

УДК 343.3.7

КРИМІНАЛЬНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ІНФОРМАЦІЙНИХ ПРАВОВІДНОСИН

Тугарова О.К., к. ю. н.,
доцент кафедри організації захисту інформації з обмеженим доступом
Національна академія Служби безпеки України

У статті аналізуються нормативні приписи чинного кримінального законодавства, якими забезпечується охорона та захист інформаційних правовідносин, пропонується оптимальна модель системи норм Кримінального кодексу України, що встановлюють відповідальність за порушення порядку обігу інформації.

Ключові слова: кримінальна відповідальність, класифікація злочинів в інформаційній сфері, інформаційні правовідносини, інформаційна безпека.

В статье анализируются нормативные предписания действующего уголовного законодательства, на основании которых осуществляется охрана и защита информационных отношений, предлагается оптимальная модель системы норм Уголовного кодекса Украины, которые определяют основания юридической ответственности за правонарушения в информационной сфере.

Ключевые слова: уголовная ответственность, классификация преступлений в информационной сфере, информационные правоотношения, информационная безопасность.

Tugarova O.K. PUBLIC INFORMATION RELATIONSHIP CRIMINAL FRAMEWORK PROTECTION

The scientific article is devoted to current criminal law regulatory requirements, which provided legal information relationship refuge and protection, it is optimal model of Ukraine's Criminal Code rules system proposed, establishing responsibility for information flow order violation.

Key words: criminal responsibility, crimes classification in information sector, legal information relations, information security.

Постановка проблеми. Розбудова правової держави, що відбувається на фоні трансформації українського суспільства від постіндустріального до інформаційного, потребує створення ефективного механізму охорони та захисту суспільних відносин у сфері обігу інформації. Надійність такого механізму забезпечується як технічними, так і правовими заходами, що зосереджені в нормах чинного законодавства.

В системі правового забезпечення обігу інформації особливого значення набуває інститут кримінальної відповідальності, який виступає дієвим засобом охорони і захисту інформаційних правовідносин і спрямований на боротьбу з кримінальними правопорушеннями в інформаційній сфері.

Правову основу виникнення і настання кримінальної відповідальності за правопорушення в інформаційній сфері становить Кримінальний кодекс України (надалі – КК України), який ґрунтується на Конституції України та загальноновизнаних принципах і нормах міжнародного права [1]. За останні роки чинний КК України зазнав значних змін і доповнень, що пояснюється не лише стрімким розвитком інформаційних відносин, а й появою нових видів злочинів, спрямованих на дестабілізацію інформаційної безпеки людини, суспільства і держави. Зростає і кількість вже існуючих злочинних проявів в інформаційному просторі. Ці фактори зумовлюють потребу подальших наукових розробок з метою вдосконалення кримінально-правового регулювання правовідносин в інформаційній сфері.

Ступінь розробленості проблеми. У різні часи дослідженню проблем кримінальних правопорушень у сфері обігу інформації присвячували свої роботи О.Ф. Бантишев, К.І. Беляков,

Г.В. Виноградова, В.О. Глушков, С.В. Дрьомов, С.В. Дьяков, М.П. Карпушин, М.В. Карчевський, В.А. Ліпкан, А.І. Марущак, О.Є. Остапенко, О.С. Самойлова, Є.В. Сіра, Є.Ф. Тищенко, Н.А. Савінова, К.Г. Фітісенко, О.О. Шамсутдінов, В.М. Шлапаченко та інші дослідники. Вони сформулювали низку важливих положень, які продуктивно використовуються в теорії і практиці кримінального права протягом тривалого часу. Однак праці вказаних авторів переважно висвітлюють проблеми юридичної кваліфікації конкретних злочинів у сфері обігу інформації з обмеженим доступом, а також характеристики окремих видів інформаційної діяльності. Недостатність комплексних наукових досліджень, присвячених вирішенню проблемних питань кримінальної відповідальності за інформаційні правопорушення, не сприяє гармонізації чинного кримінального законодавства та практиці його застосування і вимагає подальших наукових розробок у даній сфері.

Метою даної роботи є аналіз нормативних приписів вітчизняного кримінального законодавства, спрямованих на охорону та захист відносин в інформаційній сфері, та створення на цій підставі оптимальної моделі системи норм КК України, що передбачають відповідальність за порушення інформаційних правовідносин.

Цільове призначення роботи зумовило розв'язання таких завдань:

- розкрити зміст поняття інформаційних правовідносин;
- окреслити та надати класифікацію правопорушень в інформаційній сфері;
- сформулювати пропозиції, спрямовані на вдосконалення кримінального законодавства у сфері охорони та захисту інформаційних правовідносин.



Виклад основного матеріалу. Життя будь-якого суспільства є вельми динамічним й різноманітним. Разом із тим функціонуванню соціуму характерна наявність досить сталих взаємовідносин між соціальними суб'єктами, які прийнято називати сферами суспільного життя. До основних із них традиційно відносять соціальну, економічну, духовну сфери тощо. Особливе місце в цій системі займає інформаційна сфера, яка у найбільш широкому розумінні сприймається як категорія, що відображає вимір буття сучасної людини, утворення інформацією, процесами її руху, переходу від однієї форми до іншої, від явищ реального світу до знань про них [2, с. 6].

Визначальним компонентом інформаційної сфери є інформаційні відносини, що відображають сформовані комунікативні зв'язки суспільства щодо реалізації наявних інформаційних потреб. Ці потреби спрямовані на отримання безперешкодного доступу до інформаційних ресурсів, отримання якісних інформаційних послуг, забезпечення належного захисту інформації.

Інформаційні правовідносини є різновидом правових відносин, через що їм притаманні всі структурні елементи останніх: суб'єкт, об'єкт та зміст. Проте інформаційні правовідносини є особливим видом відносин, які виникають, змінюються й припиняються у процесі здійснення врегульованою нормою права інформаційної діяльності: створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації. Порушення встановленого законом порядку здійснення основних видів інформаційної діяльності є підставою для виникнення і настання юридичної відповідальності, у тому числі відповідальності кримінальної.

Чинне кримінальне законодавство не містить окремого розділу, родовим об'єктом якого є відносини у сфері обігу інформації. Водночас норми Особливої частини КК України закріплюють понад 50 складів злочинів, що посягають на встановлений законом порядок створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації. З метою забезпечення системного підходу у визначенні підстав кримінальної відповідальності за правопорушення в інформаційній сфері їх доцільно класифікувати на певні групи.

Першу групу становлять кримінальні правопорушення, що посягають на врегульовані законом суспільні відносини у сфері обігу інформації з обмеженим доступом та іншої інформації, що охороняється законом.

Залежно від змісту відомостей, які охороняються нормами КК України, та суб'єктів, на яких поширюється обов'язок забезпечення їх охорони та захисту, серед підстав кримінальної відповідальності можна виділити злочини, що посягають на встановлений порядок обігу державної таємниці, професійної таємниці, таємниці особистого життя, банківської та комерційної таємниці, таємниці слідства та інших таємниць, що охороняються законом.

Злочини у сфері обігу інформації, що становлять державну таємницю, містяться у різних розділах Особливої частини КК України,

проте спільним для них є предмет злочинного посягання – відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим законом, державною таємницею і підлягають охороні державою [3].

Підстави кримінальної відповідальності за злочини, предметом яких є відомості, що становлять державну таємницю, насамперед, визначені в Розділі I КК України – «Злочини проти основ національної безпеки України». Два склади злочинів цього Розділу мають безпосереднє відношення до встановленого законом порядку охорони та захисту відомостей, що становить державну таємницю: ст. 111 КК України – «Державна зрада» і ст. 114 КК України – «Шпигунство». Об'єктивна сторона злочинів, передбачених ст. ст. 111, 114 КК України виражається у двох формах: 1) **передача** іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю; 2) **збирання** таких відомостей **з метою передачі** іноземній державі.

Підстави кримінальної відповідальності за вчинення злочинів у сфері обігу державної таємниці також містяться в Розділі XIV КК України – «Злочини у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову на мобілізацію». Ст. 328 КК України («Розголошення державної таємниці») передбачає відповідальність за розголошення відомостей, що становлять державну таємницю, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, за відсутності ознак державної зради або шпигунства. Також ст. 329 КК України («Втрата документів, що містять державну таємницю») встановлює відповідальність за втрату документів або інших матеріальних носіїв секретної інформації, що містять державну таємницю, а також предметів, відомості про які становлять державну таємницю, особою, якій вони були довірені, якщо втрата стала результатом порушення встановленого законом порядку поводження із зазначеними документами та іншими матеріальними носіями секретної інформації або предметами.

Кримінальне законодавство України встановлює відповідальність за порушення встановленого законом порядку зберігання відомостей військового характеру, що становлять державну таємницю. Розділ XIX – «Злочини проти встановленого порядку несення військової служби (військові злочини)» містить ст. 422 КК України – «Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості». З об'єктивної сторони злочин, передбачений ст. 422 КК України, може виражатися у двох формах: розголошення відомостей військового характеру, що становлять державну таємницю, за відсутності ознак державної зради (ч. 1 ст. 422 КК України) та порушення встановлених правил поводження з докумен-

тами або матеріалами, що містять відомості військового характеру, які становлять державну таємницю, а також із предметами, відомості про які становлять державну таємницю, що спричинило їхню втрату (ч. 2 ст. 422 КК України).

У системі кримінальних правопорушень, що посягають на встановлений законом порядок обігу інформації з обмеженим доступом, слід виокремити злочини, предметом яких є відомості, що становлять зміст професійної таємниці. Обов'язком зберігати такі відомості наділені представники певних професій (адвокати, журналісти, медичні працівники, нотаріуси тощо). Важливим у відношенні збереження професійної таємниці є питання довіри – особа, яка потребує певної професійної допомоги, погоджується надати чуттєву для себе інформацію, очікуючи збереження її в таємниці. Вона також очікує, що надана нею інформація може бути розголошена лише за її згоди. При цьому така інформація надається під час реалізації особою своїх прав і свобод. Тому розголошення довіреної інформації матиме наслідок обмеження прав осіб, які не зможуть вільно користуватися послугами відповідних професій, якщо не матимуть впевненості у захищеності інформації, яку вони передають [4, с. 146].

Серед кримінальних правопорушень у сфері охорони професійної таємниці законодавець, насамперед, виділяє злочин, передбачений ст. 145 КК України – «Незаконне розголошення лікарської таємниці». Безпосереднім об'єктом зазначеного злочину є встановлений законом порядок збереження лікарської таємниці, який забезпечує належний стан здоров'я громадян. Спеціальною нормою стосовно ст. 145 КК України є дії, передбачені ст. 132 КК України («Розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби»), що виражаються у розголошенні відповідною службовою особою лікувального закладу, допоміжним працівником, який самочинно здобув інформацію, або медичним працівником відомостей про проведення відповідного медичного огляду та його результатів.

До кримінальних правопорушень у сфері охорони професійної таємниці також слід відносити злочин, передбачений ст. 397 КК України – «Втручання в діяльність захисника чи представника особи». Суспільна небезпечність цього злочину полягає в тому, що він порушує нормальну діяльність осіб, які надають необхідну правову допомогу юридичним і фізичним особам у захисті їхніх законних інтересів у цивільному, адміністративному і кримінальному судочинстві.

Об'єктивна сторона злочину, передбаченого ст. 397 КК України, виражається у вчиненні будь-яких перешкод до здійснення правомірної діяльності захисника чи представника особи з надання правової допомоги або порушенні встановлених законом гарантій їх діяльності та професійної таємниці. Таке порушення може виражатися у проханні, вимозі, примушуванні надати відомості,

що становлять зміст адвокатської таємниці, примусовому вилученні, огляді документів, пов'язаних із виконанням захисником його обов'язків, а також розголошенні змісту таких документів.

Суміжною до професійних таємниць, охорона яких забезпечується нормами чинного КК України, є банківська таємниця. Її основна відмінність від професійних таємниць полягає в тому, що інформація, яка становить зміст банківської таємниці, довіряється не особі, яка належить до певної професії, а конкретній організації – банківській установі. При цьому основними умовами режиму існування такої таємниці є ознака добровільності передачі інформації клієнтом певній організації та вимога захисту цієї інформації від розголошення, навіть за відсутності прямої вказівки на це з боку фізичної чи юридичної особи [4, с. 152].

Чинний КК України містить два склади злочинів у сфері обігу банківської інформації, а саме: ст. 231 КК України – «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю» і ст. 232 КК України – «Розголошення комерційної або банківської таємниці». Протиправність дій означених правопорушень знаходить свій вираз у формі отримання відомостей з метою їх подальшого розголошення чи іншого використання і незаконному використанні відомостей, що становлять комерційну або банківську таємницю.

Кримінальний закон визнає злочинним діяння, що посягає на встановлений порядок обігу інсайдерської інформації – інформації про емітента, його цінні папери та похідні (деривативи), що перебувають в обігу на фондовій біржі. Ст. 2321 КК України передбачає відповідальність за незаконне використання такої інформації, що виражається у її розголошенні чи іншому використанні і може суттєво вплинути на ринкову вартість цінних паперів компанії.

Суміжною до професійних таємниць, охорона яких забезпечується нормами чинного КК України, є таємниця досудового розслідування. Ст. 387 КК України встановлює відповідальність за розголошення даних оперативно-розшукової діяльності, досудового розслідування. Протиправність зазначених дій виражається у розголошенні даних оперативно-розшукової діяльності або досудового розслідування як особою, попередженою в установленому законом порядку про обов'язок не розголошувати такі дані, так і суддею, прокурором, слідчим, працівником оперативно-розшукового органу незалежно від того, чи приймала ця особа безпосередню участь в оперативно-розшуковій діяльності, досудовому розслідуванні.

Посяганням на встановлений законом порядок забезпечення таємниці досудового розслідування та конфіденційності іншої інформації, пов'язаної з виявленням та розкриттям злочинів, слід визнавати злочин, передбачений ст. 381 КК України – «Розголошення відомостей про заходи безпеки щодо особи, взятої під захист». Предметом цього злочину є відомості про заходи безпеки щодо особи, взятої під захист, які визначені в Законі



України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві» [5]. Це може бути інформація про особистого охорону, охорону житла і майна особи, взятої під захист, про зміну її місця роботи або навчання, про переселення в інше місце проживання, про зміну прізвища чи інших конфіденційних відомостей про цю особу тощо.

Злочини у сфері обігу інформації, що становить зміст таємниці особистого життя, містяться в Розділі V Особливої частини КК України і встановлюють відповідальність за розголошення відомостей, що становлять зміст таємниці кореспонденції (листування, телефонних розмов, телеграфної та іншої кореспонденції), таємниці усиновлення, таємниці голосування. Протиправний характер зазначених дій виражається в розголошенні певної інформації, незаконному ознайомленні з відомостями, що становлять зміст відповідної таємниці, усному чи письмовому повідомленні відомостей тощо.

Окрему групу кримінальних правопорушень утворюють злочини, що посягають на порядок обігу інформації, що не є обмеженою у доступі. Проте використання такої інформації відбувається у визначеному законом порядку. Об'єктивна сторона таких діянь може виражатися у:

1) наданні завідомо неправдивої інформації (ст. 158, ч. 1 ст. 2091, ч. 1 ст. 2231, ч. 1 ст. 2232, ст. 238, ст. 259, ст. 358, ч. 1 ст. 366, ч. 1 ст. 383, ч. 1 ст. 384 КК України);

2) приховуванні або неподанні інформації (ст. 136, ч. 1 ст. 209, ч. 1 ст. 2091, ч. 1 ст. 2232, ст. 238, ч. 3 ст. 243, ст. 285, ч. 1 ст. 385, ст. 396 КК України).

Другу групу правопорушень у сфері обігу інформації, відповідальність за які передбачена нормами чинного кримінального законодавства, становлять злочини, що посягають на врегульовані законом суспільні відносини у сфері технічного захисту інформації.

Законодавець у Розділі XVI Особливої частини КК України – «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» – закріпив шість складів злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. ст. 361, 3611, 3612, 362, 363, 3631 КК України), об'єктивна сторона яких виражається у таких формах:

– несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ч. 1 ст. 361 КК України);

– створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ч. 1 ст. 3611 КК України);

– несанкціоновані збут або розповсюдження інформації з обмеженим доступом,

яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства (ч. 1 ст. 3612 КК України);

– несанкціоновані зміна, знищення або блокування інформації (ч. 1 ст. 362 КК України) та несанкціоновані перехоплення або копіювання інформації (ч. 2 ст. 362 КК України), яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах, або зберігається на носіях такої інформації;

– порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України);

– умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів (ч. 1 ст. 3631 КК України).

Спеціальною нормою по відношенню до злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, є дії, передбачені ст. 3761 КК України – «Незаконне втручання в роботу автоматизованої системи документообігу суду». Метою функціонування такої системи є об'єктивний та неупереджений розподіл справ між суддями, надання учасникам судового процесу відповідної інформації, централізоване зберігання процесуальних документів, підготовка статистичних даних, реєстрація вхідної і вихідної кореспонденції та етапів її руху.

Об'єктивна сторона складу злочину, передбаченого ст. 3761 КК України, може виражатися у таких формах:

– умисне внесення неправдивих відомостей до автоматизованої системи документообігу суду;

– несвоєчасне внесення відомостей до автоматизованої системи документообігу суду;

– несанкціоновані дії з інформацією, що міститься в автоматизованій системі документообігу суду, та інше втручання в роботу автоматизованої системи документообігу суду.

Третю групу правопорушень становлять злочини, що посягають на врегульовані законом суспільні відносини у сфері інформаційно-психологічної безпеки особи та суспільства.

Закон України «Про основи національної безпеки України» серед загроз у сфері інформаційної безпеки поряд із розголошенням інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованою на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави, комп'ютерною злочинністю та тероризмом, окремо виділяє прояви обмеження свободи слова та доступу до публічної інформації, та намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упе-

редженої інформації [6]. Чинний КК України містить ряд статей, нормами яких визначаються підстави кримінальної відповідальності за вчинення вищезазначених протиправних дій. Сукупність злочинів, що посягають на свободу слова і доступу до публічної інформації, особисту і суспільну свідомість, утворюють особливу групу протиправних діянь у сфері інформаційно-психологічної безпеки.

Ст. 171 КК України встановлює кримінальну відповідальність за «Перешкоджання законній професійній діяльності журналістів». Суспільна небезпечність даного злочину полягає у порушенні встановленого порядку здійснення професійної діяльності журналістів, спрямованої на забезпечення конституційного права людини на свободу думки і слова, вільне вираження своїх поглядів і переконань, права вільно збирати, зберігати, використовувати і поширювати інформацію. З об'єктивного боку злочин може виражатися у формі перешкоджання законній діяльності журналістів (ч. 1 ст. 171 КК України) або переслідування журналіста за виконання професійних обов'язків або за критику (ч. 2 ст. 171 КК України).

Деструктивний вплив на сферу інформаційно-психологічної безпеки особи і суспільства чинять злочини, передбачені ст. 298 КК України – «Незаконне проведення пошукових робіт на об'єкті археологічної спадщини, знищення, руйнування або пошкодження об'єктів культурної спадщини» та ст. 2981 КК України – «Знищення, пошкодження або приховування документів чи унікальних документів Національного архівного фонду». Суспільна небезпечність зазначених протиправних діянь полягає у завданні істотної шкоди культурній спадщині українського народу, що, у свою чергу, впливає на рівень національної самосвідомості та принципів морального життя суспільства. Об'єктивна сторона зазначених злочинів може проявлятися в умисному незаконному знищенні, руйнуванні або пошкодженні об'єктів культурної спадщини чи їх частин (ч. 2 ст. 298 КК України); умисному незаконному знищенні, руйнуванні або пошкодженні пам'яток національного значення (ч. 3 ст. 298 КК України); умисному знищенні, пошкодженні або приховуванні документів Національного архівного фонду (ч. 1 ст. 2981 КК України); умисному знищенні, пошкодженні або приховуванні унікальних документів Національного архівного фонду (ч. 2 ст. 2981 КК України).

Злочини, пов'язані з негативним інформаційно-психологічним впливом на особу і суспільство також знаходять свій вираз у різного роду публічних закликах (ст. ст. 109, 110, 2582, 295, 436 КК України); розпалюванні національної ворожнечі (ст. 161 КК України); пропаганді насильства та аморального способу життя (ст. ст. 300, 301, 436 КК України); впливі на діяльність державних службовців (ст. ст. 343, 344, 376, 397 КК України) тощо.

Зазначені злочини містяться у різних розділах Особливої частини КК України, проте спільним для них є об'єкт посягання – інформаційно-психологічна безпека особи і суспільства, яка, у свою чергу, є складовою

частиною інформаційної безпеки держави і має займати особливе місце в державній політиці під час її забезпечення.

Висновки. Проведений аналіз норм чинного кримінального законодавства засвідчив, що інститут кримінальної відповідальності є дієвим правовим засобом забезпечення охорони та захисту інформаційних відносин, які відображають сформовані комунікативні зв'язки суспільства щодо реалізації наявних інформаційних потреб.

На сьогодні вітчизняне кримінальне законодавство містить значну кількість нормативних приписів, якими визначаються підстави виникнення та настання відповідальності за порушення встановленого законом порядку створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації. Злочини у сфері обігу інформації можна класифікувати за такими групами:

1. Злочини, що посягають на врегульовані законом суспільні відносини у сфері обігу інформації з обмеженим доступом та іншої інформації, що охороняється законом.

2. Злочини, що посягають на врегульовані законом суспільні відносини у сфері технічного захисту інформації.

3. Злочини, що посягають на врегульовані законом суспільні відносини у сфері інформаційно-психологічної безпеки особи та суспільства.

Звичайно, запропонована класифікація має доволі умовний характер і не позбавлена можливості її подальшого обговорення у наукових колах. Водночас, очевидним є факт ідентичності форм об'єктивної сторони злочинів у сфері обігу інформації та загроз інформаційній безпеці людини, суспільства і держави. До числа наявних та потенційно можливих явищ і чинників, що створюють небезпеку життєво важливим національним інтересам України в інформаційній сфері, закон відносить:

1) прояви обмеження свободи слова та доступу до публічної інформації;

2) поширення засобами масової інформації культу насильства, жорстокості, порнографії;

3) комп'ютерну злочинність та комп'ютерний тероризм;

4) розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави;

5) намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [6].

З огляду на зазначене, вбачається доцільним об'єднання в окремому розділі Особливої частини КК України злочинів у сфері обігу інформації, родовим об'єктом яких виступатиме інформаційна безпека людини, держави і суспільства. Такий підхід забезпечить системний підхід у визначенні кола потенційних і реальних загроз інформаційній безпеці, та сприятиме довершеності положень кримінального законодавства України.



ЛІТЕРАТУРА:

1. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III // Відомості Верховної Ради України. – 2001. – № 25-26. – Ст. 131.
2. Тихомиров О. Юридична відповідальність за правопорушення в інформаційній сфері: навчальний посібник / О. Тихомиров, О. Тугарова. – Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2015. – 200 с.
3. Про державну таємницю : Закон України від 21.01.1994 р. № 3855– XII // Відомості Верховної Ради України. – 1994. – № 16. – Ст. 93.

4. Закон України «Про доступ до публічної інформації»: Науково-практичний коментар (видання ініційоване Комітетом Верховної Ради України з питань свободи слова та інформації і рекомендоване для використання в адміністративній та судовій практиці) / Р. Головенко, Д. Котляр, О. Нестеренко. – К. : Фундація «Центр суспільних медіа», 2012. – 335 с.
5. Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві: Закон України від 23.12.1993 р. № 3782–XII // Відомості Верховної Ради України. – 1994. – № 11. – Ст. 51.
6. Про основи національної безпеки : Закон України від 19.06.2003 р. № 964–IV // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

УДК 351.746.1: 343.326: 623.454.8

ЮРИДИЧНА ПРИРОДА АНТИТЕРОРИСТИЧНОЇ БЕЗПЕКИ ЯДЕРНИХ ОБ'ЄКТІВ

Устїч Р.С., аспірант
Академія Служби безпеки України

Автором на підставі аналізу науково-теоретичних та законодавчих засад проаналізовано базові поняття у сфері, що досліджується, а саме «тероризм», «ядерний тероризм» та «ядерні об'єкти». На цій основі запропоновано власне формулювання поняття «антитерористична безпека ядерних об'єктів».

Ключові слова: тероризм, ядерний тероризм, ядерні об'єкти, безпека, антитерористична безпека ядерних об'єктів.

Автором на основе анализа научно-теоретических и законодательных положений проанализированы базовые понятия в исследуемой сфере, а именно «терроризм», «ядерный терроризм» и «ядерные объекты». На этой базе предложено собственное формулирование понятия «антитеррористическая безопасность ядерных объектов».

Ключевые слова: терроризм, ядерный терроризм, ядерные объекты, безопасность, антитеррористическая безопасность ядерных объектов.

Ustich R.S. LEGAL NATURE OF ANTITERRORIST SAFETY OF NUCLEAR OBJECTS

The author based on the analysis of scientific-theoretical and legal framework analyzes the concept of «terrorism», «nuclear terrorism» and «nuclear objects» and on this basis the actual wording of «antiterrorism safety of nuclear objects».

Key words: terrorism, nuclear terrorism, nuclear objects, safety, antiterrorism safety of nuclear objects.

Після розпаду Радянського Союзу і проголошення у 1991 р. незалежності перед Україною, яка дістала у спадщину третій у світі (після США і Росії) ядерний арсенал, постало питання про долю цієї зброї. 14 січня 1994 р. у Москві президенти України, США та Росії підписали тристоронню заяву, в якій були зафіксовані домовленості щодо практичної реалізації рішення України відмовитись від ядерної зброї. На 1 червня 1996 р. на території України не залишилося жодного ядерного боєзаряду або боєприпасу.

Здавалося б, для України питання ядерного тероризму не є актуальним, враховуючи зазначені історичні події. Проте Україна посідає сьоме місце у світі та п'яте в Європі за обсягами виробництва електроенергії на АЕС і має реальні шанси створення у перспективі власного ядерного паливного циклу, залучаючи зарубіжні потужності лише для збагачення урану. Ядерно-енергетичний комплекс України складає 4 АЕС, дослідні ядерні реактори, науково-дослідні інститути, 7 науково-дослідних і проектно-конструкторських закладів, 28 заводів виробників обладнання, 30 будівельно-монтажних організацій, Східний гірничо-збагачувальний комбінат (Жовті

Води Дніпропетровської області), дослідно-промисловий комплекс сухого сховища відпрацьованого ядерного палива (Запорізька АЕС), транспортні та інші комунікації.

У Міжнародній конвенції про боротьбу з актами ядерного тероризму [6] зазначено, що акти ядерного тероризму можуть призводити до самих серйозних наслідків і можуть створювати загрозу міжнародному миру та безпеці, відзначаючи також, що в існуючих багатосторонніх положеннях міжнародного права дії напади не розглядаються належним чином.

Особливу стурбованість викликає зростаюча зацікавленість терористів у придбанні подільних та радіоактивних матеріалів для цілей ядерного шантажу. Відомо, що з-поміж інших засобів масового знищення ядерна зброя спричиняє миттєву та найбільшу руйнацію об'єктів міської та техногенної мегаструктури, масові жертви, а наслідки її застосування є довготривалими [14, с. 74].

У зв'язку з цим та з метою превентивних заходів, а також запобігання та припинення ядерного тероризму є актуальним питання антитерористичної безпеки ядерних об'єктів. Як на доктринальному, так і на законодавчо-