ISSN 1995-6134

УДК 351.74
О.В. БОЙЧЕНКО, канд. техн. наук, доц.,
Кримський юридичний інститут Одеського державного університету внутрішніх справ

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ПРАВООХОРОННИХ ОРГАНІВ ДЕРЖАВ У ГАЛУЗІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Ключові слова: *міжнародні інформаційні телекомунікації, кіберпростір, кіберзлочинність, транснаціональні комп'ютерні злочини, Конвенція про кіберзлочиннність*

Стрімке зростання застосування сучасних інформаційних технологій в діяльності організацій, установ і відомств вимагає нагального вирішення проблем інформаційної безпеки. Це визначається тим, що окрім прямого збитку від можливих фактів несанкціонованого доступу до інформації, її модифікації або знищення, інформатизація може перетворитися на засіб придушення свободи людини, стати джерелом серйозної загрози державності і духовному життю особи.

Зростання науково-технічного прогресу обумовлює негативні тенденції розвитку злочинного світу, приводить до появи нових форм і видів злочинних посягань за рахунок того, що злочинні групи активно використовують у своїй діяльності новітні досягнення науки і техніки, застосовують сучасні інформаційно-телекомунікаційні технології.

Окремі питання проблематики взаємодії правоохоронних органів держав у боротьбі з міжнародною кіберзлочинністю розглядалися в роботах Ю.М. Батуріна, П.Д. Біленчука, М.С. Вертузаєва, В.Б. Вехова, В.О. Голубева, О.П. Снегірьова, Б.В. Романюка, В.С. Цимбалюка та інших видатних фахівців [1-4]. Комплексні дослідження проблематики заходів протидії міжнародній кіберзлочинності у колі питань інформаційної безпеки держав до нашого часу не проводились. Необхідність подальшого наукового дослідження проблематики взаємодії правоохоронних органів держав у боротьбі з міжнародною кіберзлочинністю обґрунтовує також стрімкий розвиток науково-технічного прогресу у поєднанні з високою динамікою розвитку міжнародних відносин.

Зазначене свідчить про те, що дослідження проблематики заходів протидії міжнародній кіберзлочинності правоохоронними органами держав у комплексі питань захисту інформаційних ресурсів має відповідну наукову новизну.

Метою роботи є комплексне вивчення проблем, пов'язаних з питаннями взаємодії правоохоронних органів держав у боротьбі з міжнародною кіберзлочинністю та розробка пропозицій, направлених на вироблення дієвих механізмів протидії міжнародній кіберзлочинності силами правоохоронних органів держав.

Впровадження в повсякденне життя суспільства сучасних інформаційно-телекомунікаційних технологій призводить до зростання дії інформаційних погроз на інформаційно-аналітичні системи державних органів і комерційних структур з боку кримінального світу з метою здійснення протиправних дій.

Транснаціональний характер злочинності з використанням комп'ютерної мережі дає підстави вважати, що розробка загальної політики по основних питаннях повинна бути частиною будь-якої стратегії боротьби з кіберзлочинністю. Така загальна політика має важливе значення для запобігання виникненню «правового даху», зокрема, в рамках тих правових систем, в яких певні дії не криміналізовані.

Кіберзлочиність не має державних кордонів, тому злочинець однаково здатний загрожувати інформаційним системам, які розташовані в будь-якій державі світу. Крім того, такі злочини істотно відрізняються від інших, давно відомих злочинів, що обумовлює складність процедури розслідування відповідно із чинними законодавствами держав.

Одним із факторів зростання кіберзлочинності є широке застосування зловмисниками комп'ютерних вірусів і програм. Так,

ISSN 1995-6134

аналіз статистичних даних щодо інформаційних загроз з боку комп'ютерних вірусів і програм наголошує про їх різке збільшення протягом останніх років. За даними «Лабораторії Касперського», в 2006 році було зафіксовано появу 169 тис. нових вірусів, в 2007 - 472 тис. шкідливих програм, а в 2008 році їх кількість зросла до 1,6 млн. Проте згідно звіту CSI/FBI, в 2007 році втрати від вірусів зайняли лише друге місце, поступившись втратам від фінансового шахрайства. За даними Symantec, опублікованим в середині 2007 року, в трійку країн, відповідальних за розповсюдження шкідливих програм, входять США (35 %), Китай (30 %) і Бразилія (14,3 %). За ними йде Росія, якій приписують відповідальність всього лише за 4,1 % всіх шкідливих програм.

За географічною ознакою найбільшими генератором різноманітної «комп'ютерної гидоти» у 2008 році стали США (36 %), Китай (13 %) та Україна (6 %). Росія в даному рейтингу зайняла 6-е місце, проте РФ є лідером в списку спам-розсилок по регіону EMEA (55389 фішингових веб-сайтів), що на 66 % більше, ніж в 2007 році [5, 6].

Половина зафіксованих комп'ютерних злочинів у світі відноситься до несанкціонованого доступу до комп'ютерної інформації. При цьому росте корислива спрямованість комп'ютерних злочинів з нанесення великого матеріального збитку, кількість злочинів, здійснених групами зловмисників, а також кількість трансграничних комп'ютерних злочинів. Комп'ютерні злочини стають лише першим кроком у ланцюжку кримінальних діянь, направлених на інші, традиційні злочини - розкрадання, здирство, шахрайство та ін.

Проблему загострює те, що останнім часом у військових діях збройних сил різних держав відстежується тенденція масового застосування методів комп'ютерного підриву. При цьому інша держава теж протистоятиме комп'ютерному підриву, застосовуючи більш досконалі методи боротьби. Результатом цього всього може стати поява глобальних «інформаційних війн». З кожним днем злочини стають більш досконалими та скритними, а їх результатом є величезний економічний та політичний збиток практично усім країнам світу.

Про необхідність зміцнення інформаційного суверенітету держави як однієї із складових національної безпеки України зазначено в Стратегії національної безпеки України, яка була затверджена Указом Президента України 12.07.2007 року.

В п.2.8 стратегії, зокрема, зазначено, що в даний час посилюється негативний зовнішній вплив на інформаційний простір України, що у свою чергу загрожує розмиванням суспільних цінностей і національної ідентичності; недостатніми залишаються обсяги виготовлення конкурентного національного інформаційного продукту; наближається до критичного стан безпеки інформаційно-комп'ютерних систем у сфері державного управління, фінансової і банківської сфери, енергетики, транспорту, внутрішніх і міжнародних комунікацій та ін.

Зазначене вимагає створення сприятливих зовнішніх умов для розвитку і безпеки держави, яка передбачає забезпечення інформаційної безпеки при інтеграції національних інформаційно-телекомунікаційних систем в структури глобального інформаційного суспільства [7].

Як уже було зазначено, найбільшою проблемою сьогодення в діяльності правоохоронних органів щодо протидії злочинності є суттєве зростання комп'ютерних злочинів з приводу широкого розповсюдження комп'ютерних систем і технологій у всіх сферах життєдіяльності суспільства. Зрозуміло, що в такому випадку постає питання оперативного реагування на факт скоєння злочину та притягнення винних осіб до відповідальності.

Кіберзлочинність є об'єктивним наслідком глобалізації інформаційних процесів і появи глобальних комп'ютерних мереж. Із зростанням використання інформаційних технологій в різних сферах діяльності людини росте і використання їх з метою скоєння злочинів. Кіберзлочинність за своєю суттю набагато ширше за комп'ютерну злочинність і включає цілий спектр протиправних діянь.

ISSN 1995-6134

Під кіберзлочинністю розуміється сукупність злочинів, що здійснюються в кіберпросторі з допомогою або за допомогою комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж, і проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних.

Кіберзлочин – це досконале суспільно небезпечне втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні діяння, які здійснюються за допомогою комп'ютерів, комп'ютерних мереж і програм, а також інших пристроїв доступу до модему за допомогою комп'ютера інформаційного простору, за скоєння чого передбачається кримінальна відповідальність згідно з чинним законодавством.

Кіберзлочинність володіє високою латентністю, тому офіційна статистика правоохоронних органів не відображає достовірної картини стану кіберзлочинності як на рівні держави, так і на загальносвітовому рівні.

Для оцінки стану кіберзлочинності необхідно використовувати інші способи отримання даних, такі як інтерв'ювання, фокусні групи, огляди, а також метод «реєстрації звернень» – віктимологічний метод, що полягає в зборі відомостей про кіберзлочини від потерпілих. Використання цих методів разом із аналізом офіційної статистики дозволяє досліджувати масштаби кіберзлочинності та її тенденції з урахуванням злочинів, що залишилися за рамками зареєстрованих правоохоронними органами суспільно небезпечних діянь.

Аналіз статистичних даних свідчить про швидке зростання кіберзлочинності, про можливість спричинення цими злочинами значного фінансового збитку громадянам і організаціям при мінімальному ризику для злочинця, а також про зростання взаємозв'язку кіберзлочинності з організованою злочинністю. Це свідчить про підвищену небезпеку подібного роду діянь і обумовлює необхідність реагування на них кримінально-правовими заходами.

Кримінально-правова боротьба з кіберзлочинністю – глобальна проблема внаслідок того, що кіберзлочинність носить транскордонний характер. Тому для ефективної боротьби з кіберзлочинами необхідне не тільки ухвалення відповідних кримінально-правових норм на національному рівні, але й вироблення єдиних міжнародних стандартів, таких як визначення кола діянь, що підлягають криміналізації, вироблення єдиного понятійного апарату і єдиної термінології, перегляд існуючих кримінально-правових норм з урахуванням стандартів, встановлених міжнародно-правовими документами.

Результати порівняльного аналізу законодавства держав миру, присвяченого боротьбі з кіберзлочинністю, показують, що в більшості розвинених країн криміналізовані в тій або іншій формі наступні види діянь:

- посягання на конфіденційність даних;
- несанкціоноване проникнення в комп'ютери і комп'ютерні мережі;
- посягання на конфіденційність інформації, що містить комерційну таємницю;
- комп'ютерний саботаж (втручання у функціонування, зміну, знищення даних та ін.);
- економічні кіберзлочини (зокрема, комп'ютерне шахрайство).

Аналіз практики діяльності ОВС щодо протидії комп'ютерній злочинності визначає, що однією з серйозних причин складності розслідування комп'ютерних злочинів є їх транснаціональний характер (зловмисник може знаходитися в будь-якому місці миру і здійснювати протиправні дії відносно будь-якої держави або комерційної структури). Тому, для успішного розслідування, збору доказів і притягнення зловмисників до відповідальності за злочини з використанням комп'ютерів, виникає необхідність відстежування злочинної діяльності та її наслідків через ланцюжок проксі-серверів і інших служб Інтернету, що нерідко знаходяться в різних державах.

Поряд із зазначеним, під час боротьби із злочинами у сфері інформаційних технологій виникають численні проблеми правового ха-

ISSN 1995-6134

рактеру, що обґрунтовано нематеріальністю та недовговічністю електронних доказів. Тому складність вирішення проблем протидії кіберзлочинності вимагає організації міжнародної співпраці країн через застосування відповідних і сумісних між собою правових, процесуальних і нормативних засобів.

Практика розслідування комп'ютерних злочинів приводить до необхідності налагодження взаємодії між правоохоронними органами різних держав. Однак у наш час, напрями міжнародної співпраці мають недостатній характер і не отримують належного розвитку в конкретних двосторонніх і багатосторонніх проектах у сфері інформатизації і захисту інформації.

Для ефективного попередження транснаціональних комп'ютерних злочинів необхідний узгоджений міжнародний підхід на різних рівнях. На національному рівні для розслідування кіберзлочинів потрібний добре підготовлений штат співробітників. Внесення змін і доповнень до чинного національного законодавства з метою формування правової основи для забезпечення слідчої, оперативно-розшукової діяльності правоохоронних органів і спецслужб, а також судових органів по правопорушеннях в інформаційній сфері, зокрема, по припиненню таких видів злочинів.

На міжнародному рівні необхідні оперативні дії, що спираються на координацію зусиль національних центрів по попередженню і розслідуванню транснаціональних комп'ютерних злочинів з аналогічними міжнародними центрами в інших країнах. Для врегулювання існуючих проблем на національному і міждержавному рівні виникла необхідність юридично визначитися в найбільш важливих правових нормах поведінки їх учасників, у боротьбі з правопорушеннями, пов'язаними з використанням мережі Інтернет.

Хоча зацікавлені країни вже враховують проблеми транснаціональних комп'ютерних злочинів, на міждержавному рівні такій формі злочинності не приділяється достатня увага. Причини відсутності уваги до кіберзлочинності можуть включати відносно низький рівень участі в міжнародних електронних комунікаціях, недостатній рівень досвіду в правоохоронній сфері та занижені оцінки соціальних витрат, які, як очікується, можуть спричиняти за собою злочини, що здійснюються в електронному середовищі.

В рамках глобальної комп'ютерної мережі Інтернет кримінально-правова політика окремої держави надає пряму дію на міжнародне співтовариство. Кіберзлочинці можуть направляти свої дії в електронному середовищі через певну державу, де такі діяння не криміналізовані, що дозволяє їм знаходитися під захистом закону такої країни. Навіть якщо в коло конкретних національних інтересів тієї або іншої держави не входить криміналізація певних діянь, вона може розглянути питання про вживання таких заходів, з тим, щоб не перетворитися на «правовий дах» і не поставити себе в умови міжнародної ізоляції. Тому забезпечення міжнародної співпраці правоохоронних і судових органів різних держав неможливе без узгодження і ухвалення норм кримінального права відносно кіберзлочинів.

Одним із кроків у розробці єдиних підходів до заходів протидії комп'ютерним злочинам стало набуття чинності міжнародної Конвенції по боротьбі з кіберзлочинністю, яка прийнята в рамках Ради Європи 23.11.2001 року та ратифікована Україною у вересні 2005 року. Дана Конвенція стала першою міжнародною угодою по юридичних і процедурних аспектах розслідування та кримінального переслідування кіберзлочинів. У Конвенції передбачаються скоординовані на національному та міждержавному рівнях дії, направлені на недопущення несанкціонованого втручання в роботу комп'ютерних систем [8].

Окремий розділ Конвенції присвячений міжнародній співпраці за наступними питаннями: екстрадиція у зв'язку з кримінальними правопорушеннями, передбаченими цією Конвенцією; проведення розслідування або переслідування кримінальних злочинів, визначених цією Конвенцією; процедур, пов'язаних із запитами про взаємну допомо-

ISSN 1995-6134

гу у разі відсутності міжнародних угод між країнами. Також у документі описані проблеми взаємодії правоохоронних органів у випадках, коли кіберзлочинець і його жертва знаходяться в різних країнах і підкоряються різним законам.

У Конвенції висвітлено питання зберігання особистої інформації клієнтів Інтернет-провайдерів на випадок, якщо є необхідність її використання при розслідуванні кіберзлочинів.

Стаття 23 Конвенції визначає загальні принципи, що стосуються міжнародної співпраці, згідно з якими «Сторони повинні тісно співробітничати одна з одною за допомогою застосування відповідних міжнародних документів з міжнародної співпраці в сфері кримінального правосуддя, договорів, укладених на основі однорідного, взаємного та державного законодавства, з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними або з метою збирання доказів в електронній формі, що стосуються таких правопорушень».

У статті 25 даної Конвенції закріплені загальні принципи взаємної допомоги, згідно з якими «Сторони зобов'язуються надавати один одному широку взаємодопомогу для розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів в електронній формі по кримінальному переслідуванню».

У Конвенції присутній ряд положень, здатних повноцінно забезпечити і з правової точки зору обґрунтувати методи побудови взаємної співпраці по конкретних кримінальних справах. Першорядного значення набуває декілька чинників: отримання запиту від зарубіжного партнера, виконання оперативних або слідчих заходів стороною, що отримала такий запит, передача результату ініціаторові, або сумісна реалізація отриманої інформації.

Безперечно, з правової точки зору велике значення мають і загальні принципи, що стосуються міжнародної співпраці, які визначені в Конвенції. Це питання видачі комп'ютерних злочинців і надання один одному широкої взаємодопомоги для розслідування кримінальних справ, пов'язаних з комп'ютерними системами і даними, так само як і для збору електронних доказів.

Зазначаючи безсумнівні переваги проаналізованого нормативного документу, не можна не відзначити і деякі складнощі в реалізації положень Конвенції. Так, Конвенція «Про кіберзлочинність» набула чинності 1 липня 2004 р. До кінця 2005 р. її підписали 38 країнчленів Ради Європи (у тому числі, й Україна), а також США, Канада, Японія і ПАР, але ратифікували її на сьогоднішній день всього 18 країн. Деякі держави, у тому числі й Російська Федерація, не ратифікували Конвенції, що безумовно знижує ефективність застосування комплексу заходів міжнародної співпраці по протидії кіберзлочинності.

Під егідою Виконавчого комітету СНД розроблені і узгоджені проекти Концепції забезпечення інформаційної безпеки Співдружності Незалежних Держав і Комплексного плану заходів щодо її реалізації на період з 2005 по 2008 роки.

Існує ряд двосторонніх договорів, створюються об'єднані робочі групи правоохоронних органів різних держав по взаємодії і співпраці в даній сфері. Так, наприклад, в червні 2005 року в МВС Росії відбулося друге засідання об'єднаної російсько-американської робочої групи по координації взаємодії в боротьбі з транснаціональною організованою злочинністю. На думку багатьох аналітиків, діяльність російсько-американської робочої групи по протидії міжнародній організованій злочинності можна розглядати як один з найбільш перспективних напрямів у сфері правоохоронної співпраці між Росією і США.

Існує в світі також практика проведення сумісних заходів при розслідувань комп'ютерних злочинів. Сумісні операції проводяться в рамках боротьби з дитячою порнографією, шахрайських дій в мережі Інтернет, міжнародним тероризмом, розробки системи захисту інформації, що передається по каналах міжнародної мережі національних контактних пунктів, при цьому можуть

ISSN 1995-6134

застосовуватися засоби криптографії, створення захищених віртуальних мереж, особливі методи ідентифікації тощо.

З урахуванням специфіки соціального феномена кіберзлочинності, масштабів інформатизації і розвитку глобальної мережі Інтернет стає все менш вірогідним, що злочини такого вигляду будуть обмежені територією окремої держави. В процесі проведення розслідувань правоохоронні органи різних держав повинні співробітничати між собою, причому як офіційно, використовуючи такі рамки і структури як Інтерпол, так і неофіційно, надаючи потенційно корисну інформацію безпосередньо правоохоронним органам іншої держави.

У зв'язку з правовою допомогою при розслідуванні кіберзлочинів неминуче виникатимуть і інші додаткові проблеми. Якщо внутрішнім правом однієї зі сторін не передбачені конкретні повноваження на пошук доказів в електронному середовищі, то така сторона буде не в змозі адекватно реагувати на прохання про надання допомоги. З цієї причини важливою умовою міжнародної співпраці є узгодження повноважень щодо прийняття необхідних заходів для розслідування таких видів злочинів.

Обмеженість національного законодавства та відсутність єдиної правової бази правоохоронних органів в боротьбі з цим видом правопорушень є однією з головних причин стрімкого зростання кіберзлочиності.

На нашу думку протистояти тенденції зростання кіберзлочинності та «відставання» соціально-правового контролю над нею можна тільки шляхом органічного поєднання кримінально-правових і криміналістичних стратегій боротьби з цим видом злочинів. При цьому важливою складовою такої стратегії повинна стати міжнародна співпраця в цій сфері, оскільки вже очевидно, що контролювати транснаціональну складову кіберзлочинів на рівні окремих держав практично неможливо. Міжнародна співпраця в боротьбі із злочинністю у сфері використання комп'ютерних технологій має потребу в наявності правового, організаційного і науково забезпечення. Це той комплекс проблем, який необхідно вирішувати міжнародному співтовариству у сфері боротьби з кіберзлочинністю в XXI столітті.

Підсумовуючи зазначимо, що вирішення нагальних проблем боротьби з міжнародною кіберзлочинністю може буди здійснено через впровадження в практику взаємодії правоохоронних органів держав типових формалізованих документів інформаційного обміну; розробки словника умовних кодів виявлених кіберзлочинів; формування переліку видів трансграничних злочинів, фактів прояву тероризму і екстремізму, шахрайських схем і фактів хакерських атак. Зазначена інформація повинна негайно передаватися правоохоронним органам сторони, яка потерпіла, з використанням каналів мережі національних контактних пунктів.

Крім того, необхідний подальший розвиток співпраці у сфері забезпечення інформаційної безпеки на основі двосторонніх і багатосторонніх договорів через гармонізацію національних законодавств у сфері інформаційної безпеки, організацію спільних виробництв засобів захисту інформації, а також підготовку і перепідготовку фахівців у сфері інформаційної безпеки інформаційно-телекомунікаційних систем.

Таким чином, успішне вирішення проблем інформаційної безпеки можливо лише при ефективній взаємодії державних структур різних держав на основі прийнятих та ратифікованих нормативно-правових документів у сфері інформаційної безпеки держав.

ЛІТЕРАТУРА

1. Біленчук П. Д. Актуальні проблеми підготовки персоналу ОВС для розслідування комп'ютерних злочинів / П. Д. Біленчук, Л. В. Борисова, М. В. Козир // Актуальні проблеми управління персоналом ОВС Україні : матеріали наук.-практ. конф. – Х. : Вид-во Нац. ун-ту внутр. справ, 2002. – С. 211-214.

2. Біленчук П. Д. Комп'ютерна злочинність: навчальний посібник [для студ. вищ. навч. за-

ISSN 1995-6134

кл.] / П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін. – К. : Атіка, 2002. – 204 с.

3. Голубєв В. О. Правові проблеми захисту інформаційних технологій / В. О. Голубєв // Вісник Запорізьк. юрид. ін-ту. - 1997. – № 2. – С. 35–40.

4. Снегірьов О. П. Проблеми класифікації злочинів у сфері комп'ютерної інформації / О. П. Снегірьов, В. О. Голубєв // Вісник Ун-ту внутр. справ. – 1999. - Вип. 5. – С. 25–28.

5. Гейл Хамилтон. Symantec объявляет о новой комплексной стратегии информационной защиты предприятий / Гейл Хамилтон [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/377810.php.

6. Бойченко О. В. Інформаційна безпека в органах внутрішніх справ України (організаційно-правові засади) : монографія / О. В. Бойченко. – Сімферополь : Кримськ. юрид. ін-т ОДУВС, 2009. – 288 с.

7. Указ Президента України «Про Стратегію національної безпеки України» : від 12.02.2007 р., № 105/2007 [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/5728.html.

8. Конвенція про кіберзлочинність : від 23.11.2001 р. [Електронний ресурс]. – Режим доступу: www.crime-research.org/library/Conven.htm.

Бойченко О. В. Міжнародне співробітництво правоохоронних органів держав в галузі забезпечення інформаційної безпеки / О. В. Бойченко // Форум права. – 2009. – № 2. – С. 56–62 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2009-2/09bovzib.pdf

Проведено аналіз напрямків міжнародної співпраці правоохоронних органів держав по протидії міжнародній кіберзлочинності. Визначено глобальну проблему кримінально-правової боротьби з кіберзлочинністю, яка визначається її трансграничним характером. Запропоновано вирішення проблеми зростання кіберзлочинності шляхом органічного поєднання кримінально-правових і криміналістичних стратегій боротьби з цим видом злочинів.

***

Бойченко О.В. Международное сотрудничество правоохранительных органов государств в отрасли обеспечения информационной безопасности

Проведен анализ направлений международного сотрудничества правоохранительных органов государств по противодействию международной киберпреступности. Определена глобальная проблема криминально-правовой борьбы с киберпреступностью, которая определяется ее трансграничным характером. Предложено решение проблемы роста киберпреступности путем органического сочетания криминально-правовых и криминалистических стратегий борьбы с этим видом преступлений.

***

Boychenko O.V. International Collaboration of Law Enforcement Authorities of the States in the Branch of Providing of Informative Safety

The analysis of directions of international cooperation of law enforcement authorities of the states on counteractions to international cyber criminality was held. Besides, global problem of criminal-law fight against cyber criminality, which is determined by its transfrontal character, was defined. And also the solution of problem of cyber criminality growth by organic combination of criminal-law and criminalist strategies of fight against this type of crimes was offered.