УДК 343.974: 351.864.1: 65.012.8

Гавловський Владислав Данилович —
начальник відділу Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України, кандидат юридичних наук, сстарший науковий співробітник,

Бутузов Віталій Миколайович —
головний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України, кандидат юридичних наук, сстарший науковий співробітник

Протидія організованій злочинності у сфері інформаційних технологій як окремий аспект кримінологічної безпеки

У статті розглянуто основні питання протидії організованій злочинності у сфері інформаційних технологій як окремий аспект кримінологічної безпеки. Визначено загальні поняття та структуру організованої злочинності у сфері інформаційних технологій, а так само проблеми, що існують при протидії цьому явищу в Україні.

Ключові слова: організована злочинність, кіберугрупування, кіберзлочинність, кримінологічна безпека, інформаційні технології, мережа Інтернет.

Розвиток глобальних інформаційно-телекомунікаційних мереж став потужним каталізатором багатьох інтеграційних процесів у сучасному суспільстві, створив умови для реалізації програм оперативного доступу до інформаційних, інтелектуальних та матеріальних ресурсів, розташованих на віддалених територіях. Він став також і потужним фактором для розвитку організованої злочинності та подальшої її трансформації. Інформаційно-телекомунікаційні засоби дозволили організованим злочинним групам усунути територіальні бар'єри, що розділяли різні організовані злочинні групи, і об'єднати їхні зусилля для

спільного досягнення обраної злочинної мети. Із цими процесами пов'язана поява особливих соціальних формацій — злочинних мережевих або віртуальних співтовариств, які створюються на території обраної ними держави або кількох держав.

За останній час характер і масштаби поширення злочинів у сфері інформаційних технологій значно змінилися. Небезпека, яку вони несуть для особи, суспільства та держави значно збільшилася. На сьогодні такі злочинні дії характеризуються розширенням масштабів загрози та посиленням їх економічної і політичної складових. Середовищем учинення злочинів у сфері інформаційних технологій стають глобальні інформаційні мережі, які організовані злочинні угруповання використовують не тільки для вчинення суто комп'ютерних злочинів (незаконного проникнення в корпоративні та приватні бази даних, мережеве шахрайство, розповсюдження вірусних програм тощо) але й активно використовують як агітаційний та комунікаційний засіб терористичних організацій, для підбурювання вчинення злочинів на ґрунті расизму, екстремізму та ксенофобії, створення нелегальних ринків збуту зброї, вибухових пристроїв, наркотиків, людських органів, розповсюдження порнографічної продукції за участю дітей, а також як засіб переслідування з метою шантажу тощо. Все більшого обсягу набирає використання в мережі Інтернет електронних платіжних систем при шахрайствах і в процесі "відмивання" коштів та фінансування тероризму.

У таких умовах гостро відчувається необхідність забезпечення кримінологічної безпеки у сфері інформаційних технологій, як однієї з важливих складових національної безпеки країни.

Слід зазначити, що проблему кримінологічної безпеки варто визнати малодослідженою як у класичній кримінології, так і в теорії безпеки, що активно стала розроблятися в Україні з початком здійснення стратегічних реформ. У пострадянській кримінології, за винятком досліджень С. Я. Лебедєва та В. О. Плєшакова, змістовний аналіз цієї проблеми не проводився. У наукових працях з теорії безпеки розглянута тема, як правило, розкривається лише в контексті економічної безпеки.

Разом з тим, окремі аспекти протидії організованій злочинності у сфері інформаційних технологій висвітлювались у працях таких правників, як Т. В. Авер'янова, В. Б. Вєхов, Ю. В. Гаврилін, В. О. Голубєв, В. Є. Козлов, В. В. Крилов, В. О. Мещеряков, В. О. Мілашев, О. І. Мотлях, Л. П. Паламарчук, В. Ю. Рогозін, О. А. Самойленко та інших. Однак, не дивлячись на беззаперечну теоретичну й практичну значимість зазначених досліджень, у цілому можна констатувати недостатню розробленість поняття кримінологічної безпеки, неповноту запропонованих змістовних характеристик організованої злочинності у сфері ін-

формаційних технологій та недостатню визначеність підходів до її аналізу і забезпечення з позицій найбільш зацікавлених суб'єктів.

Зазначимо, що під кримінологічною безпекою слід розуміти стан захищеності законних інтересів особи, суспільства і держави від зовнішніх та внутрішніх погроз, джерелами яких виступають явища, певною мірою пов'язані зі злочинністю, суспільно небезпечними посяганнями, кримінальною діяльністю, інтересами криміналітету.

Таким чином, забезпечення протидії організованій злочинності у сфері інформаційних технологій слід вважати складовою частиною кримінологічної безпеки, яка має певну ієрархічну структуру і специфічну спрямованість.

Водночас, злочинну діяльність у сфері інформаційних технологій на сучасному етапі розвитку, враховуючи особливості функціонування даної сфери, необхідно розуміти як систему об'єднаних загальними мотивами і цілями злочинних дій як у фізичному, так і в електронному середовищі, пов'язаних з використанням методів автоматизованої обробки даних, заснованих на використанні інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем і мереж, а також з використанням самих інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем і мереж.

Злочини у сфері інформаційних технологій на сучасному етапі розвитку необхідно розглядати як передбачені кримінальним законом суспільно-небезпечні протиправні дії, вчинені з використанням зазначених вище методів.

У ході проведення анкетування співробітників правоохоронних органів було визначено найбільш характерні риси, притаманні злочинам у зазначеній сфері, які у відсотковому відношенні характеристики розподілились наступним чином:

— транскордонність — 57 %;

— висока технічна озброєність злочинців — 53 %;

— використання як знарядь злочину інформаційних та телекомунікаційних технологій — 53 %;

— високий рівень латентності — 42 %;

— електронне середовище, як місце вчинення злочину — 36 %;

— організований характер — 27 %;

— корупційні зв'язки у правоохоронних органах — 8 % [1 ; 2 ; 3].

Разом з тим, практичними працівниками правоохоронних органів було зазначено, що однією з найхарактерніших рис, притаманних зазначеній категорії злочинів, є надзвичайно високий рівень латентності. На думку 67 % респондентів виявляється лише близько 10 % правопорушень, 29 % респондентів вважають, що виявляється близько поло-

вини правопорушень. Окремі респонденти взагалі відзначили, що виявляється навіть менше 5 % злочинів [1 ; 2 ; 3].

Зарубіжні дослідники так само відмічають надвисокий рівень латентності. Так, за даними Стенфордського дослідного інституту лише 10—15 % таких злочинів потрапляє в офіційну статистику. Згідно з даними тільки в одному з 20 випадків про факти злочинів у сфері інформаційних технологій повідомляється в поліцію [4].

Як уже зазначалося вище, на сучасному етапі криміналізація суспільства обумовлює поширення організованої злочинності у середовищі глобальних інформаційних мереж, які давно вже перетворилися в електронний аналог суспільного життя. Як відмічають фахівці, найбільш характерним для сучасних організованих злочинних груп є зростання їх кримінального професіоналізму та подальше вдосконалення технічної оснащеності, що базується на новітніх досягненнях науково-технічного прогресу.

Тому, важливою умовою підвищення ефективності протидії організованій злочинності у середовищі глобальних інформаційних мереж стає знання специфіки злочинних процесів, пов'язаних з функціонуванням цього середовища.

Поширення глобальних інформаційних мереж та розвиток системи суспільних відносин в їх середовищі призвели до появи такого феномену, як кіберзлочинність. У науковій літературі висвітлювалися лише окремі аспекти організованих форм кіберзлочинності, але відсутнє визначення поняття організованої кіберзлочинності, яке має важливе теоретичне і практичне значення для подальшого вдосконалення правотворчої та правозастосовної діяльності.

Організована злочинність у мережі Інтернет знаходить свій прояв у вчиненні конкретних злочинів. При цьому, як зазначалось вище, особливості функціонування мережі Інтернет надають можливість організованим злочинним угрупованням вчиняти традиційні злочини новими способами, отримувати від злочинної діяльності надприбутки при низьких ризиках викриття (вимагання, шахрайства, "відмивання" коштів, незаконне надання інформаційних та телекомунікаційних послуг тощо).

Кримінальні структури адаптують можливості комп'ютерних інформаційних технологій до традиційних сфер злочинного "бізнесу", формуючи нові його напрямки. Крім того, перетворення різних форм організованої злочинності в Інтернет-злочинність тісно пов'язане з іншою тенденцією — організована злочинність стає причетною до того, що називається "білокомірцевою злочинністю".

Фахівці вважають, що злочинність у сфері інформаційних технологій стає одним із найбільш прибуткових видів діяльності організованих злочинних угруповань. Доходи від зазначених злочинів, за оцін-

ками Інтерполу, на початок тисячоліття посідали третє місце після доходів наркоділків та постачальників зброї.

У сфері інформаційних технологій, на даний період їх розвитку, можна виділити такі види організованої злочинності:

— традиційна організована злочинність (як загальнокримінальної, так і економічної спрямованості), пов'язана з поширенням традиційними організованими злочинними угрупованнями свого впливу на сферу інформаційних технологій (наприклад, використання комп'ютерних мереж при розповсюдженні наркотичних засобів, залучення окремих хакерів до злочинної діяльності тощо);

— "білокомірцева" організована злочинність у сфері інформаційних технологій, пов'язана з використанням особливостей сучасних методів автоматизованої обробки інформації для протиправного збагачення (наприклад, протиправне надання інформаційних або телекомунікаційних послуг, порушення авторських прав тощо);

— організована кіберзлочинність (організована злочинність у віртуальному просторі), пов'язана з діяльністю у кіберпросторі організованих злочинних угруповань його користувачів (наприклад, злочинна діяльність у кіберпросторі співтовариств хакерів, кардерів тощо).

Розглядаючи організовану кіберзлочинність як підвид загальної організованої злочинності, доцільно взяти за основу традиційне визначення організованої злочинності у чинному законодавстві України — сукупність злочинів, що вчиняються у зв'язку зі створенням та діяльністю організованих злочинних угруповань.

При цьому ознаками організованої кіберзлочинності є: сукупність злочинів певного виду — кіберзлочинів; специфічне середовище діяльності особливих організованих злочинних угруповань — кіберпростір; особливі форми організованих злочинних угруповань у зазначеному середовищі — кіберугруповання.

Отже, логічним буде визначити організовану кіберзлочинність як сукупність кіберзлочинів, що вчиняються у зв'язку зі створенням та діяльністю у кіберпросторі організованих злочинних угруповань (кіберугруповань).

Під кіберзлочинами (кібернетичними злочинами) пропонується розуміти злочини, пов'язані з протиправним використанням кібернетичних комп'ютерних систем (мереж).

До протиправного використання кібернетичних комп'ютерних мереж у загальному вигляді можна віднести: несанкціоноване отримання прав управління такою системою (наприклад, використання шкідливого програмного забезпечення спотворення інформації про стан об'єкту в каналі зворотного зв'язку та спотворення керуючого сигналу в каналі прямого зв'язку тощо) та її нерегламентоване використання (наприклад, для

спричинення аварії на виробництві, дезорганізації діяльності підприємства тощо), а також створення та використання у злочинних цілях однієї кібернетичної комп'ютерної системи проти іншої (наприклад, створення мережі "зомбованих" комп'ютерів для здійснення атак на web-сайти, створення несанкціонованого автоматизованого робочого місця у системі електронного переказу коштів тощо).

Вітчизняними та зарубіжними дослідниками відмічається, що висока соціальна небезпека кіберзлочинності випливає, насамперед, із суспільних відносин, яким вона загрожує, а також з її транснаціонального та організованого характеру. Хоча у Конвенції Ради Європи про кіберзлочинність (ратифікована Україною у 2005 році) не розкрито поняття кіберзлочину, проте визначено перелік протиправних діянь, за які на національному рівні повинна встановлюватися кримінальна відповідальність. Тлумачення положень даної Конвенції та Додаткового протоколу до неї, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи (ратифікований Україною у 2006 році), дозволяє віднести до кіберзлочинів лише такі злочинні посягання:

— проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, вчинені з використанням технічних засобів і комп'ютерних даних;

— пов'язані з комп'ютерами (комп'ютерна підробка, комп'ютерне шахрайство);

— пов'язані з виробленням, володінням або пропонуванням громадськості чи наданням доступу через комп'ютерні системи, розповсюдженням, передаванням або набуттям за допомогою комп'ютерних систем інформації, яка за своїм змістом є: дитячою порнографією; матеріалами расистського та ксенофобного характеру; погрозами з расистських та ксенофобних мотивів; образами з расистських та ксенофобних мотивів; запереченням, значною мінімізацією, схваленням або виправданням геноциду чи злочинів проти людства; пособництвом та підбурюванням до вчинення будь-якого з правопорушень расистського та ксенофобного характеру;

— пов'язані з порушенням за допомогою комп'ютерних систем авторських і суміжних прав, учинені свідомо, в комерційних розмірах [5].

У кіберпросторі виділяють систему суспільних відносин, що виникають у результаті інформаційної взаємодії суб'єктів Інтернет-співтовариства — сформованої в процесі спільної діяльності відносно стійкої системи зв'язків і відносин між користувачами мережного інформаційного простору. При цьому, загальна схема інформаційного процесу певного суб'єкта залишається незмінною й у кіберпросторі,

проте цей процес супроводжують інші (специфічні) загрози, пов'язані з особливостями існування і передачі інформації в новому середовищі.

Усі переваги кіберпростору залишаються перевагами, і не стають недоліками, доки не з'являється індивід — учасник Інтернет-спілкування, налаштований агресивно, зацікавлений у втручанні в сферу Інтернет-відносин з метою одержання матеріальної вигоди, або з хуліганських спонукань; особливості технологій мережі Інтернет, що допомогли їй поширитися по всьому світу, в той же час створюють сприятливі можливості для багатьох видів злочинної діяльності.

Зазначене дозволяє зробити висновок, що наявність системи суспільних відносин та особливого психологічного середовища у мережі Інтернет сприяє встановленню у кіберпросторі стійких взаємозв'язків між кримінально орієнтованими особами, що, у свою чергу, призводить до утворення в мережному середовищі їх віртуальних співтовариств (організованих злочинних кіберугруповань).

З розвитком глобальних інформаційних мереж (зокрема, мережі Інтернет), а також системи суспільних відносин у кіберпросторі, діяльність злочинних кібертовариств набуває все більш організованого характеру, відзначається стійка тенденція до об'єднання хакерів у групи, в тому числі міжнародні, для вчинення великомасштабних злочинів.

Аналіз процесів, пов'язаних зі створенням та діяльністю кібертовариств, дозволяє відмітити у них характерні риси, притаманні організованим злочинним угрупованням у реальному світі, а саме:

— кількісний склад учасників (користувачів мережі);

— попередня зорганізованість цих осіб в об'єднання з метою вчинення злочинів (на основі використання комунікаційних можливостей мережі Інтернет), у тому числі й зорганізованість в об'єднання за попередньою змовою для спільної діяльності з метою:

а) безпосереднього вчинення учасниками злочинної організації тяжких або особливо тяжких злочинів;

б) керівництва чи координації злочинної діяльності інших осіб;

в) забезпечення функціонування як самої злочинної організації, так і інших організованих злочинних груп;

— стійкість цих об'єднань та їх ієрархічність (об'єднання навколо певного веб-сайту злочинної спрямованості з різними правами доступу до нього);

— наявність єдиного плану для вчинення кіберзлочинів, відомого всім учасникам групи та розподілу функцій учасників групи, спрямованих на досягнення цього плану.

Крім зазначених характерних рис організованої злочинності у сфері інформаційних технологій на сучасному етапі до них слід віднести ще такі:

— набуття характеру промислу (незаконні дії з персональними даними (викрадення, розповсюдження) стали окремим видом бізнесу; викрадення ідентифікаційних даних осіб, використання яких дозволяє злочинцям отримувати доступ до чужих банківських рахунків, безоплатно користуватися послугами Інтернет-провайдерів та операторів зв'язку);

— наявність складних видів діяльності, які здійснюються в широких масштабах шляхом створення та експлуатації ринків незаконних товарів і послуг, а також надання законних послуг і товарів у незаконній формі (несанкціонована зміна маршрутизації міжнародного телефонного трафіку, шахрайство як операторів зв'язку, так і абонентів телекомунікаційних компаній);

— потреба у спеціальних навичках і професіоналізмі з боку представників злочинного бізнесу (інформація щодо реквізитів (персональних даних) сторонніх осіб привласнюється за допомогою методів і засобів соціоінженерії та спеціально розроблених програм для незаконного втручання до комп'ютерів, систем, комп'ютерних мереж і мереж електрозв'язку; з'явилися нові злочинні напрямки добування інформації: "фішинг", "фармінг", "вішинг" та ін.);

— здійснення злочинної діяльності за умовою координації та конспірації (реальні кардинг-портали: BOA Factory, Qwertycc. com, StealthDivision, Shadowcrew, CarderPortal, DumpsMarket, Mazafaka. cc, CardersArmy; реальні Інтернет-псевдоніми: "Klukva", "SCRIPT", "LIRATTO", "LIR L", "Duk", "Rudik Duk", "Dark", "Leviafan", "Myo", "Raiden"; використання позабанківських електронно-платіжних систем: WebMoney, E-Gold, Western Union, PayPal, Roboxchange);

— використання системи захисту від соціального контролю із застосуванням насильства, залякування, корупції;

— здійснення розмивання кордонів між організованою злочинністю та IT- бізнес-злочинністю ("білокомірцевою");

— одержання фінансового прибутку незаконним способом з подальшою його легалізацією, проникнення в дохідні законні види діяльності, повна або часткова монополізація ринків та отримання влади.

Узагальнюючи вищенаведене, до характерних ознак організованої кіберзлочинності, як окремого виду організованої злочинності у сфері інформаційних технологій, необхідно віднести:

— сукупність протиправних діянь (кіберзлочинів), учинених шляхом використання кібернетичних комп'ютерних систем управління та обробки інформації (кіберзлочинність);

— вчинення злочинів даного виду в зв'язку зі створенням та діяльністю організованих злочинних кіберугруповань — кримінально орієнтованих співтовариств користувачів кіберпростору;

— середовищем вчинення кіберзлочинів та діяльності організованих злочинних кіберугруповань є кіберпростір — штучне електронне середовище існування інформаційних об'єктів у цифровій формі, створене у результаті функціонування кібернетичних комп'ютерних систем.

Розуміння сутності організованої злочинності у сфері інформаційних технологій та процесів, що відбуваються у кіберпросторі у зв'язку з діяльністю організованих злочинних кіберугруповань, сприятиме розробці нових, більш ефективних методів і засобів боротьби як з даним видом організованої злочинності, так і організованою злочинністю у сфері інформаційних технологій.

До числа основних причин та чинників розвитку організованої злочинності у сфері інформаційних технологій можна віднести наступні:

— нездатність більшості держав здійснювати ефективний контроль над національним сегментом інформаційного простору через те, що: по-перше, проти цього виступає значна частина світової спільноти, яка дбає про права та свободу особи; по-друге, для такого контролю ще немає сформованої правової бази (ані національної, ані міжнародної), розвиток якої відстає від розвитку інформаційно-телекомунікаційних технологій; по-третє, відсутність відповідних ефективно діючих правоохоронних структур; по-четверте, для його впровадження необхідні значні фінансові, технологічні та кадрові ресурси;

— злочинність у сфері інформаційних технологій має не тільки організований характер, а ще й транснаціональний, який у даному випадку полягає, по-перше, у використанні інформаційно-телекомунікаційних систем та мереж, які не мають державних кордонів; по-друге, у наймі, використанні фахівців ІТ-галузі з інших країн світу та здійсненні злочинних посягань, проявів наслідків на території обраних злочинцями держав та, по-третє, латентність злочинності в сфері інформаційних технологій, яка перевищує рівень латентності організованої злочинності в інших галузях;

— відсутність достатньої судової практики по кримінальних справах щодо організованої злочинності у сфері інформаційних технологій;

— геополітичні чинники: незацікавленість провідних "гравців" (держав, ТНК) в розвитку інших національних технологій та посилення контролюючих органів;

— політичну, економічну, соціальну нестабільність у суспільстві та корупцію;

— життєздатність транснаціональних злочинних організацій, що пов'язана з ігноруванням державних кордонів, національного суверенітету, можливістю вибору зручної юрисдикції, у той час як міжнародні та національні сили, що ведуть з ними боротьбу, зобов'язані діяти за правовими нормами.

Низька ефективність протидії проявам організованої злочинності у сфері інформаційних технологій в Україні обумовлюється:

— недостатньою врегульованістю суспільних відносин у сфері інформаційних технологій (чинне законодавство не встигає за процесом інформатизації, впровадженням все новіших технологій обробки інформації);

— відсутністю у чинному законодавстві, що регулює боротьбу з організованою злочинністю, положень, які б враховували особливості цієї боротьби у специфічному середовищі кіберпростору;

— відсутністю в Україні Міжвідомчого центру по боротьбі з кіберзлочинністю, що координував би діяльність усіх правоохоронних органів у цьому напрямку (у т. ч. і боротьбу з організованою злочинністю у цій сфері);

— відсутністю у складі МВС України повноцінного спеціалізованого підрозділу по боротьбі з кіберзлочинністю (у тому числі відсутністю спеціалістів такого напрямку в ГУБОЗ МВС України).

Зазначене підтверджується проведеним анкетуванням. Так, за оцінкою самих правоохоронців сьогодні ефективність діяльності правоохоронних органів у боротьбі зі злочинами у сфері інформаційних технологій знаходиться на середньому та низькому рівнях (43,3 % та 35 % респондентів відповідно). 16,3 % респондентів узагалі зазначили, що сьогодні ефективність діяльності правоохоронних органів знаходиться на дуже низькому рівні. Лише 8,8 % опитаних вказали, що цей показник є достатнім. Разом з тим, правоохоронці визначили чинники, які, на їхню думку, також впливають на ефективність боротьби із зазначеною категорією злочинності [1, 2, 3].

З огляду на гостроту та актуальність питання протидії новітнім загрозам і викликам, так само і організованій злочинності, яка постійно трансформується, у стратегічній перспективі, особливої уваги набуває проблематика адекватного формування організаційної та функціональної структури державного сектора безпеки, який на сьогодні не завжди відповідає поставленим перед ним завданням. Настала необхідність у новому підході щодо питання протидії транснаціональній організованій злочинності, коли у процесі створення ефективної спеціальної організаційно-функціональної системи протидії транснаціональній організованій злочинності потрібно формувати відносини та об'єднувати зусилля різних силових відомств. У питанні створення такої системи повинні бути зацікавлені й розвідувальні органи, які мають функції по захисту державних інтересів, як за кордоном, так і всередині держави.

Список використаних джерел

1. Про результати анкетування працівників експертних установ МВС України з окремих питань визначення шляхів удосконалення протидії організованій злочинності у сфері інформаційних технологій та особливостей розслідування комп'ютерних злочинів, вчинених із використанням мережі Інтернет [К. В. Тітуніна] : аналіт. довідка, № 289 від 17 листоп. 2009 р. — К. : Міжвід. наук.-досл. центр з проблем б-би з орг. злочинністю при РНБО України, 2009. — 21 с.

2. Про результати анкетування працівників слідчих підрозділів МВС України з окремих питань визначення шляхів удосконалення протидії організованій злочинності у сфері інформаційних технологій та особливостей розслідування комп'ютерних злочинів, вчинених із використанням мережі Інтернет [К. В. Тітуніна] : аналіт. довідка, № 294 від 20 листоп. 2009 р. — К. : Міжвід. наук.-дослід. центр з проблем б-би з орг. злочинністю при РНБО України, 2009. — 30 с.

3. Про результати анкетування оперативних працівників з питань пошуку і фіксації фактичних даних про злочини у сфері високих технологій [В. П. Шеломенцев] : аналіт. довідка, № 20 від 20 листоп. 2009 р. — К. : Міжвід. наук.-досл. центр з проблем б-би з орг. злочинністю при РНБО України, 2009. — 27 с.

4. Security Gazette. — 1989. — P. 7. — September.

5. Конвенція Ради Європи про кіберзлочинність : ратифіковано із застереженнями і заявами Законом України від 7 верес. 2005 року № 2824-IV / [Електронний ресурс]. — Режим доступу :
http://zakon1. rada. gov. ua/cgi-bin/laws/main. cgi? nreg=994_575.

В статье рассмотрены основные вопросы противодействия организованной преступности в сфере информационных технологий как отдельный аспект криминологической безопасности. Определены общие понятия и структуру организованной преступности в сфере информационных технологий, а так же проблемы, которые существуют при противодействии этому явлению в Украине.

The article is dedicated to the main questions of counteraction to organized crime in the information technologies sphere as a separate aspect of the criminological security. General concepts and structure of organized crime in the information technologies sphere, and also the problems existing during the counteraction to this phenomenon in Ukraine are determined.

Стаття надійшла до редакції журналу 25 квітня 2010 року.