І.В. ЄВРОПІНА
(Національна академія прокуратури України)

ВИДИ ПРОТИПРАВНИХ ДІЯНЬ У СФЕРІ НОВІТНІХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Ключові слова: *комп'ютерні злочини; використання комп'ютерів, комп'ютерні мережі, мережі електрозв'язку, кіберпростір, Інтернет, Інтернет-технології, кримінальна відповідальність.*

Відповідно до доктрини сучасного міжнародного кримінального права злочини з використанням комп'ютерних технологій (інакше «кіберзлочини») віднесені до злочинів міжнародного характеру. Перелік видів кіберзлочинів визначається Конвенцією про кіберзлочинність (2001 р.), яка називає серед інших наступні склади: незаконний доступ до комп'ютерної системи, нелегальне перехоплення технічними засобами комп'ютерних даних, втручання у комп'ютерні данні, втручання у функціонування комп'ютерної системи, підробку та шахрайство, пов'язані з комп'ютерами, правопорушення, пов'язані з дитячою порнографією, тощо.

У п. 14 Доповіді Комітету II Десятого Конгресу ООН 2000 р. з попередження злочинності і поводження з правопорушниками зазначено, що існує дві категорії злочинів: 1) кіберзлочини у вузькому розумінні («комп'ютерні» злочини) — будь-яке протиправне діяння, здійснюване шляхом електронних операцій, метою якого є подолання захисту комп'ютерних систем і оброблюваних ними даних; 2) кіберзлочини в широкому розумінні (злочини, пов'язані з використанням комп'ютерів) — будь-яке протиправне діяння, що вчинюється шляхом або в зв'язку з комп'ютерною системою або мережею, включаючи такі злочини, як незаконне зберігання, пропонування або розповсюдження інформації через комп'ютерні системи або мережі [2, 338]. Кримінальну відповідальність за кіберзлочини як у вузькому, так і широкому розумінні врегульовує Конвенція про кіберзлочинність (2001 р.). Кримінальне законодавства окремо взятих країн світу, визначає карну відповідальність за кіберзлочини лише у вузькому розумінні, що можна підтвердити на прикладі України.

В Особливій частині її Кримінального кодексу є Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Жодна із 6-ти статей цього розділу не містить норми, згідно з якою можна було притягти до відповідальності особу, що вчинила, наприклад, шахрайство шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ч. 3 ст. 190 КК), або окремі суспільно-небезпечні дії, передбачені ст. 200 КК. Як зазначають А.А. Музика та Д.С. Азаров, і варто з цим погодитись, застосування комп'ютерів для вчинення названих діянь є лише певним способом вчинення злочину, який зазвичай не включається до обов'язкових ознак об'єктивної сторони складу злочину. За наявності певних фактичних обставин ці злочини можуть кваліфікуватись за сукупністю зі злочинами, передбаченими Розділом XVI Особливої частини КК України [4]. Потрібно також зауважити, що завдяки застосуванню комп'ютерних технологій значна кіль-

кість «звичайних» злочинів перейшла сьогодні до категорії «кіберзлочинів». До того ж способи їх вчинення істотно полегшились, а «географія» розширилась. До таких злочинів, що перейшли з реального, фізичного світу до кіберпростору, можна назвати тероризм, розповсюдження порнографічної інформації, відмивання грошей тощо [6].

Дослідники зазначають, що «кіберзлочини» мають низку особливостей, завдяки яким вони посягають через комп'ютерні системи на сфери міжнародного правопорядку, і зокрема — на міжнародний обмін інформацією. Сьюзанн В. Бреннер виділяє наступні ознаки «кіберзлочинів», що відрізняє їх від «звичайних» злочинних посягань та значно підвищує їх суспільну небезпечність. По-перше, «кіберзлочин» не вимагає фізичного зближення жертви та суб'єкта злочину в момент вчинення такого. По-друге, «кіберзлочин» є «автоматизованим» злочином. Це означає, що суб'єкт злочину за допомогою комп'ютерних технологій протягом короткого періоду часу може збільшити кількість протиправних діянь до декількох тисяч. По-третє, суб'єкт «кіберзлочину» не підвладний обмеженням, які існують у реальному, фізичному світі. Так, «кіберзлочини» можуть бути вчинені моментально, і тому потребують швидкої реакції у відповідь. І, по-четверте, «кіберзлочинність» і досі залишається новим феноменом, і наука ще не здатна встановлювати моделі розповсюдження різних видів злочинів географічно та демографічно, як це має місце зі злочинами, що вчиняються у реальному, фізичному світі [8]. Окрім криміналістичних проблем, досліджених цією авторкою, існує й низка інших, не врегульованих правових питань. Зокрема, щодо визначення місця злочину, вчиненого за допомогою мережі Інтернет. Право якої держави потрібно застосувати, якщо правопорушник і об'єкт посягання знаходяться у різних країнах? Як має бути вирішено питання про межі можливого та необхідного застосування кримінального права країни до «кіберзлочинів», вчинених поза її територією?

Аллан Р. Стейн зокрема стверджує, що найбільш проблемною характеристикою Інтернету з точки зору юрисдикційної політики є те, що він стирає межу між внутрішньодержавною і міжнародною передачею інформації [9]. Інтернет сформувався та являє собою позатериторіальний засіб комунікації та обміну інформацією, який не має централізованого управління. Кожний індивідуум і його комп'ютер діють автономно та формують єдину транснаціональну мережу, яка виходить за межі географічної концепції державних кордонів. Інтернет-адреси, що підтримуються мережею, нематеріальні, і навіть адреси сайтів, які містять URL-індикатори країни походження, наприклад, «ua», «pl» не обов'язково мають бути точними. Інтернет-адреси є довільними та можуть залишатись незмінними, у той час як сервери переміщаються у фізичному просторі [1, 24-31]. Така особливість Інтернету ставить науку і практику перед необхідністю вироблення нових підходів до протидії злочинам міжнародного характеру з використанням комп'ютерних технологій та побудови юрисдикційної політики стосовно таких злочинних посягань.

Існує декілька основних напрямів вирішення проблеми подальшого регулювання Інтернету та кримінальної відповідальності за злочини міжнародного характеру з використанням комп'ютерних технологій. Відповідно до першого із них рекомендується пристосувати до злочинів, які вчиняються з використанням новітніх інформтехнологій, традиційні принципи кримінальної юрисдикції. Що стосується другого, — пропонується розглядати Інтернет як самостійний «віртуальний» кіберпростір та розробляти нові правила застосування кримінальної юрисдикції щодо злочинів, які у ньому вчиняються.

Прихильники першого напряму вважають, що нові Інтернет-технології автоматично не змінюють правову доктрину кримінальної юрисдикції, і вона може бути застосована до «кіберзлочинів» міжнародного характеру. Правові підстави для поді-

бних дій нібито передбачені Конвенцією про кіберзлочинність (2001 р.). Дійсно, Конвенція визначає традиційну схему кримінальної юрисдикції щодо регульованих злочинів, допускаючи територіальний і національний принципи кримінальної юрисдикції. Частина 1 ст. 22 Конвенції каже, що кожна із Сторін вживає таких законодавчих й інших заходів, які, на її думку, можуть бути необхідними для встановлення юрисдикції стосовно будь-якого злочину, криміналізованого Конвенцією, якщо він вчинений:

a. на її території;

b. на борту судна, яке плаває під прапором такої Сторони, або

c. на борту літака, зареєстрованого відповідно до законодавства такої Сторони, або

d. одним з її громадян, якщо таке правопорушення карається кримінальним законодавством у місці його вчинення, або якщо правопорушення вчинено поза межами територіальної юрисдикції будь-якої Держави.

Однак Конвенція не розтлумачує питання, які «кіберзлочини» слід вважати вчиненими на території даної країни, та поняття «місце вчинення злочину» і залишає це на розсуд національних судів. Міжнародна практика засвідчує, що єдиного підходу до вирішення цього питання на національному рівні немає. Різне тлумачення місця вчинення злочинів, що пов'язані із комп'ютерними технологіями, а так само відсутність його чіткого правового регулювання на міжнародному рівні можуть призвести з одного боку до позитивних конфліктів кримінальних юрисдикцій різних країн, коли дві і більше країни претендують на застосування закону про кримінальну відповідальність щодо одного злочинного діяння, а з іншого — до негативних конфліктів кримінальних юрисдикцій, коли жодна країна не вдається до переслідування вчиненого злочину.

У міжнародній правозастосовчій практиці питання кримінальної юрисдикції поставлене в залежність від існуючого поділу кіберзлочинів за колом об'єктів:

- злочини, що націлені та спричинюють шкоду конкретним об'єктам (наприклад, установі банку, електронній скринці приватної особи тощо);
- злочини, що націлені та посягають на невизначене коло об'єктів (наприклад, у разі розповсюдження комп'ютерних вірусів або порнографічної продукції).

Питання застосування закону держави про кримінальну відповідальність до «кіберзлочинів», які посягають на конкретні об'єкти, найчастіше вирішується за правилами об'єктивної територіальності. Знаходячись в одній країні, особа спрямовує злочинне діяння на територію інших юрисдикцій, застосовуючи сучасні комп'ютерні мережі. Правоохоронні органи країни фізичного місця знаходження правопорушника найчастіше навіть не здогадуються про вчинені ним кримінальні діяння, і виявляють їх за наслідками, які настають в іншій країні. У таких випадках кримінальне переслідування злочинця стає неможливим без міждержавного співробітництва.

Правопорушник притягається до відповідальності на території країни перебування, або ж видається «потерпілій» країні за умов наявності відповідних міжнародних договорів та задоволення інших правових вимог, які супроводжують процедуру екстрадиції (правило подвійної кримінальності, правило невидачі власних громадян тощо). Однак процедура екстрадиції є досить складною і скоріше винятком, ніж правилом розв'язання подібних питань.

Міжнародний досвід також демонструє виняткові випадки, коли «потерпіла» країна вирішує питання про притягнення злочинця до кримінальної відповідальності без звернення до країни його місця знаходження.

Так, у 2000 р. громадянин Російської Федерації О. Іванов, здійснивши «хакерську атаку» на систему захисту корпорації з електронної комерції, яка знаходиться у штаті Коннектикут, США, отримав ключові паролі доступу і контролю над

усією системою. Він погрожував знищити всю комп'ютерну мережу корпорації, якщо керівництво відмовить йому у трудовлаштуванні на посаду експерта з безпеки. О. Іванова запросили на співбесіду до США, де він був заарештований та відданий правосуддю. У суді О. Іванов намагався довести, що суд США не має предметної юрисдикції щодо вчиненого ним злочину, оскільки в момент «хакерської атаки» він знаходився в Росії. Суд відкинув ці аргументи, а у судовому вироку зазначив, що О.Іванов прагнув спричинити своїми діями шкоду на території США, хоча і перебував під час реалізації злочинного наміру за її межами, на території Росії, та застосував до нього статут, що не має прямої екстериторіальної дії [6].

Дещо по-іншому вирішуються питання застосування кримінальної юрисдикції країни до «кіберзлочинів», які посягають на невизначене коло об'єктів та відповідно порушують правопорядок у невизначеній кількості країн. У таких випадках, притягнення особи до кримінальної відповідальності можливе за правилами екстериторіальності, проте із застереженням — за умови наявності в ній кримінальної заборони щодо «кіберзлочинів».

На підставі викладеного можна дійти висновку, що сьогодні країнами світу до «кіберзлочинів» і «кіберзлочинів» застосовуються традиційні принципи кримінальної юрисдикції, засновані на ідеології географічної територіальності. Оскільки технологія сучасних комп'ютерних мереж функціонує поза межами територіального суверенітету та є позатериторіальною за своєю природою, існуючі принципи кримінальної юрисдикції часто стають неефективними і, крім того, породжують низку юридичних питань.

Між тим, право на існування має й інший підхід до регулювання правових відносин в мережі Інтернет, який може стати альтернативою традиційному, оскільки, на нашу думку, краще підходить до реалій сьогодення. Його прихильники пропонують вважати місцем вчинення «кіберзлочину» не територію певної країни або будь-яку іншу географічну територію, а безпосередньо кіберпростір.

Верховний Суд США дав таке визначення кіберпростору: «Унікальний носій, який не знаходиться на певній території, але доступний кожному в будь-якій точці світу через Інтернет» [3, 152]. Інституціональним втіленням кіберпростору є Інтернет, що являє собою глобальну інформаційну систему, яка складається з інших інформаційних систем і дозволяє користувачам обмінюватися інформацією з будь-яким комп'ютером у цій системі [7].

Цілком логічно, з урахуванням вищезазначеного, надати правовому режиму Інтернету статус, аналогічний територіям спільного користування (космічний простір, відкрите море, Антарктида тощо). Це дозволить запровадити відповідальність за протиправні діяння у кіберпросторі згідно з принципом кримінальної юрисдикції, який діє в інших територіях загального користування. Тобто особа, яка вчинила злочин у кіберпросторі, буде нести відповідальність перед країною свого громадянства. Це правило може набути чинності лише за умови прийняття універсального зводу правил користування Інтернетом та запровадження принципу обов'язкового співробітництва між країнами у розслідуванні злочинів, що вчиняються у кіберпросторі [3, 156]. До прийняття відповідних правових актів, правоохоронні органи і суди України, при розслідуванні і розгляді справ про злочини міжнародного характеру, вчинені у кіберпросторі, а так само з використанням комп'ютерних технологій, мають враховувати наступні фактори доцільності застосування кримінальної юрисдикції:

- настання або можливість настання тяжких суспільно-небезпечних наслідків для інтересів держави або її громадян;
- зв'язок із суб'єктом злочину (національність, місце постійного проживання);
- зв'язок злочину і злочинця з територією країни ;

– відповідність правил здійснення кримінальної юрисдикції чинним нормам міжнародного права і міжнародним зобов'язанням держави;
– правові підстави застосування кримінальної юрисдикції іншою державою та вірогідність колізії кримінальних юрисдикцій.

Оцінюючи «кіберзлочини» в історичному ракурсі, згадаємо, що зародились вони в Америці, де у 1945 р. була створена перша ЕОМ (комп'ютер), яка використовувалась для розшифровування німецьких військових кодів, а згодом й з іншою метою. Те саме має місце і в наш час, коли суперкомп'ютери та мережні системи багатоцільової паралельної дії використовуються, в основному, для вирішення завдань інформаційної безпеки, а вже потім — для інших локальних цілей.

З появою та розповсюдженням комп'ютерної техніки в країнах світу факти злочинів з використанням комп'ютерів і передових інформаційних технологій стали масовими, що не могло залишити байдужими криміналістів-практиків і науковців, які побачили в цьому реальну загрозу національній безпеці своїх держав і спрогнозували негативні глобальні наслідки для технологічно розвинутих країн й інформаційного світу в цілому.

Починаючи з 1958 р., дані правової статистики Стенфордського дослідницького інституту так характеризують види «комп'ютерних» злочинів XX століття:

- випадки пошкодження і розкрадання комп'ютерного устаткування, розкрадання інформації;
- шахрайство або розкрадання грошей, здійснені із застосуванням комп'ютерів;
- несанкціоноване використання комп'ютерів або розкрадання машинного часу.

У 1966 р. зафіксований перший випадок використання ЕОМ як інструмента при пограбуванні банку в Міннесоті.

Першою людиною, що застосувала ЕОМ для вчинення податкового злочину на суму 620 тис. доларів і постала за це перед американським судом у 1969 р., був Альфонсо Конфессоре.

Подальша історія «комп'ютерних» злочинів відмічена такими найбільш «яскравими» подіями:

- кінець 70-х — пограбування «Секьюріті пасифік банк» (10,2 млн. доларів);
- 1979 р. — комп'ютерне розкрадання у Вільнюсі (78584 крб.);
- 1984 р. — повідомлення про перший в 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.

Початок XXI століття ознаменувався широким впровадженням на світовому рівні комп'ютеризованих (автоматичних) інформаційно-технологічних систем у виробничій, комерційній, банківській та інших сферах, у зв'язку з чим головною і водночас невідкладною для вирішення проблемою стала розробка адекватної системи захисту цих систем від несанкціонованого вторгнення. Проблема загострювалась пропорційно зростанню обсягів інформації, обіг якої забезпечувався названими інформаційно-технологічними сис-

темами, в тому числі й переважно завдяки активному функціонуванню глобальної комп'ютерної мережі Інтернет.

Не обійшов процес розвитку комп'ютерної інфраструктури і Україну. Її національні фінансові установи, а так само й інші юридичні та фізичні особи отримали доступ до міжнародних платіжних систем, електронного бізнесу, різного роду міжнародних проектів і програм, наприклад, таких як дистанційні освіта, науково-дослідницька діяльність тощо. Чисельність користувачів мережі Інтернет перевищила мільйонну межу.

Водночас із позитивом виявили себе й чисельні недоліки, які можна вважати своєрідним виміром зворотного боку технічного прогресу. Надшвидкими темпами почали зростати злочини з використанням можливостей комп'ютерної мережі Інтернет і новітніх комп'ютерних технологій. З'явились нові кваліфіковані види злочинів — «кібертероризм», «кібершахрайство», «кіберрозкрадання», «кіберпорнографія» тощо.

Специфіка цих злочинів не вимагала ані ретельного готування до них, ані часу для втілення злочинного замислу. Широка географія, віддаленість об'єкта посягання (за тисячі і сотні тисяч кілометрів від місця вчинення злочину), складнощі з виявленням, доведенням вини, а так само висока дохідність, зробили цей вид злочинної діяльності одним з найбільш привабливих для «фахівців» злочинного світу.

За даними Інтерполу, оголошеними на Шостому засіданні Робочої групи зі співробітництва правоохоронних органів країн Центральної та Східної Європи (в серпні 2000 р.) у сфері боротьби з «кіберзлочинністю», доходи злочинців, пов'язані з незаконним використанням новітніх технологій, посіли третє місце в світі після доходів від торгівлі наркотиками і зброєю [5]. А за повідомленням, зробленим агентством Reuters, обіг коштів, що викрадалися і вимагалися «кіберзлочинцями» в 2004 р., склав 105 млрд. дол. США.

За висновком американських експертів, середня вартість збитку від одного «кіберзлочину» в США становить 500 тис. дол., тоді як одне фізичне пограбування банку обраховується у 3,2 тис. дол. За заявою ФБР, американські бази даних щомісяця зазнають понад тисячу атак іноземних хакерів.[1] Збитки від одного «кіберзлочину» на Заході складають в середньому від 450 тис. до 1 млрд. дол. США. Щорічні втрати фірм США — 100 млрд. дол., Великобританії — 4,45 млрд. дол., країн Західної Європи — 39 млрд. дол.

Відповідно до соціологічного опитування, проведеного Інститутом комп'ютерної безпеки та ФБР, 57% організацій-респондентів вважають комп'ютерну мережу Інтернет місцем організації та реалізації небажаних інформаційних і електронних атак, 30% — джерелом несанкціонованого проникнення до їх комп'ютерних мереж сторонніх осіб, 26% — заявили про факти крадіжки інформації з обмеженим доступом та приватного характеру через Інтернет.

Не випадково злочини у цій сфері ще у 1992 р. були внесені Організацією Об'єднаних Націй до списку 14 видів транснаціональних злочинів, поставивши їх в один ряд із «відмиванням» грошей, терористичною діяльністю, організованим наркобізнесом, крадіжкою витворів мистецтв, інтелектуальної власності, незаконною торгівлею зброєю, захватом повітряних суден, морським піратством, заволодінням наземного транспорту, шахрайством, екологічними злочинами, торгівлею людьми, людськими органами і тканинами.

Детальне висвітлення проблем «кіберзлочинності» відбулося на першому міжна-

[1] *Лише упродовж доби після початку військових дій в Іраку «хакерським» атакам було піддано понад 400 сайтів мережі Інтернет, під час яких застосовувався так званий «іракський» комп'ютерний вірус. Розробники цього вірусу, використовуючи загальний інтерес до перебігу вказаних подій, надсилали електронне повідомлення з написом «Go USA!!!» та пропозицією проглядання останніх фотографій з місця військових подій. Серйозні неприємності очікували тих, хто пристав на таку пропозицію: їх комп'ютери, локальні мережі були інфіковані, системи захисту пошкоджені, системні програми, файли, важлива інформація знищені.*

родному стратегічному Конгресі «E-Crime Congress 2002», що проходив у Лондоні в грудні 2002 р. Ініціатором та організатором цього Конгресу виступив Національний центр по боротьбі із злочинами у сфері високих технологій (National Hi-Tech Crime Unit — NHTCU) — перша в історії Великобританії національна правоохоронна організація, завданням якої є боротьба з «комп'ютерною» злочинністю та співпраця з іншими правоохоронними структурами.

У роботі конгресу «E-Crime» взяли участь близько 400 делегатів, зокрема, з Австралії, Нової Зеландії, Кореї, Гонконгу, Росії, Латвії, США, які представляли державні та недержавні організації, що займаються проблемами захисту інформації та розслідуванням комп'ютерних злочинів. Своїх делегатів репрезентували також МВС Великобританії, Інтерпол, ФБР, Управління «Р» (Росія), Microsoft, Symantec, IBM, Sun Microsystems Ltd., VISA, MasterCard, eBay, Bank of New York, Swedbank.

На Конгресі наголошувалося, що високотехнологічна злочинність, до того ж в організованих формах, зростає високими темпами, «завдячуючи» насамперед глобальній мережі Інтернет. Адже знаходячись у мережі, можна порушувати закон на відстані, незалежно від громадянства та місця перебування, легко одурювати людей, приховувати докази і викрадене. Для критичних інфраструктур країн світу, їх економічної, екологічної, військової безпеки такі дії являють значну небезпеку, про що свідчать дані, наведені в одній із доповідей учасників Конгресу.

Тільки у США 90% організацій щорічно виявляють порушення інформаційних систем (у жовтні 2002 р. кібернетична атака упродовж години вивела з ладу 9 із 13 головних комп'ютерів керівників глобальним рухом в мережі ІНТЕРНЕТ); 80% організацій підтверджують фінансові збитки (один лише вірус NIMDA спричинив матеріальну шкоду у розмірі більше 1,8 млрд. фунтів); щорічно відбувається розкрадання приватної інформації на суму понад 38 млрд. фунтів.

За компетентними прогнозами в недалекому майбутньому можливе стрімке зростання кількості «кіберзлочинів», і передусім таких особливо небезпечних як «кібервійни», «кібертероризм», «кібершпигунство» тощо. За повідомленнями інформаційного агентства Washington ProFile, терорист номер один — Усама Бен Ладен отримав комп'ютерну програму «Promis» (розробник — компанія Inslaw Inc), що дозволяє йому проникати в урядові інформаційні мережі США та інших країн і відслідковувати потоки інформації з обмеженим правом доступу. Беручи до уваги, що користувачами цієї програми поряд з іншими урядовими організаціями є ФБР і ЦРУ (США), неважко уявити масштаб загрози і пов'язаних з нею наслідків. Якщо Бен Ладен дійсно має «Promis», він може спостерігати за діями спецслужб, отримувати інформацію про їх стратегічні плани, без проблем уникати переслідувань, а також «відмивати брудні гроші» та вчиняти інші протиправні дії. Фахівці не виключають й того факту, що назване програмне забезпечення використовувалося «Аль Каєдою» для підготовки та проведення терористичних атак на Нью-Йорк і Вашингтон 11 вересня 2001 р. Ймовірність його використання з такою ж метою можлива і в подальшому.

Прогнозування такого розвитку подій спонукає до пошуку і впровадження адекватних засобів протидії, що мають базуватись насамперед на досягненнях в галузі кримінального права і криміналістики, ґрунтовних наукових дослідженнях міжнародного та національного значення.

Список літератури:

1. *Ансельмо Э.* Киберпространство в международном законодательстве: опровергает ли развитие Интернета принцип территориальности в международном праве? / Э. Ансельмо

// Экономические стратегии. — 2006. — № 2.

2. *Волевоз А.Г.* Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волевоз. — М.: Юрлитинформ, 2002.

3. *Мазолина О.В.* Вопросы международно-правового регулирования Интернета / О.В. Мазолина. — Московский журнал международного права. — 2004. — № 4.

4. *Музика А.А.* Законодавство України про кримінальну відповідальність за комп'ютерні злочини: науково-практичний коментар і шляхи вдосконалення / А.А. Музика, Д.С. Азаров. — К: Вид-во Паливода А.В., 2005.

5. *Сабадаш В.* Компьютерная преступность — проблемы латентности / В. Сабадаш. — Джерело: http://www.crime-research.ru/articles/sabodash06/

6. *Юртаєва К.В.* Визначення місця вчинення злочинів з використанням комп'ютерних технологій [Електронний ресурс]/ К.В. Юртаєва. — Режим доступу : http://www.nbum.gov.ua

7. ASLU v.Reno,929 F. Supp 824 (E.D.Pa.1996).

8. *Brenner S.W.* Toward a Criminal Law for Cyberspace A New Model of Law Enforcement? 30 Rutgers Computer & Tech. L.J.1 (2004).

9. *Stein A.R.* Simposium: Personal Jurisdiction and the Internet: Seeing Due Process Through the Lens of Regulator Precision. 98 Nw. U.L.Rev. 411 (2004).

РЕЗЮМЕ

В статье рассматриваются вопросы о сути противоправных деяний в сфере новейших информационных технологий, отнесенные по классификаторам международного и национального права к преступным и подлежащие уголовному преследованию.

SUMMARY

In the article questions are examined about essence of illegal actions in the field of the newest information technologies, classified by classifiers of international and national law to criminal and subject to the criminal proceeding.

Рекомендовано кафедрою кримінального процесу та криміналістики

Подано 10.09.10