

і кінцева мета реформи наукової доктрини і практики реалізації українського адміністративного права на сучасному етапі. Але, треба зауважити, що без нової реформи, враховуючи економічні, соціальні та інші потреби громадян нашої держави, стає дедалі важче контролювати, забезпечувати всі гілки влади.

У ході реформування адміністративного права, перш за все, потребує більш ґрунтовного усвідомлення і сприйняття не тільки представниками влади, а й всіма верствами населення фундаментальна конституційна формула, яка прописана в статті 3 Конституції України «Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави». Але, для цього Конституції та її дотримання не достатньо, як і в будь-якій демократичній державі повинно бути формування демократичної правової держави, яке пов'язане з висвітленням зміцнення законності і правопорядку, підвищення ефективної роботи правоохоронних органів, без чого неможливі жодні прогресивні зміни у суспільстві. Забезпечення належного громадського порядку в країні, який відповідав би вимогам сучасного періоду, є однією з важливих функцій держави. У здійсненні цієї функції беруть участь всі державні органи, посадові особи та громадяни.

Важлива роль у забезпеченні виконання цієї функції відводиться органам внутрішніх справ, для яких, згідно з їх правовим положенням, громадський порядок в країні - є головне завдання.

Активізація діяльності ОВС щодо протидії кіберзлочинності в умовах реформування України як правової держави та її євроінтеграції

Підюков П.П., доктор юридичних наук, професор, заслужений юрист України, завідувач наукової лабораторії з проблем психологічного забезпечення навчально-виховного процесу ННІПП НАВС

Варлакова Є.О., кандидат психологічних наук, науковий співробітник наукової лабораторії з проблем психологічного забезпечення навчально-виховного процесу ННІПП НАВС

За даними Департаменту інформаційних технологій МВС України, відсоток нерозкритих справ, пов'язаних із кіберзлочинами, щороку зростає. Його фахівці пояснюють це низкою причин, серед яких основними є:

1) швидкоплинність і прихованість, переважно транскордонний характер таких злочинів;

2) високий рівень технічної оснащеності кіберзлочинців, залучення ними до протиправних операцій у кіберпросторі висококваліфікованих фахівців-професіоналів;

3) неузгодженість процедур обміну оперативною інформацією стосовно кіберзлочинів та їх суб'єктів між правоохоронними органами, насамперед зарубіжних країн;

4) недовіра до правоохоронних органів з боку потерпілих юридичних і фізичних осіб, зумовлена нерідко і небажанням можливого широкого розголосу фактів вдалих посягань на їхні комп'ютерні системи, що може призвести до втрати ними власних прибутків через зниження довіри партнерів до рівня їх фаховості, ділової репутації й т. ін.;

5) практична відсутність профільних вузів (факультетів) з інноваційними навчальними програмами і методиками підготовки фахівців у цій досить специфічній галузі (які, окрім юридичної освіти та певного фахового досвіду в цій сфері мають володіти сучасними спеціальними знаннями в галузі

системотехніки та програмування), і як результат - досить низький рівень професійної кваліфікації особового складу та спеціального оснащення правоохоронних структур порівняно з підготовкою, кваліфікацією та комп'ютерним оснащенням кіберзлочинців;

б) брак соціальної привабливості та належного фінансування праці співробітників спецпідрозділів з протидії кіберзлочинності, що значно ускладнює і навіть унеможливує залучення до їх складу вже підготовлених висококваліфікованих фахівців і обдарованої молоді з числа цивільних осіб;

7) прояви нездорової конкуренції між підрозділами по боротьбі з кіберзлочинністю різних відомств (нерідко СБУ передає за підвідомчістю до спецпідрозділів МВС оперативні матеріали за фактами виявлення тих кіберзлочинів, які вважаються безнадійними й безперспективними для розкриття);

8) наявність антипатії - чи, принаймні, потенційної недовіри правоохоронних органів до професіоналів цивільних установ чи бізнес-структур у галузі комп'ютерних технологій [1].

Для того, щоб успішно здолати кіберзлочинність у нашій країні, бажано невідкладно вжити заходів, серед яких першочерговими мають бути:

1. Розробка порядку взаємодії правоохоронних та інших зацікавлених міністерств і відомств держави, а також обмін інформацією в боротьбі з незаконним використанням високих технологій у злочинних цілях.

2. Узагальнення прокурорсько-слідчої і судової практики у справах про кіберзлочини і на цій основі розробка інноваційних методичних рекомендацій, їх запровадження на місцях.

3. Організація і проведення науково-практичних конференцій за участю іноземних фахівців і практичних співробітників із проблем запобігання та активізації протидії комп'ютерній злочинності.

4. Підготовка методичних рекомендацій щодо запобігання, виявлення, припинення і розслідування злочинів у сфері високих технологій.

5. Створення у складі експертно-криміналістичних установ підрозділів для проведення спеціальних (комп'ютерних) експертиз у кримінальних провадженнях про кіберзлочини.

6. Порівняльний і системний аналіз чинного національного законодавства стосовно боротьби з кіберзлочинністю з метою підготовки проектів відповідних законодавчих актів, у тому числі про внесення доповнень у діюче законодавство.

7. Створення міжвідомчого науково-практичного центру для дослідження проблем досудового провадження по злочинах, що вчиняються з використанням комп'ютерних та інформаційних систем, достовірності й повноти даних протоколів реєстрації користувачів та іншої службової інформації;

8. Розробка й запровадження навчальних комплексів і програм підготовки на базі ВНЗ МВС кадрів для подальшої діяльності в спецпідрозділах, пов'язаних із сферою високих технологій, введення до існуючих навчальних програм відомчих ВНЗ циклу лекцій з проблем боротьби кіберзлочинністю та підготовка серії профільних навчальних посібників, у тому числі для фахівців відповідних спеціальних підрозділів ГУ-УМВС за цим напрямом [2].

Запровадження запропонованих вище заходів значно підвищить ефективність діяльності правоохоронних органів щодо більш активної протидії та подолання кіберзлочинності, що неодмінно позитивно позначиться як на економічній безпеці, так і на інтеграції України у європейській і світовий простір.

Список використаних джерел:

1. Кіберзлочинність в Україні: перспективи протидії / Тижневик «Україна. Бізнес. Ревю», № 5-6, від 11.02 2013. [Електронний ресурс]. - Режим доступу: http://www.ukrbizn.com/vlast_biznes/632-kberzlochmst-mozhna-zupmiti-tki-splnmi-zusllyami.html

2. Шапочка С.В. Історичні та соціальні передумови виникнення шахрайства, що вчиняється з використанням комп'ютерних мереж // «Вісник Вищої ради юстиції». - 2012. - № 2 (10). - С 108-121.

Використання міжнародного досвіду боротьби з фінансуванням тероризму в контексті розбудови України як правової держави та її інтеграції в європейський і світовий простір

Осипенко Р.І., здобувач кафедри оперативного-розшукової діяльності НАВС
Підюков П.П., доктор юридичних наук, професор, заслужений юрист України, завідувач наукової лабораторії з проблем психологічного забезпечення навчально-виховного процесу ННПП НАВС

Тероризм традиційно вважається одним із найнебезпечніших різновидів політичної злочинності. Водночас, його правова природа нерідко має економічні, релігійні й інші складові, що зумовлює дослідження цього соціально-правового явища також у контексті економічної кримінології, кримінології та інших галузей сучасної науки. При цьому варто, як нам здається, констатувати той факт, що проблема боротьби з фінансуванням тероризму залишається серед них поки що однією з найменш досліджуваних науковцями, не зважаючи на своє вже понад 20-річне визначення в міжнародному праві.

Для вітчизняної правової науки означена проблема набуває ще більшої актуальності у зв'язку із загальновідомими подіями в східних регіонах України, наслідками яких стали захоплення заручників, цивільних та військових об'єктів, загострення суспільно-політичної обстановки та людські жертви, що неминуче й закономірно загостило невідкладну необхідність виявлення й позбавлення осіб, пов'язаних із терористичною та сепаратистською діяльністю, джерел фінансування.

Отже, поняття «фінансування терористичної діяльності» вперше було нормативно закріплено в міжнародному праві у 1994 році в прийнятій ООН Декларації про заходи щодо ліквідації міжнародного тероризму (затверджена Резолюцією 49/60 Генеральної Асамблеї ООН від 9 грудня 1994 року). У цьому документі Організацією Об'єднаних Націй було закріплено обов'язок країн-учасниць «утримуватись від організації терористичної діяльності, підбурювання до неї, сприяння її здійсненню, фінансування, заохочення чи проявлення терпимості до неї та приймати належні практичні заходи щодо забезпечення того, щоб їхні відповідні території не використовувались для створення терористичних баз чи навчальних таборів для підготовки та організації терористичних актів, спрямованих проти інших держав та їх громадян».

У 1996 році ООН закликала всі держави світу (підпункт (1) пункту 3 Резолюції 51/210 Генеральної Асамблеї від 17 грудня 1996 року) «здійснити кроки, з тим, щоб запобігати й протидіяти відповідними внутрішніми заходами фінансуванню терористів і терористичних організацій, незалежно від того, здійснюються таке фінансування прямо чи опосередковано через організації, які також мають або стверджують, що мають на меті благодійні, суспільні чи культурні цілі, або також залучені у заборонені види діяльності, як незаконне постачання зброї, незаконний обіг наркотиків та вимагательства, включаючи використання осіб з метою фінансування терористичної діяльності». Майже через рік потому, в Резолюції 52/165 Генеральної Асамблеї від 15 грудня 1997 року Організація Об'єднаних Націй знову закликала держави світу розглянути, зокрема, питання про здійснення