч. 2.	Позбавлення волі на строк до п’яти років з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку, які є власністю винної особи.
Стаття 361-2 ч. 1.	Штраф від п’ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавлення волі на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.
Стаття 361-2 ч. 2.	Позбавлення волі на строк від двох до п’яти років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.
Стаття 362 ч. 1.	Штраф від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправні роботи на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було вчинено несанкціоновані зміна, знищення або блокування інформації, які є власністю винної особи.

Стаття 362 ч. 2.	Позбавлення волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи.
Стаття 362 ч. 3.	Позбавлення волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані дії з інформацією, які є власністю винної особи.
Стаття 363 ч. 1.	Штраф від п’ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеження волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.
Стаття 363-1 ч. 1.	Штраф від п’ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеження волі на строк до трьох років.
Стаття 363-1 ч. 2.	Обмеження волі на строк до п’яти років або позбавлення волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено масове розповсюдження повідомлень електрозв’язку, які є власністю винної особи.

Як видно з Таблиці, наведені санкції, що містяться в статтях, включених до Розділу XVI КК України і передбачають відповідальність за кіберзлочини, є настільки різними, що не завжди можна зрозуміти позицію законодавця. Однак, слід зазначити, що негативні наслідки кіберзлочинів за своєю сутністю тотожні, і можуть відрізняютися головним чином розміром завданої шкоди. А відтак вбачається за доцільне в певний спосіб уніфікувати відповідальність. Передбачена законом можливість застосування суддями широкого спектру видів покарань часто дозволяє винним особам за рахунок різного роду впливу на суддівський корпус, в тому числі за рахунок корупційних схем, уникати більш суворої відповідальності, обмежуючись покараннями, які не відображають реального ступеня вини кіберзлочинців та наслідків кіберзлочинів. Тому вважається за доцільне переглянути відповідальність за скоєння кіберзлочинів в бік її уніфікації, тобто розробки декількох (три-чотири) стандартних конструкцій покарання різної тяжкості, виходячи, головним чином, із наслідків, завданих злочинними діяннями, але в той же час враховуючи інші обставини злочину (спосіб скоєння, особа злочинця тощо).

Аналізуючи міжнародну практику регулювання відповідальності за кіберзлочини, приходимо до висновку, що на сьогодні існує загальна тенденція посилення відповідальності в цій сфері. Зокрема, в Японії в 2011 році відбулася реформа Кримінального кодексу, згідно з яким відповідальність за вчинення кіберзлочинів стала більш суворою: за створення і розповсюдження комп’ютерних вірусів передбачається покарання у вигляді позбавленні волі на строк до трьох років та штраф у розмірі до 500 тисяч ієн. Запроваджено покарання і за новий склад злочину – поширення порнографії по електронній пошті, а також порнографії та дитячої порнографії в установах корпоративного та публічного права.

Як зауважує П.П. Андрушко необхідність боротьби з кіберзлочинами нині усвідомили майже всі країни, в яких велике значення мають комп’ютерні технології. Ще 1973 року у Швеції було прийнято закон, згідно з яким встановлена відповідальність за неправомірну зміну, знищення або доступ до записів на комп’ютерних носіях (інформаційні зловживання), до якого вносяться зміни та уточнення майже щорічно, враховуючи особливість нових видів кіберзлочинів. Подібні спеціальні норми про

комп’ютерні злочини були прийняті у США, Великій Британії, Австрії, Канаді, Данії, Австралії, Франції, Португалії та в інших країнах [11, с. 1164-1167].

Що стосується Європейського Союзу, то слід зазначити, що Європарламентом ухвалений проект Директиви про посилення кримінальної відповідальності за кіберзлочини яка регламентує встановлення максимальних термінів за злочини, скоєні у у сфері інформаційного права в країнах-членах ЄС таким чином: два та більше років ув’язнення – за злочини, що кваліфікуються як несанкціоновані втручання чи доступ до інформаційних систем, засобів комунікацій, відомостей та даних, та додатково за навмисне вироблення та збут засобів й приладів для скоєння подібних злочинів. Також встановлюється максимальна міра покарання за кіберзлочини (п’ять років ув’язнення) за напади, що скоєні на інфраструктурні об’єкти, пов’язані з національною безпекою, наприклад, електричні, транспортні, внутрішні інформаційні мережі тощо. Принаймні трирічний строк ув’язнення в межах Єврозони чекає на хакерів, які використовують в злочинних цілях ботнети, що встановлюють масовий контроль за комп’ютерами та інфікують їх вірусними програмами. Треба також візначити, що в подальшому буде впроваджено кримінальну відповідальність не тільки фізичних, а й юридичних осіб за злочини, що скоєні у сфері інформаційного права країн-членів ЄС.

У США боротьба з кіберзлочинністю спершу розпочалася на рівні окремих штатів. На початок 70-х років XX століття відповідні закони були видані в шести штатах, а робота над законопроектами велася у дванадцяти інших. До 1985 року такі акти були прийняті в 47 штатах. У штаті Флорида Закон про комп’ютерні злочини набув чинності 1 січня 1978 року. Він є найбільш ґрунтовним з аналогічних актів інших штатів. Згідно з даним Законом конкретні види комп’ютерних злочинів розподілені на три групи [6]:

злочини проти інтелектуальної власності;

злочини, що завдають шкоди комп’ютерному обладнанню;

злочини проти користувачів комп’ютерів.

Протягом останніх років XXI ст. у США прийнято низку федеральних законів, що створили основу для проведення політики боротьби з кіберзлочинністю [8, с. 79-84].

Отже можна побачити, що за кордоном, у більш розвинутих країнах, законодавство щодо боротьби із кіберзлочинністю розвивається вже давно. І на сучасному етапі відбувається переосмислення органами державної влади, задіяними в цьому процесі, природи, сутності кіберзлочинність та наслідків, яких завдає подібна протизаконна діяльність.

Визначаючи причини посилення відповідальності за скоєння кіберзлочинів, слід відзначити низку особливих рис, притаманних подібного роду правопорушенням, які власне і обумовлюють необхідність застосування до винних осіб більш суворих заходів впливу.

По-перше, негативні наслідки кіберзлочинів частіше за все проявляються не одразу, а лише з часом в процесі реалізації суспільних відносин. Наприклад, це може призвести до того, що інформація чи технологія, яку її користувачі або власники вважають унікальною, вже давно використовується іншими особами, які отримали до неї неправомірний доступ та використовують для задоволення власних потреб. Це спотворює економічний зміст суспільних відносин, а відтак завдає суттєвої шкоди учасникам господарських відносин.

По-друге, особи, які скоюють кіберзлочини характеризуються неординарними розумовими здібностями, що у поєднанні із девіантною поведінкою може призводити до появи нових негативних суспільних явищ, що в свою чергу несе в собі суттєві ризики для користувачів інформації. Так, зокрема, з’явилися такі явища як хакерство, смішінг тощо.

Проблема полягає у тому, що подібні явища можуть певний час розвиватися майже без перешкод, оскільки право не настільки динамічно розвивається, щоб максимально оперативно реагувати на негативні суспільні явища створюючи відповідні захисні механізми суспільних відносин.

По-третє, об’єктом кіберзлочинів часто виступає специфічна інформація яка стосується сфери національної інформаційної безпеки. Це може обумовлювати негативні наслідки кіберзлочинів вже не на корпоративному чи приватному, а на публічному державному рівні. Протиправне заволодіння такою інформацією та її подальше поширення призводить і до більш масштабних негативних наслідків – загрози національній безпеці держави.

В цьому контексті особливої уваги заслуговує таке явище як кібертероризм. Це надзвичайно небезпечний та такий, що постійно прогресує, вид терористичної діяльності, залишення якого поза уваги правоохоронної системи загрожує суттєвими наслідками для суверенітету держави. Тому у вітчизняному законодавстві, окрім відповідальності за кіберзлочини, доцільно розвивати інститут боротьби із кібертероризмом, в тому числі шляхом посилення мір відповідальності за подібні діяння.

Висновки.

Кіберзлочинність, як вид асоціальної та протиправної поведінки, останнім часом отримала новий поштовх до розвитку через появу сучасних комп’ютерних технологій нового покоління. Власне, такий розвиток та диференціація форм кіберзлочинності буде відбуватися кожного разу після досягнення науковцями та технологами нових революційних результатів в сфері інформаційних технологій та комп’ютерних мереж. Це вимагає відповідної реакції з боку держави та компетентних органів в аспекті підвищення безпеки відносин у віртуальній реальності. Оцінюючи зростання негативних наслідків кіберзлочинів, що обумовлюється специфікою інформаційних технологій як засобів реалізації господарської діяльності, та специфіку інформації як об’єкту суспільних відносин, приходимо до висновку про необхідність посилення відповідальності за скоєння кіберзлочинів, цілком доцільного з огляду на ті наслідки, до яких вони призводять, а також на той злочинний потенціал, який розкривається в процесі їх скоєння та використання їх результатів.

Використана література

1. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.01 р. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/994_575

2. Кримінальний кодекс України : Закон України від 05.04.01 р. № 2341-III. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2341-14

3. Про деякі заходи щодо захисту державних інформаційних ресурсів у мережі передачі даних : Указ Президента України від 24.09.01 р. № 891/2001. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/891/2001

4. Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень : Указ Президента України від 14.07.00 р. № 891. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/891/2000

5. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні : Указ Президента України від 31.07.00 р. № 928/2000. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/928/2000

6. Відповідальність за кіберзлочини стає все суворішою. – Режим доступу : http://ukr-pravo.com.ua/index.php?option=com_content&view=article&id=4445:2011-07-11-09-23-13&catid=2 : komentar

7. Волеводз А.Г. Конвенция о киберпреступности : новации правового регулирования // Правовые вопросы связи. – 2007. – № 2. – С. 17-25.

8. Голубєв В.О. Інформаційна безпека : проблеми боротьби з кіберзлочинами / В.О. Голубєв. – Запоріжжя, 2003. – С. 79-84.

9. Довбиш М.О. Кіберзлочинність в Україні : *матеріали Міжнар. наук. конф. [“Наука – от теории к практике”], (Сопот, Польща, 29.03.13 р.).* – Сопот : ТОВ “БТТ”. – 2013. – С. 16-25.

10. Кіберзлочинність можна зупинити тільки разом // Україна : бізнес-ревю. – 2013. – № 5-6. – С. 5

11. Науково-практичний коментар до Кримінального кодексу України / [П.П. Андрушко та ін.] ; ред. П.П. Андрушко та ін. – [2-ге вид., перероб. та доп.]. – К. : Дакор, 2008. – С. 1164-1167.

12. Протасевич А.А. Борьба с киберпреступностью как актуальная задача современной науки // Крминологический журнал ОГУЭП. – 2011. – № 3 (17). – С. 30-37.

13. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики : дис. на соискание науч. степени канд. юрид. наук / М.В. Старичков. – Иркутск, 2006. – С. 109-112.

14. Суслопаров А.В. Компьютерные преступления как разновидность преступлений информационного характера : дис. на соискание науч. степени канд. юрид. наук / А.В. Суслопаров. – Красноярск, 2010. – 210 с.

15. Тропина Т.Л. Киберпреступность. Понятие, состояние, уголовно-правовые меры борьбы : монографія / Т.Л. Тропина. – Владивосток, 2009. – 237 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~