

12. Петрянина О.А. Проституция как сфера теневой экономики: уголовно- правовой анализ, квалификация, причины и предупреждение: автореферат диссертации на соискание ученой степени кандидата юридических наук. — Нижний Новгород, 2013. — 30 с.
13. Нурмухаметова А.М.- Уголовная ответственность за преступления, связанные с проституцией, и их предупреждение: автореферат диссертации на соискание ученой степени кандидата юридических наук. -Н. Новгород, 2012. — 34 с.
14. Станская А.А. Проституция несовершеннолетних – социальная и правовая проблема. / Науч. Ред. С.Ф. Милюков. — СПб.: Издательство Юридический центр пресс, 2005. – С. 19.
15. Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. А.И. Рарог. М., 2005. – С. 425.
16. Герасимов Н.В. Уголовно-правовой анализ организации занятия проституцией: Автореферат диссертации на соискание ученой степени кандидата юридических наук. — Самара, 2011. — 18 с.
17. Турсунов А.С., Ганиев Ш.А. Ижтимоий-салбий хулқ тури сифатида фоҳишаликнинг тушунчаси ва белгилари // Ўзбекистон Республикаси ИИВ Академиясининг ахборотномаси. — 2010. — 3-сон. — Б. 82.
18. Ниёзова С.С., Фазилов И.Ю. Фоҳишахона саклаш ёки қўшмачилик қилишга қарши курашнинг жиноят-хукукий чоралари: Ўқув қўлланма. — Т.: ТДЮИ нашриёти, 2011. — Б. 56.
19. Шибанова Е. В. Выявление и расследование преступлений, связанных с проституцией: Автореферат диссертации на соискание ученой степени кандидата юридических наук. — Саратов, 2005. — 30 с.
20. Цыркун С.А. Выявление и расследование преступлений, связанных с содержанием притонов для занятия проституцией: Автореферат диссертации на соискание ученой степени кандидата юридических наук. — М., 2004. — 25 с.

Onyshchenko Y.N.

PHD in Public Administration

Kharkiv National University of internal affairs, Ukraine

Kobzev I.V.

PHD in Technical Sciences, Associated Professor

Mynko P.E.

PHD in Technical Sciences, Associated Professor

Kharkiv Regional Institute of Public Administration of the National Academy of Public Administration attached to the Office of the President of Ukraine, Ukraine

FEATURES OF ORGANIZATIONAL AND NORMATIVELY-LEGAL PRINCIPLES OF FIGHT AGAINST CYBERCRIME

Онищенко Ю.М.

кандидат наук з державного управління

Харківській національній університет внутрішніх справ

Кобзев І.В.

кандидат технічних наук, доцент

Минко П.Є.

кандидат технічних наук, доцент

Харківський регіональний інститут державного управління Національної академії державного управління при Президентові України

ОСОБЛИВОСТІ ОРГАНІЗАЦІЙНИХ ТА НОРМАТИВНО-ПРАВОВИХ ЗАСАД БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

In the article examined to the feature of organizational and legal principles of fight against cybercrime. It is determined that the special attention is required by coordination of different initiatives from creation of projects of normatively-legal acts between state structures.

Keywords: *the state, cybercrime, national safety, legislation, normatively acts*

У статті розглядаються особливості організаційних та правових засад боротьби з кіберзлочинністю. Визначається, що особливої уваги потребує координація різних ініціатив зі створення проектів нормативно-правових актів між державними структурами.

Ключові слова: *державна, кіберзлочинність, національна безпека, законодавство, нормативні акти*

Міжнародні організації визнають і небезпеку кіберзлочинності, і її транскордонний характер, обмеженість одностороннього підходу до вирішення цієї проблеми і необхідність постійної та активної міжнародної співпраці як щодо вжиття необхідних технічних заходів,

так і в розробленні міжнародного законодавства. Рада Європи, Європейський Союз, ООН та Інтерпол – усі ці організації відіграють важливу роль у координації міжнародних зусиль, побудові міжнародної співпраці в боротьбі зі злочинами у сфері високих технологій.

Продуктом багаторічних зусиль Ради Європи стала прийнята 23 листопада 2001 р. в Будапешті Конвенція Ради Європи про кіберзлочинність [1]. Це один із найважливіших правових актів, що регулюють правовідносини у сфері глобальної комп'ютерної мережі, і поки що єдиний документ такого рівня.

Конвенція про кіберзлочинність на сьогодні є одним із базових міжнародних правових актів у сфері права телекомунікацій. Її можна поставити на один щабель з Окинавською хартією глобального інформаційного суспільства [2]. Та якщо в останній ідеться, швидше, про закріплення загальної концепції розвитку інформаційно-комунікаційних технологій, то в Конвенції пропонується реальний механізм правового регулювання.

Незважаючи на очевидну громадську значущість Конвенції, цей документ не позбавлено недоліків, що зумовили його негативне сприйняття багатьма членами мережевого інформаційного співтовариства. У низці міждержавних нормативно-правових актів визнано, що кіберзлочинність сьогодні становить загрозу не лише національній безпеці окремих держав, а загрожує людству і міжнародному порядку.

17 липня 2014 р. Кабінет Міністрів України розглянув проект Указу Президента України «Про Стратегію забезпечення кібернетичної безпеки України». Проект Указу був розроблений адміністрацією ДССЗЗІ на виконання рішення РНБО України від 28 квітня 2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України», уведеного в дію Указом Президента України від 1 травня 2014 р. № 449. Проект Указу був схвалений Урядом та переданий на розгляд РНБО.

Національна система кібербезпеки повинна розглядатись як сукупність політичних, економічних, соціальних та інформаційних відносин разом з технологічними та адміністративними заходами, реалізація яких вбачається можливою в тісній взаємодії державного і приватного секторів і громадянського суспільства. Проект Указу був підтриманий та погоджений без зауважень Міністерством внутрішніх справ, Міністерством фінансів України, Державним агентством з питань науки, інновацій та інформатизації України (Держінформнауки) та Державною службою України з питань захисту персональних даних. Частково було враховано зауваження та пропозиції СБУ, Міністерства економічного розвитку і торгівлі та Міністерства юстиції України. Наступним кроком у формуванні національної системи кібербезпеки має стати прийняття Закону України «Про основні засади забезпечення кібербезпеки України» [3].

Проект цього Закону, розроблений адміністрацією ДССЗЗІ, вже пройшов обговорення за участю представників громадськості та зацікавлених державних органів. Сьогодні він перебуває на етапі остаточного погодження та найближчим часом буде поданий на розгляд Кабінету Міністрів України. Ця робота здійснювалась з урахуванням основних принципів забезпечення кібербезпеки України, покладених в основу проекту Стратегії.

Дослідженням встановлено, що правоохоронними органами з 1994 р. щорічно в Україні офіційно реєструється до 100 злочинів, що здійснюються з використанням інформаційно-телекомунікаційних технологій. Проте офіційні статистичні показники не відповідають реальному стану справ. З'ясовано, що цей вид злочинів у нашій країні має дуже високий рівень латентності: вони приховані від офіційної статистики. Показники щодо злочинів, здійснюваних із використанням комп'ютерних технологій, розсіяно у відомчих обліках. За експертними оцінками, рівень латентності кіберзлочинності складає 90–95 %.

Високий рівень латентності кіберзлочинності серед інших чинників зумовлений: низьким рівнем спеціального технічного оснащення правоохоронних органів сучасними засобами комп'ютерної техніки і комп'ютерними технологіями, відсутністю знань і навичок виявлення, розслідування й розкриття кіберзлочинів через обмеження доступу до тактики, техніки і методик, низьким рівнем інформаційної культури, підготовленості широкого кола

кадрів правоохоронних органів і суддів, недовірою потерпілих до правоохоронних органів (пов'язано з вищезгаданими чинниками) та ін.

Аналіз змісту вітчизняних підручників із криміналістики, кримінології, кримінально-процесуального і кримінального права свідчить, що вказаній проблематиці не приділялося належної уваги. Ґрунтовному дослідженню проблем запобігання та протидії кіберзлочинності також перешкоджала відсутність показників у державній кримінальній статистиці. Більшість виявлених злочинів, що здійснюються з використанням комп'ютерних технологій, розсіяно в звітності різних підрозділів правоохоронних органів серед показників економічної та інших видів злочинності.

Порівняльний аналіз досліджень зарубіжного досвіду боротьби з кіберзлочинністю свідчить, що вона має тенденцію до збільшення. Однією з умов її зростання є ускладнення технічних систем глобального зв'язку (телефонної, радіо, супутникової) та спрощення доступу до використання комп'ютерних технологій широкого кола користувачів через персональні комп'ютери.

Дослідження проблем боротьби з кіберзлочинністю показало, що орієнтація тільки на технічні й технологічні засоби забезпечення інформаційної безпеки (технічного захисту інформації) в умовах інформатизації, у тому числі профілактики кіберзлочинів, не має значного успіху. Парадокс полягає в тому, що чим складніше стає комп'ютерне програмно-математичне забезпечення, тим більш вразливими виявляються традиційні організаційні заходи і засоби інженерно-технічного захисту інформації в автоматизованих (комп'ютерних) системах, зокрема відносно несанкціонованого доступу.

Проблемою наступного порядку також є і те, що з розвитком сучасних електронних засобів інформації розвиваються технічні засоби перехоплення й доступу до інформації, що обробляється й передається в електронних системах зв'язку. Доступ до цих засобів не створює проблеми для злочинних формувань.

Найбільшу небезпеку для суспільства, держави становить транскордонна організована кіберзлочинність: комп'ютерний тероризм; диверсії, інші прояви антагоністичної інформаційної боротьби кримінальних формувань з державою, правоохоронними органами; крадіжки інформації з комп'ютеризованих баз даних і порушення права інтелектуальної власності на комп'ютерні програми; шахрайства з використанням комп'ютерних технологій, особливо у сфері міжнародних економічних відносин (кредитно-фінансова, банківська) та ін.

Прагнення України відповідати на сучасні виклики в цій сфері віддзеркалюється основними державними організаційно-правовими заходами, що спрямовані на протидію кіберзлочинності. Урядом України створені спеціальні організаційні структури з координації напрацювань державної політики у сфері організаційно-правового забезпечення входження нашої держави до світового інформаційного суспільства.

За своїм змістом Концепція реформування спрямовується на системну, комплексну організаційно-правову реалізацію на законодавчому рівні державної політики у сфері суспільних інформаційних відносин. Кодекс про інформацію є науковою концепцією стосовно кодифікації інформаційного законодавства і покликаний сприяти, серед іншого, правовому забезпеченню боротьби з кіберзлочинністю. Заходи з розроблення остаточного варіанта Концепції реформування та наступного її втілення включено в завдання Національної програми інформатизації України. Проте реалізація цих заходів здійснюється повільно через певні організаційні бюрократичні чинники.

Питаннями вдосконалення правового регулювання, визначення й організації реалізації державної політики у сфері інформаційних стосунків займаються також Міжвідомчий комітет з проблем захисту прав на об'єкти інтелектуальної власності, Міжвідомча робоча група з розроблення й узгодження Концепції легалізації програмних продуктів і боротьби з їх нелегальним використанням.

Результативність діяльності державних структур визначається введенням економічних санкцій США відносно України за неналежний рівень боротьби з порушеннями прав інтелектуальної власності, в основному, щодо програмних продуктів, і включення нашої

держави Міждержавною групою розроблення фінансових заходів боротьби з «відмиванням» грошей у список країн, що не пішли на співпрацю.

Аналіз емпіричного матеріалу дозволяє зробити прогноз, що в разі невирішення проблем боротьби з організованою кіберзлочинністю, особливо у сфері міжнародних економічних відносин, на Україну з боку міжнародного співтовариства посилюватиметься інформаційний, політичний та економічний тиск.

Правові основи протидії комп'ютерній злочинності на національному рівні визначено у прийнятому новому ККУ. Окремі види комп'ютерних злочинів (кіберзлочинів) виділено в окремий розділ XVI Особливої частини – «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж» (ст. 361, 361, 363).

За скоєння злочинів проти основ національної безпеки (конституційного ладу України): проти життєво важливих інтересів особи, суспільства держави, громадської безпеки, або скоєння інших злочинів, передбачених чинним ККУ, з використанням функціональних можливостей (технологій) комп'ютерних мереж, комп'ютерних систем, комп'ютерних інформаційних ресурсів та інших електронних інформаційних технологій, покарання призначається за статтями Особливої частини, у яких передбачається відповідальність за такий злочин.

Такий правовий захід дозволить забезпечити здійснення організаційних та інших заходів, у тому числі об'єктивного моніторингу і статистику комп'ютерних злочинів і комп'ютерної злочинності в Україні.

Серед інших організаційних заходів в Україні на урядовому рівні створено багато робочих груп, що розробляють проекти законодавчих і підзаконних актів у сфері громадських інформаційних стосунків, які прямо або побічно відбивають питання протидії та запобігання кіберзлочинності і взаємодію з різними транснаціональними організаційними структурами.

Аналіз різних ініціатив зі створення проектів нормативно-правових актів свідчить, що між вказаними та іншими державними структурами немає взаємодії, координації діяльності. На законодавчому рівні лобіюються суперечливі антидержавні потреби та інтереси на тлі сповідання ідей правового нігілізму з чинним законодавством, що провокує масовий правовий хаос, у тому числі у правотворчій діяльності. Сьогодні у сфері інформаційного законодавства створено умови, що дозволяють злочинцям «законно» уникати відповідальності, використовуючи конфлікти різних юридичних норм. Вказаний чинник можна розглядати як додаткову ознаку латентності кіберзлочинності.

Література:

1. Convention on Cybercrime. Budapest, 23.XI.2001. – Режим доступу : <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>
2. Окинавская Хартия глобального информационного общества № 998-163 від 22.07.2000 / Okinawa Charter on Global Information Society // Дипломатический вестник. – 2000. - № 8. – С. 51-56.
3. Уряд погодив проект національної Стратегії забезпечення кібернетичної безпеки, розроблений Держспецзв'язку / Держ. служба спец. зв'язку та захисту інформації України. – Режим доступу : http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=114674&cat_id=112509.