Науково-дослідний інститут інформатики і права
Національної академії правових наук України

Апарат Ради національної безпеки і оборони України

Київський науково-дослідний інститут судових експертиз
Міністерства юстиції України

Навчально-науковий центр інформаційного права
та правових питань інформаційних технологій ФСП
Національного технічного університету України
«Київський політехнічний інститут»

«ТЕОРІЯ І ПРАКТИКА ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ПРАВОПОРУШЕННЯ В ІНФОРМАЦІЙНІЙ СФЕРІ»

МАТЕРІАЛИ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
08 червня 2016 року

Київ – 2016

УДК 34:004]

ББК 67.404.3я43

Т33 Теорія і практика юридичної відповідальності за правопорушення в інформаційній сфері: Матеріали науково-практичної конференції / 08 червня 2016 р., м.Київ / Упорядн. : В.М.Фурашев, С.Ю.Петряєв. – К.: НДІІП НАПрН України, Апарат РНБО України, КНДІСЕ Мінюсту України, НТУУ «КПІ», 2016. – 200с.

ISBN978-966-622-779-2

Подано матеріали з актуальних питань проблем юридичної відповідальності за правопорушення в інформаційної сфері. Доповіді учасників конференції, що опубліковані у збірнику можуть бути корисними для законодавців, вчених, фахівців та експертів інформаційної сфери, науково-педагогічних працівників, аспірантів, докторантів, студентів вищих навчальних закладів, а також усіх, хто цікавиться сучасними суспільно-правовими проблемами розвитку інформаційного суспільства, а також проблемами захисту прав людини в інформаційному суспільстві.

Організаторами заходу виступили: Навчально-науковий центр інформаційного права та правових питань інформаційних технологій ФСП НТУУ «КПІ», Науково-дослідний інститут інформатики і права НАПрН України, Апарат Ради національної безпеки і оборони України, Київський науково-дослідний інститут судових експертиз Міністерства юстиції України. Участь у конференції взяли провідні експерти і вчені наукових установ і навчальних закладів України, представники зацікавлених державних органів та громадських організацій. Інформаційну підтримку у проведенні заходу надали: журнали «Інформація і право», «Правова інформатика», «Теорія і практика», «Інформація та безпека», Вісник НТУУ «КПІ» «Політологія. Соціологія. Право» та Міжвідомчий науково-методичний збірник «Криминалистика и судебная экспертиза» КНДІСЕ МЮ України.

Матеріали викладено в авторській редакції.

Упорядники: **Фурашев В.М., Петряєв С.Ю.**

Оформлення обкладинки:
Лабораторія технічної естетики та дизайну ФСП НТУУ «КПІ» (designlab.kpi.ua@gmail.com)
Балашов Д.В. (balashov.dim@gmail.com)

Рекомендовано до друку
Вченою радою Науково-дослідного інституту інформатики і права
Національної академії правових наук України
Протокол № 6 від 09.06.2016 р.

Вченою радою факультету соціології і права Національного технічного
Університету України «Київський політехнічний інститут»
Протокол №11 від 29.06.2016 р.

ISBN978-966-622-779-2

З М І С Т

Н.А.Савінова,
д.ю.н., с.н.с.,
НДІ ІП НАПрН України

ІНФОРМАЦІЙНО-ПРАВОВА ПОЛІТИКА УКРАЇНИ: МІФИ І РЕАЛЬНІСТЬ В ПЕРІОД КРИЗИ

Інформаційно-правова політика сучасної України не витримує критики: вона не орієнтована ані на формування у суспільстві позитивної національної єдності, ані - на захист населення від інформаційно-маніпулятивних впливів, якими наповнені як зовнішнє, так і внутрішнє мовлення українського ефіру.

Такій необхідності було приділено належної уваги рішенням РНБО України. Реалізація їх протягом 2014 року до сьогодні майже лишилися міфом.

Міфи. 1 квітня 2014 року РНБО України було визначено для Кабінету Міністрів України ***у місячний строк*** серед іншого розробити за участю Національного інституту стратегічних досліджень, Служби безпеки України, представників громадянського суспільства та подати на розгляд Ради національної безпеки і оборони України ***проект Стратегії розвитку інформаційного простору України***, в якому, зокрема, визначити мету, завдання, структуру та режим функціонування національної системи забезпечення інформаційної безпеки держави та проект Стратегії кібернетичної безпеки України, а також, протягом того самого терміну «***розробити і впровадити комплексні заходи організаційного, інформаційного і роз'яснювального характеру*** щодо:

- всебічного висвітлення заходів з реалізації державної політики у сфері забезпечення інформаційної безпеки;

- ***посилення контролю за додержанням законодавства з питань інформаційно-психологічної*** та кібернетичної безпеки»[1]) жирний курсив мій – Н.С.[2]).

Тим же рішенням у ***тримісячний строк*** Кабінету Міністрів України доручалося розробити за участю Національного інституту стратегічних досліджень, Служби безпеки України, інших державних органів і науково-дослідних установ та подати на розгляд Ради національної безпеки і оборони України ***проект нової редакції Доктрини інформаційної безпеки України***;

розробити і внести на розгляд Верховної Ради України: /…/

- проект Закону України про кібернетичну безпеку України; /…/;

ужити заходів щодо забезпечення поширення у світі об'єктивних відомостей про суспільно-політичну ситуацію в Україні, зокрема, шляхом створення відповідного медіа-холдингу для підготовки якісного конкурентоздатного інформаційного продукту».

Цілком зрозуміло, що ані у місячний, ану і тримісячний термін жодного з зазначених завдань вирішено не було. Однак, їх не вдалося вирішити і протягом двох років після прийняття відповідного наведеного рішення РНБО. Більш того: не вдалось цього зробити і протягом понад півтора роки з моменту утворення Міністерства інформаційної політики України, яке «є головним органом у системі центральних органів виконавчої влади у сфері забезпечення інформаційного суверенітету України, зокрема з питань поширення суспільно важливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів».[3]

Натомість, Міністерство інформаційної політики у 2016 році відзвітувало: у 2015 році в законодавчій ініціативі головними досягненнями міністерства були…:

- «Доктрина інфорбезпеки
- Закон про інфобезпеку
- Державна програма розвитку інфопростору»[4].

Очевидно, що після таких звітів Міністерства перед народом України, слід, насамперед, говорити про містифікації, адже в реаліях (станом на червень 2016 року) ані Доктрини, ані концепції інформаційної безпеки в державі реально н існує.

Так, Доктрина інформаційної безпеки України, затверджена Указом Президента України від 08.07.2009 № 514/2009[5] втратила чинність на підставі Указу Президента України «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про скасування деяких рішень Ради національної безпеки і оборони України» та визнання такими, що втратили чинність, деяких указів Президента України від 06.06.2014 № 504/2014[6], а нова Доктрина прийнята так і не була – вона лишилася у проекті[7]. Так само, у проекті лишилася і Концепція інформаційно безпеки[8], яка не витримала критики.

Державної програми розвитку інформаційного простору України не існує взагалі, навіть, на рівні будь-яких оприлюднених на офіційних сайтах проектів, як і вказаного вище Закону.

Що ж таке сьогодні українська інформаційно-правова політика? Це – взагалі-то цілковитий міф, хоча його реалізатор – Міністерство інформаційної політики і існує. Постулати такої політики, як напрям діяльності Кабінету Міністрів визначні ще на рівні наведеного вище рішення РНБО. Само ж Міністерство інформаційної політики, відповідно до визначених для нього КМУ повноважень основними завданнями має:

1) забезпечення інформаційного суверенітету України, зокрема з питань поширення суспільно важливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів;

2) забезпечення здійснення реформ засобів масової інформації щодо поширення суспільно важливої інформації[9].

Останнє особливо вражає: яка інформація в нашій державі є соціально важливою, якщо навіть (не будемо поки говорити про актуальність цього) промови політиків щодо «національної ідеї» та істориків стосовно «історичної пам’яті» перетворюються на посміховисько в контексті перевантаження ефіру прайм-тайм негативними та/або агресивними новинами та ток-шоу, спрямованими на активацію прихильників тих чи інших політичних сил у державі.

У той же час, регіональним новинам у національному ефірі не приділяється належної уваги: регіональні новини висвітлюються ситуативно, і лише в випадках виникнення екстраординарних подій у тому чи іншому регіоні. В цілому ж, UA:Перший та інші канали національного мовлення не витримують конструкцій мовлення, які б забезпечували належне висвітлення позитивних загальнонаціональних та в цілому регіональних новин. Отже, сучасне вітчизняне телебачення не вживає належних заходів для формування розуміння єдності у населення країни, самоідентичності українця, спільності очікувань чи то проблем.

Чи потрібно в країні, населення якої яскраво продемонструвала світові свій патріотизм, демонструвати його? Чи не краще присвятити ефір підтримці такого патріотизму, поваги, гідності людини в країні, яка продовжує переживати кризу в умовах зовнішнього втручання в її справи? Хіба не потрібно виховувати власну молодь на надбаннях вітчизняної культури і мистецтва, традиціях? І чи варто робити акценти на мові мовлення в країні, яка історично розмовляє на мовах 134 національностей її населення: чи не краще забезпечувати якісне багатомовне мовлення, даючи змогу людям в країні розвиватися в мультимовному та інтернаціональному середовищі?

Але ж варто повернутися до реалій інформаційно-правової політики. І, як не дивно, вона існує саме на рівні міжетнічних, мультикультурних національних відносин у державі.

Реалії. Результати опитування Центру Разумкова за Проектом “Формування спільної ідентичності громадян України в нових умовах: особливості, перспективи і виклики” реалізується за підтримки програми “Matra” МЗС Нідерландів, SIDA МЗС Швеції, Фонду Конрада Аденауера (2016)[10] продемонстрували такі результати, що наводяться мною нижче у прямих цитатах з тексту звіту. (Всі ***наведені нижче виділення жирним курсивом у тексті – мої, Н.С.***).

Ідентифікація з певною територіальною спільнотою:

«***Однакові частки (по 40%) респондентів засвідчили, що "у першу чергу" пов'язують себе з Україною та з конкретним населеним пунктом(містом, селом), де вони проживають. 11,4% опитаних вказали, що пов'язують себе з регіоном проживання.***

З іншими спільнотами засвідчили свою ідентичність незначні частки респондентів (2,1% – з Радянським Союзом, 1,5% – з Європою, 0,6% – з Росією).

У якості другого вибору відносна ***більшість (33%) опитаних визначили Україну, 26% – свій населений пункт, 22% – свій регіон.*** Європу в якості другого вибору назвали 7,4% опитаних, СРСР – 2,3%, Росію – 1,2%»[11].

Ставлення до українського громадянства:

«***Більшість респондентів***, які є громадянами України, ***пишаються своїм українським громадянством (68%)***, не пишаються – 23%. Порівняно з опитуванням 2005 р., ***частка тих, хто пишається українським громадянством, зросла на 12%***».[12]

Ставлення до країни як до Батьківщини:

«***Україну сприймають як Батьківщину переважна більшість жителів усіх регіонів країни – від 98%*** на Заході до 83% на Донбасі. Водночас, ***за наявності можливості обирати, Україну обрали б Батьківщиною 72% громадян***, не обрали б – 13%».[13]

Потреба пишатися країною

«***Відносна більшість (48%) респондентів для щастя в житті відчуває необхідність пишатися своєю країною***. Для 41% опитаних для щастя достатньо особистого благополуччя».[14]

Оцінка громадянами досягнень України

«***Громадяни України найбільше відчувають гордість*** за свою країну за її досягнення ***у спорті*** (73%); ***за історію*** України (69%); ***за національний характер українців***, здатність боротися за свою державу і свої права (68%); за ***досягнення в мистецтві, літературі*** (65%); ***за Збройні Сили країни***

(57%)11. Майже половина (49%) опитаних відчувають гордість ***за досягнення в галузях науки та технологій***».[15]

Розуміння патріотизму

«Найважливішими якостями для того, щоб бутипатріотом України (4,2-4,0 балів за п'ятибальною шкалою, в порядку зменшення), респонденти вважають:

- бажання ***виховувати в дітях любов до України***;
- ***повагу до своєї держави***, державних символів і свят;
- піклування про ***стабільний добробут своєї сім'ї***;
- ***повагу до законів і інститутів влади*** України;
- ***знання історії і культури*** України;
- ***готовність боротися за дотримання прав і свобод*** громадян України.

Дещо ***менш важливими*** (3,9-3,5 бали) громадяни визначили: працю на благо України; готовність публічно захищати репутацію своєї країни перед громадянами інших країн; готовність навіть ціною життя захищати Україну від зовнішніх ворогів; знання української мови; готовність навіть ціною життя захищати територіальну цілісність України (не дозволити регіонам відокремлюватись від України); прагнення до рівності прав усіх національностей; дотримання українських народних традицій у повсякденному житті; виступати за повне відновлення територіальної цілісності України (повернення Криму та Донбасу); наявність українського громадянства»[16].

Висновки: Очевидно, що такі дані, красномовніші, ніж будь-які коментарі. І коментувати варто лише інформаційно-правову політику держави, яка, нехтуючи думкою власного населення, нав'язує застарілі ідеологеми, не розвиваючі у мовленні ті інституції, на які очікують громадяни, які сприйматимуться населенням як природні механізми розвитку патріотичного Української суспільства і, відповідно, Української держави:

- державний та регіональний (інтегрований!) патріотизм, заснований на повазі до людини та традиційних, культурних, мистецьких, наукових, освітянських, технологічних, спортивних та інших досягненнях великої та малої Батьківщини;
- добробут людини, сімей, спільнот;
- інтернаціоналізм та багатомовність, засновані на знанні історії традиції України та поєднані з повагою до української мови та традиції.

Крім того, період не лише воєнного протистояння, а й мирний час розвитку держави важливе значення інформаційно-правової політики має приділятися питанням захисту Батьківщини від зовнішньої агресії та терористичних актів. Такі питання не лише необхідні у умовах гібридних холодних війн в умовах геополітичних колапсів, а й підтримують патріотичну свідомість населення, розуміння взаємної залежності миру в країні і життя людини в ній.

Література:

1. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України" // Офіційний сайт Верховної Ради України / http://zakon3.rada.gov.ua/laws/show/449/2014
2. Доповідач умисно не акцентує увагу у доповіді на питаннях відсутності інформаційно-політичних і інформаційно-правових заходів в сфері кібербезпеки, вважаючи їх окремим, самостійним блоком невирішених в державі питань.
3. Див. абз. 2 п. 1 Положення про Міністерство інформаційної політики України, затверджене Постановою Кабінету Міністрів України 14.01.2015 № 2 ЇЇ Офіційний сайт Верховної Ради України / http://zakon4.rada.gov.ua/laws/show/2-2015-%D0%BF
4. Міністерство інформаційної політики України: план на 2016 рік / Офіційний сайт Міністерства інформаційно політики України // http://mip.gov.ua/files/Presentation/MIP_activity_2016.pdf
5. Указ Президента України Про затвердження Доктрини інформаційної безпеки України від 08.07.2009 № 514/2009 // Офіційний сайт Верховної Ради України / http://zakon3.rada.gov.ua/laws/show/514/2009
6. Указ Президента України Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про скасування деяких рішень Ради національної безпеки і оборони України» та визнання такими, що

втратили чинність, деяких указів Президента України від 06.06.2014 № 504/2014 // Офіційний сайт Верховної Ради України // http://zakon3.rada.gov.ua/laws/show/504/2014
7. Проект Указу Президента України "Про Доктрину інформаційної безпеки України" // Офіційний сайт Державного комітету телебачення і радіомовлення України / http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025
8. Проект Концепції інформаційної безпеки України // Офіційний сайт Міністерства інформаційної політики України / http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf
9. Див. п. 3 Положення про Міністерство інформаційної політики України, затверджене Постановою Кабінету Міністрів України 14.01.2015 № 2 ЇЇ Офіційний сайт Верховної Ради України / http://zakon4.rada.gov.ua/laws/show/2-2015-%D0%BF
10. Центр Разумкова. ІДЕНТИЧНІСТЬ ГРОМАДЯН УКРАЇНИ В НОВИХ УМОВАХ: СТАН, ТЕНДЕНЦІЇ, РЕГІОНАЛЬНІ ОСОБЛИВОСТІ: Інформаційно-аналітичні матеріали до Фахової дискусії “Формування спільної ідентичності громадян України: перспективи та виклики” 7 червня 2016 р. / Проект “Формування спільної ідентичності громадян України в нових умовах: особливості, перспективи і виклики” реалізується за підтримки програми “Matra” МЗС Нідерландів, SIDA МЗС Швеції, Фонду Конрада Аденауера //
11. Там же – С. 4.
12. Там же – С. 4.
13. Там же – С. 4.
14. Там же – С. 5.
15. Там же – С. 5
16. Там же – С. 5.

----------***----------

І. М.Забара,
к.ю.н., доцент кафедри міжнародного права Інституту міжнародних відносинКиївського національного університету ім. Т. Шевченка

ТЕОРЕТИЧНІ І ПРАКТИЧНІ АСПЕКТИ МІЖНАРОДНО-ПРАВОВИХ ВІДНОСИН ВІДПОВІДАЛЬНОСТІ В ІНФОРМАЦІЙНІЙ СФЕРІ

Проблематика міжнародно-правової відповідальності виступає однією із самих складних у теорії і практиці міжнародного права. Її дослідженню

присвячена значна частина теоретичних робіт вітчизняних і іноземних дослідників. Проте, низка проблем не втрачає своєї актуальності.

Однією із цікавих і недосліджених виступає проблема міжнародно-правових відносин відповідальності.

У доктрині міжнародного права стверджується, що «соціальна природа міжнародних відносин, а також характер їх суб'єктів визначають особливі якості міжнародно-правових відносин» [1, с. 117]. Таке твердження дає підстави розмежувати і визначити їх за групами, а саме:

I) *правовідносини, що засновані на юридичній рівності сторін* (характеризуються суверенною рівністю суб'єктів міжнародного права, незалежним один від одного станом, вільним волевиявленням, реалізацію прав власними силами і засобами);

II) *правовідносини, що не засновані на юридичній рівності сторін* (характеризуються нерівнозначним волевиявленням сторін, порушеннями з боку одного із суб'єктів міжнародного права (наприклад, правовідносини між державами, одна з яких несе відповідальність за агресію щодо іншої; правовідносини між державою і міжнародною організацією, яка застосовує до неї санкції)) [1, с. 117].

Враховуючи запропонований у теорії міжнародного права підхід до класифікації міжнародних правовідносин – за критерієм походження суб'єктивних прав та обов'язків учасників міжнародних правовідносин (В.М. Шуршалов, В.Г. Буткевич) – *правовідносини, що засновані на юридичній рівності сторін*, в якості правової основи мають: а) права та обов'язки, які випливають з основних принципів сучасного міжнародного права; б) права та обов'язки, які випливають з міжнародних договорів; в) права та обов'язки, які випливають із звичаїв міжнародного права; г) права та обов'язки, які є наслідком рішень міжнародних органів (міжурядових організацій, міжнародних судових та арбітражних інституцій); д) права та обов'язки, які є наслідком односторонніх дій учасника правовідносин і згоди на те інших учасників [2, с. 453-454].

Разом з тим, *правовідносини, що не засновані на юридичній рівності сторін* представляють собою особливий різновид правовідносин, які у якості правової основи мають права і обов'язки, що є наслідком порушення обов'язків за міжнародним правом.

Такі правовідносини у доктрині міжнародного права визначають як міжнародно-правові відносини відповідальності (І.І. Лукашук).

Вони характеризуються наступним.

Міжнародно-правові відносини відповідальності представляють центральну ланку у механізмі реалізації відповідальності. Це випливає із самого поняття права міжнародної відповідальності, яке регулює відносини, що породжуються порушенням норм міжнародного права, визначає права і обов'язки, що з них випливають. Зокрема, «термін «міжнародна відповідальність» охоплює усю сукупність нових правовідносин, що виникають за міжнародним правом у зв'язку з міжнародно-протиправним діянням…» [3, с. 81].

Правовідносини відповідальності – форма здійснення відповідальності (І.І. Лукашук) [3, с. 81]. За таких правовідносин правопорушник несе обов'язок прийняти певні негативні наслідки, пов'язані із його діями, а потерпіла держава отримує право використовувати усі правомірні для даних умов засоби у цілях захисту своїх законних прав і інтересів [1, с. 121]. Інакше кажучи, у міжнародному праві «такі правовідносини покладають на правопорушника обов'язок припинити протиправне діяння, ліквідувати або компенсувати наслідки, а потерпілому надає право вимагати вчинення вказаних дій» [3, с. 81].

В цілому «відповідальність виступає необхідною умовою конкретного правопорушення. Для міжнародного права найбільш типовими відносинами відповідальності є такі, у силу яких суб'єкт, що порушує свої обов'язки, позбавляється можливості користуватись і відповідними правами. Іншими словами, правопорушення або зупиняє, або припиняє дію правовідносин.

Останні заміняються або доповнюються відповідними правовідносинами відповідальності. Це підтверджувалось у міжнародній практиці» [1, с. 121].

У минулому міжнародно-правові відносини відповідальності носили виключно двосторонній характер. Сторонами у них були тільки потерпіла держава і держава-правопорушниця. У наш час у міжнародному праві знайшла відображення *концепція колективної протидії* держав особливо серйозним міжнародним правопорушенням, що зачіпають корінні спільні інтереси» [3, с. 82].

В контексті обраної теми, варто, на нашу думку, навести приклади, що характеризують міжнародно-правові відносини відповідальності в інформаційній сфері.

Враховуючи досить тривалий час становлення цих правовідносин, численні теоретичні і практичні міжнародно-правові підходи до їх визначення, а також сучасні тенденції у їх розвитку, варто зазначити, що сукупність таких відносин охопила широке коло, до якого увійшли:

- питання відповідальності держав за діяльність національних засобів масової інформації (державних, приватних),

- питання відповідальність держав за міжнародні зобов'язання, пов'язані з боротьбою з кримінальними та терористичними злочинами в сфері інформаційно-комунікаційних технологій, а також

- питання відповідальності держав за діяльність і використання інформаційно-комунікаційних технологій і засобів, що порушує міжнародний мир і безпеку.

Вважаємо, що кожен аспект потребує окремого короткого розгляду.

1. *Міжнародно-правові відносини відповідальності держав за діяльність державних засобів інформації* виникають з факту порушення норми міжнародного права. В разі, якщо відбувається порушення державним інформаційним органом міжнародно-правових норм поширення інформації у міжнародних відносинах, це тягне, як наслідок, міжнародно-правову відповідальність держави.

Як правило, відповідальність держав за діяльність державних засобів інформації настає у певних випадках зокрема, коли це стосується поширення інформації щодо пропаганди війни, втручання у внутрішні справи держав, закликів до повалення існуючого ладу (або уряду), пропаганди расизму, геноциду тощо. Такі порушення розглядаються як міжнародні протиправні діяння, за що держава повинна нести відповідальність.

2. *Міжнародно-правові відносини відповідальності держав за діяльність підконтрольних державі засобів масової інформації* є такими, що прирівнюється і розглядається як відповідальність держави за діяльність державних засобів інформації. Умовою для покладення відповідальності є особливий фактичний зв'язок між державою, як суб'єктом міжнародного права, і засобом інформації. При цьому, такий зв'язок може бути двох видів. По-перше, він має місце коли відповідне протиправне діяння здійснюється за вказівкою суб'єкта. По-друге, коли воно здійснюється під керівництвом або контролем суб'єкта.

Варто додати, що і надання засобів комунікації та програмного забезпечення з метою поширення інформації (щодо втручання у внутрішні справи держав, закликів до повалення існуючого ладу та уряду) може розглядатися, на нашу думку, як міжнародне протиправне діяння, за що держава повинна нести відповідальність.

Тематика «Twitter- та Facebook- революцій» (надання можливості користування міжнародною соціальною мережею Facebook, глобальним соціальним сервісом Twitter (у тому числі з арабським інтерфейсом artwitter.com), You Tube, сателітними мережами (у першу чергу «Аль Джазіра»), йорданськими мережами Jeeran, Maktoob, Watwet) набуває вагомого значення, враховуючи, наприклад, достатньо швидке створення протестних настроїв та організацій акцій протесту на Близькому Сході у 2011 році.

3. *Міжнародно-правові відносини відповідальності держав за міжнародну інформаційну діяльність приватних засобів масової інформації,*

що знаходяться під її юрисдикцією є актуальним, складним і дискусійним аспектом проблеми відповідальності.

Погляди на можливість покладання відповідальності на державу за інформаційну діяльність фізичних і юридичних осіб різняться.

При цьому варто зазначити, що в доктрині переважно зверталася увага на питання відповідальності за діяльність традиційних засобів масової інформації (радіомовлення, телевізійне мовлення, поширення друкованої, візуальної та звукової продукції).

Вважаємо, що в умовах глобалізації діяльність фізичних осіб може нанести не меншої шкоди і іншими засобами поширення інформації, ніж традиційні засоби. Мова йде про поширення інформації за допомогою Інтернет. Зокрема, несанкціоноване поширення інформації, що впливає на міжнародну і національну безпеку.

Достатньо згадати, у зв'язку з цим, оприлюднення фізичною особою офіційних секретних документів на веб-порталі WikiLeaks. Розміщена на сайті, та поширена іншими засобами, інформація (250 тисяч із заявлених 3 млн. документів) містила державні таємниці цілої низки держав і здатна була здійснити значний вплив на розвиток міжнародних відносин. «При цьому, одномоментне охоплення пресою, радіо і телебаченням склало, за різними підрахунками, від 2,5 до 3 млрд. [осіб] - … половину населення планети» [4].

У зв'язку з цим питання відповідальності держави за міжнародну інформаційну діяльність приватних засобів масової інформації, як і окремих фізичних осіб, що знаходяться під її юрисдикцією, набуває значної ваги. Необхідно визнати, що питання залишається неврегульованим в міжнародному праві.

Зазначимо, що питання відповідальності за шкоду, завдану при здійсненні інформаційної діяльності, мають важливе значення, оскільки здатні впливати на репутацію, довіру, авторитет держави у міжнародних відносинах.

4. *Міжнародно-правові відносини відповідальності державза міжнародні зобов'язання, пов'язані з боротьбою з кримінальними злочинами в сфері інформаційно-комунікаційних технологій* випливають з положень Угоди про співробітництво держав-учасниць Співдружності Незалежних Держав у боротьбі із злочинами у сфері комп'ютерної інформації 2001 року, Конвенції про кіберзлочинність 2001 року та Угоди між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки 2009 року.

Вона може полягати у недотриманні державою зобов'язань щодо прийняття законодавчих та інших заходів, які можуть бути необхідними для встановлення кримінальної відповідальності винних осіб відповідно до її внутрішнього законодавства у сфері ІКТ; визначення повноважень і процедур, з метою конкретних кримінальних розслідувань або переслідувань.

5. *Міжнародно-правові відносини відповідальності держав за міжнародні зобов'язання, пов'язані з боротьбою з терористичними злочинами в сфері інформаційно-комунікаційних технологій* випливає з положень Угоди між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки 2009 року.

В цьому випадку, як і у попередньому, відповідальність може полягати у недотриманні державою зобов'язань щодо прийняття законодавчих та інших заходів, які можуть бути необхідними для встановлення відповідальності винних осіб відповідно до її внутрішнього законодавства у сфері ІКТ; визначення повноважень і процедур, з метою конкретних розслідувань або переслідувань.

6. *Міжнародно-правові відносини відповідальності держав за діяльність і використання інформаційно-комунікаційних технологій і засобів, що порушує міжнародний мир і безпеку* може покладатися за доволі специфічне використання державою інформаційно-комунікаційних технологій у міжнародних відносинах.

Особливою проблемою постає інформаційна війна, як засіб проведення зовнішньої політики держави. Не можна не зауважити, що окремі автори розглядаючи інформаційну війну з позицій Статуту ООН, наголошують на тому, що вона є своєрідним застосуванням сили і носить протиправний характер.

Таким чином, питання відповідальності держави за інформаційну діяльність вже на зводиться тільки до відповідальності за діяльність державних, контрольованих державою і приватних засобів інформації. Воно набуває нового змісту у зв'язку з поширенням та протиправним використанням інформаційно-комунікативних технологій і засобів у кримінальних, терористичних і військових (військово-політичних) цілях.

Реалізація міжнародно-правових відносин відповідальності відбувається у конкретних видах і формах. Для інформаційної діяльності суб'єктів міжнародного права властивою є політична (нематеріальна) відповідальність, як один з видів міжнародно-правової відповідальності.

Відшкодування за шкоду, заподіяну суб'єктами міжнародного права за інформаційну діяльність відбувається у формі сатисфакції.

Так, «відповідальність держави за передачу протиправної інформації може передбачати, в першу чергу, припинення таких передач, визнання їхньої міжнародної протиправності, офіційне вибачення перед потерпілою державою, притягнення до відповідальності осіб, що здійснили таку передачу» [5, с. 28]. Варто додати, що за шкоду заподіяну честі, гідності, репутації держави такого роду інформацією, можливим є ще і інші заходи зокрема, «запевнення в тому, що подібні акції не повторяться у майбутньому; визнання неправомірності вчинення дій; дезавуювання дій представника держави; виявлення пошани і належних почестей прапору потерпілої держави та виконання гімну в урочистій обстановці; видання спеціального нормативного акту для забезпечення виконання відповідних зобов'язань [2, с. 485].

У випадках, коли відбувається поширення неправдивої або перекрученої інформації, яка може заподіяти шкоди міжнародним відносинам, можливим є спростування такої інформації.

Право на спростування неправдивої або перекрученої інформації передбачено міжнародним правом - у 1952 році ООН було прийнято Міжнародну конвенцію про міжнародне право спростування.

У випадках протиправного використання державою інформаційно-комунікаційних технологій у міжнародних відносинах, на нашу думку, можливим може бути відшкодування у формі компенсації, оскільки вона передбачає відшкодовування потерпілій державі майнових втрати, пов’язані із знищенням або пошкодженням її інформаційно-комунікаційної інфраструктури.

Розглянувши питання забезпечення відповідальності держави за інформаційні міжнародно-протиправні діяння варто зазначити наступне.

Міжнародно-правові відносини відповідальності держав за інформаційну діяльність мають особливості, викликані характером міжнародних інформаційних відносин.

Конвенційні та доктринальні джерела розглядають питання відповідальності держави, як суб’єкта міжнародного права, виключно з позицій поширення інформації традиційними засобами інформації (радіомовлення, телевізійне мовлення, поширення друкованої, візуальної та аудіо продукції). При цьому міжнародно-правова відповідальність передбачається виключно за поширення протиправної, неправдивої або перекрученої інформації.

На формування міжнародно-правових відносини відповідальності значним чином впливає розвиток інформаційно-комунікаційних технологій, а також загрози, пов’язані із використанням таких технологій і засобів у цілях, які несумісними з підтримкою міжнародної безпеки. Переважна більшість таких відносин не є врегульованими нормами міжнародного права на універсальному рівні, або є врегульованими тільки на регіональному рівні.

Література:
1. Лукашук И.И. Механизм международно-правового регулировани / И.И. Лукашук – Киев: Вища школа. Изд-во при Киев. ун-те, 1980. – 168 с.
2. Міжнародне право. Основи теорії: підручник / за ред. В.Г. Буткевича. - К.: Либідь, 2002. – с. 608.
3. Лукашук И.И. Право международной ответственности / И.И. Лукашук – М.: Волтерс Клувер, 2004. – 432 с.
4. Закревский Н. WikiLeaks: игры в компромат по правилам госдепа? [Електронний ресурс] – Режим доступу: //http://2000.net.ua/2000/forum/puls/70703.
5. Ермишина Е. В. Международный обмен информацией: правовые аспекты / Е.В.Ермишина. – М.: Международные отношения, 1988. – 144 с.

----------***----------

УДК 343.32
321.011 342.3
342.727 303.6
32.019.51

О.Е. Радутний,
доктор філософії (PhD) з юридичних наук, доцент кафедри кримінального права № 1 Національного юридичного університету імені Ярослава Мудрого (м. Харків)
Ідентифікатор ORCID
orcid.org/0000-0002-6521-3977
ResearcherID: E-6683-2015

ЗАХИСТ СУВЕРЕНІТЕТУ В ІНФОРМАЦІЙНІЙ СФЕРІВ МЕРЕЖІ ІНТЕРНЕТ-ПРОСТОРУ

Відповідно до положень ст. 17 Конституції України захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. Невід'ємною складовою частиною суверенітету України виступає її інформаційний суверенітет, під яким на підставі положень ст. 1 Закону України «Про Національну програму інформатизації» № 74/98-ВР від 04.02.1998 розуміють здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави

Згідно до положень ст.7 Закону України «Про основи національної безпеки України» № 964-IV від 19 червня 2003 року[1] загрозами національним інтересам і національній безпеці України в інформаційній сфері визнано прояви обмеження свободи слова та доступу до публічної інформації, поширення засобами масової інформації культу насильства, жорстокості, порнографії, комп'ютерну злочинність та комп'ютерний тероризм, розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави, намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Але не меншу загрозу в собі несуть також: посягання на державний суверенітет України та її територіальну цілісність, територіальні претензії з боку інших держав; спроби втручання у внутрішні справи України з боку інших держав; розвідувально-підривна діяльність іноземних спеціальних служб; загроза посягань з боку окремих груп та осіб на державний суверенітет, територіальну цілісність, економічний, науково-технічний і оборонний потенціал України, права і свободи громадян; зрощення бізнесу і політики, організованої злочинної діяльності; злочинна діяльність проти миру і безпеки людства, насамперед поширення міжнародного тероризму; спроби створення і функціонування незаконних воєнізованих збройних формувань та намагання використати в інтересах певних сил діяльність військових формувань і правоохоронних органів держави; прояви сепаратизму, намагання автономізації за етнічною ознакою окремих регіонів України; можливість втягування України в регіональні збройні конфлікти чи у протистояння з іншими державами тощо.

Зазначені загрози можуть втілитися у реальне життя, в тому числі, і шляхом зловживань чи здійснення правопорушень в інформаційній сфері.

Загрози нас оточують навкруги: поява транспортних засобів створила небезпеку для життя і здоров’я людини, прискорення їх швидкості лише

підсилило її, нові форми виробництва постійно створюють виклики безпечним умовам праці, здобутки в дослідженні ядерної енергії поставили людство на межу катастрофи (адже загрозами національним інтересам і національній безпеці України також визнаються загроза використання з терористичною метою ядерних та інших об'єктів на території України; можливість незаконного ввезення в країну зброї, боєприпасів, вибухових речовин і засобів масового ураження, радіоактивних і наркотичних засобів; поширення зброї масового ураження і засобів її доставки) тощо.

Вже стали буденними і тому підсвідомістю відштовхуються на задній план такі загрози, як значне антропогенне і техногенне перевантаження території України, зростання ризиків виникнення надзвичайних ситуацій техногенного та природного характеру; непідтримання в належному технічному стані ядерних об’єктів на території України; небезпека техногенного, у тому числі ядерного та біологічного, тероризму; нераціональне, виснажливе використання мінерально-сировинних природних ресурсів як невідновлюваних, так і відновлюваних; погіршення екологічного стану водних басейнів, загострення проблеми транскордонних забруднень та зниження якості води; неконтрольоване ввезення в Україну екологічно небезпечних технологій, речовин, матеріалів і трансгенних рослин, збудників хвороб, небезпечних для людей, тварин, рослин і організмів, екологічно необґрунтоване використання генетично змінених рослин, організмів, речовин та похідних продуктів; посилення впливу шкідливих генетичних ефектів у популяціях живих організмів, зокрема генетично змінених організмів, та біотехнологій; застарілість та недостатня ефективність комплексів з утилізації токсичних і екологічно небезпечних відходів тощо.

У зв’язку з цим не слід як перебільшувати значення негативного впливу прискореного розвитку засобів комунікації та інформаційних технологій, так і зменшувати його значення для окремої людини або всього людства у порівнянні з екологічними, ресурсними (корисні копалини, чиста вода тощо) та іншими загрозами.

На сьогодні Інтернет, як загальнодоступна мережа всесвітньої комунікації, розширив свої межи від поєднання між собою окремих стаціонарних пристроїв до розповсюдження на засоби, які постійно перебувають на зв'язку у будь-якій географічній точці (смартфони, планшети), завдяки чому суб'єкт інформаційних правовідносин постійно перебуває у хвилі інформаційного потоку та все більше залучається у взаємодію з віртуальним соціумом.

За ефективністю впливу Інтернет впевнено і переконливо обігнав телебачення та інші засоби масової комунікації[2].

Користувачі поступово відходять від спостерігання та пасивного споживання інформаційної продукції та перетворюються на активних її фігурантів та творців. Раніше окрема фізична особа мала можливість поширювати певну інформацію лише серед доволі обмеженого кола людей (близькі, родичі, знайомі, колеги тощо), держава або інше соціально-політичне утворення теж було певним чином обмежено своєю територією або традиційними засобами комунікації. Завдяки унікальним можливостям мережі Інтернет з'явилася можливість звертатися до безмежно невизначеного кола співрозмовників, здійснювати вплив на величезну кількість людей.

Принциповою особливістю мережі Інтернет у порівнянні з іншими традиційними засобами комунікації є подолання значних відстаней, включення звичайного користувача-спостерігача до процесу взаємодії (користувачі стають активними виробниками контенту, спостерігач стає частиною експерименту, в якому приймає безпосередню) за рахунок використання ефекту присутності, інтерактивності та вільної навігації, відносної доступності інформації, можливості включення в інтерсуб'єктну реальність[3] великої кількості людей (загальне для всіх багатовимірне інформаційне поле) тощо.

Посилення комунікаційної функції мережі Інтернет призводить до зміни формату масової політичної комунікації, що виникає між суб'єктами

політичних відносин у широкому сенсі слова з метою впливати на свідомість населення і спонукати до певного типу політичної поведінки[4].

Такий стан взаємодії є великим здобутком людства, але й вимагає усвідомлення можливих загроз та негативних побічних ефектів (за своїм соціальним змістом та впливом це схоже на легалізацію зброї для населення, коли старими формами взаємодії користуватися вже не можливо, оскільки треба звикати жити і діяти по-новому у змінених умовах).

Є всі підстави віднести до комунікаційних переваг мережі Інтернет високу швидкість обміну інформацією, свободу слова, відносну доступність певних даних, можливість поширення власної інформації, відносну анонімність, широке географічне проникнення, сприяння реалізації творчого потенціалу, можливість спілкуватися на значній відстані тощо.

Втім, раніше окремій людині значно простіше було забезпечувати приватність свого особистого життя. Сьогодні завдяки спокусі використання наданих можливостей, особа сама добровільно надає доступ для інформації, яка її ідентифікує. Але це може статися також і без участі та відома самої особи, коли її близькі або знайомі поширюють пов’язані з нею дані. Таку інформацію здатні використовувати злочинці, недруги, спеціальні служби держави або іноземних держав тощо.

Вільне спілкування за допомогою віртуальних майданчиків, блогів і мікроблогів, форумів і порталів, які підтримують функцію зворотного зв’язку, виводить комунікативні можливості на якісно новий рівень, але збільшує вразливість і створює сприятливі можливості для зловживань.

Таким зловживаннями можуть бути, перш за все, практично всі кримінальні правопорушення, відповідальність за які передбачена в Особливій частині КК України (за винятком окремих, як, наприклад, зґвалтування або пошкодження чи зруйнування релігійної споруди або культового будинку): доведення до самогубства (ст.120 КК), шахрайство з фінансовими ресурсами (ст.222 КК) та звичайне шахрайство (ст.190 КК), публічні заклики до насильницької зміни чи повалення конституційного ладу

або до захоплення державної влади (ч.2 ст.109 КК), шпигунство (ст. ст. 111, 114 КК), перешкоджання законній діяльності Збройних Сил України та інших військових формувань (ст.114-1 КК), погроза вбивством (ст. 129 КК), розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби (ст. 132 КК) тощо. За вказані дії чи бездіяльність чинним законодавством України вже передбачено кримінальну відповідальність.

Поширення таких форматів повідомлень, які тільки зовні виглядають простими за своєю формою, але насправді спрямовані на донесення основної думки через свідомість та підсвідомість, призвело до появи так званих мотиваторів та демотиваторів – візуальних картин, що поєднані з стислим коментарем або закликом та покликані створити певний настрій чи образ сприйняття. Їх популярність обумовлена зручністю, відносною простотою створення та швидким досягнення мети повідомлення.

Обізнана в сучасних комунікаційних засобах молодь стає зручним об'єктом впливу, як прямого (заклики, рекомендації, залучення до участі у флеш-мобах[5], що у подальшому закріплює стереотип бажаної поведінки), так і опосередкованого (створення моди на певну соціальну позицію, наслідування популярним фігурантам блогосфери, удаване ототожнення якостей адресата з якостями відомих людей, оцінка за асоціативним рядом, нав'язування думки про тотожність інтересів маніпулятора з інтересами аудиторії, удаване розкриття таємної інформації тощо).

В якості логічного наслідку з'ясування реальності кожної з наведених загроз постає спокуса негайного внесення змін у чинне законодавство, а саме – передбачити кримінальну відповідальність за посягання на інформаційний суверенітет України.

До розв'язання цього питання слід підійти вельми обережно з наступних причин. Так, зокрема, місія Європарламенту під керівництвом його екс-голови Пета Кокса у своєму звіті за 2016 рік зазначила, що Верховна Рада України в сфері законодавчої діяльності є «слабкою ланкою»,

перенавантажена великою кількістю законопроектів, які мають доволі низьку якість та являють собою «законодавче сміття» («законодавчий спам», «законодавче цунамі»)[6].

Розглянемо ті можливості ефективного забезпечення суверенітету в інформаційній сфері, які закріплені у чинному законодавстві України.

Перш за все, слід звернути увагу на те, що посягання на відносини з забезпечення суверенітету в інформаційній сфері завжди виявлятиметься не в загальній формі (якій відповідає формула «… посягання на інформаційний суверенітет України …»), але у конкретних проявах поведінки.

Це можуть бути, наприклад, заклики до дій, спрямованих на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, надання інформаційної допомоги іноземній державі, збирання з метою передачі або передача відомостей, що становлять державну, банківську, комерційну таємницю, відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, розголошення державної таємниці тощо. Проте, відповідальність за такі дії вже передбачена ст. ст. 109, 111, 114, 231, 328, 330 КК України.

Крім того, не слід забувати, що Особлива частина КК України містить цілий розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку».

Формами та способами порушення суверенітету в інформаційній сфері, в тому числі, в мережі Інтернет, також можуть бути і перешкоджання здійсненню виборчого права або права брати участь у референдумі, роботі виборчої комісії або комісії з референдуму чи діяльності офіційного спостерігача (ст. 157 КК України), надання неправдивих відомостей до органу ведення Державного реєстру виборців або фальсифікація виборчих документів, документів референдуму, підсумків голосування або відомостей Державного реєстру виборців (ст. 158 КК України), порушення таємниці

голосування (ст. 159 КК України), порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163 КК України), перешкоджання законній діяльності професійних спілок, політичних партій, громадських організацій (ст. 170 КК України), посягання на здоров'я людей під приводом проповідування релігійних віровчень чи виконання релігійних обрядів (ст. 181 КК України), приховування або перекручення відомостей про екологічний стан або захворюваність населення (ст. 238 КК України), публічні заклики до вчинення терористичного акту (ст. 258^2 КК України), завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (ст. 259 КК України), погроза вчинити викрадання або використати радіоактивні матеріали (ст. 266 КК України), заклики до вчинення дій, що загрожують громадському порядку (ст. 295 КК України), ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 300 КК України), ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301 КК України), схиляння до вживання наркотичних засобів, психотропних речовин або їх аналогів (ст. 315 КК України), спонукання неповнолітніх до застосування допінгу (ст. 323 КК України), схиляння неповнолітніх до вживання одурманюючих засобів (ст. 324 КК України), незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації (ст. 359 КК України), умисне пошкодження ліній зв'язку (ст. 360 КК України) тощо.

Таким чином, є всі підстави стверджувати, що чинний закон про кримінальну відповідальність на сьогодні без прогалин описує практично всі конкретні форми злочинної поведінки. Зазначене вказує на відсутність необхідності внесення змін в КК України. Втім, це не виключає можливості реагування на нові виклики (неохоплені форми злочинної поведінки), що вимагатиме відповідних змін у чинному законодавстві.

Ще одну проблему вбачають в тому, що через швидкоплинність та високу щільність інформаційних потоків, а так само – через інформаційну залежність, споживач інформації не завжди може перевірити її за ознаками належності та достовірності.

Відверто кажучи, так було, є і буде завжди. Споживача (в тому числі, користувача мережею Інтернет) не вбережеш заборонами чи встановленням помірковано-дозованого доступу до інформації. Логічним продовженням такої надмірної опіки над громадянином з боку держави було б встановлення заборони на вживання алкогольних напоїв та тютюнопаління, користування гострими предметами побуту, знайомство з новими технологіями, що можуть містити елементи ризику, тощо.

Кожна особистість несе обов'язок сама перед собою, близькими та оточуючими, нащадками та суспільством щодо постійного невтомного саморозвитку, формування властивості критично сприймати та аналізувати будь-яку інформацію тощо. Для цього вона має можливість залучати і користуватися тими критеріями, які вже були сформульовані попередніми поколіннями та окремими видатними представниками людства: відповідність раніше засвоєним знанням, досвіду та законам, в тому числі логіки та здорового глузду, узгодженість з ними; відсутність протиріч; можливість парадоксальності; конкретність (не буває істини взагалі, поза чіткими умовами); як вона, певна інформація, відкликається в серці людини, наодинці з собою в моносуб'єктній реальності.

Література:

1. Відомості Верховної Ради України (ВВР), 2003, № 39, ст.351
2. TNS Web Index [Електроннийресурс]. – Режимдоступу: http://www.tns-global.ru/ services/media/media-audience/internet/information
3. Щодомоносуб'єктноїтаінтерсуб'єктноїреальностідодатководив.: *РадутнийО.Е.*Сакральністькримінально-правовогопростору / Питанняборотьбизізлочинністю: зб. наук. пр. / редкол.: В.І. Борисовтаін. – Х.: Право, 2013. – Вип. 26. – 360 с. – с. 42 – 52.; *РадутнийО.Е.*Додатковіметодиупізнаннікримінальногоправавінформаційн уепоху / Правоваінформатика: Науковийжурналзпроблемінформатизації, інформаційнихтехнологій, інформаційногоправа,

інформаційногозаконодавстваінформаційнихресурсіввіншихгалузяхправа / Редакційнарада: В.М. Брижкотаін. – К.: Науково-дослідниййінститутінформатикиіправаНаціональноїакадеміїправовихнаукУкраїни, ІнститутзаконодавстваВерховноїРадиУкраїни, 2015. – № 2(46)/2015. – с. 54 – 61
4. *Сковиков А. К.* Гаэтано Моска об акторах политического управления и власти / А. К. Сковиков // PolitBook. – 2012. – №4. – с. 104–114 – с. 108–109 [Електронний ресурс] – Режим доступу: https://cyberleninka.ru/article/n/gaetano-moska-ob-aktorah-politicheskogo-upravleniya -i-vlasti
5. Флешмо́б (також *флеш моб* і *флеш-моб*, англ. *flash mob* – «спалахуючий натовп», *flash* – спалах, *mob* – натовп), або раптівка – неочікувана поява групи людей в заздалегідь запланованому місці; після закінчення запланованої акції, її учасники розчиняються в натовпі перехожих людей, що і викликає ефект раптовості; зазвичай раптівки організовуються через мережу Інтернет або інші сучасні засоби комунікації [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/флешмоб
6. Шпайхер Т. В Европе назвали украинских депутатов «творцами законодательного мусора» / Экономические известия, 13.03.2016 // [Електронний ресурс] – Режим доступу: http://news.eizvestia.com/news_politics/full/655-v-evrope-nazvali-ukrainskih-deputatov-tvorcami-zakodatelnogo-musora

----------***----------

Кравчук Олексій Олегович,
професор кафедри господарського та адміністративного права НТУУ «КПІ», уповноважена особа університету з питань запобігання та виявлення корупції, д.ю.н., доцент

ДЕЯКІ АСПЕКТИ АДМІНІСТРАТИВНОЇ ВІДПОВІДАЛЬНОСТІ В СФЕРІ ЗАБЕЗПЕЧЕННЯ ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ

Адміністративна відповідальність за правопорушення у сфері забезпечення доступу до публічної інформації передбачена нормами ст. 212-3 КпАП. Це декілька складів адміністративних правопорушень: неоприлюднення інформації, обов'язкове оприлюднення якої передбачено Законом України «Про доступ до публічної інформації» (ч. 1 ст. 212-3);

необґрунтоване віднесення інформації до інформації з обмеженим доступом, ненадання відповіді на запит на інформацію, ненадання інформації, неправомірна відмова в наданні інформації, несвоєчасне або неповне надання інформації, надання недостовірної інформації (ч. 2 ст. 212-3); обмеження доступу до інформації або віднесення інформації до інформації з обмеженим доступом, якщо це прямо заборонено законом (ч. 4 ст. 212-3). Окрім того згадана стаття містить ще декілька складів правопорушень у частині забезпечення доступу до інформації – неправомірна відмова, несвоєчасне або неповне надання інформації, надання інформації, що не відповідає дійсності, у відповідь на адвокатський запит, а також деякі інші порушення законів «Про звернення громадян», «Про доступ до судових рішень».

Згідно з даними Держстату, за 2015 рік адміністративні стягнення за порушення права на інформацію за ст. 212-3 КпАП надійшло до судів справ для розгляду 466, з яких: повернуто 115 (24,7%), розглянуто з винесенням постанови 333, із яких 258 справ закрито, в т.ч. 96 (20,6% від загальної кількості справ) – у зв'язку з відсутністю складу адміністративного правопорушення, 143 (30,7% від загальної кількості справ) – у зв'язку із закінченням строків накладення адміністративного стягнення. Лише 75 (16,1% загальної кількості справ) закінчилися накладенням на осіб адміністративного стягнення.

Наведемо для порівняння, що статистика притягнення до адмінвідповідальності за ст. 212-2 – порушення законодавства про державну таємницю за той самий період є кардинально іншою – надійшло до розгляду 712 справ, з яких накладено стягнення на 637 осіб, 74 справи закрито, із них закінчення строків 27. Як бачимо, кількість осіб, на яких накладено адміністративні стягнення за порушення законодавства про державну таємницю за ст. 212-2, - в 8,5 разів більше, ніж за ст. 212.3 КпАП [1]. В той час, як сфера правовідносин, в яких йдеться про право на інформацію (з урахуванням кількості складів правопорушень, уміщених в ст. 212-3) – в тисячі разів ширша, ніж сфера охорони державної таємниці. Із цього видно,

що адміністративна відповідальність за порушення права на інформацію не забезпечує ефективного захисту цього права, держава більше схильна захищати свою інформацію, ніж захищати право особи на доступ до неї. Абсолютна більшість проваджень про адміністративне правопорушення за ст. 212-3 КпАП не призводить до накладення адміністративного стягнення.

Важливими проблемами притягнення осіб до адміністративної відповідальності за правопорушення у сфері доступу до публічної інформації є дотримання процесуальних вимог при складанні протоколу, дотримання стислих строків, правильність кваліфікації.

Враховуючи, що ст. 212-3 КпАП містить декілька суміжних складів правопорушень, при складанні протоколу і розгляді справи необхідно відмежовувати вчинені правопорушення від суміжних (як передбачених різними частинами статті, так і передбачених однією і тією самою частиною, але такі, що мають різні підходи до визначення моменту вчинення правопорушення).

Так зокрема за ч. 2 ст. 212-3 КпАП настає відповідальність за ненадання відповіді на запит на інформацію, неправомірну відмову в наданні інформації, що є разовими правопорушеннями, які є вчиненими в момент спливу строку надання відповіді або в момент відмови. Строк давності для накладення стягнення за таке адміністративного правопорушення обчислюється з дня спливу відповідного строку для надання відповіді або з дня відмови. Також ч. 2 ст. 212-3 КпАП передбачено відповідальність за ненадання інформації, що є триваючим правопорушенням строк давності для якого обчислюється з дня виявлення правопорушення. Скасовуючи рішення суду першої інстанції, Апеляційний суд Київської області в своїй постанові від 30.06.2015 вказує на те, що днем вчинення правопорушення є останній день виконання вимог закону щодо надання інформації [2]. Апеляційний суд Харківської області в постанові від 29.03.2016 вказує, що оскільки відповідь розпорядника інформації на запит не є проміжною, а є остаточним рішенням про відмову у наданні інформації особі, яка її запитувала, очевидним є те, що

правопорушення, про яке йдеться у протоколі є саме неправомірною відмовою в наданні інформації та характеризується вчиненням одноразової дії у певний час, а тому висновок суду першої інстанції про триваючий характер правопорушення є хибним [3].

Спостерігаються неоднозначні підходи в судовій практиці до визначення суб'єкта адміністративної відповідальності за правопорушення у сфері забезпечення доступу до публічної інформації. Суди в різних випадках визначають суб'єктом такої відповідальності посадову особу, що підписала відповідь з неправомірною відмовою, відповідальну особу з питань доступу до публічної інформації, особу, що розглядала запит (виконавця) або навіть працівника підрозділу з діловодства. Застосування формулювань санкцій статті 212-3, що містить вказівку про накладення штрафу саме на посадових осіб – не дає можливості розв'язати неоднозначність внаслідок надто широкого розуміння поняття посадової особи в сфері державної служби або служби в органах місцевого самоврядування.

Закон України «Про доступ до публічної інформації» в ст. 12 відносить до числа суб'єктів відносин у сфері доступу до публічної інформації запитувачів інформації, розпорядників інформації а також структурні підрозділи або відповідальну особу з питань доступу до публічної інформації розпорядників інформації. При цьому згідно зі ст. 14 згаданого Закону, розпорядники інформації зобов'язані зокрема мати спеціальні структурні підрозділи або призначати відповідальних осіб для забезпечення доступу запитувачів до інформації та оприлюднення інформації. Згідно зі ст. 16 цього ж Закону, відповідальної особи з питань доступу до публічної інформації розпорядників інформації є відповідальні за опрацювання, систематизацію, аналіз та контроль щодо задоволення запиту на інформацію, надання консультацій під час оформлення запиту, а також за оприлюднення інформації, передбаченої цим Законом. Ці особи не приймають рішень щодо надання або ненадання інформації та не можуть відмовляти чи задовольняти відповідні запити. На нашу думку, ці особи не виконують адміністративно-

господарських або організаційно-розпорядчих повноважень, і не належать до посадових осіб, що є суб'єктами адміністративної відповідальності за порушення права на доступ до публічної інформації за ст. 212-3 КпАП (звичайно, крім випадків, коли це є відповідний керівник розпорядника, його заступник, який є посадовою особою в силу інших обставин, а не у зв'язку з покладенням на нього обов'язків відповідальної особи). Так, в ч. 4 ст. 22 Закону зазначається, що у відмові в задоволенні запиту на інформацію має бути зазначено прізвище, ім'я, по батькові та посаду особи, відповідальної за розгляд запиту розпорядником інформації (а згідно з наведеного вище це не є особа, відповідальна з питань доступу до публічної інформації, що є відповідальною не за розгляд, а за опрацювання, систематизацію, аналіз та контроль).

На нашу думку, відповідну неоднозначність слід усунути шляхом передбачення в ст. 12, 14, 16 Закону України «Про доступ до публічної інформації» правила, відповідно до якого відповідальною особою з питань доступу до публічної інформації є керівник розпорядника або його заступник згідно з розподілом обов'язків. Саме ця особа, а не виконавець, – приймає по суті рішення про надання інформації або відмову в її наданні, і якщо таке ненадання є неправомірним, то саме ця особа, а не виконавець або працівник підрозділу діловодства – вчиняють розглянуте правопорушення.

Список використаних джерел:

1. Адміністративні правопорушення в Україні у 2015 році. Статистичний бюлетень. – К., 2016. – С. 86
2. Постанова Апеляційного суду Київської області від 30.06.2015. – Електронний ресурс. Режим доступу: [http://www.reyestr.court.gov.ua/Review/45946201#].
3. Постанова Апеляційного суду Харківської області від 29.03.2016. – Електронний ресурс. Режим доступу: [http://www.reyestr.court.gov.ua/Review/56773417].

----------***----------

М. М. Тараненко,
к.ю.н., ст. викладач кафедри публічного права ФСП НТУУ «КПІ»

ІНФОРМАЦІЙНІ ЗАСОБИ ОРГАНІЗАЦІЇ МАСОВИХ ЗАВОРУШЕНЬ

В числі основних завдань вітчизняної юридичної науки є вироблення і забезпечення необхідних гарантій врівноваженого співвідношення інтересів особи і держави у боротьбі зі злочинністю. В числі найбільш небезпечних проявів цього явища є такий злочин, як масові заворушення, відповідальність за вчинення яких передбачена ст. 294 Кримінального кодексу (далі КК) України.

Однією з форм об'єктивної сторони масових заворушень є їх організація. Без чітко спланованих організаційних та інформаційно-агітаційних заходів їх розгортання, і, головне, досягнення кінцевої мети є неможливим. З огляду на це, метою статті є визначення конкретного змісту організаційної та інформаційно-агітаційної діяльності по розгортанню масових заворушень, що в диспозиції ст. 294 КК України законодавцем фактично не розкривається. До видів такої діяльності відноситься: об'єднання людей для участі у масових заворушеннях, керівництво натовпом, підбурювання до вчинення дій, які становлять собою масові заворушення, провокаційні дії, вчинені з метою викликати відповідну поведінку великих груп людей. Вчинення будь-яких з перелічених вище протиправних дій є достатнім приводом для встановлення вини особи в організації масових заворушень.

Процесс підготовки масових заворушень, методи первинного етапу їх організації можуть бути різними. Як правило, він включає: 1) розробку організатором детального плану (сценарію) проведення масових заворушень; 2)створення «ініціативної групи» з числа надійних прибічників та розподіл між ними конкретних ролей і функцій; 3) інформаційно-агітаційне

забезпечення розгортання масових акцій шляхом виготовлення листівок, прокламацій, звернень, декларацій, спецвипусків газет, або інших друкованих видань, адресованих широким верствам населення; 4) добір і підготовку «активу» та формування з нього спеціальних загонів для виконання в ході масових заворушень конкретно визначених завдань.

Як правило, організаторами масових заворушень проводиться робота по озброєнню таких осіб, заготівлі різноманітних предметів, які в умовах масових протиправних акцій можуть бути використані ними в якості зброї.

Слід врахувати, що всі заздалегідь проведені підготовчі організаторські та інформаційно-агітаційні заходи носять, зазвичай, чітко продуманий і завуальований зміст та характер і можуть мати вигляд цілком легітимної діяльності. Зокрема, організаторами доволі часто напередодні таких акцій практикується підготовка і подання численних декларацій, звернень та петицій до органів влади із начебто законними і справедливими вимогами населення міста, району, регіону, які, за їх словами, базуються на справжньому волевиявленні народних мас, вивченні їх запитів і потреб вимагають негайного практичного розв’язання.

Наступний етап організації масових заворушень полягає в **діях по збиранню та об’єднанню агресивно налаштованого людського натовпу.**

В разі «мовчання органів влади» та «ігнорування законних вимог народу» організатори масових заворушень, під виглядом цілком законного публічного висловлення думок та вимог народу, оперативного вирішення найбільш наболілих соціальних проблем, звертаються до владних структур з проханням надати дозвіл на проведення в громадських місцях масових акцій: мітингів, зборів, маніфестацій, демонстрацій, ходів тощо. Як правило, такого дозволу вони не отримують, або одержують санкцію на проведення масових акцій протесту на віддалених від центральних публічних місць майданчиках. В таких випадках організатори, ігноруючи рішення органів влади, самочинно визначають дату і місце проведення протиправного масового заходу.

Однак при цьому мітинги, демонстрації, маніфестації, ходи, збори, які за словами їх організаторів, покликані вирішувати гострі соціальні проблеми, фактично переслідують ціль навпаки радикально загострити вже доволі напружену ситуацію, сколихнути населення, спровокувати його на активні асоціальні дії. Тут визначається ядро можливих активних учасників безладів та відбувається процес концентрації екстремістські налаштованих сил для практичної реалізації запланованих наступних масових протиправних акцій.

Напередодні розгортання масових заворушень їх організатори активно залучають для роботи з масами всі можливі наявні засоби інформаційно-агітаційного забезпечення: активне розповсюдження в громадських місцях та по місцю проживанню населення заздалегідь підготовлених агітаційних видань – звернень, програм, листівок, прокламацій, брошур, спецвипусків газет, де, піддається гострій критиці діяльність органів влади, акцентується увага різних категорій населення на найбільш болючих проблемах їхнього повсякденного життя, містяться спонукаючі до активних радикальних дій результати буцімто проведених об'єктивних соцопитувань, брехливі чутки, палкі заклики взяти активну участь у визначений день у масових акціях народного невдоволення – мітингах, маніфестаціях, зборах тощо.

Ця інформація може бути адресована як невизначеному колу осіб, так і конкретно визначеним групам населення («афганцям», «чорнобильцям», молоді, представникам певної професії, соціального прошарку, національності, релігійної конфесії, тощо); учасникам різноманітних заходів (глядачам, слухачам, виборцям, делегатам тощо); членам політичних і громадських організацій, робітникам підприємств, установ, шахтарям, аграріям, військовослужбовцям та іншим верствам населення. Адресатами таких закликів можуть бути обрані й різні представники громадськості, засоби масової інформації, міжнародні організації, чи навіть керівники зарубіжних держав, які можуть втрутитись в хід масових заворушень своєю моральною чи матеріальною підтримкою.

В переддень масових заворушень найбільш активно і наполегливо носії інформації – агітатори «працюють» в молодіжному, насамперед, студентському середовищі, яке, зазвичай, позитивно реагує на підбурюючі заклики радикального змісту і завжди налаштоване на рішучу і активну боротьбу за свої права і соціальну справедливість.

Як свідчить практика організації сучасних масових заворушень, одним з найбільш ефективних інформаційних засобів залучення до них великої кількості молоді, стали соціальні мережі в Інтернеті. Зокрема, саме завдяки їм за прикладом організації масових заворушень антиглобалістів в США та ряді Європейських держав, що відбувалися в 2011-2012 рр., були вчинені настирливі спроби розгорнути «кольорові революції» на пострадянському просторі. Враховуючи серйозну роль соціальних мереж в організації масових заворушень, радник держсекретаря США Алек Росс назвав Інтернет «Че Геварою XXI століття».

Нерідко інформація чи заклики до масових заворушень стають доступними великій кількості людей шляхом нанесення на стіни агітаційних написів, гасел, сатиричних малюнків, розміщення плакатів, транспарантів, завдяки використанню аудіовізуальних засобів, звукопідсилювачів тощо. Кількість осіб, які сприйняли ці підбурюючі звернення, не має вирішального значення. Головне в цих інформаційно-пропагандистських акціях – їх відкритість, гласність, прозорість, доступність, зверненість до багатьох категорій осіб. Підбурюючі провокаційні заклики можуть здійснюватися не тільки в «чистому» вигляді, а й нерідко супроводжуватися достатньо переконливою і аргументованою фактологічною інформацією, провокуючою на вчинення конкретного роду злочинних дій.

Визначений організаторами день розгортання масових протиправних акцій нерідко з ранку супроводжуються подачею тривожних звуків, сигналів, гудків гучною трансляцією через гучномовці пісень, гасел та закликів до активних дій. Особам, що увійшли до складу зібраного натовпу, керівниками нерідко можуть видаватись спиртні напої, наркотичні, психотропні речовини,

або їх аналоги з метою їх відповідного збудораження та налаштування на агресивні дії. Окремі групи учасників запланованих масових акцій, як правило, збираються в різних місцях міста і після попередньої інформаційно-агітаційної та матеріальної «підготовки» спрямовуються організаторами у заздалегідь визначене громадське місце з метою об'єднання в єдиний, численний за кількістю учасників агресивно налаштований натовп.

Третій етап організації масових заворушень полягає в **безпосередньому керівництві** протиправними діями зібраного організаторами натовпу**.** Він включає в себе: 1) агітаційні виступи з жорсткою критикою діяльності органів влади, демонстрацією «тяжкого становища населення» та публічними провокаційними закликами до вчинення протиправних дій; 2) чітке спрямування дій активних учасників агресивно налаштованого натовпу в ході вчинення погромів, підпалів та інших дій, якими супроводжуються масові заворушення.

На цьому етапі масових заворушень, організатори влаштовують виступи перед зібраним натовпом спеціально підготовлених промовців, які здатні своїми ораторськими здібностями і вмілою маніпуляцією провокаційною, часто брехливою інформацією ефективно впливати на стан та настрої великої кількості людей. Нерідко, ці провокаційні звернення, як своєрідний умовний сигнал, адресовані особам, що перебувають у натовпі, які заздалегідь можуть бути озброєними холодною або вогнепальною зброєю, палицями, металевими прутами, камінням, пляшками з легкозаймистими речовинами та іншими небезпечними для життя людини предметами. Заклики на зразок «покарати іновірців», «помститись міліції за всі її діяння», «комуняку на гіляку» сприймаються значною кількістю осіб як такі, що спонукають учасників натовпу до активних агресивних протиправних дій, кінцева мета яких не може не усвідомлюватись їх ініціаторами та конкретними виконавцями.

Відкритий заклик до натовпу вчинити протиправні дії з певного підвищення (автомобіля, постаменту, сходів, подіуму, балкону, трибуни

тощо) через різноманітні засоби підсилення звуку (рупор, мегафон, мікрофон тощо), коли звичайний учасник масових заворушень фактично бере на себе функції керівника агресивно налаштованого натовпу, буде означати його організаційну діяльність. Так, під час проведення 9 березня 2001 року резонансної політичної акції «Україна без Кучми!» Л., М., З., К. та Ш. - лідери політичної партії Українська Національна Асамблея (УНА) та керівники організації Українська незалежна солідарна організація (УНСО), щоб вчинити масові безпорядки під час покладання квітів до пам'ятника Т. Г. Шевченку в м. Києві вищими посадовими особами України, вишикували своїх прибічників і спрямували їх на шеренгу працівників міліції, які забезпечували охорону правопорядку, з закликами прорвати «цей кордон». Особливою активністю при цьому відзначився Л., котрий підбурював розлючений натовп постійними провокаційними закликами: «Шикуйтеся в колону по шість!», «За кожен трофей буде винагорода!», «Слава нації – смерть ворогам!», «Зрадників на палю!», «УНСО – до штурму!», «УНА – до влади!», «За трофеями вперед!» тощо [4].

Як свідчить судова практика, зміст таких звернень слід зафіксувати відповідними аудіо і відео технічними засобами. За відсутності цього, дії таких осіб не можуть оцінюватись, як організаторські. Так, дії М. під час масових заворушень в січні 1990р. в Душанбе слідство також кваліфікувало як організацію масових безпорядків. Однак суд зазначив, що зафіксовані на відео плівці дії М., коли він перебував на східцях будівлі ЦК Комуністичної партії Таджикистану, виражалися лише у тому, що він «приседал и махал руками, жестикулируя призывно…». При цьому в справі були відсутні дані щодо конкретного змісту його закликів. За таких умов, суд цілком справедливо визнав, що такі дії не можуть бути необхідною підставою для визнання М. організатором масових заворушень [7, с.42].

Трапляються випадки, коли під час масових заворушень стихійні, некеровані як слід дії екзальтованого натовпу можуть вийти з-під контролю його організаторів. В такому разі в ході заворушень доволі часто вчиняються

зовсім інші, взагалі непередбачені розробленим організатором планом (сценарієм) розвитку подій злочини: пограбування, вбивства, зґвалтування, крадіжки, захоплення та утримання заручників тощо.

У підсумку зазначимо, що організація масових заворушень проявляється в трьох формах: 1) підготовча робота, що націлена на поетапне розгортання масових заворушень; 2) дії по збиранню та об'єднанню агресивно налаштованого до влади, окремих соціальних прошарків, інших національностей, релігійних конфесій тощо людського натовпу; 3) керівництво діями натовпу, що спрямовані на провокування у його учасників нерідко неправдивою інформацією негативного ставлення до чинної влади, громадського порядку і громадської безпеки та на підбурювання до вчинення насильства над громадянами, погромів, підпалів, знищення майна, озброєного опору представникам влади, захоплення будівель, насильницького виселення громадян.

У роботі по організації масових заворушень їх організатори заздалегідь визначають цілу низку ефективних інформаційно-агітаційних засобів. Особлива увага при цьому надається інформаційному забезпеченню масових протиправних дій, яке покликане об'єднати окремих осіб в натовп, налаштувати їх негативно та спровокувати до активних дій.

Література:

1. Кримінальна справа № 1-13/09 від 17.06.2009 р. // Архів Печерського районного суду м. Києва за 2009 рік.

Кримінальна справа № 4-518/08 // Архів Печерського районного суду м. Києва за 2008 рік.

Кузнецов В. В. Злочини проти громадського порядку та моральності (практ. посіб.) за заг ред. В. І. Шакунова / В. В. Кузнецов. – К. : Паливода А.В., 2007. – 160 с.

2. Лебедь Н. До 10 річчя «України без Кучми» / Н. Лебедь : [Електронне джерело]. – Режим доступу : http://www.obozrevatel.com/politics/do-10-richchya-ukraini-bez-kuchmi.htm
3. Науково-практичний коментар кримінального кодексу України. 5-те вид., переробл. та доповн. / За ред. М. І. Мельника, М. І. Хавронюка. – К. : Атіка, 2012. – 1316 с.Тараненко М.М. Кримінально-правова

характеристика масових заворушень. / М. М. Тараненко – дис. канд. юрид. наук. – К, 2014. – 255 с.
4. Науково-практичний коментар до Кримінального кодексу України / Відпов. ред. С. С. Яценко, (4-те вид., переробл. та доповн.). – К. : АСК., 2005. – 934 с.
5. Фортуна Н.Г. Уголовно-правовая борьба с массовыми беспорядками. / Н.Г. Фортуна // Вестник МГУ. Серия 11. Право. – 1992. - №2. – с.42

----------***----------

О. М. Головко,
аспірант НДІІП НАПрН України

ДО ДЕЯКИХ ПИТАНЬ МЕДІАБЕЗПЕКИ УРАЗЛИВИХ КАТЕГОРІЙ НАСЕЛЕННЯ УКРАЇНИ

Інформаційна безпека людини, як нині наголошується в науковій доктрині, є невід'ємним елементом національної безпеки. Негативні наслідки нехтування цим сегментом безпеки в Україні зараз створюють нагальну потребу в розробці комплексу заходів по захисту людини, її свідомості та психіки саме в інформаційній сфері. Більше того, наголошувати необхідно не лише на убезпеченні інформаційно-психологічної безпеки особистості, але й на аспектах нейтралізації наслідків негативного деструктивного впливу на людську свідомість.

Зокрема, зазначимо, що серед таких наслідків особливо небезпечними є інформаційна залежність людини від визначеного кола медіа-джерел, так звані, медіа аддикції, що входять до складу ретристської залежності. В результаті виникає причинно-наслідковий зв'язок між цим видом аддикції та інформаційною віктимізацією внаслідок дезінформації чи пропаганди, аномією чи повною фрустрацією суспільства.

На цьому наголошують й інші вчені, роблячи акцент на тому, що «маніпуляції впливами на людську свідомість шляхом поширення через систему масових комунікацій певної інформації та дезінформації призводять до порушення суспільної стабільності, завдають шкоди психічному й фізичному здоров'ю людей, збуджують національну або релігійну ненависть і ворожнечу, провокують насильство, жорстокість та ін. Ці дії призводять до

розмивання моральних і культурних норм суспільного поводження, духовної деградації людини й суспільства в цілому» [1, с. 33].

Так, враховуючи складність ситуації з новими категоріями населення України в контексті правового забезпечення життєдіяльності, варто піднімати питання не тільки соціально-економічного, а й безпекового характеру. Так, особи, котрі й досі проживають на території зони АТО, а також внутрішньо переміщенні особи (далі – ВПО), є тими уразливими категоріями, які потребують поточної реабілітації з питань персональної безпеки у медіапросторі. Звичайно, що для ефективності забезпечення даного підвиду інформаційної безпеки має бути передбачена відповідальність за посягання на неї, особливо якщо це призвело до тяжких наслідків. Однак, при такій постановці питання не варто втрачати усвідомлення потреби в роботі з жертвами медіанасилля, деструктивної пропаганди та інших небезпечних медіавпливів.

Таким чином, пропонуємо розглянути деякі пропозиції щодо роботи з цими категоріями населення в контексті агресивного інформаційного протиборства в сучасному медіапросторі. Перш за все, існує потреба в інформування вразливих категорій про такі ресурси в Інтернеті, які дають можливість з'ясувати правдивим є медіа-повідомлення чи ні. Наприклад, найбільш ефективними в протидії фейкам та пропаганді є такі ресурси як StopFake, ресурс ГО «Інтерньюз-Україна» – Verify.org.ua та інші. Оскільки ці категорії осіб зневірились у правдивості будь-яких медіа-джерел, необхідно створити концепт, за яким споживання інформації уразливими групами стане не сліпим чи байдужим, а свідомим.

Доречно зазначає О.Е. Радутний, що «для перепрограмування народу, нації найбільш ефективними слід вважати прийоми, що мають емоційне забарвлення й належать до таких сфер, як масова культура, мистецтво, релігія тощо. Аналіз даних щодо таких способів показує, що багато країн світу зараз створюють у себе системи захисту від інформаційної агресії, яка іноді має вигляд культурної експансії» [2, с. 161].

Зазначимо, що населенню, котре проживає на території АТО варто надати можливість користуватися альтернативними медіа джерелами, а не тільки російськомовними, які, судячи зі свідчень ВПО навіть «ловлять» в цій місцевості краще, аніж українські канали – радіо, телебачення, не кажучи вже друковані ЗМІ. Тобто потреба у «приглушення» ворожих частот, на яких надмірна кількість дезінформації, фейкових новин та пропаганди.

Щодо категорії ВПО, то існує нагальна потреба у забезпеченні підґрунтя для їх нормального співжиття з місцевим населенням на території, підконтрольній Україні. Адже саме суспільство проявляє недовіру і вороже ставлення до представників ВПО, вживаючи «мову ворожнечі» та стереотипи щодо них. Таким чином, «мова ворожнечі» є серйозним негативним фактором, якому треба протидіяти. Окрім акцентуванні уваги на цій проблемі варто, зокрема, заохочувати підприємців у наданні переваги в працевлаштуванні фіксованому відсотку ВПО. При цьому держава має це заохочувати через надання таким підприємцям пільг у їх комерційній діяльності. Представникам ВПО це дасть можливість пристосуватися до нового місця проживання швидше та відчути турботу держави та приналежність до української спільноти.

Також, тим ВПО, котрі мають можливість створити свій бізнес варто надавати певні заохочення чи пільги на початковому етапі для розвитку соціального підприємницька, зокрема, у сферах інформаційної культури та безпеки. Це зменшить тягар держави в цих питаннях і дасть можливість підвищити рівень медіаосвіти населення, що є нагальною потребою ІС. Окрім цього, оскільки ВПО є особами, що безпосередньо стали жертвами деструктивних медіа впливів варто провести з ними навчання, зокрема, по напряму медіаосвіти та протидії пропаганді, й таким чином, надати їм можливість спочатку на громадських засадах, а потім можливо й на державному рівні передавати ці знання в українських навчальних закладах, щоб мінімізувати можливість такого впливу у подальшому. Адже хто краще

може розказати про негативні медіа впливи як не ті, хто безпосередньо відчули потребу протидіяти ним.

Більше того, існує необхідність у проведенні систематичних соціологічних опитувань щодо встановлення рівня інформаційної віктимізації населення в Україні. Найбільш ефективно така діяльність може бути реалізована на базі Науково-дослідних установ, котрі мають навички та науково-теоретичну базу для розробки методології по даному напрямку. До того ж, варто заохочувати так зване, «інформаційне волонтерство», тобто поширення суспільно корисної інформації в медіапросторі, зокрема, й щодо соціологічних опитувань та інших досягнень у сфері медіа досліджень та медіа безпеки.

Отже, зазначимо також, що необхідним є передбачений законодавством баланс між «позитивними» і «негативними» новинами та іншими видами медіа контенту, в тому числі й розважального змісту, оскільки це може викликати фрустрацію, аномію та навіть інформаційну віктимізацію суспільства. Зокрема, йдеться про зменшення кількості негативної інформації в ЗМІ (смерті, катастрофи, політичні міжусобиці тощо) та встановлення норм «сенсаційного» матеріалу політичного характеру, за перевищення яких необхідно передбачити санкцію, оскільки подібні матеріали, окрім того, що приносять прибуток приватним медіа джерелам, нівелюють статус державного службовця та репутацію держави Україна з боку власного ж населення.

Література:

1. Головань В.Г., Дроздов О.М., Сергєєв В.В., Герасимов В.М. Інформаційна безпека держави: аспект інформаційно-психологічних загроз / В.Г. Головань, О.М. Дроздов, В.В. Сергєєв, В.М. Герасимов // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: зб. наук. праць. – 2011. – Вип. 5. – С. 33-41
2. Радутний О. Е. Соціально-економічний чинник обумовленості кримінально-правової охорони інформаційних відносин / О. Е. Радутний // Проблеми законності. – 2012. – Вип. 119. – С. 157-165. – [Електронний ресурс]. Режим доступу: http://nbuv.gov.ua/UJRN/Pz_2012_119_20

----------***----------

А.В.Коростиленко,
к.ю.н., в.о. начальника наукової лабораторії Національної академії Служби безпеки України

ВИЗНАЧЕННЯ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ВЧИНЕННЯ ПРОПАГАНДИ ТА ПОШИРЕННЯ ІДЕОЛОГІЇ ТЕРОРИЗМУ

Враховуючи активізацію пропаганди та поширення ідеології тероризму з використанням засобів масової інформації та мережі Інтернет, протидія цьому виду терористичної діяльності в умовах проведення антитерористичної операції на Сході України стає пріоритетним завданням загальної державної системи боротьби з тероризмом. Важливим є те, що саме пропаганда і поширення ідеології тероризму стає одночасно платформою і каталізатором тероризму [1].

Вказане обумовлює необхідність створення нових підходів і шляхів попередження та припинення цієї протизаконної діяльності, формування законодавчого комплексу заходів протидії, у тому числі й профілактики тероризму.

Для ефективного вирішення цих проблем вкрай необхідне узгоджене та несуперечливе, як у міжнародному, так і внутрідержавному правовому полі, антитерористичне законодавство.

Нажаль, законодавство України не тільки не визначає юридичної відповідальності за пропаганду і поширення ідеології тероризму, але й не розкриває самих понять вказаної терористичної діяльності. Така невизначеність унеможливлює застосування основного принципу боротьби з тероризмом – невідворотності покарання за вчинення терористичної діяльності, у зв’язку з цим, зменшує ефективність роботи іншого принципу – пріоритетності попереджувальних заходів.

З метою узгодження норм українського законодавства з існуючим міжнародним – антитерористичним, у 2013 році народним депутатом України Журавським В.С. був внесений на розгляд Верховної Ради України

проект Закону України «Про внесення змін до деяких законодавчих актів України (щодо запобігання тероризму)» (реєстр. № 2219а від 4 червня 2013), у якому пропонувалося внести зміни до Кримінального кодексу України, законів України «Про боротьбу з тероризмом», «Про основи національної безпеки України» для встановлення кримінальної відповідальності за пропаганду і поширення ідеології тероризму. У частині доповнення Кримінального кодексу України пропонувалася «Стаття 258-6. Пропаганда і поширення ідеології тероризму». Однак, Верховним Судом України було зауважено, що за змістом запропонованої статті 258-6 КК України поняття «пропаганда ідеології тероризму» мала оціночний характер, оскільки визначалась за допомогою оцінних термінів (зокрема категорій «системне поширення», «явища, пов'язані з ескалацією...», «ідеал спільноти») [2].

Крім того, ця стаття частково дублювала положення статті 258-2 КК України, а тому прийняття першої створювала б небажану конкуренцію кримінально-правових норм. При цьому санкція частини першої чинної статті 258-2 КК України, окрім обмеження та позбавлення волі, містила такі основні альтернативні види покарань, як виправні роботи та арешт. Тоді як у запропонованій законопроектом статті 258-6 найменш суворим видом покарання було обмеження волі строком до п'яти років. Тобто в положеннях запропонованої законопроектом статті було допущено порушення принципу співмірності покарання вчиненому діянню.

Враховуючи викладене та зважаючи на відсутність вимог Конвенції Ради Європи щодо встановлення кримінальної відповідальності за пропаганду і поширення ідеології тероризму, указана законодавча пропозиція була визнана неприйнятною. Після цього суб'єкти законотворчої ініціативи тривалий час не ініціювали питаннякриміналізації пропаганди.

З урахуванням подій, що відбуваються у світі, у тому числі на Сході України, 28 жовтня 2015 року у м. Страсбург від імені України підписано Додатковий протокол до Конвенції Ради Європи про запобігання тероризму

(2005р.), який передбачає криміналізацію окремих злочинних діянь терористичного характеру [3].

Зважаючи на важливість зазначеного правового інструменту в міжнародних зусиллях у боротьбі з тероризмом та потребу здійснення внутрішньодержавних процедур, необхідних для набрання ним чинності для України, суб'єктами законодавчої ініціативи розпочата розробка пропозиції щодо внесення змін до Кримінального, Кримінального процесуального кодексів та інших законодавчих актів України, необхідних для імплементації положень згаданого міжнародного договору.

Додатковий протокол до Конвенції Ради Європи про запобігання тероризму передбачає криміналізацію певних діянь терористичного характеру та внесення відповідних змін до Кримінального кодексу України, що приведе до юридичних колізій. Так, при імплементації положень статей 5 та 6 згаданого міжнародного договору повинна визначатись відповідальність за фінансування виїзду за кордон та за організацію чи сприяння іншим способом виїзду за кордон з метою усіх видів терористичної діяльності, крім пропаганди і поширення ідеології тероризму.

Зауважуємо, що в українському антитерористичному законодавстві залишається єдиний не криміналізований (із шести, визначених статтею 1 Закону України «Про боротьбу з тероризмом» [4]) вид терористичної діяльності – пропаганда та поширення ідеології тероризму. Тобто, особа, яка буде фінансувати виїзд за кордон чи організовувати, сприяти іншим способом виїзду за кордон з метою пропаганди та поширення ідеології тероризму не буде притягнута до кримінальної відповідальності. У той же час, особа, що безпосередньо буде вчиняти однин із видів терористичної діяльності – пропаганду та поширення ідеології тероризму, також уникне будь-якої юридичної відповідальності, у тому числі кримінальної, або адміністративної.

Нажаль, Україна продовжує зазнавати значних людських втрат під час довготривалої антитерористичної операції, та стала однією з шести

країн, які у 2014 році вперше потрапили до рейтингу дослідження «Глобального індексу тероризму», оскільки кількість смертей від тероризму перевищила 500. Крім цього Україна опинилась на 12-му місці, ставши єдиною європейською державою, що потрапила до двадцятки країн у цьому рейтингу (знаходиться між Філіппінами (11 місце в рейтингу) і Єгиптом (13 місце). Дане дослідження опубліковане на сайті Інституту економіки і миру (Institute for Economics and Peace) [5]. Як зазначається, дослідження охоплює терористичну активність за останні 15 років у 162 країнах з наголосом на 2014 рік. Загалом у дослідженні враховані дані про 144 тис. терористичних інцидентів. У 2014 році кількість смертей в результаті актів тероризму зросла на 80% у порівнянні з 2013 роком. «Терористична діяльність зосереджена в основному в 5 країнах Іраку, Нігерії, Афганістані, Пакистані, Сирії. На ці країни припадає 78% втрачених у 2014 році життів», - йдеться у дослідженні.

Реагуючи на події сьогодення та враховуючи, що пропаганда і поширення ідеології тероризму тісно пов’язана й передує терористичним злочинам, ідеологічно обґрунтовує їхнє вчинення, Народним депутатом України Рабіновичем В.З. був внесений на розгляд Верховної Ради України проект Закону України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо відповідальності за пропаганду і поширення ідеології тероризму» від 23.11.2015 № 3506 [6] у якому пропонується доповнити Кримінальний кодекс України статтею 258-6 «Пропаганда і поширення ідеології тероризму».

У пояснювальній записці, доданої до законопроекту, народний депутат України вказав: - «Стало зрозуміло що сьогодні одним із першочергових завдань держави є побудова такої ідеології, яка висвітлювала ту небезпеку, яку складає для інтересів суспільства тероризм та однозначно показувала на єдність національних та індивідуальних інтересів кожного члена суспільства в боротьбі з тероризмом. Тобто події сьогодення

вимагають встановлення на законодавчому рівні кримінальної відповідальності за пропаганду і поширення ідеології тероризму.».

Разом із тим, при більш поглибленому розгляді наданих пропозицій, виникають питання, чому не надаються визначення «пропаганди тероризму» та «ідеології тероризму», а в статті 258.6 не визначається кримінальна відповідальність за виготовлення чи зберігання з метою розповсюдження матеріалів, що містять ідеологію тероризму, чи ввезення на територію України, транзит через її територію або вивіз за її межі таких матеріалів, або вчинення даного виду терористичної діяльності за попередньою змовою групою осіб.

Висновки. Не зважаючи на окремі недоліки, наявні у законопроекті, необхідно констатувати, що криміналізація даного виду терористичної діяльності сприятиме боротьбі з тероризмом у всіх його проявах і ще раз підтвердить прихильність України до неухильного виконання своїх зобов'язань перед світовою спільнотою стосовно протидії тероризму, її позицію засудження всіх актів, методів практики тероризму, а також свідчитиме про підтримку нашою державою дій, що вживаються проти тероризму відповідно до норм міжнародного права та вимог ООН, Ради Європи та інших міжнародних організацій.

Крім того значно підвищиться ефективність діяльності суб'єктів боротьби з тероризмом у загальнодержавній системі боротьби з терористичною діяльністю, особливо з пропагандою і поширенням ідеології тероризму.

Література:

1. Коростиленко А.В. Актуальні питання протидії пропаганді тероризму // Деструктивна пропаганда: шляхи протидії та проблеми відповідальності: матеріали науково-практичної конференції (21 травня, 2015р., м. Київ) / Упорядн.: Фурашев В.М., Поперечнюк В.М. – Київ. – ТОВ «ІВА». - 2015. – С. 149-151.
2. Висновок на проект Закону України про внесення змін до законодавчих актів України (щодо запобігання тероризму) / [Електронний ресурс]. – Режим доступу : http: // www.skourt.gov.ua.

3. Україна підписала протокол до Конвенції Ради Європи про запобігання тероризму / [Електронний ресурс]. – Режим доступу : http: //www.unn.com.ua.
4. Закон України «Про боротьбу з тероризмом» від 20 березня 2003 р. // Відомості Верховної Ради України. − 2003. − № 25. − Ст. 180.
5. Дослідження «Глобального індексу тероризму» / [Електронний ресурс]. – Режим доступу : http: // economicsandpes.org./wp-content/uploads/2015/11/2015 -Global-Terrorism-Index-Report.pdf.
6. Проект Закону про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо відповідальності за пропаганду і поширення ідеології тероризму / [Електронний ресурс]. – Режим доступу : http: // w1.c1.rada.gov.ua/pls/zweb2/.

----------***----------

УДК 343.97

В.А.Василишин,
Броварской межрайонный суд
Киевской области, судья

ФАКТОРЫ РАСПОСТРАНЕНИЯ ПРОПАГАНДЫ ТЕРРОРИЗМА В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ: КРИМИНОЛОГИЧЕСКИЙ АСПЕКТ

Распространение терроризма, в том числе пропаганды террористической идеологии, является одной из глобальных угроз человечества. Для Украины террористическая угроза особенно актуальна, поскольку наша страна имеет исключительное географическое положение, что предопределяет заинтересованность международных террористических организаций к ее территории как особой транзитной зоне.

Концепция борьбы с терроризмом, утвержденная Указом Президента Украины от 25.04.2013 №230, определяет перечень внутренних и внешних факторов, обусловливающих возникновение и распространение терроризма, а также способствующих этому процессу [1].

Среди указанных факторов упоминается распространение идей терроризма в сети Интернет.

Следует рассмотреть отдельные факторы, которые в определенной степени способны оказать влияние на распространение пропаганды терроризма.

Среди этих факторов выделяются политические, социально-экономические, социально-психологические и организационные.

Политические факторы важны для объяснения детерминации терроризма. Среди причин политического характера чаще всего указываются обострения политической борьбы, межгосударственные, межэтнические конфликты, кризис системы государственной власти (коррумпированность государственных институтов, их неспособность оказывать адекватные ответы на вызовы современности, кризис общественного доверия к ним и т.п.), неадекватное реагирование государства на социальные изменения. Терроризм как следствие социально несбалансированного общества, порождает общество с другими характеристиками – вроде образовавшегося в Сомали.

Среди социально-экономических причин чаще всего называются социальное и экономическое неравенство, неблагоприятные социально-экономические обстоятельства в стране, снижение уровня жизни и социальной защищенности значительных слоев населения [2].

Наиболее полно совокупность социально-экономических факторов, благоприятствующих возникновению и развитию в обществе конфликтной ситуации, разрешаемой, в том числе, террористическим способом, можно изложить следующим образом: отсутствие действенной социальной политики и рост социально-экономического неравенства; безработица, особенно в беднейших регионах страны; коренные изменения в социальной структуре, приведшие, в частности, к маргинализации некоторых социальных групп; социальная напряженность; падение уровня жизни; кризис в экономическом развитии государства.

Социально-психологические факторы в значительной степени продуцируемые факторами предыдущей группы, прежде всего

материальными проблемами и социальными искажениями, и имеют решающее значение в объяснении детерминации террористической преступности. Эти факторы, как правило, связаны с несправедливой властью, а их содержание в значительной степени зависит от доминирующих в обществе этических ценностей и потребностей – главных доминант общественного сознания.

Обостренное чувство социальной неустроенности и тревоги, испытываемое значительной частью населения, и утрата веры в способность государства обеспечить безопасность граждан – это спутники любого общества, переживающего либо переходные этапы развития, часто выраженные в «ломке» прежних правил и устоев без эффективных обновлений и альтернатив, либо кризисы, природа которых может быть различной.

Кроме того, как было отмечено В.Л. Васильевым, фактором, косвенно способствующим развитию терроризма или блокирующим его, является система отношений к этому явлению в различных общественных группах, позиция средств массовой информации [3, с.281].

В рамках организационных факторов детерминации пропаганды терроризма следует обратить внимание на недостатки в проведении среди населения информационно-разъяснительной и профилактической работы, направленной на неприемлемость терроризма и отказ от идей использования террористических методов для достижения политических целей; повышение уровня осведомленности общества об опасности и масштабах терроризма. Можно также выделить факторы, связанные с правоохранительной и правоприменительной деятельностью. В данном контексте речь идет о недостатках в организации и функционировании деятельности субъектов борьбы с терроризмом. Трудно представить более опасный сценарий развития пропаганды терроризма, как, например, возможность перехвата (установки) террористами контроля над основными мировыми информационными каналами [4, с.109]. Тенденции развития компьютерных

технологий, которые проникают в деятельность современных СМИ практически делают возможным такой сценарий развития событий.

Генезис террористической пропаганды имеет весьма сложную природу, поскольку он предопределяется самыми различными условиями, предпосылками, причинами и факторами, которые в конечном итоге порождают терроризм.

Основой профилактики пропаганды терроризма должна быть система мер, направленных на локализацию и устранение (или хотя бы минимизацию) тех факторов и причин, которые порождают террористическую идеологию.

Литература:

1. Концепція боротьби з тероризмом [Електронний ресурс] : Указ Президента України від 25.04.2013 р. № 230 / Верховна Рада України. – [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/230/2013. – Заголовок з екрана.
2. Матчанова З.Ш. Социальная напряженность как один из факторов терроризма / З.Ш. Матчанова // Правовая инициатива. – 2015. – № 2. – http://49e.ru/ru/2015/2/10. – Заголовок з екрана.
3. Васильев В.Л. Юридическая психология. – СПб.: Питер, 2004. – С. 380.
4. Матчанова З.Ш. К вопросу о классификации факторов распространения терроризма в современной России / З.Ш. Матчанова // Герценовские чтения. Актуальные проблемы теории права и гражданско-правового образования: материалы Всероссийской научно-практической конференции. – СПб.: АЙСИНГ, 2013. – С. 108-111.

----------***----------

УДК 343.3/.7

О. К.Тугарова,
к.ю.н., доцент, Навчально-наукового інституту інформаційної безпеки Національна академія Служби безпеки України

ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ІНФОРМАЦІЙНИХ ПРАВОВІДНОСИН У КРИМІНАЛЬНОМУ ЗАКОНОДАВСТВІ

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 – ККУ) [1]. За останні роки діючий ККУ 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.

Чинне кримінальне законодавство не містить окремого розділу, родовим об’єктом якого є відносини у сфері обігу інформації. Водночас норми Особливої частини ККУ 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 відносиниу сфері обігу інформації з обмеженим доступом та іншої інформації, що охороняється законом.

Залежно від змісту відомостей, які охороняються нормами ККУ, та суб’єктів, на яких поширюється обов’язок забезпечення їх охорони та

захисту, серед зазначених правопорушень можна виділити злочини, що посягають на встановлений законом 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 ККУ, 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 встановленому законом порядку державною таємницею і підлягають охороні державою [2].

Підстави кримінальної відповідальності за злочини, предметом яких є відомості, що становлять державну таємницю, насамперед, визначені у Розділі І ККУ – «Злочини проти основ національної безпеки України», два склади злочинів якого мають безпосереднє відношення до встановленого законом порядку охорони та захисту державної таємниці: ст.111 ККУ – «Державна зрада» і ст.114 ККУ – «Шпигунство».

Підстави кримінальної відповідальності за вчинення злочинів у сфері обігу державної таємниці також містяться в Розділі XIV ККУ – «Злочини у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову на мобілізацію» (ст.328 ККУ «Розголошення державної таємниці, ст.329 ККУ- «Втрата документів, що містить державну таємницю»). Крім того, Розділ XIX ККУ містить ст.422 – ККУ, нормами якої встановлено відповідальність за розголошення відомостей військового характеру, що становлять державну таємницю, або втрату документів чи матеріалів, що містять такі відомості.

До групи кримінальних правопорушень у сфері обігу професійної таємниці, насамперед, слід відносити протиправні дії, передбачені ст.145 ККУ– «Незаконне розголошення лікарської таємниці» та ст.132 ККУ –

«Розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби» (лікарська таємниця). Також злочином у сфері обігу професійної таємниці слід визнавати діяння, визначені ст.397 – ККУ («Втручання в діяльність захисника чи представника особи»), об'єктивна сторона якого може бути виражена у проханні, вимозі, примушуванні надати відомості, що становлять зміст адвокатської таємниці, примусовому вилученні, огляді документів, пов'язаних з виконанням захисником його обов'язків, а також розголошенні змісту таких документів.

Суміжною до професійних таємниць, охорона яких забезпечується нормами чинного ККУ, 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 [3, с.152]. Чинний ККУ містить два склади злочинів у сфері обігу банківської інформації, а саме: ст. 231 ККУ – «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю» і ст. 232 ККУ – «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 використання відомостей, що становлять комерційну або банківську таємницю.Кримінальний закон також 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 ККУ).

Суміжною до професійних є таємниця досудового розслідування. Нормативні приписи ст. 387 ККУ встановлює відповідальність за розголошення даних оперативно-розшукової діяльності, досудового розслідування. Протиправність зазначених дій виражається у розголошенні даних ОРД або досудового розслідування як особою, попередженою в установленому законом порядку про обов'язок не розголошувати такі дані, так і відповідною службовою особою (суддею, прокурором, слідчим тощо).

Посяганням на встановлений законом порядок забезпечення таємниці досудового розслідування та конфіденційності іншої інформації, пов’язаної з виявленням та розкриттям злочинів, також слід визнавати злочинні дії, передбачені ст.381 ККУ – «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» [4].

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, 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 відповідних відомостей.

Окрему групу кримінальних правопорушень утворюють злочини, що посягають порядок обігу інформації, що не є обмеженою у доступі. Проте, використання такої інформації відбувається у визначеному законом порядку. Об’єктивна сторона таких діянь знаходить вираз у 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 ККУ) та приховуванні чи

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. 396ККУ).

Окрему групу кримінальних правопорушень у сфері обігу інформації, становлять злочини, що посягають на врегульовані законом суспільні відносини у сфері технічного захисту інформації.Розділ XVI Особливої частини ККУ («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 ККУ), об'єктивна сторона яких виражається у наступних формах: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ч.1 ст.361 ККУ); створення, розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу зазначених систем (ч.1 ст.3611 ККУ); несанкціонований збут або розповсюдження інформації з обмеженим доступом, яка в них зберігається (ч.1 ст.3612 ККУ); несанкціонована зміна, знищення або блокування інформації (ч.1 ст.362 ККУ) та несанкціонованого перехоплення або копіювання інформації (ч.2 ст.362 ККУ); 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 ККУ). Спеціальною нормою по відношенню до зазначених злочинів є дії, передбачені ст.3761 ККУ – «Незаконне втручання в роботу автоматизованої системи документообігу суду».

Третю групу правопорушень становлять злочини, що посягають на врегульовані законом суспільні відносиниу сфері інформаційно-

психологічної безпеки особи та суспільства. Чинний КК України містить ряд статей, нормами яких визначаються підстави кримінальної відповідальності за вчинення протиправних дій, що посягають на свободу слова і доступу до публічної інформації, особисту і суспільну свідомість (ст.171 ККУ – «Перешкоджання законній професійній діяльності журналістів, ст.298 ККУ – «Незаконне проведення пошукових робіт на об'єкті археологічної спадщини, знищення, руйнування або пошкодження об'єктів культурної спадщини», ст. 2981 ККУ – «Знищення, пошкодження або приховування документів чи унікальних документів НАФ»).

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 ККУ); пропаганді насильства та аморального способу життя (ст.ст. 300, 301, 436 ККУ); впливі на діяльність державних службовців (ст.ст. 343, 344, 376, 397 ККУ) тощо. Зазначені злочини містяться у різних розділах Особливої частини ККУ, 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.

З огляду на зазначене, вбачається доцільним об'єднання в окремому розділі Особливої частини ККУ 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. Про державну таємницю: Закон України від 21.01.1994 р. № 3855- XII// Відомості Верховної Ради України. – 1994. – № 16. – Ст. 93.

3. 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.
4. Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві: Закон України від 23.12.1993 р. N 3782-XII // Відомості Верховної Ради України. – 1994. – № 11. – Ст. 51.

----------***----------

А. М. Благодарний,
к.ю.н., с.н.с., завідувач кафедри
загальноправових дисциплін
Національної академії
Служби безпеки України

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ АДМІНІСТРАТИВНО-ПРАВОВИХ ЗАХОДІВ ПРОФІЛАКТИКИ ПРАВОПОРУШЕНЬ В ІНФОРМАЦІЙНІЙ СФЕРІ

Невід'ємною складовою гібридної війни, яка ведеться проти України, є інформаційна війна, тому одним із актуальних завдань реформування українського адміністративного права є втілення в життя належного і ефективного правового регулювання діяльності органів державної влади, зокрема, діяльності посадових осіб правоохоронних органів, спрямованої на запобігання правопорушенням в інформаційній сфері.

Заходи адміністративного попередження можна визначити як комплекс заходів організаційного, психологічного, фізичного та іншого впливу, спрямованих на виявлення та недопущення правопорушень, забезпечення безпеки держави, громадського порядку та особистої безпеки громадян [1, с. 100]. Як зазначав В.Б. Авер’янов, заходи адміністративного попередження виконують особливі правоохоронні функції, які відрізняють їх від інших заходів адміністративного примусу. Окремі запобіжні заходи за своїм характером наближені до заходів адміністративного припинення, у зв'язку з чим у літературі не завжди однозначно вирішується питання про віднесення певних конкретних заходів до відповідного виду примусу.

Основним і єдиним критерієм відмінності є наявність або відсутність правопорушення.

Заходи адміністративного попередження не виконують функції покарання особи, до якої вони застосовуються,що характерно для адміністративних стягнень, тому не потребують встановлення вини порушника як обов'язкової умови застосування [2, с. 421].

Ці заходи є різноманітними, застосовуються у різних галузях суспільного життя й різними суб'єктами (поліцією, органами охорони державного кордону, СБ України, контрольно-наглядовими органами (державними інспекціями) тощо). Законодавчою базою застосування таких заходів є КУпАП та Митний кодекс України, закони України: "Про Національну поліцію", "Про оперативно-розшукову діяльність", "Про контррозвідувальну діяльність", "Про Службу безпеки України", "Про боротьбу з тероризмом", "Про Державну прикордонну службу України", "Про дорожній рух" тощо.

Для попередження правопорушень в інформаційній сфері найбільше значення, на наш погляд, має застосування таких адміністративно-попереджувальних заходів:

− профілактика правопорушень, яка реалізується із використанням комплексу оперативних та адміністративних заходів. Проект закону України "Про профілактику правопорушень" визначає профілактику як обов'язкову діяльність органів державної влади, місцевого самоврядування, підприємств, установ, організацій незалежно від форм власності, зокрема громадських організацій, спрямовану на виявлення та усунення причин і умов, які сприяють учиненню правопорушень, а також виявлення осіб, схильних до вчинення правопорушень, та застосування заходів до їх виправлення [1, с. 112];

- огляд (особистий огляд і огляд речей, багажу, транспортних засобів, різних об'єктів) як захід адміністративного попередження може застосовуватись різними органами державної влади.

Метою огляду є попередження та виявлення правопорушень, забезпечення громадської безпеки. Суть даного заходу полягає у законодавчо закріпленому обов'язку громадян пред'явити на вимогу уповноваженої особи певні предмети (речі), документи. У разі відмови, особу може бути піддано особистому огляду або огляду його речей, транспортних засобів;

− офіційне застереження про неприпустимість протиправної поведінки. Даний захід застосовується до осіб, які систематично порушують громадський порядок, у випадках, коли немає достатніх підстав для притягнення особи до кримінальної чи адміністративної відповідальності. Метою офіційного застереження є не тільки реакція на протиправну поведінку, але й недопущення її продовження в майбутньому. Правові підстави цього заходу встановлені законами України "Про Службу безпеки України", "Про контррозвідувальну діяльність" тощо, порядок застосування визначається відомчими нормативними актами;

- відвідування підприємств, установ та організацій, входження на земельні ділянки, у житлові та інші приміщення громадян. Загалом, здійснювати даний захід уповноважені посадові особи багатьох державних органів для виконання контрольних та наглядових функцій, при цьому мета та об'єкти застосування суттєво різняться, але суть завжди полягає у входженні, проникненні на відповідну територію, об'єкт чи у приміщення [1, с. 102];

- внесення подання про усунення причин і умов, які сприяють вчиненню правопорушень, відрізняється від інших адміністративно-запобіжних заходів головним чином тим, що його мета полягає в запобіганні вчиненню правопорушень не шляхом їх виявлення і наступного припинення чи встановлення особи порушника, а шляхом запобігання вчиненню правопорушень конкретним органом чи посадовою особою в майбутньому завдяки впливу на обставини, які їх породжують [3, с. 95]. Щодо адміністративних правопорушень таке правило встановлено у ст. 282 КУпАП, відповідно до якої орган (посадова особа), який розглядає справу,

встановивши причини та умови, що сприяли вчиненню адміністративного правопорушення, вносить у відповідний державний орган, громадську організацію або посадовій особі пропозиції про вжиття заходів щодо усунення цих причин та умов. Про вжиті заходи протягом місяця із дня надходження пропозиції слід повідомити орган (посадову особу), який вніс пропозицію.

Підсумовуючи викладене, слід зазначити, що до основних заходів адміністративного попередження, які мають право застосовувати посадові особи правоохоронних органів України для протидії правопорушенням в інформаційній сфері, слід віднести такі заходи як: профілактика правопорушень; огляд (особистий огляд і огляд речей, багажу, транспортних засобів, різних об'єктів); офіційне застереження про неприпустимість протиправної поведінки; відвідування підприємств, установ та організацій, входження на земельні ділянки, у житлові та інші приміщення громадян; внесення подання про усунення причин і умов, які сприяють вчиненню правопорушень.

Література:

1. Адміністративне право України : підруч. / [А.М. Благодарний, Ю.П. Бурило, І.М. Гриненко та ін. ; за заг. ред. Є.Д. Скулиша]. – К. : Наук.-вид. центр НА СБ України, 2012. – 560 с.
2. Адміністративне право України. Академічний курс: Підр.: У двох томах: Том 1. Загальна частина /Ред. колегія: В.Б.Авер'янов (голова (та інш.) – К.: ТОВ "Видавництво "Юридична думка", 2007. – 591 с.
3. Комзюк А.Т. Заходи адміністративного примусу в правоохоронній діяльності міліції: поняття, види та організаційно-правові питання реалізації / А.Т.Комзюк, О.М.Бандурка (заг. ред.) ; МВС України ; Національний ун-т внутрішніх справ. – Х. : Вид-во Національного ун-ту внутрішніх справ, 2002. – 355 с.

----------***----------

І. Ф. Корж,
д.ю.н., завідувач сектору НДІІП
НАПрН України

ЗНАЧИМІСТЬ ПРИНЦИПІВ, НЕДОТРИМАННЯ ЯКИХ ПРИЗВОДИТЬ ДО НАСТАННЯ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ В ІНФОРМАЦІЙНІЙ СФЕРІ

Права громадян в інформаційній сфері сучасного суспільства потребують належного правового захисту. Зазначене регулюється як міжнародним правом, та і різними галузями національного права, зокрема кримінальним, адміністративним, цивільним тощо.

Водночас існує необхідність удосконалення правового регулювання у інформаційній сфері, що обумовлюється потребою в підвищені ефективності захисту інформаційних прав громадян. Зазначене випливає з того, що кількість конфліктів, що виникає в інформаційній сфері, пропорційна кількості проблемним питанням (суспільних відносин), що виникають внаслідок неврегульованості чи неналежної їх урегульованості правом. На сьогоднішній день норми, що регламентують доступ до інформації, їх принципи та відповідальність за порушення норм «розпорошені» по різним джерелам галузей права, тому актуальність і значимість упорядкування і правових норм, і принципів нині зростає.

Загальновизнано, що демократична система може функціонувати найбільш ефективно лише у випадку, коли громадськість максимально поінформована. Більше того, через соціальний і технологічний розвиток сучасне життя стало настільки складним, за якого державні органи часто володіють великою кількістю документів та інформації, що представляє суспільний інтерес і є суспільно важливими. Для забезпечення адекватної участі громадян у суспільному житті, необхідно забезпечити з урахуванням неминучих виключень і обмежень доступ громадськості до інформації, що знаходиться в розпорядженні державних органів всіх рівнів. З огляду на зазначене важливого значення набуває чітке дотримання усіма принципів

доступу до інформації, тобто основних ідей, вихідних положень, які закріплені в законі, мають загальну значущість, вищу імперативність (веління) і відображають суттєві положення права . Невиконання зазначеного призводить до вчинення відповідного правопорушення, що тягне за собою настання юридичної відповідальності.

Зазначені принципи впливають на весь процес підготовки нормативно-правових актів, їх видання, встановлення гарантій дотримання правових вимог. Вони є основним критерієм для правотворчої, правозастосовної та правоохоронної діяльності державних органів. Від рівня їх дотримання залежить стабільність та ефективність правової системи.

Принципи національного права доступу до інформації базуються на принципах міжнародного права, які зазначені в конвенціях, пактах, хартіях, рекомендаціях тощо. Основні принципи доступу чітко сформульовані, наприклад, у Йоханнесбурзьких принципах національної безпеки, свободи слова і доступу до інформації, які були сформовані в 1990-95 роках і опубліковані в 1995 році на форумі фахівців в галузі міжнародного права, скликаному організацією «Стаття 19», Міжнародним центром проти цензури разом з Центром прикладних правових досліджень при Університеті Вітватерсранда [1]. Такими, також, є принципи, зазначені в Рекомендації № R (81) 19 Комітету міністрів Ради Європи [2], в якій зазначено, що доступ громадськості до інформації, передбачає зміцнення довіри громадськості до державного управління, а також акцентується на важливості отримання громадськістю в демократичному суспільстві адекватної інформації із суспільно важливих питань.

Як зазначено в Рекомендації, ці принципи слід розуміти як вказівку на загальний стандарт, а не як пересторогу для держав-членів від визнання додаткових або ширших прав й гарантії для забезпечення доступу до інформації або розширення сфери їх застосування. Тому дотримання цих принципів у відповідності до Рекомендації є сумісним з вимогами доброго та

ефективного управління, а також із бажанням досягнення максимально можливого ступеня доступу до інформації.

У 2002 році була ухвалена Рекомендація [3], в якій були зазначені конкретні принципи доступу до офіційних документів, головним з яких є те, що держави-члени повинні гарантувати кожній особі, після здійснення нею запиту, право доступу до офіційних документів, які є в розпорядженні органів державної влади.

У міжнародному праві напрацьовано низку принципів, які дозволяють визначити, чи насправді внутрішнє законодавство забезпечує доступ до інформації. Тут згадати слід два принципи:

– перший, це принцип максимального оприлюднення: вся інформація, яку зберігають державні органи влади, підлягає оприлюдненню, винятки можуть бути тільки для дуже обмеженого числа випадків;

– другий принцип характеризує вимоги щодо обмежень:

а) виключення повинні бути ясними;

б) описуватися вузько;

в) підлягати суворому контролю на предмет наявності «шкоди» і впливу на «суспільні інтереси».

В державного органу оприлюднити інформацію є виправданою, якщо:

по-перше, інформація має відношення до легітимної мети, передбаченої законом;

по-друге, її оприлюднення має дійсно загрожувати тим, що буде завдано суттєвої шкоди легітимній меті;

по-третє, шкода, яка може бути заподіяна меті, повинна бути вагомішою, ніж суспільний інтерес в отриманні інформації. З цих принципів однозначно витікає, що перелік відомостей, які входять до кола обмежень, має бути вичерпно визначений і оприлюднений» [4].

В Українському законодавстві цей принцип звучить, як гарантованість права на інформацію [5], що є сукупністю умов та засобів, спрямованих на забезпечення цього права. Зазначене підтверджується статтею 34 Конституції

України, а саме, право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб на свій вибір. Дане положення передбачає наявність механізмів захисту свої права, є певним гарантом відкритості та прозорості органів державної та місцевої влади. Адже лише «широкий доступ до інформації дозволяє громадянам виробити адекватне бачення та сформувати критичні погляди щодо стану суспільства, в якому вони живуть, та щодо органів влади, які ними керують, тим самим заохочуючи громадян до поінформованої участі в питаннях, що становлять спільний інтерес, сприяє більшій дієвості та ефективності адміністративних органів і допомагає підтримувати їхню цілісність, запобігає ризику корупції, є чинником, що підтверджує легітимність органів управління в якості державних служб, і посилює довіру громадськості до органів державної влади.

Однак законодавчі гарантії і практика щодо реалізації права на інформацію різняться. Як зазначають в правозахисних, адвокатських і журналістських колах, посадові і службові особи органів державної влади відносяться до інформації, як до особистої власності. Ними порушуються терміни розгляду інформаційних запитів, насамперед строків повідомлення про неможливість задовольнити інформаційний запит, про відстрочку задоволення запиту. Значні недоліки відмічаються у питанні повноти наданої інформації, щодо обґрунтованості відмови чи обмеження наданої інформації тощо.

Основні причини у зазначеному, на нашу думку, і не тільки на нашу, криються у наступному:

- у правовому нігілізмі, насамперед, у неповазі до права з вірою у свою безнаказаність, тобто, причина у недієвості одного з основних принципів юридичної відповідальності – невідворотності відповідальності. Визначення заборон, обов’язків і санкцій за їхнє порушення має сенс лише за умови, що особи-порушники притягуються до відповідальності і піддаються заходам примусу, передбачених відповідними санкціями порушених правових норм.

Невідворотність відповідальності залежить в більшій мірі від налагодженої роботи правоохоронних органів, від підготовки, компетентності і добросовісності працівників, уповноважених притягувати до відповідальності і застосовувати санкції. Говорити про готовність правоохоронних органів у нинішніх умовах плідно працювати над зазначеними недоліками суспільства не приходиться, і це підтверджують нинішні реалії у державі;

- у низькому рівні фахової підготовки посадових та службових осіб, низьким знанням ними інформаційного законодавства. Всупереч багатьом обіцянкам політиків, основним при прийнятті на державну службу не є принципи професійності і компетентності, а продовжують діяти принципи особистої відданості і політичної належності. Є маса прикладів на підтвердження зазначеного. Зазначене призводить до нездатності посадових і службових осіб тлумачити норми закону, що в кінцевому результаті призводить до хибного розуміння духу та букви Конституції та законів України;

- на сьогоднішній день ми ще не маємо належної культури інформаційної відкритості державної влади внаслідок важкого спадку держави «великих ілюзій та гнилої моралі». Незважаючи на вживані всебічні заходи, включаючи прийняття Національної стратегії у сфері прав людини [6], на міжнародну допомогу у цій сфері, похвастатися належною відкритістю у своїй діяльності державна влада ще не може. Цьому «сприяють» і наявні недосконаліть законодавства, що регламентує доступ до інформації та встановлює відповідальність за його порушення, а також неналежний рівень матеріально-технічного забезпечення.

Тому дотримання згаданих принципів при забезпеченні пріоритетності прав і свобод людини як визначального чинника під час визначення державної політики, прийняття рішень органами державної влади та органами місцевого самоврядування залишається на сьогоднішній день для українського суспільства актуальним.

Література:

1. Принципи національної безпеки та доступ до інформації. [Електронний ресурс]. – Режим доступу: http://khpg.org/index.php?do=print&id=1317625159.
2. Про доступ до інформації, що знаходиться у розпорядженні державних органів: Рекомендація № R (81) 19 Комітету міністрів Ради Європи, прийнята 25 листопада 1981 року на 340 зустрічі заступників міністрів. [Електронний ресурс]. – Режим доступу: http://medialaw.org.ua/library/rekomendatsiya-r-81-19-pro-dostup-do-informatsiyi-shho-znahodytsya-u-rozporyadzhenni-derzhavny(h-organiv/.
3. Про доступ до офіційних документів: Рекомендація R (2002) 2 Комітету міністрів Ради Європи, ухвалена 21 лютого 2002 року на 784 засіданні заступників міністрів. [Електронний ресурс]. – Режим доступу: http://www.coe.kiev.ua/docs/km/r(2002)2.htm.
4. Международные принципы доступа к информации. [Електронний ресурс]. – Режим доступу: http://pravo-ukraine.org.ua/blogs/pravo-na-informatsiyu/13006-mezhdunarodnye-principy-dostupa-k-informacii.
5. Про інформацію: Закон України від 2 жовтня 1992 року // Відомості Верховної Ради України. –1992. – № 48. – Ст. 650.
6. Про затвердження Національної стратегії у сфері прав людини: Указ Президента України від 25 серпня 2015 року № 501/2015 // Офіційний вісник Президента України. – 2015. – № 20. – Ст.1203.

----------***----------

В. С. Цимбалюк,
д.ю.н., с.н.с., завідувач лабораторією теорії та історії інформаційного права Науково-дослідногоінституту інформатики та права Національної академії правових наук України

ЗАСТОСУВАННЯ ЗАГАЛЬНИХ ПОЛОЖЕНЬ ДЕЛІКТОЛОГІЇ У КОНСТРУЮВАННІ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ПРАВОПОРУШЕННЯ В ІНФОРМАЦІЙНІЙ СФЕРІ СУСПІЛЬСТВА

У порядку постановки проблеми в загальному вигляді пропонується звернути увагу на окремі проблеми теоретико-методологічного змісту щодо застосування загальних положень деліктології у конструюванні юридичної відповідальності за правопорушення в інформаційній сфері суспільства.

Мета даної публікації полягає у поданні на розгляд зацікавленої наукової громадськості та практиків окремих результатів наукових досліджень стосовно правового забезпечення інформаційної сфери суспільства у контексті окремих загальних положень деліктології.

Зазначені дослідження проводяться в Науково-дослідному інституті інформатики і права Національної академії правових наук України за темою «Теоретико-правові основи формування і розвитку інформаційного суспільства». Ця тема є продовженням багаторічних наукових досліджень пов'язаних з систематизацією, у її складі інкорпорацією, консолідацією та кодифікацією законодавства України щодо інформації [1;2].

Виклад окремих, основних результатів досліджень пропонується розпочати із сформованих методологічних, концептуальних та доктринальних положень теорії і практики правового регулювання суспільних відносин щодо інформації у аспекті деліктології.

Деліктологія є одним із важливих інститутів загальної теорії права, що екстраполюється без винятку на всі інші інститути, підгалузі, провідні, комплексні та спеціальні галузі сучасного права. Не є винятком з них і така комплексна галузь права як й інформаційне права, та у його складі – галузева деліктологія [3].

Під деліктологією інформаційної сфери суспільства (інформаційною деліктологією) в науці інформаційного права пропонується розуміти його інститут – множину знань, вчення про правопорушення, протиправну поведінку, порушення прав пов'язаних з інформацією, технологіями її прояву та встановленням відповідної відповідальності правопорушників.

Серед різних концепцій загальних положень, основного змісту інформаційної деліктології найбільш продуктивною, раціональною, праксеологічною вважається та, що базується на постулаті, що всі прояви деліктів щодо інформації мають розглядатися у площині відповідної відповідальності провідних галузей права: чи дисциплінарної (трудової); чи цивільної; чи адміністративної; чи то кримінальної.

Деліктологія як вчення є комплексною наукою. Її складовими є питання, що вивчають не тільки у юридичних науках, але й у психології, соціології, етики, філософії та інших науках. Невід'ємними складовими деліктології є й криміналістика та кримінологія. Якщо розглядати право в складі його приватної та публічної парадигм, що доповнюють одна одну, у єдиній фрактальній, об'ємній матриці, то деліктологія відображає в своїй герменевтичній сутності обидва полюси права так само, як і інші галузі, інститути та їх юридичні режими [4].

Головним постулатом деліктології є те, що всі юридичні інститути, підгалузі, галузі права визначаючи приписи, заборони, дозволи у гіпотезах, диспозиція та галузевих санкціях за делікти (юридичні правопорушення) мають однозначно трактувати поняття термінів, категорій, змісту правовідносин при визначенні (конструюванні) галузевої відповідальності. Зазначене положення в основному дотримується і при конструюванні юридичної відповідальності за правопорушення в інформаційній сфері суспільства, але є і винятки, що породжують правовий хаос.

Для прикладу пропонується звернути увагу на формулювання окремих положень із Кримінального кодексу України (ККУ): порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст.163 ККУ). У цій статті вживається слово «комп'ютер», «зв'язок». Проте у спеціальному законодавстві визначення цих понять немає. Відповідно до пунктів 1,5,12 ст.92 Конституції України положення статті 163 ККУ мають бути екстрапольовані виключно на закони. Принципи зазначених конституційних положень підсилені і у ст. 19 Основного Закону, де зазначено, що правовий порядок в Україні ґрунтується на засадах, відповідно до яких ніхто не може бути примушений робити те, що не передбачено законодавством. А органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України. Тобто, таким чином

виключається можливість трактування понять, категорій, змісту правовідносин у формулюваннях підзаконних актів.

Так, ст. 1 Закону України «Про телекомунікації» пропонує визначення змісту лише електрозв'язку у змісті телекомунікації – передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах. З точки зору фізики під сучасний зміст цього терміну підпадають і сутності інших понять статті 163 ККУ. Таким чином розробники змісту зазначених законодавчих актів не тільки не врахували термінологічну відповідність їх, у тому числі щодо положенням Конституції України, але і відповідність їх між собою. Отже, по суті, створено колізію стосовно можливості застосування відповідальності за ст..163 ККУ. Подібно такі колізії спостерігаються і щодо можливостей застосування відповідальності й за ряд інших статей ККУ (див. розділ 16 Особливої частини, щодо злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Окремо пропонується звернути увагу на положення розділу 4 Закону України «Про інформацію» (далі: Закон). Назва розділу на перший погляд має викликати відповідну юридичну рефлексію: відповідальність за порушення законодавства про інформацію. У цьому розділі перша його стаття (ст.27) має аналогічну назву розділу.Знову ж, на перший погляд, юридичний зміст та сутність цієї статті є зрозумілим для встановлення міжгалузевого правового зв'язку (гіперзв'язку), у тому числі з кримінальним правом (як виключно деліктним правом), а також з деліктними підгалузями трудового права (у його складі дисциплінарного права), а також адміністративного та цивільного права. Тобто, єдиний у цій статті пункт 1 має формулювання (конструкцію), що порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову,

адміністративну або кримінальну відповідальність згідно із законами України.

Але виникає питання: а з якими законами України? У цій та ряді інших статей Закону вживається категорія «законодавство України про інформацію» та подібні за сутністю до нього поняття (наприклад, законодавство про інформацію тощо). Але загальної статті, де б визначалася система законодавства про інформацію, цей Закон не містить. Згадування про окремі закони України йде у окремих статтях Закону. З точки зору юридичної догматології можна таку систему сформувати із аналізу норм у статтях цього Закону. Але ні ККУ, ні Цивільний кодекс України (далі: ЦКУ), ні Кодекс України про адміністративні правопорушення не мають розділів де прямо визначається деліктна складова щодо порушення законодавства про інформацію. З цього випливає, що зазначена норма є лише декларативною.

На окрему увагу з точки зору загальних положень деліктології заслуговує аналіз змісту та сутності ст. 29 у тому ж розділі Закону,де мова йде про поширення суспільно необхідної інформації. За сутністю зміст цієї статті зводить нанівець всі положення законодавства України щодо інформації з обмеженим доступом, у тому числі можливості державного захисту правовідносин щодо цього виду інформації, його деліктної складової, у тому числі стосовно таємниці, зокрема і державної таємниці.

Окремі висновки із проведеного дослідження пропонуються такі:

1. Підтримується концептуальна позиція тих дослідників, які вважають, що подальше удосконалення законодавства України про інформацію пропонується здійснювати за доктриною кодифікації його: на рівні розробки проекту Кодексу України про інформацію, де має бути також консолідовано понятійний апарат інформаційного права з урахуванням загальних положень деліктології, зокрема у розумінні її як вчення, що має ознаки юридичної гіперсистеми міжгалузевого змісту.

2. З точки зору техніки законотворення за основу для створення проекту Кодексу України про інформацію має бути взятий Закон України

«Про інформацію». Цей Закон, після прийняття цього кодексу, має втратити чинність, а перевірені практикою конструкції його норм мають бути враховані у галузевій деліктології, та знайти відображення у іншому законодавстві, у тому числі у Кримінальному Кодексі України, Кодексі України про адміністративні правопорушення та Цивільному Кодексі України тощо .

Література:

1. Цимбалюк В. С. Інформаційне право (основи теорії і практики) : Монографія. / В. С. Цимбалюк. – К.: « Освіта України », 2010. – 388 с.
2. Цимбалюк В. С. Інформаційне право: концептуальні положення до кодифікації інформаційного законодавства : Монографія. / В. С. Цимбалюк. – К.: « Освіта України », 2011. – 426 с.
3. Максименко Ю. Інформаційна деліктологія: історичні витоки / Ю. Максименко // Підприємництво, господарство, право : науково-практичний господарсько-правовий журнал. – 2014. – № 9. – С. 67-70.
4. Пєтков С. Адміністративна деліктологія /С. Пєтков. [Електронний ресур]. – Режим доступу: http://adminpravo.blogspot.com/2013/10/blog-post_7.

----------***----------

І. В. Павленко,
к.ю.н., доцент кафедри публічного права ФСП НТУУ «КПІ»

ПРОБЛЕМНІ ПИТАННЯ КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ ІНФОРМАЦІЙНИХ ПРАВОВІДНОСИН

Інформаційні правовідносини можна визначити як відносини, предметом яких є інформація, і які врегульовані нормами права. Зазначимо, що найбільш цінні, важливі з них знаходяться під охороною кримінального закону. Так, чинний Кримінальний кодекс України (далі КК України) містить чимало діянь, за які встановлена кримінальна відповідальність в інформаційній сфері: ст. 114 шпигунство, ст. 159 порушення таємниці голосування, ст. 163 порушеннятаємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер, ст. 220-1 порушення порядку ведення бази даних про

вкладників або порядку формування звітності, ст. 232 розголошення комерційної або банківської таємниці, ст. 238 приховування або перекручення відомостей про екологічний стан або захворюваність населення, ст. 328 розголошення державної таємниці та багато інших. Загалом норми Особливої частини налічують понад 50 складів злочинів, що посягають на встановлений законом порядок створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації.

Як видно, всі такі діяння розпорошені по різним розділам Особливої частини. У зв'язку з цим, в наукових колах піднімається питання щодо їх групування в окремий розділ. Так, дотримуючись вказаної позиції О.К. Тугарова вказує, що «вбачається доцільність 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» [1, с. 65].

Крім того, такі пропозиції неодноразово розглядались й на рівні законопроектів. Так, в 2011 року до Верховної Ради України було внесено проект Закону України “Про внесення змін до деяких законодавчих актів України щодо відповідальності за посягання у сфері інформаційної безпеки”(законопроект №9575).

Законопроектом пропонувалось вилучити з КК України такі статті: ст. 132 розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби, ст. 145 незаконне розголошення лікарської таємниці, ст. 159 порушення таємниці голосування, ст. 163 порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв’язку або через комп’ютер, ст. 168 розголошення таємниці усиновлення (удочеріння), ст. 182 порушення недоторканності приватного життя, ст. 231 незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську

таємницю, ст. 232 розголошення комерційної або банківської таємниці, ст. 328 розголошення державної таємниці, ст. 330 передача або збирання відомостей, що становлять конфіденційну інформацію, яка знаходиться у володінні держави, а також положення ст. 158 фальсифікація виборчих документів, документів референдуму чи фальсифікація підсумків голосування, надання неправдивих відомостей до органів Державного реєстру виборців чи фальсифікація відомостей Державного реєстру виборців щодо втручання або інших несанкціонованих дій з базою даних, та положення статті 209-1 щодо розголошення у будь-якому вигляді інформації, яка відповідно до закону надається спеціально уповноваженому центральному органу виконавчої влади із спеціальним статусом з питань фінансового моніторингу, особою, якій ця інформація стала відома у зв'язку з професійною або службовою діяльністю.

Натомість, пропонувалось узагальнити і включити склади злочинів вилучених з вищенаведених статей у статті 361-363-1 розділу XVI КК і замінити назву розділу зі «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» на «Злочини у сфері інформаційної безпеки», а також запровадити відповідальність за: незаконні дії з комп'ютерними даними (ст. 361); незаконні дії в сфері телекомунікаційних послуг (ст. 361-1); порушення правил здійснення масових розсилок електронних повідомлень (ст. 361-3); незаконне надання доступу до інформації (ст. 361-2); заподіяння необережної шкоди через незаконні дії з комп'ютерними даними (ст. 362); заподіяння необережної шкоди через незаконне створення перешкод для надання телекомунікаційних послуг або їх незаконне отримання (ст. 362-1); заподіяння необережної шкоди через незаконне надання доступу до інформації (ст. 362-2); заподіяння необережної шкоди через порушення правил здійснення масових розсилок електронних повідомлень (ст. 362-3); порушення вимог інформаційної безпеки (ст. 363); незаконне отримання доступу до інформації (ст. 363-1) [2, електронний ресурс].

Такий підхід є цікавим і не позбавлений конструктивізму, проте, на нашу думку, виникає ряд питань, які можуть заплутати ситуацію. Так, новий розділ охоплюватиме ряд діянь, цінність, важливість охорони яких є різною. Скажімо, не можна в один ряд поставити охорону державної таємниці і охорону приватної інформації фізичної особи. Саме тому виникає питання - яке місце в системі Особливої частини КК України отримає такий новий розділ, адже, як відомо, в Особливій частині законодавець згрупував злочини у розділах за порядком від найбільш охоронюваних до найменш з точки зору їх важливості та цінності.

Крім того, ще одним проблемним питанням є питання щодо включення в цей новий розділ *всіх* діянь, предметами яких є інформація. Йдеться, зокрема, про інформацію порнографічного характеру в ст. 301 КК України як приватну інформацію фізичної особи [3, с. 67].

Означені питання є актуальними, адже інформатизація - це вже неминучий новий еволюційний етап цивілізаційного розвитку суспільства. Саме тому питанням охорони інформаційних правовідносин має приділятися належна увага. Отже, означені нами проблемні питання кримінально-правової охорони інформаційних відносин потребують дискусії, обговорення та подальшої наукової розробки.

Література:

1. Тугарова О.К. Кримінально-правове забезпечення охорони інформаційних правовідносин / О.К. Тугарова // Науковий вісник Херсонського державного університету. Серія юридичні науки. – 2015. – Випуск 4. Том 3. – с. 61-66
2. Відповідальність за посягання у сфері інформаційної безпеки // Центр демократії та права / [Електронний ресурс]. – Режим доступу: http://medialaw.org.ua/news/vidpovidalnist-za-posyagannya-u-sfer/
3. Павленко І.В. Проблемні питання предмету злочину, відповідальність за який передбачена ст. 301 КК України / І.В. Павленко // Журнал східноєвропейського права. – 2015. – № 11. – с. 67-69

----------***----------

Н. В.Карчевский,
д.ю.н., профессор.
Луганский государственный
университет внутренних дел
им. Э.А. Дидоренко

КАКИМ ДОЛЖНО БЫТЬ УГОЛОВНО-ПРАВОВОЕ ОТРАЖЕНИЕ СОЦИАЛЬНЫХ ТЕНДЕНЦИЙ ИНФОРМАТИЗАЦИИ?

Появление преступлений в сфере компьютерной информации является далеко не единственным последствием взрывной информатизации общества. Значительным потенциалом общественной опасности характеризуются также следующие факторы: чрезмерная капитализация информационного пространства; развитие возможностей манипуляции общественным сознанием в политической сфере; формирование сверхмощных баз персональных данных, представляющих опасность тотального контроля над личностью; рост уровня идеологической уязвимости политических систем из-за наличия глубоких социальных конфликтов, которые могут быть задействованы путем использования информационных технологий; интеллектуальная и духовная деградация общества и т.д. Все это означает, что задача совершенствования уголовно-правового обеспечения противодействия преступлениям в сфере компьютерной информации должна решаться не самостоятельно, а в контексте уголовно-правового обеспечения процессов информатизации в целом.

Прежде всего должен быть решен вопрос объекта уголовно-правовой охраны в сфере информатизации. Какие общественные отношения должны охраняться нормами права с тем, чтобы обеспечивать развитие положительных и минимизацию негативных социальных последствий информатизации? Очевидно, что речь идет об общественных отношениях, в пределах которых обеспечивается реализация информационной потребности граждан, общества или государства. Именно необходимость реализации возрастающей информационной потребности вызвала в своё время появление речи, письма и технологий книгопечатанья, стимулировала развитие радио и

телевидения и обусловливает сегодня постоянное совершенствование и расширение сферы применения современных компьютерных технологий. Поэтому правовое регулирование и охрана именно этих отношений, отношений в сфере реализации информационной потребности, может обеспечить предупреждение негативных последствий информатизации.

Для обозначения системы общественных отношений, направленных на обеспечение реализации информационной потребности граждан, общества или государства предлагается использовать термин «информационная безопасность». Информационную безопасность субъекта следует считать обеспеченной тогда, когда он имеет возможность получать полную, достоверную и достаточную для принятия эффективных решений информацию. Такое состояние достигается социальной активностью в трех взаимосвязанных группах общественных отношений, представляющих собой структурные элементы информационной безопасности. Это общественные отношения: в сфере использования информационных технологий, в сфере обеспечения доступа к информационному ресурсу и в сфере формирования информационного ресурса.

В пределах первой группы общественных отношений выполняется задание обеспечения функционирования эффективных средств информационной деятельности, в пределах второй – обеспечивается возможность субъектов получать беспрепятственный доступ к необходимым информационным ресурсам, а в пределах третьей – обеспечивается формирование информационного ресурса, который отвечает потребностям субъектов [3].

Функционирование и эффективность каждого из элементов системы информационной безопасности обусловлены другими её элементами. Предоставление доступа к информации не имеет смысла без формирования информационного ресурса и является неэффективным без использования информационных технологий. Значение формирования информационного ресурса определяется возможностью дальнейшего доступа к нему и

обеспечивается путем использования информационных технологий. Функционирование информационных технологий приобретает социальное значение именно как средства доступа и формирования информационных ресурсов.

Социальная значимость как формирования информационного ресурса, так и предоставления доступа к информации, а также использования информационных технологий определяется значением тех общественных отношений, в пределах которых возникает информационная потребность. То есть общей чертой отношений информационной безопасности является то, что целесообразность их уголовно-правовой охраны определяется социальной значимостью тех общественных отношений, в пределах которых возникает информационная потребность. Именно актуальность последних определяет значимость отношений информационной безопасности, а также целесообразность и интенсивность соответствующих мер правового регулирования. Например, значимость доступа к информации и, как следствие, необходимость его правового регулирования не является самостоятельной и определяется важностью той деятельности, для осуществления которой нужен доступ. Последствия незаконного получения доступа к информации определяются не самим фактом незаконного ознакомления с определенной закрытой информацией, а содержанием тех отношений, в пределах которых возникла потребность ограничения доступа. Опасность нарушения функционирования определенной компьютерной сети определяется важностью заданий, для которых она используется, именно последние выступают критерием обоснованности применения соответствующих средств уголовной юстиции.

Таким образом, информационная безопасность понимается как система общественных отношений, обеспечивающих возможность реализации информационной потребности граждан, общества, государства. Реализация информационной потребности осуществляется путем получения доступа к

необходимой информации, базируется на использовании информационных технологий и обеспечивается формированием информационного ресурса.

В наиболее общем понимании лицо следует считать находящимся в состоянии информационной безопасности тогда, когда его потребность в информации обеспечена должным образом. То есть тогда, когда лицо имеет возможность получать достоверную и достаточную для осуществления эффективной деятельности информацию. А общественно опасными следует признавать такие посягательства в сфере информационной безопасности, которые исключают или значительно усложняют реализацию информационной потребности.

Отметим также, что термин «информационная безопасность» достаточно широко применяется в информатике и обозначает, как правило, комплекс мероприятий по обеспечению защиты информации от уничтожения или незаконного доступа; совокупность организационных, программных и технических средств, обеспечивающих целостность, конфиденциальность и доступность данных. Тем не менее, применение его в юридическом контексте для обозначения самостоятельного объекта уголовно-правовой охраны, также представляется обоснованным. Вызвано это достижением соответствующими отношениями социального значения, требующего применения средств уголовной юстиции. Можно утверждать, что современные тенденции информатизации позволяют рассматривать информационную безопасность как в узком смысле (обеспечение защиты информации) так и в широком – обеспечение реализации социальной информационной потребности.

Итак, обеспечение уголовно-правового стимулирования положительных и минимизации негативных социальных последствий информатизации, предполагает определение в качестве самостоятельного объекта уголовно-правовой охраны системы общественных отношений, обеспечивающих реализацию информационной потребности. Для обозначения данной системы предлагается использовать термин

«информационная безопасность», её структуру составляют отношения в сфере формирования информационного ресурса, обеспечения доступа к информации, а также отношения в сфере использования информационных технологий. Социальная значимость отношений информационной безопасности, а следовательно, и целесообразность их уголовно-правовой охраны, определяются значимостью тех отношений, в пределах которых возникает информационная потребность.

Вместе с тем, обеспечение уголовно-правовой охраны каждой из обозначенных групп имеет определённую специфику.

Начнём с отношений в сфере использования информационных технологий. Основная правовая проблема здесь – обеспечение нормативно-правовой базы противодействия так называемым «компьютерным» преступлениям. С учётом высказанных ранее положений, сформулируем следующее положение: критерием отнесения определённых деяний к преступлениям в сфере использования информационных технологий следует считать вред, причиняемый той социально значимой деятельности, для осуществления которой применяется компьютерная техника. Очевидно, что уничтожение информации, обрабатываемой в компьютерной системе, опасно настолько, насколько социально значимой является задача, для решения которой используется определенный компьютер. Тем не менее, законы об уголовной ответственности некоторых государств не учитывают такой специфики. Так, судя по решению, принятому украинским законодателем, утечка, потеря, подделка, блокирование информации, нарушение установленного порядка ее маршрутизации или искажение процесса ее обработки (ст. 361, 362 УК Украины) признаются общественно-опасными сами по себе. Лишь на уровне квалифицирующих признаков мы встречаем зависимость уголовной ответственности от наступления «существенного вреда».

Подобная ситуация приводит к вполне ожидаемым проблемам: из-за отсутствия в законодательных определениях преступлений в сфере

использования информационных технологий четких критериев общественной опасности под уголовно-правовой запрет и, соответственно, в сферу действия уголовной юстиции попадают не только деяния, которые действительно являются общественно опасными, но и не являющиеся таковыми. Это приводит к существенному снижению эффективности уголовно-правового противодействия указанным преступлениям. Данный вывод был доказан в ходе исследования практики применения украинского уголовного законодательства [3]. Проведенное исследование судебных решений, связанных с применением ст.ст. 361–362 КК Украины, позволяет утверждать, что эффективность уголовно-правовых мер противодействия преступлениям в сфере использования информационных технологий является недостаточной. Большинство исследованных приговоров не могут рассматриваться как средство противодействия действительно общественно опасным проявлениям в отмеченной сфере. При этом непоследовательность изученных судебных решений не в последнюю очередь обусловлена недостатками действующего уголовного законодательства, отсутствием в нем четких, понятных критериев общественной опасности посягательств в сфере использования информационных технологий. Необходимо отметить: при криминализации преступлений в сфере использования электронно-вычислительных машин, систем, компьютерных сетей и сетей электросвязи был нарушен принцип общественной опасности. Сущность этого нарушения можно сформулировать следующим образом: из-за отсутствия в законодательных определениях данных преступлений четких критериев общественной опасности под уголовно-правовой запрет и, соответственно, в сферу действия уголовной юстиции попадают не только деяния, которые действительно являются общественно опасными, но и не являющиеся таковыми. Именно это отчасти и приводит к существенному снижению эффективности уголовно-правового противодействияисследуемым преступлениям.

Исправление ситуации в первую очередь предусматривает включение в диспозиции соответствующих уголовно-правовых норм четких положений относительно критериев общественной опасности посягательств. Одним из возможных и наиболее оптимальных решений является обращение к законодательным конструкциям, свойственным преступлениям с производными последствиями. Структура объективной стороны преступлений в сфере использования компьютерной техники должна включать: 1) основные последствия - различные формы нарушения информационных отношений, выступающих непосредственными объектами (уничтожение, блокирование, нарушение целостности информации и т.д.); 2) производные последствия - нарушение отношений в сфере реализации прав и свобод отдельных физических лиц, государственных или общественных интересов, деятельности юридических лиц. Лишь при наличии совокупности таких последствий совершенное посягательство следует считать преступлением в сфере использования информационных технологий.

В самом общем смысле, правовое регулирование отношений обеспечения доступа к информации представляет собой поиск баланса между двумя группами противоположных социальных интересов: с одной стороны - интересов определенных субъектов в ограничении доступа к информации, а с другой - интересов определенных субъектов в получении информации. Поэтому, сущность нарушений информационной безопасности в данной сфере заключается в том, что нарушение реализации информационной потребности обусловлено или нарушением установленного режима доступа к определенному ресурсу, или неправомерным ограничением доступа к определенной информации. Следует отметить, что отношения доступа к информации весьма продолжительный период времени регулировались правом и охранялись уголовным законом, хотя до определенного уровня технологического развития не имели самостоятельного значения. С компьютеризацией общества, появлением Интернета произошел взрывной рост количественных и качественных показателей накопления и

использования информации во всех сферах социальной жизни и жизни отдельных граждан. Современные информационные технологии радикально изменили структуру и формы общения. Сегодня сама форма организации общества, его эффективность прямо зависят от обеспечения достоверности информации, сохранения сформированных потоков данных и скорости их передачи. Если еще сто лет тому назад посягательства на информационные отношения преимущественно не рассматривались как такие, что характеризуются существенной общественной опасностью, то сегодня есть все основания ставить знак равенства между информационной безопасностью и безопасностью общества в целом. Нужно признать, что уголовным законодательством такие изменения остались скорее незамеченными. Нормы об уголовной ответственности за нарушения ограниченного доступа к информации рассредоточены, встречаются в различных законах об уголовной ответственности, хотя очевидно, что интенсивность уголовно-правовой охраны отношений в сфере ограниченного доступа к информации должна определяться не видом информации (государственная тайна, коммерческая, тайна усыновления и т.д.), а содержанием наступивших последствий.

Таким образом, имеющаяся в действующем законодательстве система норм об ответственности за преступления в сфере информационной безопасности должна рассматриваться с позиций ее оптимизации. Очевидно, что в ходе ее совершенствования должен решаться вопрос о целесообразности, обоснованности и пределах замены имеющейся рассредоточенной системы специальных уголовно-правовых запретов такими нормами, которые бы обеспечивали охрану более широких сегментов отношений информационной безопасности. Есть смысл отказаться от чрезмерной детализации уголовно наказуемых видов нарушений ограниченного доступа к информации.

Наконец, об уголовно-правовой охране общественных отношений в сфере формирования информационного ресурса. Следует отметить, что

проблема уголовно-правового обеспечения формирования информационных ресурсов не является новой. Уголовное законодательство подавляющего числа государств содержит нормы об ответственности за: призывы к насильственному свержению конституционного строя; умышленные действия, направленные на разжигание национальной, расовой или религиозной вражды и ненависти, на унижение национальной чести и достоинства, или обиды чувств граждан в связи с их религиозными убеждениями; публичные призывы к совершению террористического акта; призывы к совершению действий, которые угрожают общественному порядку; изготовление или распространение порнографических предметов и т.д.

Однако, в современных условиях – условиях повышения интенсивности массовой коммуникации – соответсвующие угрозы, обусловленные нарушениями в сфере формирования информационного ресурса, гораздо глубже и сложнее. Уже сегодня специалисты отмечают, что средства массовой коммуникации все чаще вводят своего потребителя в состояние, при котором действуют механизмы и неписаные законы личного обогащения, отчужденности, безразличия к обществу, все более развращают его насилием, пропагандой наркотиков, алкоголя, преступности и безнаказанности [5]. Обосновывается, что одним из факторов формирования мотивации противоправного поведения несовершеннолетних является деструктивное влияние СМИ [1]. Современная массовая коммуникация, ориентированная в первую очередь на философию потребления, может привести к духовному и интеллектуальному вырождению общества [4].

При этом обоснованно прогнозировать, что ожидаемое увеличение интенсивности массовой коммуникации существенно обострит данные угрозы, приведет к тому, что их развитие ускорится. Зафиксировав, настолько тревожные социальные тенденции, рассмотрим, какие меры уголовно-правовой охраны могут быть использованы для их предупреждения и минимизации последствий. Наиболее распространенным и, возможно,

исторически первым средством противодействия общественно опасным проявлениям в сфере формирования информационного ресурса является контроль за содержанием сообщений и ограничение доступа к ним. Именно к таким средствам следует относить упомянутые ранее нормы действующего уголовного законодательства. Однако эти уголовно-правовые запреты нельзя рассматривать как целостную систему, они представляют собой законодательную реакцию на наиболее опасные проявления нарушений формирования информационного ресурса, относящиеся к разнообразным сферам социального бытия: национальной безопасности, противодействию расовой неприязни и ксенофобии, общественной безопасности, морали и т. д.

Возможно, установленные общественно опасные последствия современных процессов формирования информационного поля требуют уголовно-правовых запретов более широкого спектра действия? Таких, которые бы обеспечивали противодействие включению любого негативного контента в общественный информационный ресурс, исключали бы возможность манипулирования общественным сознанием [див. 7]?

Ответ на поставленные вопрос является негативным. И дело не только в том, что усиление государственного контроля за деятельностью средств массовой информации путем включения дополнительных уголовно-правовых норм потенциально опасно свертыванием процессов демократизации и, естественно, повлечет нарушения прав человека. Попытка сформулировать подобные новеллы приведет к ожидаемой проблеме: принципиально невозможно сформулировать определение для обозначения тех сведений, включение которых в информационное поле следует считать общественно опасным. Весьма проблематичной будет и попытка четкого (что является обязательным для уголовно-правовой нормы) определения общественно опасных последствий. Такая ситуация с необходимостью приведет к формулировке уголовно-правового запрета на основе оценочных понятий, что, в свою очередь, создаст необоснованный риск злоупотреблений уголовным правом.

Кроме того, распространение глобальных информационных технологий (Интернет, сети спутникового вещания) вообще делает все менее эффективными методы, основывающиеся на ограничении или запрете распространения определенной информации. Например, тотальный мониторинг Интернета, по мнению западных специалистов по вопросам информационной безопасности, не может помочь в борьбе с экстремизмом даже теоретически. Плотность современных информационных потоков настолько велика, что даже для выборочной своевременной проверки отдельных информационных источников понадобится такое количество специалистов, которое в несколько раз превышает экономически обоснованную численность всех правоохранительных органов государства [6].

Стоит согласиться и с тем, что вертикальная регуляторная схема, срабатывающая относительно минимизации угроз, связанных с распространением вредоносного контента в традиционных масс-медиа, не действует в условиях интерактивности и глобальности [2]. Ярким примером здесь может послужить широко известный «эффект Стрейзанд».

Очевидно, что комплекс вопросов, связанных с правовым регулированием процессов формирования информационного ресурса, имеет свое решение преимущественно за пределами уголовно-правового поля. Вместе с тем, следует учитывать, что вывод о потенциальной неэффективности и, как следствие, отсутствии целесообразности расширения средств уголовно-правовой охраны отношений информационной безопасности в сфере формирования информационного ресурса, сделан с учетом современного уровня развития науки и техники. Вместе с тем развитие компьютерных технологий, психологии, социологии и криминологии может обеспечить возможность формулирования четких уголовно-правовых норм. В таком случае, дополнение предложенного УК нормами, обеспечивающими уголовно-правовую охрану отношений в сфере формирования информационного ресурса станет целесообразным.

Таким образом, основные требования к содержанию уголовно-правовой охраны общественных отношений в сфере информатизации заключаются в следующем:

1) объектом уголовно-правовой охраны в данной сфере следует считать информационную безопасность – систему общественных отношений, в пределах которых обеспечивается реализация информационной потребности граждан, общества, государства;

2) указанная система состоит из трёх элементов – отношения в сфере формирования информационного ресурса, отношения в сфере обеспечения доступа к информации, отношения в сфере использования информационных технологий;

3) целесообразность уголовно-правовой охраны информационной безопасности, определяются значимостью тех отношений, в пределах которых возникает информационная потребность;

4) повышение эффективности уголовно-правовой охраны отношений в сфере использования информационных технологий предполагает включение в соответствующие законы четких положений относительно критериев общественной опасности посягательств, обеспечивающих применение средств уголовной юстиции только в тех случаях, когда имеет место обусловленное посягательством в сфере информационных технологий существенное нарушение отношений в сфере реализации прав и свобод отдельных физических лиц, государственных или общественных интересов, деятельности юридических лиц;

5) система норм об уголовной ответственности за преступления в сфере ограниченного доступа к информации требует оптимизации, в ходе ее совершенствования должен решаться вопрос о целесообразности, обоснованности и пределах замены имеющейся рассредоточенной системы специальных уголовно-правовых запретов такими нормами, которые бы обеспечивали охрану более широких сегментов отношений информационной безопасности;

6) несмотря на то, что количественные и качественные показатели информатизации позволяют прогнозировать усиление развития негативных социальных последствий в сфере формирования информационных ресурсов, расширение уголовно-правовых средств в данной сфере, дополнение уголовного законодательства новыми нормами об ответственности за распространение «общественно опасной информации», является нецелесообразным из-за прогнозируемой неэффективности таких норм, непринадлежности решений данных социальных проблем к уголовно-правовому полю.

Література:

1. Бугера О. Засоби масової інформації: проблема вдосконалення діяльності щодо запобігання протиправної поведінки неповнолітніх / О. Бугера // Підприємництво, господарство і право. – 2005. – № 7. – С. 70–73.
2. Зернецкая О. Интернет-ловушка для молодежи [Электронный ресурс] / О. Зернецкая // Зеркало недели. – 2007. – № 11. – Режим доступу: http://zn.ua/articles/49507.
3. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія / М. В. Карчевський – Луганськ, 2011. – 538 с.
4. Кендюхов О. Суспільство споживання як національна трагедія України [Електронний ресурс] / О. Кендюхов // Дзеркало тижня. – 2011. – № 1. – Режим доступу: http:// dt.ua/articles/73290.
5. Коваленко В. В. Сучасна масова комунікація: носій добра чи криміногенний фактор? / В. В. Коваленко // Право України. – 2008. – № 4. – С. 84–89.
6. Паньо Е. Сито со слишком большими дырочками [Электронный ресурс] / Е. Паньо, Т. Паньо // Зеркало недели. – 2006. – № 24. – Режим доступу : http://zn.ua/articles/47040.
7. Савінова Н. А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти : монографія / Н. А. Савінова. – К. 2012. – 340 с.

----------***----------

Г. К. Авдєєва,
к.ю.н., с.н.с., провідний науковий співробітник НДІ вивчення проблем злочинності ім. академіка В.В. Сташиса

РОЛЬ СУДОВОЇ ЕКСПЕРТИЗИ У ЗАБЕЗПЕЧЕННІ ПРИНЦИПУ ОБГРУНТОВАННОСТІ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ПРАВОПОРУШЕННЯ В ІНФОРМАЦІЙНІЙ СФЕРІ

На сьогодні правопорушення в інформаційній сфері є однією з найдинамічніших груп посягань, кількість та суспільна небезпечність яких збільшується щороку. Це зумовлене постійним і стрімким розширенням сфери застосування інформаційних технологій в усіх галузях діяльності людини.

Принцип обґрунтованості юридичної відповідальності є одним з її основних принципів. Сутність його полягає в об'єктивному вивченні справи, зборі та всебічній оцінці доказів, аналізі всіх обставин, що обтяжують та пом'якшують відповідальність [1]. Цей принцип безпосередньо пов'язаний з іншими принципами юридичної відповідальності, а також з її змістом, функціями, підставами, гарантіями та процедурами здійснення. Дотримання принципу обґрунтованості юридичної відповідальності в інформаційній сфері завдяки специфіці об'єкту посягань потребує використання спеціальних знань, що слугує підґрунтям для встановлення конкретних фактів і обставин у справі.

Одним з видів правопорушень в інформаційній сфері є використання зі злочинною метою шкідливих програмних продуктів, завдяки яким здійснюється крадіжка особистих персональних і комерційних даних користувачів, конфіденційної інформації, ключів захисту, використання «комп'ютера-жертви» для здійснення мережевих атак, несанкціонованої розсилки повідомлень і виконання «брехливих» банківських операцій та ін. На сьогодні в усьому світі кількість злочинів з використанням

телекомунікаційних мереж і мережевих технологій складає 30-40 % від загальної кількості злочинів. Кінцевою метою зловмисників часто є заволодіння «великими грошами», протизаконне отримання яких не потребує безпосередньої участі правопорушника.

На сьогодні розроблена значна кількість ефективних сучасних засобів пошуку (відновлення) знищеної електронної інформації. Практика показує, що якнайповніше доказову базу можна сформувати, залучаючи до проведення експертиз кваліфікованих фахівців у галузі інформаційних технологій, які постійно використовують у своїй повсякденній діяльності новітні програмні засоби та які не є працівниками державних спеціалізованих експертних установ. Однак, монопольне право на проведення криміналістичних експертиз (у т. ч. – експертиз відео - і звукозапису, цифрових документів та ін.) у відповідності до ст. 7 Закону України «Про судову експертизу» належить виключно державним спеціалізованим експертним установам. На сьогодні в низці таких державних установ окремі види експертиз не проводяться через відсутність спеціального обладнання і відповідних фахівців. Монопольне право на навчання та атестацію судового експерта, видачу Свідоцтва на право проведення судових експертиз також належить експертно-кваліфікаційними комісіями державних органів, до сфери управління яких належать державні спеціалізовані експертні установи України. Однак, експертно-кваліфікаційні комісії МЮ України не мають можливості атестувати експертів і видавати їм Свідоцтва на право проведення комп'ютерно-технічної і телекомунікаційної експертиз через відсутність в їх складі відповідних фахівців.

Методики судово-експертного дослідження комп'ютерної техніки, програмних продуктів і телекомунікаційних мереж вимагають постійного оновлення та доопрацювання у зв'язку з тим, що через кожні 2-3 роки змінюються формати представлення даних, операційні та файлові системи, протоколи і середовище перенесення даних, технічні засоби, що

забезпечують процес передання інформації. Удосконалення таких методик можливо лише при використанні праці вчених і кваліфікованих фахівців в інформаційній сфері, які не є працівниками державних експертних установ. Тобто, в багатьох випадках правоохоронні органи України марно сподіваються на отримання результатів повного, всебічного експертного дослідження об'єктів телекомунікаційної та комп'ютерно-технічної експертиз [2, с. 102].

До принципів юридичної відповідальності можна також віднести загальні принципи правосуддя: змагальність процесу як засіб досягнення об'єктивної істини; право на захист особи, що притягується до відповідальності, тощо[1].

У кримінальному судочинстві згідно зі ст. 243 КПК України «Сторона захисту має право самостійно залучати експертів на договірних умовах для проведення експертизи». На перший погляд, є всі умови для реалізації принципу процесуальної змагальності і рівності у збиранні та наданні доказів, в даному випадку – шляхом залучення експерта. Однак, на сьогодні завдяки закріпленій в законодавстві України монополії державних судово-експертних установ на проведення більшості видів судових експертиз та підготовку судових експертів, право сторони захисту на проведення альтернативної судової експертизи незалежним судовим експертом реалізувати повною мірою неможливо.

Монопольне право на проведення криміналістичних експертиз та підготовку судових експертів державними судово-експертними установами завдяки відсутності в атестаційних комісіях відповідних фахівців унеможливлює отримання досвідченим фахівцям в інформаційній сфері Свідоцтва на право самостійного проведення судових експертиз (згідно зі ст. 102 КПК України у Висновку повинен міститися номер такого Свідоцтва) та обмежує можливості слідчого і суду на отримання обґрунтованого

експертного висновку щодо дослідження доказової інформації, пов'язаної з правопорушеннями в інформаційній сфері.

Об'єктивність вивчення справи, збір та всебічна оцінка доказів, якість аналізу всіх обставин, що обтяжують та пом'якшують юридичну відповідальність в інформаційній сфері безпосередньо залежить від якості проведення комп'ютерно-технічних та телекомунікаційних судових експертиз. Скасування монополії державних судово-експертних установ на проведення криміналістичних експертиз і підготовку експертних кадрів, законодавче забезпечення розвитку інституту недержавної судової експертизи в Україні дозволить підвищити рівень підготовки судових експертів в інформаційній сфері та об'єктивність висновків судових експертів. Це слугуватиме основою для забезпечення принципу змагальності у кримінальному процесі (зокрема, права сторони захисту на самостійне залучення незалежного експерта) та принципу обґрунтованості юридичної відповідальності за правопорушення в інформаційній сфері.

Література:

1. Навчальний посібник для студентів вищих навчальних закладів / А. П. Гель, Г. С. Семаков, С. П. Кондракова. – К.: МАУП, 2004. – 272 с.
2. Авдеева Г.К. Проблемы назначения судебной экспертизы в уголовном процессе Украины // Криміналістика та судова експертиза : наука, навчання, практика : зб. на-ук. пр. у 2-х т.т. – Х.: Видавнича агенція «Апостіль», 2014. – Т. 2. – 400 с. – С. 94-102.

----------***----------

Є. Д. Лук'янчиков,
д.ю.н., професор кафедри
інформаційного права та права
інтелектуальної власності
НТУУ «КПІ»

ЗАСОБИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Розслідування злочинів можна уявити як складний інформаційно-пізнавальний процес об'єктивної дійсності. Інформацію, якою оперують у

цьому процесі поділяють на процесуальну та непроцесуальну. До процесуальної відносять інформацію, що зібрана засобами та у порядку передбаченому кримінальним процесуальним законом.

Процесуальній інформації в ході розслідування надається провідна роль. Вона складає сутність, зміст судових доказів, але не вичерпується ними. Тому незрозумілим стає твердження Д. І. Бєднякова, який процесуальну інформацію ототожнює доказовій і, таким чином, обмежує її границі. Він пише: «інформація про злочин може бути або процесуальною (доказовою), або непроцесуальною» [1, с. 66-67].

Появі терміна «доказова інформація» криміналістика зобов'язана Р. С. Бєлкіну та А. І. Вінбергу, які запропонували його, досліджуючи поняття інформації з погляду теорії доказів [2, с. 173, 176]. Це поняття увійшло в теорію і практику, підтримано вітчизняними криміналістами, не викликає сумнівів при застосуванні, незважаючи на відсутність одностайності у його формуванні і визначенні змісту.

Зауважуючи Д. І. Бєднякову, Р. С. Бєлкін вважає, що доказовою є лише та інформація, що складає зміст доказів, виступає засобом і служить меті доказування [3, с. 401]. Тобто мова іде ні про що інше як про судові докази.

З зазначеним твердженням можна було б погодитись, але виникають певні сумніви щодо необхідності та доцільності його запровадження в науковий обіг саме в такому розумінні. Природнім постає запитання, чим викликана потреба вводити в обіг термін, який нічого нового не додає, а не користуватися передбаченим законом, що витримав перевірку часу і практики – докази. Адже інформація, відомості саме і утворюють зміст доказів. Прикладом виваженого і витонченого застосування термінів, що ми розглядаємо може бути стаття В. К. Лисиченка, присвячена концептуальним напрямам розвитку кримінально-процесуального законодавства [4, с. 98-104].

Інший підхід до визначення даного поняття і його змісту спостерігаємо у В. Я. Колдіна та М. С. Польового. Вони називають доказовою «будь яку

інформацію про подію, що розслідують та пов‘язані із нею обставини, яка використовується в процесі доказування з метою виявлення, збирання та оцінки доказів в процесі розкриття, розслідування та судового розгляду кримінальних справ» [5, с. 39-40].

Подібна інтерпретація вважається занадто широкою. Для виявлення, збирання і оцінки доказів може використовуватись інформація, яка міститься як у процесуальних, так і в непроцесуальних джерелах. Нею може бути інформація, яку отримано застосуванням оперативно-розшукових заходів. У такому разі не має підстав називати інформацію доказовою, якщо вона міститься не тільки в доказах? З аналізу наведеного поняття можна дійти висновку, що доказовою називають інформацію тому, що вона вказує на місця знаходження джерел нової інформації, сприяє визначенню засобів її збирання та вибору, відповідних ситуації, тактичних прийомів їх застосування. Таким чином, доказовою інформація є не тому, що міститься в судових доказах, хоча це і не виключається, а тому, що має доказовий характер. Вона своїм змістом підтверджує або спростовує ті чи інші обставини, які мають значення для встановлення істини.

В процесі розслідування слідчому доводиться оперувати не лише доказовою інформацією. Нерідко інформація, яка є в наявності у слідчого своїм змістом і характером нічого не доводить і не спростовує, але в сукупності з іншими відомостями сприяє визначенню напрямів розслідування, послідовності і тактики проведення слідчих (розшукових) дій. Тобто така інформація має орієнтуючий характер, який обумовлюється саме її змістом, а не тільки засобами отримання (збирання), як вважають інколи [2, с. 182; 6, с 37]. Орієнтуючий характер може мати інформація, яка міститься як в судових доказах, так і в матеріалах оперативно-розшукової діяльності. Наприклад, інформація про близькі зв’язки підозрюваного з деякими особами може міститися як в доказах, так і в матеріалах оперативно-розшукової діяльності. В обох випадках вона засвідчує існування близьких стосунків між такими людьми і її можна називати

доказовою відносно конкретного факту. Але ця інформація може бути використана для прийняття рішення про проведення у близьких підозрюваного обшуку, з метою відшукання і вилучення предметів, які мають значення для розслідування і можуть у них переховуватись. Тобто, відносно даних обставин інформація набуває орієнтуючого характеру, вона вказує лише на можливість знаходження у осіб, з якими підтримував зв'язки підозрюваний об'єктів, що цікавлять слідство.

Таким чином, говорити про доказовий або орієнтуючий характер тієї чи іншої інформації абстрактно, безвідносно до факту, який нею встановлюється буде не зовсім вірним. Завжди треба уточнювати, відносно яких обставин у розслідуванні інформація має доказовий або орієнтуючий характер.

Погодившись з розглянутим підходом до розв'язання зазначеного питання, можна дійти висновку, що застосування в теорії і на практиці термінів «докази» і «доказова інформація» як рівнозначних не відповідає їхній об'єктивній природі, характеру та змісту.

Потребує також уточнення думка, що докази можуть бути отримані лише провадженням слідчих (розшукових) дій [3, с. 401]. За такого підходу обмежуються процесуальні засоби отримання доказів у досудовому провадженні. Тому слід підтримати авторів, які зазначають, що доказами у кримінальному процесі є переважно ті фактичні дані (відомості про факти, інформація), що отримані самими слідчими органами, прокурором, суддею і судом внаслідок їх *процесуальної* діяльності, але цим не обмежуються (виділено нами). Як докази, зазначають вони, можуть бути також використані фактичні дані, одержані і зафіксовані із застосуванням технічних засобів оперативними підрозділами органів відповідних міністерств і відомств при здійсненні ними оперативно-розшукової діяльності (п. 2 ст. 10 Закону про оперативно-розшукову діяльність, ч. 3 ст. 15 Закону про організаційно-правові основи боротьби з організованою злочинністю), а також відомості про факти, отримані адвокатом при

здійсненні ним своєї професійної діяльності (ст. 20 Закону України Про адвокатуру та адвокатську діяльність) [7, с. 113].

Звичайно, процесуальна діяльність значно ширша ніж провадження слідчих (розшукових) дій. Вона є основою пізнавальної діяльності з розслідування злочинів, відбувається у певному соціальному середовищі, здійснюється уповноваженими суб‘єктами в межах і засобами, визначеними кримінальним процесуальним законодавством (гласні та негласні слідчі (розшукові) дії). В науковій літературі виділяються наступні групи процесуальних засобів інформаційного забезпечення розслідування:

- що визначають рух провадження і процесуальний стан її учасників (внесення відомостей про комп‘ютерний злочин до Єдиного реєстру досудових розслідувань (ЄРДР), повідомлення про підозру, роз’яснення прав учасникам тощо);

- що забезпечують можливість одержання доказової інформації та явку учасників провадження (застосування запобіжних заходів, арешт кореспонденції, організація охорони місця події та ін.);

- що реалізують процесуальні права учасників провадження (фіксація і вирішення клопотань, пред’явлення матеріалів провадження для ознайомлення та ін.);

- що направлені на збирання і перевірку доказів;

- що полягають у використанні доказів для формулювання і обґрунтування висновків про результати провадження (складання обвинувального акту) [8, с. 371].

В цілому погоджуючись з таким розподілом процесуальних дій на групи слід зазначити, що дії з організації охорони місця події до процесуальних не відносяться. Порядок їх проведення не передбачено кримінальним процесуальним законом. Вони можуть бути віднесені до забезпечуючих заходів організаційного характеру, які здійснюються не у процесуальній формі.

Прийняттям нового КПК України засоби інформаційного забезпечення розслідування суттєво розширено, що відповідає сучасним потребам слідчої практики. До КПК України включено інститут негласних слідчих (розшукових) дій, які можуть застосовуватися під час розслідування тяжких та особливо тяжких злочинів.

В структурі процесуальних засобів інформаційного забезпечення розслідування, окрім слідчих (розшукових) та інших процесуальних дій правомірно виділити специфічну групу засобів організаційного характеру. За своєю природою вони охоплюються положеннями процесуального закону, а тому, на відміну від інших організаційних заходів, мають бути визнані процесуальними (виклик слідчим, прокурором, судовий виклик, тимчасовий доступ до речей і документів, тимчасове вилучення майна, залучення осіб, які мають брати участь у слідчій (розшуковій) дії, отримання зразків для порівняльного дослідження, ексгумація).

За загальним правилом слідчий під час досудового розслідування має право викликати особу, якщо є достатні підстави вважати, що вона може дати показання, які мають значення для кримінального провадження (ч. 2 ст. 133 КПК). Таким чином, фактичною підставою для прийняття рішення про виклик на допит є наявність у слідчого інформації достатньої для припущення, що особа володіє будь-якими даними про обставини, що підлягають доказуванню або мають орієнтуючий характер. Чинний КПК не визначає рівень імовірності та джерела, з яких можуть бути отримані такі дані. Опитані слідчі і працівники оперативних підрозділів вказали, що відомості про обізнаних осіб можуть міститися в різних джерелах, зокрема: матеріалах провадження (заявах, протоколах допиту та інших слідчих дій, тощо), отримані в процесі застосування оперативно-розшукових заходів тощо.

Разом з тим, в ряді кримінальних проваджень з аналізу наявних документів інколи неможливо зробити висновок, яким чином стало відомо, що певна особа володіє даними про обставини злочину. Пояснюється це тим,

що відомості про джерело інформації можуть бути отримані в процесі застосування оперативно-розшукових заходів. Таким чином, з наведеного можна дійти висновку, що рішення про виклик особи на допит може бути прийняте як на підставі процесуальної інформації, що міститься в матеріалах провадження, так і на підставі даних, що отримані в процесі застосування оперативно-розшукових заходів. Такі дані можуть мати як вірогідний так і імовірний характер. Вірно з цього приводу зазначається, що підставами для проведення допиту є наявність достатніх відомостей про те, що певній особі відомі обставини, які мають значення для кримінального провадження [9, с. 373]. Виходячи із цього припустимо зробити висновок, що виклик особи для допиту як свідка, коли відсутня інформація про її обізнаність про обставини правопорушення є недоцільним, тягне невиправдану витрату часу слідчого та накопичення протоколів допитів, які не містять інформацію про злочин.

В тактичному плані важливо правильно визначити спосіб виклику на допит. Порядок виклику особи в кримінальному провадженні визначено в ст. 135 КПК України. Це може бути зроблено шляхом вручення повістки про виклик, надіслання її поштою, електронною поштою чи факсимільним зв‘язком, викликом по телефону або телеграмою. Змістом такої діяльності вбачають тактичні прийоми організаційного характеру і включають до підготовчого етапу даної слідчої дії. Такого висновку доходить Н. Ш. Сафін під час аналізу комплексу питань пов’язаних з організацією і тактикою допиту неповнолітнього підозрюваного [10, с. 108]. Дану думку поділяють і автори фундаментального підручника з криміналістики, але питанню, що розглядаємо, на жаль, приділяють недостатньо уваги. Йому присвячено лише один абзац із семи рядків. Автори зазначають засоби виклику та коло осіб, до яких він може застосовуватися. Відмічається, що слідчий обирає той засіб, який у даній ситуації оптимально сприяє встановленню психологічного контакту з допитуваним, збереженню в таємниці від інших самого факту виклику на допит, проведенню допита у визначений час і в

потрібному місці [11, с. 604]. На цьому рекомендації щодо визначення способу виклику на допит і порядку його реалізації вичерпуються.

Слід зазначити, що розробники нового КПК України приділили значну увагу врегулюванню порядку виклику учасника кримінального провадження до слідчого, прокурора або суду, чому присвячено глава 11 його другого розділу. В ст. 135 КПК докладно викладається порядок виклику в кримінальне провадження, розкривається зміст повістки про виклик (ст. 137). Поважні причини неприбуття особи на виклик (ст. 138) та наслідки неприбуття на виклик (ст. 139). Ці норми створюють додаткові процесуальні гарантії, що забезпечують особу від свавілля та неправомірних дій з боку правоохоронних органів.

Література:

1. Бедняков Д. И. Непроцессуальная информация и расследование преступлений / Бедняков Д. И. – М. : Юридическая литература, 1991. – 208с.
2. Белкин Р. С. Криминалистика и доказывание / Р. С. Белкин, А. И. Винберг. – М. : Юрид. лит., 1969. – 170 с.
3. Белкин Р. С. Курс криминалистики. В 3-х т. Т.3 : Криминалистические средства, приемы и рекомендации / Р. С. Бедкин. – М : Юристъ, 1997. – 480с.
4. Лисиченко В. К. Концептуальні напрямки й етапи розвитку кримінально-процесуального законодавства // Вісник Української академії внутрішніх справ. 1997. № 1. – С. 98-104.
5. Колдин В. Я. Информационные процессы и структуры в криминалистике / В. Я. Колдин, Н. С. Полевой. – М. : Изд-во МГУ, 1985. – 133 с.
6. Хлынцов М.Н. Криминалистическая информация и моделирование при расследовании преступлений. – Саратов: Изд-во Сарат. ун-та, 1982. – 159 с.
7. Михеєнко М. М. Науково-практичний коментар кримінально-процесуального кодексу України / М. М. Михеєнко, В. П. Шибіко, А. Я. Дубинський / Відп. редактори В. Ф. Бойко, В. Г. Гончаренко. – Київ : Юрінком Інтер, 1997. – 624 с.
8. Теория доказательств в советском уголовном процессе. Отв. ред. Н. В. Жогин, изд. 2-е испр. и доп. – М. : Юрид. лит., 1973. – 736 с.
9. Кримінальний процес : підручник / Ю. М. Грошевий, В. Я. Тацій, А. Р. Туманянц та ін.. ; за ред. В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. – Х. : Право, 2013. – 824 с.

10. Сафин Н. Ш. Допрос несовершеннолетнего подозреваемого в советском уголовном судопроизводстве / Н. Ш. Сафин. – Казань : Изд-во Каз. ун-та, 1990. – 160 с.
11. Криминалистика : учебник для вузов / Т. В. Аверьянова, Р. С. Белкин, Ю. Г. Корухов, Е. Р. Россинская. - М. : НОРМА-ИНФРА, 1999. – 971 с.

----------***----------

В. А.Мисливий,
д.ю.н., професор кафедри публічного права ФСП НТУУ «КПІ»

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬЗА ЗЛОЧИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Важливою тенденцією розвитку глобалізованого суспільства є актуалізація феномену його убезпечення, що обумовлюють трансформаційні процеси, які відбуваються в Україні. Визначаючи шляхи розвитку цивілізації, В. І. Вернадський відзначав, що перед людиною відкривається величезне майбутнє, якщо вона не буде використовувати свій розум і свою працю на самознищення. Проте, сьогодні світовій спільноті бракує дотримання цього застереження вченого, який прогнозував «ноосферу» як певну глобальну модель, цивілізаційну концепцію майбутнього.

Однією з проблем сучасного цивілізаційного етапу стала інформаційна безпека як віддзеркалення«інформаційного суспільства», а відтак суспільних відносин, що характеризуються створенням, збиранням, одержанням, зберіганням, використанням та іншими формами обігу інформації, які вимагають правового регулювання та охорони. Закон України «Про основи національної безпеки України» від 19 червня 2003 року визначає сферу інформаційної безпеки та захисту інформації складовими національної безпеки, захищеність яких забезпечує сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізацію реальних та потенційних загроз національним інтересам, життєво важливим інтересам людини, суспільства та держави.

Особливе місце в убезпеченні інформаційної безпеки належить кримінальному законодавству України, зокрема чинному Кримінальному кодексу України 2001 року (далі – КК України). Адже, якщо до кінця XX століття криміналізація суспільно небезпечних діянь відбувалася переважно за рахунок зростання проявів протиправної поведінки у сфері взаємодії людини і техніки, то сьогодні йдеться про збільшення деліктів на більш високому рівні – взаємодії людини і технологій.

Передумовою обґрунтованого процесу розширення кримінально-правової матерії в умовах науково-технологічного прогресу є своєчасне визначення суспільної небезпечності відповідних негативних соціальних явищ, диференціація кримінальної відповідальності, визначення її обсягу та меж, що дозволяє законодавцю формувати обґрунтовану систему окремих видів і складів злочинів, визначити їх об'єктивні та суб'єктивні ознаки, а також встановити оптимальні санкції за їх вчинення.

Разом з цим, на наш погляд, вітчизняному законодавцю поки що бракує реагування на існуючі виклики сьогодення при врахуваннівсіх найбільш важливих об'єктів кримінально-правової охорони. При цьому є дещо передчасними твердження окремих криміналістів, які вважають, що сьогодні у сферу злочинних посягань зараховані всі скільки-небудь значущі загрози для людини, суспільства і держави. Так, навряд чи можна стверджувати про досконалу і завершену модель кримінально-правової охорони найбільш важливих об'єктів, адже ст. 1 КК України серед його завдань щодо «правового забезпечення охорони прав і свобод людини і громадянина, власності, громадського порядку та громадської безпеки, довкілля, конституційного устрою України» та інших об'єктів не передбачає *інформаційної безпеки* (курсив наш – *В. М.)*, що не узгоджується зі ст. 17 Конституції України, яка, зокрема, проголошує забезпечення інформаційної безпеки однією з найважливіших функцій держави, справою всього Українського народу.

Взагалі в структурі Особливої частини КК України поки що не знайшов оптимального відображення родовий об'єкт системи однорідних кримінально-правових норм у цій сфері, зокрема таких, що пов'язані з інформаційними технологіями та телекомунікаціями. Очевидно, що процес формуваннязахисту від суспільно небезпечних проявів у сфері інформаційної безпеки має базуватись на подальшому розвитку кримінально-правової теорії, вдосконаленні законотворчого процесу з урахуваннямвідповідних емпіричних досліджень на підґрунті інтеграції технічних та гуманітарних галузей знань.

Аналіз сучасного стану кримінального законодавства показує, що криміналізація суспільно небезпечних діянь у сфері інформаційної безпеки відбувається переважно шляхом: а) формування в структурі Особливої частини КК України самостійних груп злочинів (розділів), які посягають на однорідні за об'єктом суспільні відносини, цінності та блага; б) конструювання окремих складів злочинів, які розміщуються в інших розділах Особливої частини КК. Так, чинний КК України передбачає окремий Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», родовий об'єкт якогоохоплює своїм змістом незначну кількість кримінально-правових норм, пов'язаних із вчиненням діянь у сфері інформаційної безпеки.

При цьому наявні у розділі статті 361, 361^{1},361^{2}, 362, 363, 363^{1}КК України не лише не створюють оптимальної системи охорони інформаційної інфраструктури, особливостей порядку доступу до інформації в цій системі, а також незаконного впливу на телекомунікації, але й обумовлюють ситуації суперечливої конкуренції між ними, зокрема між складами злочинів, передбачених статтями 361 та 362 КК України, особливо коли зазначені діяння вчинюються у співучасті загальними та спеціальними суб'єктами.

Не витримує критики, на наш погляд, ускладнене формулювання назви цього розділу КК України, яке, до речі, не дає точного уявлення стосовно

родового об’єкта цих злочинів, а також вдаються зайве перевантаженими назви кримінально-правових норм.

У всякому разі, на наш погляд, цілком беззастережним та відповідним Конституції України було б погодитись з думкою вчених, які пропонують сформулювати назву відповідного розділу КК України як «Злочини проти інформаційної безпеки та інформаційних технологій». У зв’язку з цим вимагає більш точного системного визначення структура найбільш важливих інформаційних суспільних відносин, які є підґрунтям для найбільш оптимального формування напрямів кримінально-правової охорони у сфері інформаційної безпеки.

Отже, з огляду на сучасний стан інформаційних відносин, вимагає уточнення методологічний підхід до побудови більш обґрунтованої системи кримінально-правових норм, зміст яких має орієнтуватись на охорону таких об’єктів: інформаційний ресурс як матеріальний субстрат інформаційних відносин; функціонування інформаційного ресурсу, його особливості та порядок доступу до нього; телекомунікації та інформаційні технології; процеси конвергенції, інтеграції та гармонізації інформаційних відносин, обумовлених науково-технологічним прогресом.

Іншими словами, для побудови в структурі Особливої частини КК України більш досконалої системи норм, які б забезпечували більш ефективну кримінально-правову охорону суспільних відносин у сфері інформаційної безпеки та інформаційних технологій, вченим цієї галузі разом з представниками юридичної науки необхідно розробити сучасну модель, досконалу парадигму системи інформаційних суспільних відносин та інформаційних технологій, визначити її структуру та основні елементи. Наявність такої моделі дозволить з’ясувати найбільш оптимальні підходи щодо більш цілеспрямованих наукових досліджень потреб криміналізації суспільно небезпечних діянь та формування їх системи у кримінальному законодавстві України.

----------***----------

М. М. Антонова,
інженер І категорії відділу оцінки та оподаткування КП «Київський інститут земельних відносин» Київської міської Ради (Київської міської державної адміністрації)
В. П. Колонюк,
к.ю.н., доцент, вчений секретар КНДІСЕ МЮ України

ІНФОРМАЦІЙНІ ДАНІ ЗЕМЕЛЬНОГО КАДАСТРУЯК ОБ'ЄКТ ДОСЛІДЖЕННЯ СУДОВОЮ ЕКСПЕРТИЗОЮ

Проблема забезпечення права людини на інформацію в Україні, особливо в контексті неприпустимості інформаційної ізольованості, спотворення життєвого інформаційного простору, сьогодні стала визначальним чинником не тільки інформаційної, а й загальної безпеки на індивідуальному, регіональному і глобальному рівнях.

Законодавство України про інформацію утворюють: Конституція України; Закон України «Про інформацію»; Закон України «Про доступ до публічної інформації», законодавчі акти про окремі галузі, види, форми і засоби інформації; міжнародні договори та угоди, ратифіковані Україною.Системоутворюючим інформаційного законодавства є Закон України «Про інформацію» [1]. Цей Закон закріплює конституційні засади щодо права громадян України на інформацію, закладає правові основи інформаційної діяльності, визначає правові форми міжнародного співробітництва в галузі інформації.

Інформаційне право в юридичній науці є міжгалузевою комплексною дисципліною, об'єкт дослідження якої — це суспільні відносини, предметом яких є інформація. Міжгалузевий зв'язок інформаційного права визначається за юридичною доктриною поділу права на галузі права як міжгалузевий комплексний інститут (субінститут) між конституційним, адміністративним, цивільним, трудовим та кримінальним правом.

Однією з гарантій дотримання права на інформацію є встановлення відповідальності за порушення законодавства про інформацію. Зокрема, відповідно до ст.7 Закону України «Про інформацію» суб'єкт інформаційних відносин може вимагати усунення будь-яких порушень його права на інформацію. Відповідно до ст.3 Закону України «Про доступ до публічної інформації» право на доступ до публічної інформації, серед іншого, гарантується встановленням юридичної відповідальності за порушення законодавства про доступ до публічної інформації [2]. Відповідно до ч.1 ст.27 Закону України «Про інформацію» порушення законодавства України про інформацію тягне за собою наступну юридичну відповідальність - дисциплінарну, цивільну, адміністративну або кримінальну згідно із законами України.

Юридична відповідальність – це одна з гострих тем сьогодення. Як зазначається у філософській літературі, відповідальність – це категорія етики і права, що відображає особливе соціальне та морально-правове ставлення особи до суспільства, яке характеризується виконанням свого морального обов’язку та правових норм тобто являється одним із проявів зв’язку і взаємної залежності особи та суспільства.

Багато вітчизняних дослідників вивчали питання правопорушень та відповідальність за скоєне. Для глибокого проникнення в сутність юридичної відповідальності необхідно з’ясувати її мету та призначення в суспільстві. На думку дослідника А.С. Шабурова мета юридичної відповідальності визначає її функції до яких він відносить: (штрафну) каральну функцію, як головну, оскільки вона виступає як реакція суспільства в особі держави на шкоду, заподіяну правопорушником; превентивну, як засіб попередження нових правопорушень; виховну, як виховання правопорушника; право відбудовну (компенсаційну) та організуючу (регулятивну) [3].

В останніх дослідженнях українських вчених вбачається аргументоване твердження про те, що право це не лише засіб, який попереджує порушення правових норма, а й засіб, який стимулює поведінку особистості.

Тобто, юридична відповідальність – це насамперед обов'язок діяти правомірно. На думку О.Г. Рувіна, відповідальність – це категорія, яка належить і праву, і етиці й відображає особливе морально-правове ставлення особистості до суспільства [4]. Як стверджував М.С.Строгович, юридична відповідальність є насамперед відповідальним ставленням людини до своїх обов'язків, відповідальністю за правильне виконання особою (фізичною та юридичною – громадянином і посадовою особою, громадською організацією й державним органом) покладених на неї Законом обов'язків [5]. Це так звана «позитивна відповідальність». М.О. Краснов, наприклад, розглядає юридичну відповідальність як цілісне явище, яке має два аспекти свого буття: по-перше, це обов'язок діяти правомірно та мати відповідну поведінку суб'єкта права (позитивний аспект); по-друге, це настання несприятливих наслідків у разі скоєння правопорушень (негативний аспект) [6].

До речі, для права зарубіжних країн не властива так звана «позитивна відповідальність», а навпаки, негативна юридична відповідальність – це відповідна реакція суспільства та держави на здійснення особою винного протиправного діяння в формі застосування до неї заходів державного примусу, серед яких: особистого (позбавлення волі); майнового (штраф); організаційного (звільнення).

Разом з тим, щоб юридична відповідальність не перетворилася виключно у карательну функцію, юридична наука і практика виробили ряд принципів, дотримуючись яких держава, діє в рамках законності і не переходить тієї межі, за якою реакція на правопорушення з'являється новим правопорушенням.

На думку Р.Л. Хачатурова та Д.А. Липинського, формою реалізації позитивного аспекту відповідальності є добровільна правомірна поведінка, негативного – державно-примусова форма реалізації як реакція на неправомірну поведінку (правопорушення) [7]. З урахуванням зазначених вище думок автори вважають за необхідне зосередити увагу на ретроспективній юридичній відповідальності за правопорушення в

інформаційній сфері. Підставою виникнення юридичної відповідальності є вчинене суб'єктом (учасником) інформаційних правовідносин правопорушення в інформаційній сфері.

Розвинені держави світу поставили собі за мету прискорений перехід до нового етапу розвитку – інформаційного суспільства, шляхом створення ефективної системи забезпечення прав людини на вільне отримання, поширення й використання інформації як найважливішої умови демократичного розвитку. Практика застосування інформаційного законодавства свідчить про порушення інформаційних прав та створення перешкод у забезпеченні інформаційної безпеки особи, суспільства й держави. Розроблені численні закони та підзаконні акти, які регулюють інформаційні відносини. Однак, їх практичне застосування досить слабке, оскільки відсутні конкретні механізми дотримання законодавства на практиці.

Наприклад, використання особою наданих їй службових повноважень та пов'язаних із цим можливостей в інформаційній сфері, що полягають безпосередньо в умисному ненаданні інформації, спотворенні інформації, наданні інформації неналежної якості, незаконному використанні інформації, яка відома особі у зв'язку з виконанням службових повноважень з метою одержанням неправомірної вигоди або прийняття обіцянки (пропозиції) такої вигоди для себе чи інших осіб або відповідно обіцянка (пропозиція) чи надання неправомірної вигоди особі, яка повноважена на виконання функції держави або місцевого самоврядування, або на її вимогу іншим фізичним чи юридичним особам з метою схилити цю особу до протиправного використання наданих їй службових повноважень та пов'язаних із цим можливостей вже характеризується проявами правопорушень у бік корупційних в інформаційній сфері. Так об'єктомпосягання даного правопорушення на відміну від інших завжди буде інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Нажаль, сучасні дослідження свідчать, що значна частина громадян України не оцінює корупцію, як прояв правопорушень, негативно і вважає за можливе вирішення особистих питань за допомогою дачі хабарів, використання службових можливостей родичів, друзів, які приміром перебувають на державній службі. На думку авторів, найвпливовішою є інформаційна нерівність, яка з одного боку є обґрунтовано-доцільною та логічною (наприклад, існування персональних інформаційних баз в державних органах, які доступні виключно працівникам цих структур, діяльність яких безпосередньо пов'язана з їх обробкою), а з іншого це надає змогу використання цієї інформації у власних цілях. Одним із таких використань являється використання службовою (посадовою) особою базу даних службової державної інформації на особистих підприємствах (фірмах). До таких осіб може застосовуватися як адміністративна, цивільна, так і кримінальна відповідальність.

З огляду на те, що доступ до інформації є складовою суб'єктивного права особи на інформацію й інститутом інформаційного (об'єктивного) права, обмеження цього права, може перетворитись на його порушення, якщо законодавством детально не передбачається механізм контролю і гарантії відновлення обмежених прав.

Не минули правопорушення в інформаційній сфері і таку вагому галузь в нашій державі як земельна. За даними Генеральної прокуратури України найбільш корумпована земельна галузь, конкурувати з якою може лише бюджетна. Так, лише за І квартал 2016 року найбільша кількість правопорушень в земельній галузі пов'язані із допущеним реальним конфліктом інтересів при вирішенні питань, пов'язаних з виділенням земельних ділянок собі та близьким родичам. А це тягне за собою і порушення у технічних документаціях із землеустрою, які являються обов'язковими для виготовлення, погодження та затвердження. Так, статтею 31 Закону України «Про землеустрій» визначено порядок внесення змін до документації із землеустрою, що вносяться особою, яка відповідно до вимог

цього закону може бути розробником документації із землеустрою, знов таки за рішенням органів виконавчої влади, органів місцевого самоврядування або власників землі та землекористувачів [8]. Недостатній контроль з боку керівників управління Держкомзему у містах та селищах й відповідальних керівників структурних підрозділів цих управлінь серед інших і в частині правильності складання витягів із технічної документації про нормативну грошову оцінку земельної ділянки. Як відомо, нормативна грошова оцінка земель використовується для визначення розміру земельного податку, державного мита при міні, спадкуванні та даруванні земельних ділянок згідно із законом, орендної плати за земельні ділянки державної та комунальної власності, втрат сільськогосподарського та лісогосподарського виробництва, а також під час розроблення показників та механізмів економічного стимулювання раціонального використання та охорони земель.

Головним регулятором у питанні попередження та виявлення правопорушень в земельній галузі являється державний нагляд (контроль) за додержанням земельного законодавства України та охорони земель. Державний контроль – вид діяльності держави, що полягає у здійсненні нею відповідними засобами та способами специфічного контрольно-владного впливу держави на стан суспільних відносин. Він характеризується рядом ознак: здійснюється уповноваженими органами влади; одержує своє закріплення в нормах, що визначають функції і правомочність контролюючих суб’єктів; держава наділяє контролюючих суб’єктів повноваженнями у здійсненні конкретних дій; закріплює повноваження контролюючих суб’єктів у відповідних нормативно-правових актах. Загальними компонентами державного контролю за використанням земель є: 1) перевірка фактичного використання, тобто встановлення факту використання чи невикористання землі; 2) перевірка використання землі відповідно до цільового призначення, для якого вона надана; 3) перевірка відповідності площі використовуваної ділянки її розмірам, визначеним у документах, що посвідчують право власності чи право користування землею.

Окремо відмітимо, що ґрунти земельних ділянок також є об’єктом особливої охорони.

Одним із засобів здійснення контролю у сфері земельних відносин в Україні є державний земельний кадастр, котрий є єдиною державною геоінформаційною системою відомостей про землі, розташовані в межах кордонів України, їх цільове призначення, обмеження у їх використанні, а також дані про кількісну і якісну характеристику земель, їх оцінку, про розподіл земель між власниками і користувачами. Значна увага в ході наукових дискусій стосовно створення кадастрово-реєстраційної системи приділялася видатними дослідниками В.С.Кісловим, Р.Ю.Козловим, В.Н.Сидоренко, М.Г.Ступенем, А.М.Третяком та іншими. Призначенням державного земельного кадастру є забезпечення необхідною інформацією органів державної влади та органів місцевого самоврядування, заінтересованих підприємств, установ і організацій, а також громадян з метою регулювання земельних відносин, контролю за використанням і охороною земель тощо. Однак, існує суттєва проблема щодо єдиної державної геоінформаційної системи відомостей про землі, що стає підґрунтям для скоєння правопорушень в даній інформаційній сфері. Земельний кадастр забезпечує: збирання інформації та її оброблення; аналіз; моделювання; постачання геопросторових даних; відображення чергового стану використання та охорони земель комунальної власності територіальної громади та інших земель; правову та орендну інформацію; дані з нормативної грошової оцінки земель держави; рішення Кабінету Міністрів України про затвердження програми використання та охорони земель, розвитку земель міських та селищних рад; матеріали інвентаризації земель, проведених на виконання Постанови Верховної Ради України «Про земельну реформу»; дані про суб’єктів землеустрою та документацію із землеустрою; клопотання щодо надання дозволу на розроблення документації із землеустрою про передачу (надання) земельних ділянок у власність чи користування та рішення відповідних рад щодо задоволення клопотання;

місцезнаходження вільних земельних ділянок для можливості передачі (надання) їх у власність, користування чи оренду, інформація щодо площ об'єктів розташування на земельній ділянці, дані нормативної грошової оцінки, розрахунок податкових зобов'язань тощо. Така інформація повинна бути доступна в режимі перегляду он-лайн державними органами державної реєстрації прав, державними органами щодо обміну інформацією про речові права на земельні ділянки, органами податкової інспекції (служби), державними органами (службовими особами) з питань земельних відносин, містобудування та архітектури, Департаменту із земельних ресурсів. Дана інформація у повному обсязі та достовірна повинна бути надана на запит не тільки державних діячів, а і фізичних та юридичних осіб. У відповідності до ст. 23 Закону України «Про доступ до публічної інформації» законодавець встановлює право на оскарження рішень, дій чи бездіяльності розпорядників інформації. Перекручення даних Державного земельного кадастру полягає в підготовці та внесенні неправдивих фактичних даних в облікові документи, передбачені відповідними нормативними актами. Ці дані можуть стосуватися як правового режиму земель і їхньої якості, так і достовірних розмірів земельних ділянок, наприклад, для зменшення обкладання податками або іншими платежами бази, що обчислюється на основі оцінки землі

В Україні юридична відповідальність, яка включає в себе самостійні види відповідальності (адміністративну, цивільну, кримінальну тощо), за інформаційне правопорушення у земельній галузі обумовлена багатьма різноплановими факторами: підвищенням рівня правової та інформаційної культури, еволюцією наукових уявлень щодо правової природи інформаційних явищ, розвитком інформаційного права і законодавства, удосконалення діяльності судової та слідчої системи. З метою запобігання порушень діючого законодавства в інформаційній сфері, якою є земельно-кадастрова система, та встановлення фактів зловживання службовим становищем, встановлення підроблення документів службовими (посадовими) особами, інформаційні дані із землеустрою являються об'єктом

дослідження при розслідуванні та попередженні злочинів й розгляду судом кримінальних, адміністративних і цивільних справ у сфері земельних відносин із застосуванням ефективної форми використання спеціальних знань яким являється судова експертиза з метою визначення розміру збитків нанесених державі та зацікавленим юридичним і фізичним особам.

Література:

1. Закон України «Про інформацію» № 2657-XII від 02.10.1992 (редакція від 21.05.2015) [Електронний ресурс].Режим доступу: http://zakon4.rada.gov.ua.
2. Закон України «Про доступ до публічної інформації» № 2939-VI від 13.01.2011 (редакція від 01.05.2015) [Електронний ресурс].Режим доступу: http://zakon4.rada.gov.ua.
3. Теория государства и права. Учебник для юрид. Вузов / Под ред. В.М. Корельского и В.М. Перевалова. – М.: Издательская группа Норма-ИНФРА – М, 1998.
4. Краснов М.А. Юридическая ответственность – целостное правовое явление / М.А.Краснов // Советское государство и право. – 1984. – № 3.
5. Строгович М.С. Сущность юридической ответственности / М.С. Строгович // Советское государство и право. – 1979. – № 5.
6. Рувін О.Г. Принцип свободи у державотворенні: філософсько-правовий вимір: автореф. дис….канд.. юрид. наук: 12.00.12 / О.Г. Рувін; Львів. держ. ун-т. внутр. справ. – Л., 2010.
7. Хачатуров Р.Л. Общая теория юридической ответственности / Р.Л. Хачатуров, Д.А. Липинский. – СПб. : Юридический центр Пресс, 2007.
8. Закон України «Про землеустрій» № 858-IV від 22.05.2003 (редакція від 01.01.2016) [Електронний ресурс].Режим доступу: http://zakon4.rada.gov.ua.

----------***----------

О. О. Кирбят'єв,
к.ю.н., інспектор відділу протидії кіберзлочинам у Запорізькій області Придніпровського управління кіберполіціїДепатаменту кіберполіції Національної поліції України

ДОСТУП ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ ПРИ ФІКСАЦІЇ ПРАВОПОРУШЕНЬ У ІНФОРМАЦІЙНІЙ СФЕРІ: ПРОБЛЕМАТИКА ТА ЙМОВІРНІ ШЛЯХИ ВИРІШЕННЯ

Сьогодні, на фоні стрімкого розвитку інформаційних технологій, також динамічно з'являються та прогресують нові види правопорушень,

відповідальність за які закріплена у відповідних статтях Кримінального кодексу України.

Разом з тим, така ситуація вимагає не менш швидкого реагування на це явище збоку відповідних правоохоронних структур, насамперед тих, які виявляють, розслідують та попереджують кримінальні правопорушення у інформаційній сфері: Національна поліція, Служба безпеки України, тощо.

У переважній більшості кримінальних правопорушень, які вчинені у інформаційній сфері, швидкість встановлення винної особи, а також отримання доказів вчинення особою правопорушення, насамперед, залежить від швидкості отримання доступу до речей і документів, які містять охоронювану законом таємницю (ст. 162 КПК України). До них відносяться: інформація, що знаходиться у володінні засобу масової інформації або журналіста і надана їм за умови нерозголошення авторства або джерела інформації; відомості, які можуть становити лікарську таємницю; відомості, які можуть становити таємницю вчинення нотаріальних дій; конфіденційна інформація, в тому числі така, що містить комерційну таємницю; відомості, які можуть становити банківську таємницю; особисте листування особи та інші записи особистого характеру; інформація, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо; персональні дані особи, що знаходяться у її особистому володінні або в базі персональних даних, яка знаходиться у володільця персональних даних тощо [1].

Алгоритм доступу до речей і документів, які містять охоронювану законом таємницю, регулюється ст. 165 КПК України. У ній зазначається, що цей доступ здійснюється шляхом виконання ухвали слідчого судді, суду про тимчасовий доступ до речей і документів. Цю ухвалу слідчий суддя постановляє у результаті задоволення клопотання слідчого, погодженого з прокурором (ч.1 ст. 160 КПК України) та після можливого судового виклику повісткою особи, у володінні якої знаходяться речі і документи, та з'ясування

усіх необхідних обставин надання тимчасового доступу (ч.1 ст. 163 КПК України). Згідно ч.1 ст. 165 КПК України, особа, яка зазначена в ухвалі слідчого судді, суду про тимчасовий доступ до речей і документів як володілець речей або документів, зобов'язана надати тимчасовий доступ до зазначених в ухвалі речей і документів особі, зазначеній у відповідній ухвалі слідчого судді, суду.

Але, нажаль, строк, у який повинен бути наданий такий доступ, законодавчо не закріплений. Тому, на практиці, процес отримання зазначених речей і документів, починаючи з клопотання слідчого та закінчуючи безпосереднім їх отриманням, може тривати від трьох тижнів до 2 місяців. Й тільки після цього, слідчий може об'єктивно оцінити ситуацію та прийняти рішення, на підставі отриманої вказаним вище порядком інформації, про необхідність проведення, наприклад, обшуку з метою виявлення та фіксації відомостей про обставини вчинення кримінального правопорушення, відшукання знаряддя кримінального правопорушення або майна, яке було здобуте у результаті його вчинення, а також встановлення місцезнаходження розшукуваних осіб (ст. 234 КПК України). Тому, практично, від дня вчинення правопорушення до безпосереднього отримання всіх необхідних доказів вини чи встановлення самої особи (день обшуку, без врахування часу для можливого призначення та проведення відповідних експертиз) може спливти 2 місяці.

На нашу думку, це не виправдано довгий час як для отримання необхідної інформації та збору доказів, тим паче, якщо взяти до уваги те, що швидко проведений обшук після вчиненого правопорушення дає більшу надію на відшукування та фіксації всіх фактів та вилучення всіх речових доказів, виключаючи їх знищення.

У Законі України «Про банки та банківську діяльність», (п. 3 ч.1 ст. 62, яка регулює порядок розкриття банківської таємниці) йдеться про те, що органам прокуратури України, Служби безпеки України, Державному бюро розслідувань, Національної поліції, Національному антикорупційному бюро

України, Антимонопольного комітету України, розкривається інформація, яка містить банківську таємницю - на їх письмову вимогу. Тобто, фактично, за запитом. Але це стосується тільки операцій за рахунками конкретної юридичної особи або фізичної особи - суб'єкта підприємницької діяльності за конкретний проміжок часу. Нажаль, на фізичних осіб дія даного нормативно-правового акту не розповсюджується [2].

Тому, виходячи з вище викладеного, з метою врегулювання даного, на нашу думку, безперечно проблемного питання, пропонується, як одне з можливих рішень, внести відповідні зміни до діючого законодавства у частині надання доступу до речей і документів, які містять охоронювану законом таємницю, на вимогу, подібно тієї, що міститься у ЗУ «Про банки та банківську діяльність» та має вигляд, врегульований ч.2 ст. 62 цього Закону, а саме: вимога відповідного правоохоронного органу на отримання інформації, яка містить охоронювану законом таємницю, повинна:

1) бути викладена на бланку державного органу встановленої форми;

2) бути надана за підписом керівника державного органу (чи його заступника), скріпленого гербовою печаткою;

3) містити номер та дату реєстрації кримінального провадження у ЄРДР, за яким запитується інформація;

4) містити мотивовані підстави для отримання цієї інформації;

5) містити посилання на норми закону, відповідно до яких правоохоронний орган має право на отримання такої інформації.

Крім цього, повинен бути встановлений термін для надання відповіді на вимогу. Пропонується, невідкладно, але не більше 5 днів з дня отримання вимоги.

Подібні пропозиції, на нашу думку, дадуть змогу правоохоронним органам ефективніше провадити заходи щодо виявлення, розкриття, доказування та попередження правопорушень у інформаційній сфері.

Література:

1. Кримінальний процесуальний кодекс України [Електронний ресурс] : Закон України від 13 квітня 2012 р. № 4651-VI [зі змінами та доп. станом на 12.05.2016 р.] // Верховна Рада України : офіційний веб-портал. – Текст. дані. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/4651-17.
2. Закон України «Про банки і банківську діяльність» [Електронний ресурс] : Закон України від 07 грудня 2000 р. № 2121-III [зі змінами та доп. станом на 01.04.2016 р.] // Верховна Рада України : офіційний веб-портал. – Текст. дані. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2121-14/page.

----------***----------

М.В. Гуцалюк,
к.ю.н., с.н.с., доцент.
Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністюпри РНБО України

ОКРЕМІ ПИТАННЯ СТРАТЕГІЇ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Одна з основних тенденцій сучасного інформаційного суспільства – стрімкий розвиток глобальної комп'ютерної мережі Інтернет та поява на її основі низки нових сервісів таких як електронний уряд, соціальні мережі (Facebook, Twitter), електронна комерція, електронний банкінг тощо. Створюється можливість для вільного доступу до мережі у загальнодоступних місцях навіть у віддалених районах сільської місцевості. З технологічної точки зору інформаційний простір характеризується ускладненням інформаційних систем, віртуалізацією обчислювальних мереж, складністю систем комунікацій, інтегруванням телекомунікацій та медіасфери. Широке використання інформаційних технологій дозволяє стрімко розвиватися різним галузям виробництва, науки, банківському сектору, особливо для країн, що розвиваються.

Водночас, загрози кібербезпеки підривають здатність уряду, підприємств і окремих користувачів максимально використовувати переваги, надані Інформаційно-комунікаційними технологіями (ІКТ).

Перехід бізнесу в он-лайн привертає до себе увагу різноманітних злочинних угруповань, які розробляють всілякі шахрайські схеми, викрадають персональні дані, втручаються у роботу електронних систем. Це призводить до втрати довіри у громадян щодо надійності інформаційних послуг і стає значною перешкодою для розвитку суспільства.

Наприклад, у березні поточного року зловмисникам вдалося викрасти фінансові активи у розмірі 28 млн. доларів Центрального банку держави Бангладеш, які зберігалися на кореспондентських рахунках у Федеральному резервному банку США в Нью-Йорку.

Протидія кіберзлочинності вимагає розробки нових підходів і прийняття відповідного законодавства, підготовки спеціальних підрозділів по боротьбі з кіберзлочинністю, проведення технічних заходів щодо забезпечення належного рівня безпеки інформаційних ресурсів, особливо для об’єктів критичної інфраструктури.

Значним кроком у виконанні цих завдань стала затверджена Указом Президента України від 15 березня 2016 р. №96/2016 «Стратегія кібербезпеки України». На сьогодні є вкрай важливим формування дорожньої карти та чітке її виконання. Серед актуальних проблем, які необхідно вирішити найближчим часом зазначимо створення вітчизняної термінологічної бази у цій сфері, вдосконалення нормативно-правових актів та їх гармонізація відповідно до міжнародних стандартів.

Що стосується термінологічної бази, то в українському законодавстві не визначено понять кіберпростір, кіберзлочинність тощо. У 2000 р. на 10-му Конгресі ООН з попередження злочинності та поводження з правопорушниками були визначені дві дефініції. Кіберзлочинність в вузькому сенсі (комп'ютерна злочинність) - це будь-яка протизаконна поведінку у формі електронних операцій, спрямована проти безпеки комп'ютерних систем і оброблюваних ними даних.

Кіберзлочинність в широкому сенсі (злочини, пов'язані із застосуванням комп'ютерів) - це будь-яка протизаконна поведінка, що

здійснюється за допомогою або в зв'язку з комп'ютерною системою або мережею, включаючи такі злочини, як незаконне володіння, пропозиція або поширення інформації за допомогою комп'ютерної системи або мережі.

Перелік видів кіберзлочинів зазначений у Європейській Конвенції про кіберзлочинність 2001 р., ратифікованої Законом України від 7 вересня 2005 р. № 2824-IV. Це зокрема, незаконний доступ, незаконне перехоплення, втручання у дані, зловживання пристроями, підробка, поширення інформації (дитяча порнографія), авторське право, расизм і ксенофобія.

Що стосується визначення понять «кіберпростір», «кіберзлочин», «кібератака» тощо, то їх не обов’язково визначати у Кримінальному кодексі. Наприклад у Республіці Польща вони визначені у Доктрині кібербезпеки 2015 року.

Натомість повинна бути посилена відповідальність щодо атак на інформаційні об’єкти критичної інфраструктури, перелік яких необхідно затвердити постановою Кабінету міністрів України. До нього можуть зокрема входити:

- Енергетичні системи.
- Телекомунікаційні системи.
- Фінансові установи.
- Системи забезпечення продуктами харчування.
- Системи водопостачання.
- Системи охорони здоров’я.
- Транспортні системи.
- Хімічні та радіоактивні підприємства.

До об’єктів критичної інфраструктури варто було б додати і різноманітні державні реєстри, на деякі з яких останнім часом здійснюються атаки. Наприклад на Реєстр нерухомості з метою змін до даних власників. Разом з тим, на нашу думку, не варто створювати нові окремі статті у Кримінальному кодексі України щодо конкретних інформаційних систем, як

наприклад Стаття 376-1 Незаконне втручання в роботу автоматизованої системи документообігу суду.

Вирішення зазначених питань дозволить більш продуктивно використовувати чинну нормативно-правову базу усім суб'єктам національної системи кібербезпеки для ефективної протидії кіберзлочинності.

Література:

1. Стратегія кібербезпеки України, затверджена Указом президента України від 15 березня 2016 р. №96/2016 [Електронний ресурс]. Режим доступу: http://www.president.gov.ua/documents/962016-19836
2. Хакерська крадіжка золотовалютних резервів Бангладеш. [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/Хакерська_крадіжка_золотовалютних_резервів_Бангладеш

----------***----------

В. Ю.Балашов,
завідувач лабораторії комп'ютерно-технічних, фоноскопічних, аналітичних, теоретичних досліджень та інформаційного забезпечення ХНДІСЕ ім.Засл. проф. М.С. Бокаріуса МЮ України

ПРОБЛЕМИ УНІФІКАЦІЇ ТЕРМІНОЛОГІЇ У СФЕРІ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Розвиток інформаційних технологій сприяє швидкому впровадженню нових технологій у побут суспільства. Сучасні технології допомагають людині виконувати широкий спектр щоденних задач, в тому числі – обробку персональних даних, керування фінансами, моніторинг стану здоров'я, продаж та придбання товарів, автоматизація бізнес-процесів, накопичення даних з обмеженим доступом (наприклад, комерційна, адвокатська або лікарська таємниця тощо). Таким чином, інформаційні системи представляють інтерес для зловмисників, які мають намір отримати контроль над інформацією, що оброблюється у інформаційній мережі.

Зростання кількості правопорушень, що виникають у сфері інформаційних технологій, або з їх застосуванням, стимулює активний розвиток окремих підрозділів з боротьби із кіберзлочинністю. Відповідні управління, департаменти, відділи за останні 10 років були створені у структурах Міністерства внутрішніх справ [1], Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України [2], Головного управління розвідки Міністерства оборони України та Службі зовнішньої розвідки. Кожен з підрозділів має власну юрисдикцію та діє самостійно керуючись законами та підзаконними нормативними актами, що регулюють їх діяльність. Аналізом низки законів, на яких базується захист інформації та засади боротьби з кіберзлочинністю, а також судово-експертною та судовою практикою виявлено, що базові терміни, які так необхідні у юридичній практиці для якісної роботи у справах, пов'язаних з кіберзлочинністю, у різних законах і підзаконних актах мають різні тлумачення. Така ситуація призводить до неоднозначного розуміння, що саме вважати «кіберзлочином», «кіберпростором», «кібератакою», «кібертероризмом», «кібербезпекою», «кіберінфраструтурою». Навіть не зважаючи на стрімке формування у органах внутрішніх справ окремого департаменту «Кіберполіції», в задачі якої входить, в тому числі, розслідування та попередження кіберзлочинів, чітке тлумачення терміну «кіберзлочин» наразі має декілька варіацій в залежності від органу, що дане тлумачення пропонує.

Перший «вектор» тлумачення терміну «кіберзлочин» полягає в тому, щоб називати кіберзлочином ті діяння, що передбачені статтями 361-363 Кримінального кодексу України (Розділ (XVI)). В даних статтях передбачено несанкціоноване втручання до автоматизованих систем та систем електрозв'язку, що призвели до певних негативних наслідків, створення з метою збуту, збут або використання шкідливого програмного забезпечення, використання мереж та автоматизованих систем з порушенням правил їх експлуатації та розсилання так званого «спаму». Присвоєння

узагальнюючого терміну «кіберзлочин» зазначеним вище неправомірним діям є коректним та логічним, але не враховує деякі практичні моменти. Так наприклад, практика розслідування злочинів, пов'язаних з використанням інформаційних технологій надає змогу впевнитися, що велика кількість неправомірних дій у цій площині, має бути кваліфікована не лише за ст. 361-363 ККУ, але й за ст.ст. 190, 192 та ін. Враховуючи, що дії, передбачені даними статтями за наведеним вище принципом тлумачення терміну «кіберзлочин», не можуть називатися кіберзлочином, то розслідування злочину не обов'язково повинно відбуватися спеціальними підрозділами з боротьби із кіберзлочинністю. Якщо ж подивитися на ресурси, що необхідні для компетентного розслідування такого злочину, то стає очевидно, що працівники, які проводять розслідування, повинні добре володіти технічними знаннями у галузі інформаційних технологій, тобто це повинні бути працівники спеціальних підрозділів з боротьби із кіберзлочинністю.

Другий «вектор» тлумачення терміну «кіберзлочин» має більш поширений підхід та не упирається лише в віднесення до терміну правопорушень, передбачених певними статтям Кримінального кодексу України. За основний критерій віднесення подій до кіберзлочину виступає використання інформаційних технологій або їх елементів при скоєнні злочину. Такий підхід є більш раціональний, ніж перший, але також має деякі практичні проблеми, які вже встигли проявитися у роботі деяких підрозділів у різних державних установах, що займаються розслідуванням злочинів у сфері високих інформаційних технологій. Як найяскравіший приклад можна навести злочини, пов'язані із шахрайством на сайтах купівлі-продажу побутових товарів, таких як OLX.ua, Klumba.ua тощо. Такі злочини, як правило, кваліфікуються як дії, передбачені ст. 190 Кримінального кодексу України, тобто шахрайство. І це логічна і вірна кваліфікація. Але розслідування такого шахрайства доручається зазначеним вище підрозділам. Величезна кількість випадків шахрайства на подібних Інтернет-ресурсах призводить до великої завантаженості цих підрозділів та не дозволяє їм

зосередити увагу на подіях, які потребують більш ретельного розслідування через свою технічну складність.

Національним інститутом стратегічних досліджень [3] виконувався аналіз багатьох термінів, що використовують у роботі більшість органів, пов'язаних із розслідуванням злочинів у сфері інформаційних технологій. За результатами дослідження наводиться перелік різновидів тлумачень терміну «кіберзлочин»:

- Служба безпеки України: Кіберзлочин - це кіберправопорушення, передбачене кримінальним законодавством, яке несе у собі суспільну небезпеку.
- ГУ розвідки Міністерства оборони України: Кіберзлочин – кримінальна дія здійснена у кіберпросторі з використанням засобів електронно-обчислювальної техніки.
- Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю РНБО України: Кіберзлочин (кібернетичний комп'ютерний злочин) - протиправне втручання в роботу кібернетичних систем, основною управляючою ланкою яких є комп'ютер (наприклад спотворення інформації про стан об'єкту в каналі зворотного зв'язку, спотворення керуючого сигналу в каналі прямого зв'язку, використання шкідливого програмного забезпечення тощо); створення та використання у злочинних цілях певної кібернетичної (комп'ютерної) системи; використання у злочинних цілях існуючих кібернетичних (комп'ютерних систем).
- Інститут телекомунікацій і глобального інформаційного простору НАН України: Кіберзлочинність – злочини, головним інструментом яких є інформаційно-комунікаційні технології.

Як вбачається з наведених тлумачень, кожне з них містить щонайменше ще один «кібертермін», який потребує додаткового тлумачення. Також під деякі тлумачення можна віднести злочини, в яких інформаційні технології відіграють не найважливішу роль і не повинні розслідуватися спеціалізованими органами розслідування кіберзлочинів.

Для вирішення проблеми тлумачення цього терміну, Національний інститут стратегічних досліджень пропонує власне тлумачення:

«Кіберзлочин – кримінальна дія, відповідальність за яку передбачено кримінальним законодавством, яка здійснена (здійснюється) у кіберпросторі (або за допомогою його технічних можливостей).»

Тлумачення, запропоноване Національним інститутом стратегічних досліджень є найдоцільнішим, проте також потребує доопрацювання в частині звуження діапазону злочинів, які підпадають під поняття даного терміну з метою.

Враховуючи наведене вище, автор вважає за необхідне створення єдиної бази-словника термінів, уніфікованих для всіх органів розслідувань, державних органів, пов'язаних із сприянням розслідуванням, адвокатам та будь-яким іншим громадянам України. Централізований підхід дозволить уникнути різних варіацій читань за закріпить поняття термінів на рівні усієї держави. Також необхідно звузити поняття «кіберзлочину» та надати йому певної конкретики з метою зниження робочого навантаження на спеціалізовані органи досудового розслідування у сфері кіберзлочинності, що дозволить раціональніше використовувати потенціал працівників зазначених органів та підвищити якість розслідувань злочинів з високим рівнем технічної складності.

Література:

1. Кіберполіція (крок реформи). Стаття в офіційному блозі / А. Аваков. [Електроний ресурс]. – Режим доступу: http://blogs.pravda.com.ua/authors/avakov/561a92c183c27/
2. Офіційний сайт CERT-UA [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/?page_id=207
3. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування. Аналітична записка / Д. Дубов, М. Ожеван [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/454/.

----------***----------

В.Д.Гавловський,
к.ю.н., с.н.с., провідний науковий співробітник.
Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при РНБО України

ДО ПИТАННЯ ОЦІНКИ СТАНУ КІБЕРЗЛОЧИННОСТІ

Кіберзлочинність завдає величезної шкоди суспільству і перетворюється в добре організовану індустрію. Цей процес потребує своєчасного та адекватного реагування державних органів. Для прийняття ними ефективних та виважених рішень в першу чергу необхідно мати об'єктивну оцінку стану кіберзлочинності, яка має величезне практичне значення для світу, країни, регіону. Вона дає змогу виявити тенденції злочинності, усвідомити темпи зростання чи скорочення цього негативного явища для ефективнішого використання коштів на боротьбу та запобігання злочинам.

Стан злочинності характеризують кількісні та якісні показники. Кількісні показники стану злочинності визначаються кількістю злочинів, зареєстрованих на певній території за певний час, і кількістю виявлених осіб, які вчинили злочини на певній території за певний час. Структура злочинності є її якісним показником.

Слід зауважити, що в зарубіжних країнах, як правило, злочини реєструються поліцією. Дві третини країн вважають свої системи поліцейської статистики недостатніми для того, щоб реєструвати кіберзлочинність. Показники кіберзлочинності, які реєструються поліцією, залежать не стільки від безпосереднього рівня злочинності, скільки від рівня розвитку країни і спеціалізованих можливостей поліції. До того ж такі статистичні дані використовуються, як правило, лише для розробки політики на національному рівні. Їх неможливо використовувати для порівнянь між країнами.

Тому в західних країнах крім реєстрації кіберзлочинів поліцією, існує ще низка інформаційних джерел, з яких можна дізнатися про злочини. Це різні механізми прийняття заяв жертв; інформація, що отримується за допомогою технологій кібербезпеки; опитування населення та обстеження підприємств.

Разом з тим відомо, що статистичні дані, що реєструються поліцією про злочини та осіб, що вчинили злочини є найбільш достовірними. Але також слід відмітити, що реєструються лише ті злочини, що потратили в поле зору поліції, а значна частина злочинів залишається латентною.

В Україні при визначенні стану злочинності використовується офіційна статистика за формами державної статистики. Проте існує низка певних проблемних питань в контексті зазначеного. Серед них.

По перше, до цього часу на законодавчому рівні не визначено термінологію. На сьогодні зустрічаються різні кримінологічні терміни – поряд з поняттям кіберзлочинність вживаються терміни комп'ютерна злочинність, злочинність у сфері високих інформаційних технологій, високотехнологічна злочинність, злочини, що вчиняються з використанням інформаційних технологій тощо. Кримінальний кодекс України оперує терміном «злочини у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Серед вищезазначених, поняття кіберзлочинність є найширшим поняттям та охоплює найбільше коло злочинних посягань у віртуальному середовищі, а також його використання передбачає міжнародне законодавство. Так, Рада Європи в листопаді 2001 року прийняла Конвенцію про кіберзлочинність. Тому ми, як і значна частина кримінологів, вважаємо обґрунтованим вживання саме цього терміну для кримінологічного дослідження цього різновиду злочинності [1].

По друге, не визначено перелік злочинів, які мають відноситися до цього виду, чи критерії їх визначення.

По третє, недосконаліть статистичних звітів. Офіційна статистика, на жаль, не дає можливості одержати достовірні дані щодо кримінологічної характеристики кіберзлочинів, можливості відслідковувати процес від реєстрації правопорушення до винесення вироку особі, яка його вчинила.

В четверте, це висока латентність, як абсолютна так і відносна. За експертними оцінками, рівень латентності кіберзлочинів становить близько 90 %. Причинами латентності найчастіше виступають складнощі виявлення та розслідування кіберзлочинів, неповідомлення потерпілих осіб про факти вчинення таких злочинів. Так, більшість великих компаній хвилюються про свою ділову репутацію та намагаються усунути наслідки кіберзлочинів власними зусиллями.

В Генеральній прокуратурі України спільно з Міністерством внутрішніх справ України, Службою безпеки України, Державною податковою службою України впроваджено Єдиний реєстр досудових розслідувань, який ведеться з метою забезпечення єдиного обліку кримінальних правопорушень та прийнятих під час досудового розслідування рішень, осіб, які їх учинили, та результатів судового провадження, а також аналізу стану та структури кримінальних правопорушень, вчинених у державі.

Генеральною прокуратурою щомісячно видається «Єдиний звіт про кримінальні правопорушення» де в Таблиці 4.15. надано дані про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. В звіті також відображено ще ряд показників про злочини, які можуть бути віднесені до кіберзлочинів.

Більше даних про цей вид злочинів надано МВС України в Звіті про результати роботи підрозділів Національної поліції України, де в Розділі XVII Відомості про кримінальні правопорушення, що вчинені з використанням високих інформаційних технологій, у тому числі виявлення і супроводження таких правопорушень працівниками підрозділів кіберполіції

крім даних по Розділу XVI КК України надано інформацію про злочини, які вважаються кіберзлочинами. Це злочини за ст.ст. 176, 185, ч. 3,4 ст.190, 200, 229, 231, ч.3,4,5 ст. 301 КК України.

В звіті судів першої інстанції про розгляд матеріалів кримінального провадження (Форма 1-1) підраховується кількість справ кримінальних проваджень загалом по Розділу XVI КК України без розбивки за статтями.

Проаналізувавши вищевказані звіти, можна констатувати, що вони були розроблені без узгодження між собою. І якщо зі звіту МВС можливо взяти дані про значну кількість злочинів, які можна віднести до кіберзлочинів, то з офіційних статистичних звітів, окрім Розділу XVI КК України, дані про кіберзлочини відсутні. Особливо недостатньо даних про кіберзлочини в звітах судочинства. В судовій звітності вказується кількість розглянутих справ кримінальних проваджень без уточнення кількості кримінальних правопорушень. Тобто неможливо відслідкувати за скількома кримінальними правопорушеннями прийнято судове рішення. До того ж в судовій статистиці відсутні дані щодо видів покарань з виділенням за злочини середньої тяжкості, тяжкі, особливо тяжкі. Це унеможливлює аналіз міри покарання за кіберзлочини.

Отже, у зв'язку з невизначеністю на законодавчому рівні термінології, пов'язаної з кіберзлочинністю, невизначеністю переліку злочинів, що відносяться до кіберзлочинів, через недосконаліть статистичної звітності, а також високу латентність на сьогодні неможливо провести об'єктивну характеристику кіберзлочинності.

Вирішення зазначених проблемних питань дозволить аналізувати і отримувати реальний стан кіберзлочинності та проводити ефективні заходи протидії.

Література:

1. Голіна В.В Кримінологія: Загальна та Особлива частини : Навчальний посібник / В.В. Голіна, Б.М. Головкін. – Х.: Право, 2014. – С. 332–337.

----------***----------

Ю. Нізовцев,
головний спеціаліст (експерт) Центру судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України,
О. Парфило,
к.ю.н., с.н.с., начальник відділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України

ЩОДО ВСТАНОВЛЕННЯ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА КІБЕРТЕРОРИЗМ У ЗАКОНОДАВСТВІ УКРАЇНИ

Комп’ютерні системи автоматизації наразі увійшли у всі сфери економіки, а ступінь комп’ютеризації всіх технологічних процесів з часом тільки збільшується. І це закономірно, оскільки дозволяє підвищити ефективність, скоротивши при цьому витрати як часу, так і матеріальних та фінансових ресурсів. Разом з тим, глобальне поширення інформаційних технологій має і негативний бік, обумовлений залежністю згаданих вище сфер від коректної роботи задіяних комп’ютерних систем. Коректність роботи зазначених комп’ютерних систем залежить від якості програмного забезпечення та захищеності від зовнішнього втручання. Належна якість програмного забезпечення досягається ретельним тестуванням та виправленням усіх виявлених помилок. Захист від зовнішнього впливу забезпечується впровадженням різноманітних механізмів захисту: міжмережевих екранів (брандмауерів), антивірусів, шифрування трафіку тощо. Водночас, як свідчить практика, не завжди задіяні захисні механізми забезпечують належний рівень безпеки, а отже, комп’ютерні системи є уразливими і для найбільш небезпечного різновиду кіберзлочинності – кібертероризму, який, у порівнянні з традиційним тероризмом, під час проведення терористичних актів використовує комп'ютерні системи та

мережі, спеціальне програмне забезпечення та сучасні інформаційні технології.

Підвищена суспільна небезпека кібертеракту полягає в тому, що він не має кордонів, кібертерористи здатні в рівній мірі загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі. Основна форма кібертероризму – інформаційна атака на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури. Їх цілі дуже різноманітні, втім найбільшу небезпеку становлять акції, спрямовані проти структур і об'єктів критичної інфраструктури, наприклад систем управління АЕС, промислових підприємств, об’єктів транспорту. Порушення або блокування їх роботи може спричинити миттєву загрозу для життя багатьох людей та стати причиною катастроф техногенного характеру та інших тяжких наслідків.

Кіберзлочинцями постійно вигадуються нові способи атак на інформаційні системи. Ці способи удосконалюються та беруться на озброєння кібертерористами, внаслідок чого виявити і нейтралізувати комп’ютерних терористів вельми проблематично через занадто малу кількість слідів, що залишаються ними в інформаційному просторі.

Високотехнологічні терористичні акти становлять сьогодні реальну небезпеку для України, саме тому необхідне своєчасне прийняття конкретних заходів протидії таким загрозам, у тому числі і шляхом удосконалення нормативно-правової бази боротьби з тероризмом, перш за все кримінального законодавства.

Слід зазначити, що важливість забезпечення інформаційної безпеки та боротьби з кіберзлочинністю закріплені у багатьох нормативно-правових актах України. Так, відповідно до ч.1 ст. 17 Конституції України «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [1]. Закон України «Про основи національної безпеки України» визнає комп'ютерну злочинність та комп'ютерний тероризм

однією з загроз національним інтересам і національній безпеці України [2]. Крім того, у 2005 році Україна приєдналася до Конвенції про кіберзлочинність[3] і таким чином імплементувала положення міжнародного акту у вітчизняне законодавство.

Одним із важливих кроків на шляху створення національної системи кібербезпеки став Указ Президента України від 15 березня 2016 року № 96, яким уведено в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» та затверджено Стратегію кібербезпеки України [4].

Відповідно до Стратегії основу національної системи кібербезпеки становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи.

Зокрема на Службу безпеки України покладені такі завдання – попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством, а також щодо готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидія кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України; розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечення реагування на комп'ютерні інциденти у сфері державної безпеки.

Згідно з п. 4.1 цієї Стратегії одним із пріоритетів та напрямів забезпечення кібербезпеки України є створення вітчизняної нормативно-правової та термінологічної бази у цій сфері.

Крім того, в Україні передбачена кримінально-правова відповідальність за ряд злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, що закріплена у статтях однойменної глави Кримінального кодексу України.

Враховуючи суспільну небезпеку, обумовлену втручанням в роботу інформаційних систем критичної інфраструктури держави, багато науковців, серед яких В.М. Бутузов, С.О. Гнатюк, В.А Голубєв, О.Г. Корченко, В.А. Мазуров, В.П. Шеломенцев та інші, вважають необхідним встановити кримінальну відповідальність за новий різновид особливо небезпечних злочинів – кібертероризм. Натомість, у Кримінальному кодексі України вже існує відповідальність за «класичний» тероризм, передбачена ст. 258, а отже залишається дискусійним питання щодо запровадження окремої статті чи внесення змін до чинних норм вітчизняного кримінального законодавства.

Слід зазначити, що в червні 2015 року Парламентська Асамблея Ради Європи ухвалила резолюцію 2070 (2015) «Зміцнення співпраці у протидії кібертероризму та іншим масштабним атакам в Інтернеті» [5], у п.3 якої міститься заклик до країн-членів Ради Європи запровадити визначення кібертероризму та відповідальності за нього.

Відповідно до цієї резолюції було підготовлено два законопроекти щодо внесення змін до Кримінального кодексу України [6]: проект Закону про внесення змін до Кримінального кодексу України (щодо посилення відповідальності за кібертероризм та кіберзлочини) (законопроект № 2328а від 10.07.2015) [7] та проект Закону про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за кібертероризм (законопроект № 2439а від 24.07.2015) [8]. Натомість пройшов вже майже рік, а зміни до Кримінального кодексу України так і не прийняті.

Автори цілком погоджується з думкою розробників законопроектів, що ухвалення відповідних змін до Кримінального кодексу України є надзвичайно актуальним, оскільки дозволить забезпечити на законодавчому

рівні захист інформаційних (автоматизованих), інформаційно-телекомунікаційних систем, електронних реєстрів та баз даних державної форми власності, об'єктів критичної національної інфраструктури. Натомість зволікання у цьому питанні може зменшити результативність роботи правоохоронних органів, призвести до неналежної кваліфікації вчинених діянь та уникненні покарань винних осіб.

Разом з тим, авторами було проведено аналіз запропонованих законопроектів. Під час аналізу враховувалося, що способи вчинення тероризму та кібертероризму різні. Відповідно, різними є знаряддя вчинення цих злочинів та їх підготовка. Все це обумовлює різні тактики розслідування, різні види експертиз, які необхідно призначати, різні спеціалізації задіяних правоохоронців (слідчих, оперативних співробітників, спеціалістів, експертів) тощо. Фактично кібертероризм є різновидом несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Вчинювані зловмисниками дії є тими самими, відмінність полягає у мотивах та більш тяжких наслідках.

Законопроект № 2439а, яким пропонується доповнити Кримінальний кодекс України окремою статтею 258^6, дає визначення поняття кібертероризму (умисна атака на інформацію, яка обробляється комп'ютером, комп'ютерну систему чи комп'ютерні мережі, що створює небезпеку для життя і здоров'я людей або призводить до інших тяжких наслідків, якщо такі дії були скоєні з політичних мотивів, з метою порушення суспільної безпеки, залякування населення, провокації військового конфлікту). На думку авторів, вітчизняне законодавство давно вже потребує нормативного закріплення визначення кібертероризму. Разом з тим, введення окремої статті може обумовити плутанину, оскільки, якщо не брати до уваги мету і мотиви (які не завжди є явними на початку розслідування), дії, передбачені запропонованою ст. 258^6 є майже ідентичними діям, передбаченим ст. 361 Кримінального кодексу.

Законопроект № 2328а передбачає викласти у новій редакції ч.2 ст. 258, доповнивши її фразою «або якщо вони пов'язані з несанкціонованим втручанням в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку об’єкту підвищеної небезпеки», а також ст. 361 доповнити новими частинами (третьою і четвертою), найбільш суттєвою з яких в рамках розглядуваної проблеми є третя: «Дії, передбачені частинами першою або другою цієї статті, якщо вони пов'язані з несанкціонованим втручанням в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку об’єкту підвищеної небезпеки та призвели до заподіяння значної майнової шкоди чи інших тяжких наслідків». Як бачимо, законопроект № 2328а має той самий недолік, що й законопроект № 2439а, а саме обумовлює конкуренцію складів злочину, на цей раз ч.2 ст. 258 та ч.3 ст. 361.

На наш погляд, більш вдалим є законопроект № 2328а. Разом з тим, автори пропонують не вносити зміни до ч.2 ст. 258, а обмежитися доповненням третьої та четвертої частин у ст. 361. При цьому в ч.3 ст. 361 замінити термін «об’єкт підвищеної небезпеки» на «об’єкт критичної інфраструктури». Що стосується визначення кібертероризму, яке пропонується законопроектом № 2439а, його слід закріпити в окремому нормативно-правовому акті, наприклад, у Стратегії кібербезпеки України [4].

Література:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр
2. Закон України «Про основи національної безпеки України» [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/964-15
3. Конвенція про кіберзлочинність [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/994_575
4. Стратегія кібербезпеки України, затверджена указом Президента України № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»» [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/962016-19836

5. Resolution 2070 (2015) «Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet» [Електроннийресурс]. – Режимдоступу: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21975&lang=en
6. У Раді пропонують встановити кримінальну відповідальність за кібертероризм / Інформаційне агентство УНІАН [Електронний ресурс]. – Режим доступу: http://www.unian.ua/politics/1106141-u-radi-proponuyut-vstanoviti-kriminalnu-vidpovidalnist-za-kiberterorizm.html
7. Проект Закону про внесення змін до Кримінального кодексу України (щодо посилення відповідальності за кібертероризм та кіберзлочини) [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=55972
8. Проект Закону про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за кібертероризм [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=56183

----------***----------

Б. Д. Леонов,
д.ю.н., с.н.с., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України

ЩОДО УДОСКОНАЛЕННЯ КРИМІНАЛЬНО-ПРАВОВОЇ ПРОТИДІЇ НЕЗАКОННІЙ ДІЯЛЬНОСТІ ЗІ СПЕЦІАЛЬНИМИ ТЕХНІЧНИМИ ЗАСОБАМИ НЕГЛАСНОГО ОТРИМАННЯ ІНФОРМАЦІЇ

Глибинна трансформація правових процесів в Україні потребує оптимізації системи кримінально-правової охорони інформації від незаконних посягань.Використання новітніх технологій у різних сферах життєдіяльності зумовлює появу нових загроз в інформаційній сфері. Зростання кількості спеціальних технічних засобів негласного отримання інформації (далі – СТЗ), удосконалення технічних характеристик цих засобів та розширення сфери їх застосування загострюють проблему кримінально-правової протидії незаконній діяльності зі СТЗ.

Боротьба з незаконним поводженням зі СТЗ, як і з будь-якими іншими злочинними проявами, має проводитися тільки за умови неухильного

додержання законності, зокрема правильного застосування кримінально-правових норм. В цьому контексті заслуговує на увагу аналіз складів злочинів, передбачених ст. 163 і 359 КК України. При цьому має бути врахована специфіка СТЗ, які, водночас, є предметом адміністративних, правоохоронних правовідносин та невід'ємною частиною системи захисту національної безпеки [1, с.79].

Окремі питання удосконалення редакцій цих статей КК України та вирішення проблем кваліфікацій таких діянь знайшли відображення, зокрема, в наукових працях П.П.Андрушка, П.С.Берзіна, І.О.Зінченко, М.В.Карчевського, Д.Ю.Кондратова, С.Я.Лихової, М.І.Мельника, М.І.Хавронюка та ін.

Не дивлячись на це, проблема протидії СТЗ залишається недостатньо розробленою. Зокрема, потребує осмислення визначення СТЗ, узгодження термінології, яка «представляє» СТЗ в КК України, співвідношення складів злочинів, де згадуються СТЗ.

Основними формулюваннями, які визначають СТЗ у чинному кримінальному законодавстві є: «спеціальні засоби, призначені для негласного зняття інформації» (ч. 2 ст. 163 КК України) та «спеціальні технічні засоби негласного отримання інформації» (ч. 1 ст. 201, ч. 1 ст. 359 КК України).

Необхідно зазначити, що наявність кількох формулювань СТЗ є одним із недоліків КК України.

На нашу думку, вдосконалення кримінального законодавства України в частині, що стосується СТЗ, передбачає:

1) чітке законодавче визначення поняття СТЗ;

2) уніфікацію термінології, яка «представляє» СТЗ в КК України;

3) визначення співвідношення злочинів, склади яких передбачені в ст. 163 КК України і ст. 359 КК України.

Спеціальні технічні засоби – це будь-які технічні засоби і пристосування, за допомогою яких особа має можливість ознайомитися із

інформацією про зміст листування, телефонних розмов, поштових, телеграфних та інших відправлень. До таких засобів відноситься, наприклад, відео- і адуио- запис, кіно- і фотозйомка, будь-які засоби для прослуховування тощо[2, с.299].

Відповідно до п. 23 ст. 7 Закону України «Про ліцензування видів господарської діяльності» підлягає ліцензуванню діяльність, пов'язана з розробленням, виготовленням, постачанням спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації (критерії належності та перелік технічних засобів негласного отримання інформації визначаються Кабінетом Міністрів України за поданням Служби безпеки України) [3]. На даний час триває робота з визначення критеріїв належності та переліку технічних засобів негласного отримання інформації.

На наш погляд, під спеціальними технічними засобами негласного отримання інформації слід розуміти апаратні, програмні та апаратно-програмні засоби, призначені для негласного отримання інформації у прихований спосіб та придатні для здійснення оперативно-розшукових заходів та негласних слідчих (розшукових) дій. Закріплення у законі такого визначення дозволить відмежувати СТЗ як від шкідливих програмних засобів, призначених для несанкціонованого втручання в роботу комп'ютерів, комп'ютерних мереж, так і від засобів побутового призначення, що можуть бути використані для негласного отримання інформації.

Статтею 359 КК України передбачено відповідальність за незаконне придбання або збут спеціальних технічних засобів негласного отримання інформації, а також незаконне їх використання. Вважаємо, що ступінь суспільної небезпечності цих діянь не є однаковим. На наш погляд, слід частково декриміналізувати ст. 359 КК України, встановивши кримінальну відповідальність лише за незаконний збут СТЗ та їх незаконне використання. З цією метою пропонуємо абзац перший частини 1 статті 359 Кримінального кодексу України викласти у такій редакції: «Незаконне використання

спеціальних технічних засобів негласного отримання інформації». До речі, така редакція цієї норми була до внесення змін до Кримінального кодексу України щодо відповідальності за незаконне поводження із спеціальними технічними засобами негласного отримання інформації (Закон України від 15.06.2010 №2338-VI). Теоретично декриміналізація злочину може полягати у переведенні як до категорії правомірних дій, так і до категорії адміністративних проступків. Тому, вважаємо, що за діяння, яке полягає у незаконному придбанні або розповсюдженні СТЗ, має наставати адміністративна відповідальність, що, в свою чергу, передбачає унесення змін і доповнень до статті 195-5 Кодексу України про адміністративні правопорушення, доповнивши її абзац перший після слів «незаконне зберігання» словом «придбання або збут».

Крім цього, потребує, на наш погляд, декриміналізації контрабанда спеціальних технічних засобів негласного отримання інформації. Відповідальність за дане діяння має наставати за ст. 333 КК України за умови поширення дії Закону України «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання» на переміщення СТЗ. З метою реалізації цієї пропозиції в абзаці першому частини 1 статті 201 КК слова «а також спеціальних технічних засобів негласного отримання інформації» слід виключити.

Що стосується співвідношення злочинів, склади яких передбачені в ч. 2 ст. 163 КК і в ч. 3 ст. 359 КК, то при їх кваліфікації виникають певні проблеми. На думку М.І.Хавронюка, ч. 2 ст. 163 КК України конкурує з ч. 3 ст. 359 КК України (Незаконне придбання або збут спеціальних технічних засобів негласного отримання інформації, а також незаконне їх використання, якщо ці діяння заподіяли істотну шкоду охоронюваним законом правам, свободам чи інтересам окремих громадян, державним чи громадським інтересам або інтересам окремих юридичних осіб). [4, с.169] Інші автори вважають, що в даному випадку слід застосувати сукупність кримінально-правових норм [5, с.714; 6, с.464]. На думку С.Я.Лихової,

незаконне використання СТЗ є способом вчинення злочину, юридичний склад якого передбачений в диспозиції ч. 2 ст. 163 КК. В той же час це діяння утворює окремий злочин, склад якого передбачений ч. 3 ст. 359 КК України. За ступенем тяжкості ці злочини однакові, тому в даному випадку конкуренція кримінально-правових норм «переростає» у сукупність[2, с.301]. Враховуючи, що всі норми, які міститься в статтях 182, 162, 163 КК України, спрямовані на охорону таємниці приватного життя, а її порушення будь-яким шляхом може бути пов'язане з використанням спеціальних засобів, призначених для негласного зняття інформації, використання СТЗ слід розглядати як самостійний склад злочину, який передбачено статтею 359 КК України [2, с.302]. За такого підходу у ч. 2 ст. 163 КК України слова «або з використанням спеціальних засобів, призначених для негласного зняття інформації» доцільно вилучити. Це сприятиме ліквідації невиправданої конкуренції між ст. 163 і ст. 359 КК України.

Для вирішення питань щодо кваліфікації порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку з використанням СТЗ, прийнятною є кваліфікація за сукупністю злочинів (ч. 1 ст. 163, ч. 1 ст. 359 КК України). Якщо ж має місце незаконне збирання з метою використання відомостей про приватне життя особи, то вчинене також слід кваліфікувати за сукупністю злочинів (ч. 1 ст. 182, ч. 1 ст. 359 КК України) [2, с.303].

Реалізація запропонованих змін і доповнень сприятиме удосконаленню кримінально-правової протидії незаконній діяльності зі СТЗ.

Література:

1. Кондратов, Д.Ю. Кримінально-правова протидія незаконному поводженню зі спеціальними технічними засобами отримання інформації за законодавством деяких зарубіжних країн // Науковий вісник Херсонського державного університету. Серія : Юридичні науки. – 2013. – Вип. 5. – С. 79-82.
2. Лихова, С. Я. Злочини у сфері реалізації громадянських, політичних та соціальних прав і свобод людини і громадянина (розділ V Особливої

частини КК України): моногр. / С. Я. Лихова. – К. : Видавничо-поліграфічний центр «Київський університет», 2006. – 573 с.
3. Закон України «Про ліцензування видів господарської діяльності» // Відомості Верховної Ради. – 2015. – № 23. – ст.158.
4. Науково-практичний коментар Кримінального кодексу України. 7-ме вид., переробл. та доповн. / За ред. М.І. Мельника, М.І. Хавронюка. – К. : Юридична думка, 2010. – 1288 с.
5. Науково-практичний коментар Кримінального кодексу України. 4-те вид., переробл. та доповн. / Відп. ред. С.С. Яценко. – К., 2005. – 848 с.
6. Кримінальний кодекс України : Науково-практичний коментар / Ю.В.Баулін, В.І.Борисов, С.Б.Гавриш та ін.; За заг. ред. В.В. Сташиса, В.Я. Тація. – К., 2003. – 1196 с.

----------***----------

І.В.Логінов,
к.ю.н., с.н.с., консультант
ДКІБ СБУ

УМОВИ НАСТАННЯ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА НЕЗАКОННЕ ЗАСТОСУВАННЯ ТЕХНІЧНИХ ЗАСОБІВ ДЛЯ НЕГЛАСНОГО ОТРИМАННЯ ІНФОРМАЦІЇ

Наприкінці 80-х − початку 90-тих років минулого століття із загостренням конкурентної боротьби між суб'єктами приватного підприємництва, послабленням державного контролю за обігом спеціальної техніки в Україні активізувалосьнезаконне використання технічних засобів для негласного отримання інформації. Небезпека використання технічних засобів для негласного здобування інформації у приватних інтересах стала однією з причин прийняття в 2001 р. статті 359 Кримінального кодексу України (далі − ККУ) "Незаконне використання спеціальних технічних засобів негласного отримання інформації". Але на той час спеціальні технічні засоби (далі − СТЗ) визначались національним законодавством як "технічні засоби, устаткування, апаратура, прилади, пристрої, препарати та інші вироби, спеціально створені, розроблені, запрограмовані або модернізовані для виконання завдань з негласного отримання інформації під час здійснення оперативно-розшукової діяльності". Тобто, злочин за ст. 359 ККУ передбачав спеціального суб`єкта, а саме, співробітників оперативно-розшукових

підрозділів. Після усвідомлення цього, зважаючи на спорадичність незаконного застосування СТЗ співробітниками оперативно-розшукових підрозділів, у правоохоронців виникла ідея поширити чинність статті 359 ККУ на інших осіб, які незаконно використовують технічні засоби для негласного отримання інформації. Для цього у січні 2011 р. змінено визначення СТЗ, що отримало наступну редакцію: “спеціальні технічні засоби – технічні, програмні засоби, устаткування, апаратура, прилади, пристрої, препарати та інші вироби, призначені (спеціально розроблені, виготовлені, запрограмовані, пристосовані) для негласного отримання інформації”. Проте, на наш погляд, з розширенням сфери дії статті 359 ККУ було знівельовано саму ідею, заради якої до законодавства уведено категорію СТЗ.

Маємо підстави стверджувати, що ця ідея полягала у забезпеченні допустимості до використання у кримінальному судочинстві фактичних даних про злочин, отриманих під час проведення правоохоронних заходів за допомогою технічних засобів.

Пригадаємо, що до кінця 80-х років минулого століття у кримінальному судочинстві не допускалось використання матеріалів, здобутих під час оперативних заходів за допомогою технічних засобів, оскільки зазначені заходи і засоби їх проведення мали секретний характер.

Ситуація змінилася з прийняттям 12 червня 1990 р. Основ кримінального судочинства Союзу РСР і союзних республік. Стаття 29 цього нормативно-правового акту передбачала застосування технічних засобів для виявлення фактичних даних, які могли б бути використані як докази у кримінальній справі після їх перевірки відповідно до кримінально-процесуального законодавства. Право оперативно-розшукового підрозділу застосовувати технічні засоби для пошуку та фіксації фактичних даних про підготовку чи вчинення злочину в інтересах кримінального судочинства було підтверджене у 1992 р. Законом України “Про оперативно-розшукову діяльність”, яким офіційно засвідчено існування ОРД в Україні. У зв’язку з

тим, що основною умовою використання результатів ОРД для доказування у кримінальній справі є прозорість їхнього формування, їх фіксація законними методами й засобами, вказані зміни у законодавстві потягли за собою необхідність часткового “розсекречування” оперативно-розшукових заходів і техніки з наданням їм статусу законного інструменту правоохоронного органу. Це завдання було вирішене шляхом уведення до Закону України “Про оперативно-розшукову діяльність” статті 8 з переліком оперативно-розшукових заходів, та затвердження “Ліцензійних умов…”[1], де визначались термін та різновиди СТЗ, в основному співставлені оперативно-розшуковим заходам.

Тепер же, після прийняття “Ліцензійних умов…” у новій редакції[2], в якій докорінно змінено визначення СТЗ і вилучено перелік їх категорій,нормотворецьпо факту відмовився від вихідної ідеї, оскільки тепер визначенню СТЗ відповідають будь-які технічні засоби негласного отримання інформації, а не лише призначені для проведення оперативно-розшукових заходів і негласних слідчих (розшукових) дій. Наприклад, окрім СТЗ, у законодавстві України згадується інша категорія технічних засобів негласного отримання інформації, – “технічні засоби розвідки”. Останні не призначені для отримання фактичних даних про злочин, оскільки слугують інструментом розвідувальної, а не оперативно-розшукової діяльності і кримінального провадження. Відповідно, вони не забезпечують повноти отриманої інформації про діяльність особи, яка підозрюється у можливій причетності до готування чи скоєння злочину, її належності до предмету доказування, через що їх не потрібно визначати у відкритих актах

[1]Ліцензійні умови провадження господарської діяльності з розроблення, виготовлення спеціальних технічних засобів для зняття інформації з каналів зв’язку, інших засобів негласного отримання інформації, торгівлі спеціальними технічними засобами для зняття інформації з каналів зв’язку, іншими засобами негласного отримання інформації, затверджені спільним наказом Державного комітета України з питань регуляторної політики та підприємництва та СБ України від 29.01.2001№ 17/17.

[2]Ліцензійні умови провадження господарської діяльності з розроблення, виготовлення спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації, торгівлі спеціальними технічними засобами для зняття інформації з каналів зв'язку, іншими засобами негласного отримання інформації, затверджені Наказом Центрального управління Служби безпеки України від 30.01.2011 № 35.

законодавства. У зв`язку з цим виникли суперечності між декількома актами національного законодавства: "Ліцензійні умови…" дають підстави стверджувати, що технічні засоби розвідки (ТЗР) – це різновид СТЗ, і тому на суб`єктів їх протиправного використання може поширюватись ст. 359 ККУ. Натомість, із Закону України "Про розвідувальні органи" випливає, що СТЗ і ТЗР – зовсім різні категорії технічних засобів, через що на суб`єктів протиправного використання ТЗР чинність ст. 359 ККУ не поширюється.

Внаслідок виявлених суперечностей, віднесення певних технічних засобів до категорії СТЗ віддано на розсуд судовим експертам. Керуючись спеціально розробленою методикою[3], експерт відносить досліджуваний об'єкт до СТЗ не за конкретними показниками певних параметрів, а за результатами суб'єктивної оцінки кожної характеристики. Зокрема, для СТЗ негласного отримання та реєстрації аудіоінформації встановлено 11 характеристик, що потребують оцінки, для СТЗ негласного візуального спостереження та фото-, теле-, відеодокументування − 14 характеристик. Наприклад, засіб відеоспостереження з мініатюрним "вічком" вважатиметься СТЗ, з великим – ні.

Ми ж вважаємо, що мініатюризація і універсалізація технічних засобів оброблення інформації є результатом невпинного науково-технічного прогресу. Намагання визначити чіткі технічні критерії для виокремлення СТЗ є, на наш погляд, спробою стати поперек науково-технічного прогресу, – через 5-10 років (а, можливо, і раніше) ці критерії застаріють. До того ж вони невідомі у країнах-основних виробниках так званих "СТЗ", – КНР, на Тайвані тощо.

Окрім того, запропонована класифікація технічних засобів за "технічними" ознаками призвела до неочікуваних її ініціаторами наслідків, насамперед, порушення принципу справедливості правосуддя і рівності усіх

[3]Віднесення об'єктів до спеціальних технічних засобів негласного отримання інформації. Загальна методика. − К. : УНДІСТ СБ України. − 2011 р. − 26 с.

учасників судового процесу перед законом і судом. Для ілюстрації цього висновку наведемо декілька прикладів.

Уявімо собі, що на відкритій лекції з української філології в університеті поряд сидять два студенти. Один конспектує лекцію у зошиті за допомогою ручки SY-119 і одночасно фіксує виступ викладача на вбудований у цю ручку диктофон. Другий конспектує текст ручкою, а виступ викладача записує за допомогою звичайного мініатюрного репортерського диктофону чи навіть MP3-плейєра. Перший студент підлягає кримінальній відповідальності за ст.359 ККУ, оскільки ручка з диктофоном, на думку експертів СБУ, є СТЗ, другий – ні. Водночас, дії обох не становлять суспільної небезпеки, оскільки спрямовані на збирання відкритої інформації.

Інший приклад. Пересилання у бандеролі окремо ручки і диктофону не є злочином, а ручки з вбудованим диктофоном кваліфікується як злочин за ст.359.

Не дивно, що Інтернет переповнений наріканнями як на законодавців, так і на виконавця – СБ України, яка застосовує ст.359 ККУ у численних випадках, схожих з наведеними прикладами. Зокрема, відомий факт притягнення до кримінальної відповідальності за ст.359 ККУ батька, який контролював поведінку своєї дитини за допомогою так званої “радіоняні”, котра за формальними ознаками потрапляє у категорію СТЗ, або спроба притягнути до кримінальної відповідальності мисливця, який тренував свого собаку полювати на качок за допомогою мініатюрної відеокамери, вбудованої в ошийник.

Причиною цих негараздів стало, на наш погляд, ігнорування нормотворцем визначальної умови настання кримінальної відповідальності за застосування технічних засобів для негласного отримання інформації. Нами обгрунтовано, що кримінальна відповідальність повинна наступати за збирання інформації з обмеженим доступом (державної таємниці, службової інформації, комерційної і банківської таємниці, конфіденційної інформації

про особу тощо – далі ІзОД) шляхом несанкціонованого власником ІзОД впровадження технічних засобів у простір, де ним контролюються оброблення ІзОД і доступ до неї. У діяльності з технічного захисту інформації цей простір іменується “контрольованою зоною”. Несанкціоноване отримання інформації у “контрольованій зоні” за допомогою негласно впроваджених до неї технічних засобів за різних обставин може кваліфікуватись як злочин за статтями 111, 114, 162, 231, 182 або 330 ККУ. При чому для їх кваліфікації як злочинних категорія технічного засобу (побутова техніка, СТЗ і т.д.) не має значення. Наприклад, якщо мініатюрний “петличний радіомікрофон”, що застосовується дикторами телебачення і не є СТЗ, буде конспіративно впроваджено у житло без дозволу його власника для прослуховування приватних розмов, то має місце злочин, передбачений ст.182 ККУ “Порушення недоторканості приватного життя”.

І навпаки, кримінальна відповідальність не може наступати за застосування будь-яких технічних засобів для негласного збирання відкритої інформації у публічних місцях. У цьому випадку мова може йти тільки про відповідальність за порушення умов поводження з технічними засобами, вилученими в Україні з власності громадян, громадських об’єднань, міжнародних організацій та юридичних осіб інших держав, або порушення визначених законом повноважень. Наприклад, технічний засіб, засекречений в Україні, повинен бути вилучений в особи, яка не має допуску до держтаємниці, а посадовець, що допустив потрапляння цього засобу у користування вказаної особи, притягається до кримінальної відповідальності за розголошення відомостей, що становлять державну таємницю (ст.328 ККУ).У СРСР іноземних дипломатів-розвідників, затриманих “на гарячому” за застосування технічних засобів розвідки для отримання розвідувальної інформації у публічних місцях (фотографування військових об’єктів з позицій поза їх межами, перехоплення у радіоефірі сигналів радіостанцій або радіотехнічних засобів) оголошували персонами “нон грата” за діяльність, несумісну з дипломатичним статусом, а не за шпигунство.

Тому ми пропонуємо повернути до “Ліцензійних умов…” попереднє визначення терміну “спеціальні технічні засоби” та їх класифікацію з чітким співставленням їх негласним слідчим (розшуковим) діям та оперативно-розшуковим заходам, що необхідно для забезпечення допустимості використання у кримінальному судочинстві фактичних даних про злочин, отриманих за допомогою технічних засобів. Зважаючи на особливу суспільну небезпеку безконтрольного використання технічних засобів, спеціально призначених для конспіративного здобування інформації під час оперативно-розшукової, розвідувальної і контррозвідувіальної діяльності, ст. 359 можливо залишити у Кримінальному кодексі та у підслідності СБУ, але її чинність повинна, як і раніше, поширюватись виключно на спеціальних суб’єктів, тобто, фізичних осіб, причетних до розроблення, виготовлення, продажу, використання спеціальних технічних засобів, з доповненням предмету цієї статті незаконним розробленням, виготовленням, продажом, використанням технічних засобів розвідки, що у теперішній час не ліцензуються, і, відповідно, не контролюються державою.

Література:

1. Логінов І.В. Поняття, класифікація та співвідношення спеціальної техніки і спеціальних технічних засобів // Державна безпека України. Науково-практичний збірник. - К., НАН України, СБ України. - 2010. -№ 20. - с.79-87.
2. Логінов І.В. Кримінальна відповідальність за незаконне використання технічних засобів, які можуть задіюватись у негласному отриманні інформації. // Науковий вісник- К.: НА СБ України. - 2011. - № 39. - С. 131-143.
3. Логінов І.В. Тищенко Є.Ф. Окремі негативні аспекти практики застосування статті 359 Кримінального кодексу України // Збірник наукових праць - К.: НА СБ України. - 2013. - № 46. - СІ 19-127.
4. Логінов І.В. Визначення терміну "спеціальні технічні засоби"/ Актуальні проблеми оперативно-розшукової діяльності правоохоронних органів у сучасних умовах: матеріали міжвідомчої науково-практичної конференції, 19 травня 2011 року. - К. - 2011. — с. 98-103.

----------***----------

О. Г.Семенюк,
к.ю.н., заступник начальника
Управління, Служба безпеки України

ОКРЕМІ ПРОБЛЕМИ ЗАСТОСУВАННЯ КРИМІНАЛЬНОГО ЗАКОНОДАВСТВА У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ

Вагомою частиною складного механізму превенції є кримінальне покарання. Виконання зазначеної ролі здійснюється як за допомогою загрози покарання, яка міститься в санкції правової норми Особливої частини Кримінального кодексу України, так і шляхом його реалізації, тобто примусового впливу на осіб, вже визнаних винними у вчиненні злочину.

Одним зі свідоцтв високого рівня кримінального законодавства є його стабільність, незмінність основних принципових положень і приписів. Водночас, залишаючись стабільним, кримінально-правові норми повинні ефективно реагувати на ті зміни, які відбуваються в політичних, соціально-економічних умовах життя суспільства і держави, адекватно відповідати на будь-які нові суспільно небезпечні виклики з боку злочинного середовища.

Практика застосування статей 111, 114, 328, 329, 422 Кримінального кодексу України, якими встановлено кримінально-правову заборону діянь, пов’язаних з посяганням на державну таємницю, висвітлила невідповідність оцінки цієї поведінки соціальним, економічним, політичним і правовим змінам, що відбулися останнім часом в суспільстві.

Так, закріплене на даний час у КК розмежування відповідальності за одні й ті саме дії (за шпигунство) порушує закріплений у ст.24 Конституції України принцип рівності громадян перед законом. На даний час громадяни України за державну зраду у формі шпигунстванесуть більш суворе покарання (від десяти до п’ятнадцяти років), ніж іноземні громадяни та особи без громадянства, які вчинили шпигунство (від восьми до п’ятнадцяти років).

Чинний закон про кримінальну відповідальність не робить різниці між умисним і необережним розголошенням державної таємниці (ст.328 КК) та передбачає відповідальність за ці різні за ступенем суспільної небезпечності

діяння в межах однієї правової норми. Отже суб'єктивна сторона цього злочину характеризується як умисною, так і необережною формами вини.

Суб'єктом розголошення державної таємниці (ст. 328 КК) може бути фізична осудна особа, якій до вчинення даного злочину виповнилося 16 років і якій ці відомості були довірені або стали відомими у зв'язку з виконанням службових обов'язків (спеціальний суб'єкт). Порядок отримання допуску та доступу до державної таємниці та перелік підстав для цього тривалий час залишалися незмінними і питань щодо суб'єкта відповідальності за цей злочин не виникало.

У 2010 році до ст.27 Закону України «Про державну таємницю» було внесено зміни та унормовано окремий порядок надання доступу до державної таємниці без попереднього отримання відповідного допуску особам, залученим до конфіденційного співробітництва з оперативними підрозділами правоохоронних та інших спеціально уповноважених органів, які проводять оперативно-розшукову, розвідувальну або контррозвідувальну діяльність. Крім цього, з прийняттям у 2012 році Кримінального процесуального кодексу України була запроваджена процедура, відповідно до якої підозрюваний чи обвинувачений бере участь у кримінальному провадженні без оформлення допуску до державної таємниці після роз'яснення йому вимог статті 28 Закону України «Про державну таємницю» та попередження про кримінальну відповідальність за розголошення відомостей, що становлять державну таємницю (пункт 3 статті 517 КПК).

Оскільки зазначені підстави отримання доступу до державної таємниці не пов'язані із виконанням службових обов'язків, то у разі розголошення таких відомостей цими суб'єктами, вони не підпадають під дію ст.328 КК.

Так само за межами кримінальної відповідальності залишаються особи, які, в порушення встановленого порядку отримання доступу до державної таємниці, умисно заволоділи такими відомостями без мети їх передачі іноземній державі, іноземній організації або їх представникам.

На даний час, коли володіння певним видом інформації стає джерелом отримання прибутку, окремі особи цілеспрямовано намагаються отримати доступ до державної таємниці та вживають для цього найрізноманітніші способи, включаючи підкуп, шантаж, вимагання, розбійний напад, викрадення (в т.ч. із застосуванням технічних засобів) та ін. Такий протиправний обіг секретної інформації перетворюється на злочинний бізнес.

Хоча ці дії не вважаються суспільно небезпечними та кримінально караними, загроза охоронюваним державою інтересам від цього не зменшується, так як незалежно від їх мотивації отримана у такий спосіб інформація буде використана на шкоду інтересам держави.

Нерідко секретна інформація потрапляє у володіння сторонніх осіб без попереднього умислу на її заволодіння. Розголошення або оприлюднення випадково підслуханої (побаченої) секретної інформації або відомостей, які містилися у знайдених матеріальних носіях такої інформації, виключають кримінальну відповідальність суб'єкта, якому вона стала відомою випадково, тобто без будь-яких намірів з його боку (в подальшому щодо таких суб'єктів пропонується застосовувати термін «випадковий розпорядник»). Водночас, незалежно від того, у який спосіб секретна інформація стала відомою певній особі, її подальше використання на шкоду охоронюваних інтересам становить суспільну небезпеку. Тому у разі усвідомлення випадковим розпорядником характеру відомостей, що стали йому відомі, такі його дії мають кваліфікуватися як злочин. У цьому випадку суспільна небезпечність такого діяння визначається не лише зовнішніми, фактичними, об'єктивними обставинами, а в більшій мірі суб'єктивними, так як усвідомлення можливості завдання шкоди суспільним інтересам дає всі підстави для визнання вини структурним елементом суспільної небезпечності такого діяння.

Наступним наочним прикладом несвоєчасного реагування КК на зміни, що відбулися у законодавстві про державну таємницю, є наявність у КК

статті 422. Дана стаття встановлює кримінальну відповідальність за розголошення відомостей військового характеру, що становлять державну таємницю, або втрату документів чи матеріалів, що містять такі відомості. Проте Закон України «Про державну таємницю», який встановлює вичерпний перелік інформації, що може бути віднесена до державної таємниці, не містить такого поняття, як відомості військового характеру. Зокрема, відповідно до ст. 8 цього Закону, до державної таємниці відноситься інформація: 1) у сфері оборони; 2) у сфері економіки, науки і техніки; 3) у сфері зовнішніх відносин; 4) у сфері державної безпеки та охорони правопорядку.

Таким чином КК встановлює відповідальність за злочин, який вчинений бути не може в зв'язку з відсутністю у сфері суспільних відносин предмету злочину – відомостей військового характеру, що становлять державну таємницю.

З урахуванням конституційного гарантування державою безпеки особистості, суспільства та держави, а також з метою формування єдиного механізму кримінально-правового захисту різних видів таємної інформації, нами пропонується ввести до юридичного обігу поняття «***чужа таємниця***» та відмовитися від диференціації відповідальності за завдання шкоди інтересам її власників внаслідок несанкціонованого витоку такої інформації. Термін «чужа таємниця» має охоплювати всі види таємної інформації, а саме таємницю фізичної особи, комерційну та державну таємниці(всі інші види таємниць – це лише похідні від зазначених).

Така позиція ґрунтується на тому, що юридичні закони поступово втрачають колишню жорстокість своїх кордонів щодо ухилу у захисті на бік інтересів держави та переорієнтовуються на найвищу соціальну цінність – людину.

На наше переконання, спроба окремих науковців обґрунтувати найбільшу суспільну цінність державної таємниці – це намагання виправдати ситуацію, за якої держава безконтрольна в питаннях засекречування

інформації, а ця сфера державно-владних повноважень виконує не тільки функцію охорони певних категорій відомостей від поширення, але й набуває політичного відтінку, перетворюючись в один із істотних елементів у механізмі державного управління.

Нашій нещодавній історії ще пам'ятна ситуація, коли державна власність визнавалася більш важливою цінністю, ніж особиста (приватна). Так, за Кримінальним кодексом УРСР 1961 року розкрадання державного або суспільного майна в особливо великих розмірах (стаття 86-1) каралося позбавленням волі на строк від десяти до п'ятнадцяти років з конфіскацією майна та із засланням на строк до п'яти років або смертною карою з конфіскацією майна. В той же час, за крадіжку індивідуального майна, яка завдала значної шкоди потерпілому або вчинену за попередньою змовою групою осіб або повторно (частина друга статті 140), призначалося покарання у вигляді позбавлення волі на строк до п'яти років з конфіскацією майна або без конфіскації.

Із прийняттям у 1991 році Закону України «Про власність» приватна, колективна та державна форми власності були визнані рівноправними. Стаття 13 Конституції України проголосила рівність усіх суб'єктів права власності перед законом і забезпечення захисту їх прав державою. КК України 2001 року відмовився від розмежування відповідальності за протиправні посягання на різні форми власності та встановив кримінальну відповідальність за крадіжку ***чужого майна*** (стаття 185), чим фактично урівняв соціальну цінність усіх форм власності.

Саме в напрямку уніфікації підходів до кримінального переслідування й покарання винних за протиправні посягання на відносини, що забезпечують збереження найбільш цінної для її власників інформації у таємниці, має просуватися кримінальне законодавство України.

При цьому кримінальна відповідальність має встановлюватися за:

- протиправне заволодіння чужою таємницею(кваліфікуючими ознаками цього злочину має бути вчинення таких дій із застосуванням

насильства або погрозою його застосування, за попередньою змовою групою осіб, з проникненням у житло або інше приміщення, завдання значної шкоди потерпілому);

- умисне (свідоме) розголошення чужої таємниці (кваліфікуючими ознаками цього злочину має бути вчинення таких дій із корисливих мотивів та завдання значної шкоди власнику таємної інформації);

- необережне розголошення чужої таємниці або втрата матеріальних носіїв інформації, що містять чужу таємницю, якщо такі дії призвели до завдання значної шкоди власнику такої інформації.

- використання чужої таємниці, якщо такі дії призвели до завдання значної шкоди інтересам її власника.

----------***----------

УДК 340.14

В. П. Колонюк,
к.ю.н., доцент, учений секретар КНДІСЕ МЮ України,
Ю.Б. Форіс,
науковий співробітник КНДІСЕ МЮ України

СУДОВО-ЕКСПЕРТНЕ ПРАВО НА ЗАХИСТІ ВІД ПРАВОПОРУШЕНЬ В ІНФОРМАЦІЙНІЙ СФЕРІ

Судово-експертне право як система норм, що забезпечують провадження судово-експертної діяльності, існує на практиці, але теоретичне обґрунтування його існування в системі правових наук, дисциплін, галузей вже понад десять років залишається дискусійним моментом в юридичній і спеціальній літературі. Вперше цей термін застосовано у науково-дослідній роботі, яка проводилась у Київському науково-дослідному інституті судових експертиз Міністерства юстиції України під керівництвом доктора юридичних наук, професора, академіка Академії правових наук України Михайла Яковича Сегая наприкінці дев’яностих років минулого сторіччя – початку двохтисячних років. В процесі цієї розробки вийшло декілька

публікацій: «Судебная экспертология: объект, предмет, природа и система науки»[1]та «О формировании судебно-экспертного права: постановка проблемы» [2], де вперше викладені концепції судової експертології в цілому та судово-експертного права як її частини.

Судово-експертна діяльність спрямована на забезпечення правосуддя незалежною, об'єктивною, кваліфікованою, науково обґрунтованою та проведеною на належному технічному рівні судовою експертизою, а також на розробку відповідних, необхідних для реалізації основної мети, засобів: методів, методик, довідкових джерел, обладнання тощо. У тому числі, засобів, необхідних і для профілактики правопорушень, виходячи з досвіду судово-експертних досліджень та спеціальних знань судових експертів. Судово-експертна діяльність складається з власне експертної, науково-дослідної і науково-методичної діяльності. Ці три блоки охоплюють як провадження судових експертиз, так і їх забезпечення методичною і довідковою базою спеціальних знань, а також полегшують (науково-методичний блок) застосування спеціальних знань у формі судової експертизи всім зацікавленим у ній особам: суддям, слідчим, адвокатам, громадянам – учасникам судового процесу, особам, які мають намір стати судовими експертами тощо.

Не слід плутати складові судово-експертної діяльності з точки зору судової експертології – науки про судово-експертну діяльність, концепція якої репрезентована у наведеній вище публікації академіка М. Я. Сегая, і складові судово-експертної діяльності з точки зору практичної діяльності судово-експертних установ і їх працівників.

Так, М. Я. Сегай виділив чотири блоки судово-експертної діяльності (далі – СЕД):

1) діяльність держави з правового забезпечення СЕД на законодавчому й відомчому нормативно-правовому щаблях;

2) діяльність державних органів виконавчої влади, які здійснюють функцію управління СЕД;

3) діяльність головних суб'єктів СЕД, які забезпечують організацію і проведення судових експертиз в державних судово-експертних установах;

4) діяльність учасників судочинства, причетних до проведення судових експертиз.

Таким чином, третьому блоку СЕД за концепцією М. Я. Сегая (діяльність головних суб'єктів СЕД, які забезпечують організацію і проведення судових експертиз в державних судово-експертних установах) відповідає поділ СЕД на судово-експертну, науково-дослідну і науково-методичну діяльність.

Першому блоку СЕД за концепцією М. Я. Сегая відповідає судово-експертне право: система загальнообов'язкових комплексних норм (правил), що регулюють відносини у сфері зайняття судово-експертною діяльністю, встановлюються і охороняються державою (детальніше ця концепція викладена у статті «Судово-експертне право: поняття, предмет, система», яка планується до публікації у міжвідомчому науково-методичному збірнику «Криміналістика і судова експертиза», а стислий зміст цієї концепції «Поняття судово-експертного права» доповідався на круглому столі «Судово-експертна діяльність: сучасний стан та перспективи розвитку» в Навчально-науковому інституті підготовки фахівців для експертно-криміналістичних підрозділів Національної академії внутрішніх справ у 2015 році)[3].

В цілому до судово-експертного права можна віднести такі нормативно-правові акти:

1) Конституція України;

2) Закон України «Про судову експертизу»;

3) Чинні в установленому порядку двосторонні та багатосторонні міжнародні договори між Україною та країнами близького і далекого зарубіжжя, укладені на їх підставі міжнародні міжвідомчі угоди в галузі судочинства і судової експертизи;

4) Кодекс законів про працю України, Цивільний кодекс України, Господарський кодекс України, Кримінальний кодекс України, Кримінальний процесуальний кодекс України, Цивільний процесуальний кодекс України, Кодекс адміністративного судочинства України, Господарський процесуальний кодекс України, Кодекс України про адміністративні правопорушення, Митний кодекс України, Закон України про виконавче провадження;

5) Постанови Кабінету Міністрів України, що регулюють окремі аспекти судово-експертної діяльності, зокрема, статус науковців, які виконують науково-дослідні роботи в галузі судової експертизи, класи судових експертів, відшкодування вартості проведення судових експертиз і відряджень до місця огляду чи місця здійснення правосуддя тощо;

6) Накази та розпорядження міністерств і відомств, які мають у своєму підпорядкуванні судово-експертні установи, що стосуються їх діяльності, та затверджені ними положення, інструкції тощо;

7) Накази та розпорядження керівників судово-експертних установ та затверджені ними положення, інструкції тощо,

причому норми кодифікованих законів, які класифікуються відповідно до сучасних підстав як процесуальні, для судового експерта належать до норм матеріального права, оскільки визначають його статус, права, обов’язки, підстави для відповідальності, алгоритми його дій тощо не тільки у відповідному виді судочинства, але і в узагальненому вигляді як його загальноправова «посадова інструкція», закріплена на рівні закону.

В світлі теми науково-практичної конференції «Теорія і практика юридичної відповідальності за правопорушення в інформаційній сфері» судово-експертне право може бути застосовано при настанні юридичної відповідальності за правопорушення в інформаційній сфері як засіб доказування складу правопорушення (висновок судового експерта) і для захисту від правопорушень в інформаційній сфері (судово-експертна профілактика).

До таких засобів у судово-експертному праві належать:

1) державний Реєстр методик судових експертиз;

2) переліки рекомендованої науково-технічної та довідкової літератури, що використовується під час проведення судових експертиз, затверджені Наказом Міністерства юстиції України від 30 липня 2010 року № 1722/5, які постійно оновлюються, змінюються та доповнюються;

3) Інструкція про призначення та проведення судових експертиз та експертних досліджень та Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень, затверджені Наказом Міністерства юстиції України від 8 жовтня 1998 року № 53/5, Зареєстровано в Міністерстві юстиції України 3 листопада 1998 р. за № 705/3145, які постійно оновлюються, змінюються та доповнюються.

Доказова цінність висновків експерта залежить від його логічної форми. У літературі з судової експертизи наведено такі класифікації висновків за цією підставою: а) за змістом предмета твердження: висновки про індивідуальний об'єкт або родову (групову) належність; вони можуть бути категоричними чи ймовірними; б) за наявністю (відсутністю) логічних союзів – альтернативні й однозначні, а також умовні й безумовні; в) за якістю зв'язку: стверджувальні та негативні [4].

Ніякі докази не мають заздалегідь встановленої сили, і тому висновок експерта не має переваг перед іншими доказами. Погляди на експертизу як на «особливий» доказ, а на експерта – як на наукового суддю належать Л. Є. Владімірову, який вважав, що судді не можуть критично ставитися до експертизи, бо для її розуміння треба набувати декілька років наукових занять. Їм залишається тільки слідувати авторитетним вказівкам експертів. Суд є самостійним в обранні експертів. Але оскільки останні «обрані», суддя йде услід за ними, як «сліпий за своїм поводирем» [5]. Дореволюційна концепція експерта як наукового судді суперечить принципу вільного оцінювання доказів. Проте в спеціальній літературі залишається думка про висновок експерта як особливе джерело доказів.

Порівняно з іншими доказами висновок експерта має специфічні риси, зумовлені його сутністю:

– він формулюється на основі використання спеціальних знань;

– є вивідним знанням, а не інформативним, як інші особисті докази (показання), знання.

У висновку доказове значення має передусім розумовий умовивід експерта, якого він дійшов за результатами дослідження [6].

Одночасно судова експертиза самим фактом свого існування стримує розвиток злочинності та інші види правопорушень, в тому числі в інформаційній сфері, оскільки наука дозволяє довести ті обставини, які були б «невловимими» без застосування спеціальних знань.

В інформаційній сфері проводиться досить широкий спектр судових експертиз: комп'ютерно-технічні, телекомунікаційні, інтелектуальної власності, товарознавчі (в широкому сенсі, з різновидами), економічні, психологічні, оціночно-земельні та оціночно-будівельні, мистецтвознавчі тощо.

Отже, судова експертиза, судово-експертна діяльність як більш широке поняття і її правове забезпечення – судово-експертне право, стоять на захисті від правопорушень в інформаційній сфері.

Література:

1. Сегай М. Я. Судебная экспертология: объект, предмет, природа и система науки / М. Я. Сегай, доктор юридических наук, профессор, академик Академии Правовых наук Украины // В зб. «Теорія та практика судової експертизи і криміналістики», Вип. 3. – Харків: Право, 2003. – С. 25-32.
2. Форис Ю. Б. О формировании судебно-экспертного права: постановка проблемы / Ю. Б. Форис // В зб. «Теорія та практика судової експертизи і криміналістики», Вип. 3. – Харків: Право, 2003. – С. 45-48.
3. Форіс Ю. Б. Поняття судово-експертного права / Ю. Б. Форіс // В зб. «Судово-експертна діяльність: сучасний стан та перспективи розвитку: збірник матеріалів круглого столу». / редкол.: Кобилянський О. Л., Антонюк П. Є., Свобода Є. Ю.; Київ. ННІПФЕКП НАВС. – К.: Навчально-науковий інститут підготовки фахівців для експертно-криміналістичних підрозділів Національної академії внутрішніх справ, 2015. – 444 с. – С. 356-358.

4. Орлов Ю. К. Заключение эксперта и его оценка по уголовным делам / Ю. К. Орлов. – М. : Юрист, 1995. – С. 16–18.
5. Владимиров Л. Е. Учение об уголовных доказательствах / Л. Е. Владимиров. – СПб. : Законоведение, 1910. – С. 197.
6. Клименко Н. І. Структура і доказове значення висновку експерта як документа, що відображує його дослідження / Н. І. Клименко, В. П. Колонюк // Теорія та практика судової експертизи і криміналістики. – 2009. – № 9. – С. 213-221.

----------***----------

Є. В. Тимко, О. В.Закс

МОЖЛИВОСТІ СУДОВОЇ ЕКСПЕРТИЗИ КОМП'ЮТЕРНОЇ ТЕХНІКИ ТА ПРОГРАМНИХ ПРОДУКТІВ ПРИ РОЗСЛІДУВАННІ ЗЛОЧИНІВ, ЯКІ ВИНИКАЮТЬ В ІНФОРМАЦІЙНІЙ СФЕРІ

В даний час пріоритет боротьби зі злочинами у сфері інформаційних технологій займає третє місце в США, після тероризму та контррозвідки.

В Україні до недавнього часу вважалося, що комп’ютерна злочинність явище, яке властиве тільки закордонним країнам, і через слабку комп’ютеризацію нашого суспільства, відсутня взагалі. Саме ця обставина і призвела до відсутності серйозних наукових досліджень цієї проблеми.

Як нерідко траплялося раніше, боротьба з окремим видом злочинності починається лише тоді, коли матеріальні втрати від неї досягають значних розмірів і починають різко виділятися на загальному тлі втрат від вже звичних для нас злочинів.

Комп'ютеризація сучасного українського суспільства зачіпає практично всі сторони діяльності людей, підприємств, організацій, держави і як наслідок породжує нову сферу суспільних відносин, яка на жаль, нерідко тепер стає об'єктом протиправних дій. Стрімкий розвиток науково-технічного прогресу торкнувся і нашої держави, і зумовив необхідність боротьби зі злочинами у сфері комп'ютерної інформації.

Скоюючи злочин, злочинець як правило завжди залишає сліди своєї діяльності, і комп'ютерні злочини не є виключенням із цього правила, однак для зібрання доказів з комп'ютерного злочину необхідно залучати фахівців, які можуть знайти ці докази, або підтвердити певні факти чи дії.

Електронні докази часто відіграють значну роль у розслідуванні кримінальних, господарських та цивільних справах, і саме вони у більшості випадків дозволяють дати відповідь на поставлені питання. Так досить часто ставляться питання стосовно таких атрибутів: як дата створення, час обробки, яким чином було перенесено інформацію до комп'ютера.

В слідчій практиці перше питання нерідко розподіляється на два: стосовно актуальної та недоступної засобами операційної системи, як часто-густо кажуть та пишуть слідчі – „видаленої" інформації. Атрибуція інформації на поточний час досить активно розвивається і має як „популярні" напрямки, інтуїтивно зрозумілі слідчим, такі, як, наприклад, встановлення дати/часу створення певних документів, так й рідкі до унікальності дослідження, в яких вирішуються питання стосовно послідовності певних дій, застосування певних програмних продуктів чи їх версій, фальсифікації службових даних операційних систем чи прикладного програмного забезпечення.

Крім того досить частоінформацію, яка має досить суттєве значення для вирішення питань справиможливо знайтив месседжерах, поштових клієнтах у вигляді отриманих та відправлених електронних повідомлень, відвіданих сайтів і вжитих ключових словах в пошукових системах, які в свою чергу потрапляють до файлів журналювання браузерів.

В більшості розслідувань аналіз історії активності користувача в мережі часто дає деякі зачіпки, які дозволяють провести аналіз та відновити значний відсоток інформації. Для проведення аналізу використовується як

комерційне так і безкоштовне (open source) програмне забезпечення для аналізу даних.

В якості досліджуваних об’єктів виступають цифрові пристрої або файлові структури, які могли бути використані для злочину чи містять в собі сліди цього злочину.

Крім того цифровий пристрій може бути використаний для здійснення фізичного злочину або може бути джерелом дії, яка порушує закон. Так в першому випадку: підозрюваний збирає в Інтернеті інформацію для підготовки фізичного злочину, а в другому випадку можливо виділити отримання несанкціонованого доступу до комп’ютера, завантаження незаконного матеріалу чи шкідливого програмного забезпечення через мережу або відправка його на електронні адреси, з метою вчинення певних дій (погроз чи розповсюдження шкідливого ПЗ).

Шкідливе програмне забезпечення є невід'ємною частиною злочинів у інформаційній сфері. Сучасні програми, які використовуються зловмисниками, здатні виконувати різні завдання, починаючи від неправомірного копіювання конфіденційної інформації і закінчуючи організацією віддаленого управління персональним комп'ютером.

Для комплексного розслідування інциденту, в якому застосовувалося шкідливе програмне забезпечення, необхідне дослідження імовірно шкідливих програм з метою встановлення їх алгоритму, функціональних можливостей і здійснюваних мережевих взаємодій.

Злочини у сфері комп’ютерних технологій являють собою одне із складних антисоціальних явищ у суспільстві. Якісний підхід для розслідування злочинів, зокрема протиправних дій, пов'язаних з використанням комп’ютерних технологій – одне з ключових питань для будь-якої держави, у тому числі й для України. Міжнародний характер

протидії цьому феномену сучасності – запорука подальшої стабільності і розвитку всіх сфер людського буття.

Література:

1. Криминалистический анализ файлових систем. – СПб.: Питер, 2007. – 480 с.: ил., Кєрриє Б.
2. Методика дослідження комп'ютерної інформації № 10.9.04

----------***----------

І. М. Мейдич,
здобувач НА СБ України

КРИМІНАЛЬНО-ПРАВОВА ОХОРОНА СЛУЖБОВОЇ ІНФОРМАЦІЇ: ПІДХОДИ ДО УДОСКОНАЛЕННЯ

Службову інформацію як новий вид інформації з обмеженим доступом, запроваджено у 2011 р. Законом України «Про доступ до публічної інформації». В законодавстві вона, по суті, замінила «конфіденційну інформацію, що є власністю держави», залишивши незмінним ступінь обмеження доступу та відповідний гриф - «Для службового користування».

Визначення службової інформації в законодавстві України на сьогодні відсутнє. У ст. 9 Закону України «Про доступ до публічної інформації» подається лише перелік відомостей (до того ж не вичерпний) які можуть до неї належати, який не містить чітких критеріїв віднесення інформації до службової. Узагальнений Перелік відомостей, що становлять службову інформацію (на кшталт ЗВДТ) законодавством не передбачений. Відомості, що становлять службову інформацію у відомчих переліках визначаються без чіткої структуризації та недостатньо конкретно. Зазначені чинники не сприяють правильному встановленню службової інформації, як предмета кримінально-правової охорони.

Аналіз повноти, достатності та, зрештою, ефективності кримінально-правової охорони службової інформації та підходів законодавця до її реалізації дозволяє констатувати наступне:

1. За часів незалежності України кримінально-правова політика стосовно охорони державної інформації з обмеженим доступом, що не становить державної таємниці (ДСК), зокрема й службової інформації, характеризується перманентною непослідовністю та незавершеністю. Це неодноразово зумовлювало фактичне призупинення її кримінально-правової охорони, створювало реальні передумови до витоку відомостей з грифом «ДСК», а за їх сукупності, – й державної таємниці.

Так, у 1997 році було запроваджено «конфіденційну інформація, що є власністю держави», а її витік Концепцією національної безпеки України визнано однією із загроз національній безпеці в інформаційній сфері. Проте, оскільки предмет злочину, передбаченого ст. 68-1 (службова таємниця) чинного на той час КК України (1960 р.) відповідних змін не зазнав, до 1 вересня 2001 року, коли набрав чинності новий Кримінальний кодекс України, кримінально-правова охорона цієї інформації не мала правових підстав і фактично не здійснювалася. Подібна ситуація сталася й після запровадження у 2011 р. службової інформації, оскільки відповідні зміни до ст. 330 КК було прийнято лише у березні 2014 р.

2. На сьогодні, пори обмеження доступу та визнання можливості завдання шкоди від розголошення всієї службової інформації (має гриф «Для службового користування»), а також того, що будь-яка її сукупність може становити державну таємницю, кримінально-правова охорона здійснюється лише щодо її частини – відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни.

3. Ефективність кримінально-правової норми, що передбачає відповідальність за передачу або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни (ст. 330 КК) є низькою, оскільки її конструкція не забезпечує збереження всієї службової інформації, як інформації з обмеженим доступом; безпідставно звужує

суб'єкт злочину, що дозволяє безкарно вчиняти криміналізовані дії іншим (стороннім) особам; передбачає кваліфіковані ознаки злочину, що є нетиповими для вчинення криміналізованих посягань; санкція норми встановлює невиправдано жорстоке покарання.

4. Законодавцем криміналізовано (та й то – частково) лише передавання певної службової інформації іноземцям (ст. 330 КК) , тоді як кримінальна відповідальність за її розголошення та втрату носіїв не передбачена.

Таким чином кримінально-правову охорону службової інформації в Україні слід визнати неналежною.

Ґрунтовною проблемою удосконалення кримінально-правової охорони службової інформації є переосмислення її статусу як виду таємної інформації та закріплення в законодавстві її визначення, що значно сприятиме конкретизації предмету злочинних посягань.

Відтак, основними шляхами удосконалення кримінально-правової охорони службової інформації вважаємо такі:

- запровадження в законодавстві України категорії «службова таємниця», як частини державних секретів (або класифікованої (секретної) інформації – за стандартами НАТО та ЄС) з грифом обмеження доступу «Для службового користування» та «Таємно», визначення сфер діяльності держави, де здійснюється її обіг, процедури віднесення інформації до цієї категорії та конкретизації шкоди, що може бути завдана в результаті витоку цієї інформації, а також зазначення необхідності охорони державою;

- розширення предмета злочинів, передбачених статтями 114, 328, 339, 422 КК України, за рахунок службової таємниці з відповідною диференціацією покарання;

- передбачити кримінальну відповідальність за незаконне заволодіння (зберігання) відомостями, що становлять службову таємницю, за відсутності ознак шпигунства, та за незаконне використання таких відомостей.

----------***----------

УДК:342.9

Л.В.Секелик,
аспірант НДІІП НАПрН України

ПРОБЛЕМА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ РОЗМІЩЕННІ СУДОВИХ РІШЕНЬ В ЄДИНОМУ ДЕРЖАВНОМУ РЕЄСТРУ СУДОВИХ РІШЕНЬ

Європейська спільнота до якої прагне також увійти й Україна, вимагає не тільки захисту персональних даних, а й здійснення відкритого доступу до всіх судових рішень.

Саме у зв'язку з цим був прийнятий Закон України «Про доступ до судових рішень» від 22 грудня 2005 року N 3262-IV (надалі – Закон № 3262-IV).

Статтею 3 Закону № 3262-IV суд загальної юрисдикції вносить до Єдиного державного реєстру судових рішень: www.reyestr.court.gov.ua (надалі – Реєстр) всі судові рішення і окремі думки суддів, викладені у письмовій формі, не пізніше наступного дня після їх ухвалення або виготовлення повного тексту.

Закон України «Про інформацію» у ст.11 закріплює, що інформація про фізичну особу (персональні дані) – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Фактично поняття інформації про особу ототожнюється у ст.5 Закону України «Про захист персональних даних».

Передумовою нормативної регламентації поняття «інформації по фізичну особу (персональні дані)» в національному законодавстві України стала Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981р., у ст.2 якої також міститься визначення терміна «персональні дані». Під ними розуміють будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною.

Тої ж думки до дотримується й Конституційний Суд України, даючи офіційне тлумачення частин першої, другої статті 32 Конституції України (Рішення Конституційного Суду України від 20.01.2012 р. N 2-рп/2012 у справі за конституційним поданням Жашковского районної ради Черкаської області відносно офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України), вказав, що персональні дані про особу - це будь-які відомості або сукупність відомостей про фізичну особу, яку ідентифіковано або може бути конкретно ідентифіковано, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальне становище, адреса, дата і місце народження, місце проживання і знаходження і т.д., дані про особисті майнові і немайнові стосунки цієї особи з іншими особами, зокрема з членами сім'ї, а також відомості про події і явища, які відбувалися або відбуваються в побутовій, інтимній, товариській, професійній, діловій та в інших сферах життя особа, за винятком даних відносно виконання повноважень особи, що обіймає посаду, пов'язану із здійсненням функцій держави або органу місцевого самоврядування.

Закон № 3262-IV визначає, що не можуть бути розголошені відомості, що дають можливість ідентифікувати фізичну особу. До таких відомостей законодавець відносить:

- імена (ім'я, по батькові, прізвище) фізичних осіб;
- місце проживання або перебування фізичних осіб із зазначенням адреси, номери телефонів чи інших засобів зв'язку, адреси електронної пошти, ідентифікаційні номери (коди);
- реєстраційні номери транспортних засобів, реєстраційні відомості реєстрів нерухомого майна;
- номери банківських рахунків, номери платіжних карток;
- інша інформація, що дає можливість ідентифікувати фізичну особу.

Окрему увагу треба приділити пп.4 п. 2 ст. 7 Закону № 3262-IV: «4) інша інформація, що дає можливість ідентифікувати фізичну особу.». Таке нечітке формулювання «персональної інформації» призводить до поширення різноманітного тлумачення, які відомості дозволяють ідентифікувати фізичну особу, а які – ні.

Норми п. 1, 2 ст. 7 Закону № 3262-IV фактично суперечать Закону України «Про судоустрій та статус суддів» від 7 липня 2010 року N2453-VI (надалі – Закон №2453-VI) та нормам процесуального законодавства. Відповідно до ст. 11 Закону №2453-VI розгляд справ усудах відбувається відкрито, крім випадків, установленим законом. Ця норма отримує подальший розвиток у процесуальних кодексах. А саме ст. 4-4 Господарського процесуального кодексу України, ст. 6 Цивільного процесуального кодексу України, ст. 12 Кодексу адміністративного судочинства України, ст. 249 Кодексу України про адміністративні правопорушення, ст. 20 Кримінально-процесуального кодексу України та в інших нормах цих кодексів.

Таким чином постає проблема щодо захисту персональних даних та відкритості доступу до судового засідання.

Проте, як показує аналіз судових рішень наявних в Реєстрі, при викладенні судових рішень не здійснюється належний захист персональних даних. Наприклад, при винесенні рішення від 19.11.2013 року у справі № 385/1287/13-ц щодо поновлення особи на роботі, були замінені деякі данні, що ідентифікують позивача, а саме: прізвище, ім’я, по-батькові, проте залишені інші ідентифікуючі данні, а саме – посада та найменування роботодавця. Таким чином, за посадою та місцем роботи позивача можна легко ідентифікувати особу.

Загалом, чинне законодавство щодо доступу до судових рішень потребує суттєвих змін, оскільки:

- не містить механізмів притягнення до відповідальності уповноважених осіб держави за порушення Закону № 3262-IV;

- не регламентує важливі процедури здійснення Закону № 3262-IV;
- не вирішує питання протиріччя принципу гласності судового розгляду і видалення персональної інформації з судових рішень.

----------***----------

І. В.Солончук,
старший викладач кафедри
інформаційного права та права
інтелектуальної власності
ФСП НТУУ «КПІ»

ЗАКРИТИЙ СУДОВИЙ РОЗГЛЯД ЦИВІЛЬНОЇ СПРАВИ ЯК СПОСІБ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Конституція України визначає гласність судового процесу як одну із основних засад, встановлених для правосуддя України [1]. При розгляді цивільних справ судочинство здійснюється усно і відкрито [2, ч. 1 ст. 6]. Відкритість судового розгляду передбачає присутність у судовому засіданні як учасників судового розгляду, так і всіх бажаючих. Цікаво, що чинний Цивільний процесуальний кодекс України (далі – ЦПК) не встановлює мінімальної вікової межі для осіб, бажаючих бути присутніми при судовому розгляді. Для порівняння, в попередньому цивільному процесуальному кодексі України (1963 р.) встановлювалась така межа: при судовому розгляді могли бути присутні лише особи, яким вже виповнилось 16 років.

Гласність, усність та відкритість судового розгляду цивільних справ є вимогами норм міжнародного права та покликані забезпечувати справедливе правосуддя. Але у випадках, чітко визначених ЦПК, допускається проведення закритого судового розгляду цивільної справи [2, ч. 3 ст. 6]. При такому розгляді в судовому засіданні, як правило, присутні лише особи, які беруть участь у справі. Але також, в разі необхідності, можуть залучатись експерти, свідки, перекладачі і спеціалісти [2, ч. 5 ст. 6].

Підставою для постановлення судом мотивованої ухвали про проведення закритого судового розгляду цивільної справи є забезпечення

захисту конфіденційної інформації, яка може бути розголошена при відкритому розгляді. Зокрема, це стосується державної або іншої таємниці, яка охороняється законом. Розголошення державної таємниці становить загрозу національній безпеці України. Відповідно до статті 1 Закону України «Про державну таємницю» державною таємницею (або секретною інформацію) є видтаємної інформації,яка у встановленому порядку визнана державною таємницею, підлягає охороні державою та охоплює відомості у сфері:

- оборони,
- економіки,
- науки і техніки,
- зовнішніх відносин,
- державної безпеки та охорони правопорядку [3].

Підставою для проведенню закритого судового розгляду цивільної справи також може бути інша інформація, яка охороняється законом: банківська таємниця, адвокатська таємниця, нотаріальна таємниця, таємниця про стан здоров'я тощо.

Також за клопотанням осіб, які беруть участь у справі, підставою для закритого судового розгляду цивільної справи може виступати:

- забезпечення таємниці усиновлення (зокрема ч. 3 ст. 254 ЦПК безпосередньо передбачає закритий судовий розгляд з метою забезпечення таємниці усиновлення) ,

- запобігання розголошення відомостей про інтимні або інші особисті сторони життя осіб, які беруть участь у справі (зокрема ч. 3 ст. 301 Цивільного кодексу України встановлює право фізичної особи на збереження у таємниці обставин свого особистого життя),

- запобігання розголошення відомостей, що принижують честь і гідність осіб, які беруть участь у справі [2, ч. 3 ст. 6].

На підставі аналізу положень ЦПК можемо зробити висновок, що спектр законодавчого регулювання захисту конфіденційної інформації в

цивільному процесі досить широкий. Для вирішення судом питання про проведення закритого судового розгляду цивільної справи є необхідним відповідне клопотання осіб, які беруть участь у справі, а також представлені ними суду обґрунтуваннях заявлених вимог. В науковій літературі, зокрема в працях Комарова В. В., Сакари Н. Ю. та інших вчених, наголошується, що чинний ЦПК не передбачає процесуальні наслідки порушення принципу гласності судочинства [5, 61; 6, 71]. Відсутні також конкретні механізми захисту процесуального права особи на закритий судовий розгляд цивільної справи у випадках, передбачених законом.

На підставі викладеного можемо дійти висновку, що закритий судовий розгляд є винятком із загального правила цивільного судочинства і може мати місце виключно з передбачених законом підстав та при додержанні встановленого процесуального порядку проведення [4]. У контексті нормативного формулювання «закритий судовий розгляд допускається» очевидно, що це не обов'язок, а право суду. Отже, вирішення питання щодо проведення чи ні закритого судового розгляду залежить від професійної свідомості та етичної культури конкретного судді, який в нарадчій кімнаті вирішує питання постановлення мотивованої ухвали про закритий судовий розгляд цивільної справи. На нашу думку є доцільним в загальній щорічній судовій статистиці відображення даних про те, скільки було заявлено клопотань про закритий судовий розгляд цивільних справ, та скільки таких клопотань судом було задоволено.

Як вже зазначалось, потребують вдосконалення положення цивільного процесуального закону, які б встановлювали дієві механізми забезпечення захисту конфіденційної інформації при здійсненні цивільного судочинства. На даному етапі в апеляційному та касаційному порядку не може бути скасоване правильне по суті і справедливе рішення суду в цивільній справі з одних лише формальних міркувань [2, ч. 2 ст. 308, ч. 2 ст. 337]. Поняття «формальні міркування» законодавець не конкретизує і не пояснює. Але в будь-якому випадку «формальні міркування» не повинні охоплювати

конфіденційні відомості, які визначені та охороняються законом у встановленому порядку. В умовах стрімкого розвитку інформаційного суспільства захист визначеної законом конфіденційної інформації має бути забезпечений у всіх сферах, в тому числі при здійсненні цивільного судочинства.

Література:

1. Конституція України: Закон України, 28 червня 1996 р. № 254к/96-ВР // Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141.
2. Цивільний процесуальний кодекс України: Закон України, 18 березня 2004 № 1618-IV // Відомості Верховної Ради України, 2004, № 40 - 41, ст. 135.
3. Про державну таємницю: Закон України, 21 січня 1994 № 3855-XII // Відомості Верховної Ради України (ВВР), 1994, N 16, ст.93.
4. Науково-практичний коментар Цивільного процесуального кодексу України, 2012р.[Електронний ресурс] – Режим доступу: http://mego.info/
5. Проблеми теорії та практики цивільного судочинства: моногр. / В. В. Комаров, В. І. Тертишніков, В. В. Баранкова та ін., за заг. ред. Проф. В. В. Комарова. – Х., 2008. – 928 с.
6. Сакара Н. Ю. Право на справедливий судовий розгляд та національна практика цивільного судочинства // Право України – 2011. - № 10. – С. 63 – 76.

----------***----------

М.Ю.Кутепов,
к.ю.н., м.н.с., Научно – исследовательского института изучения проблем преступности им. Академика В.В. Сташиса НАПрН Украины, г. Харьков

ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ АВТОРСКИХ ПРАВ В СЕТИ ИНТЕРНЕТ

Вопросы защиты информации и проблема защиты прав интеллектуальной собственности, которые обсуждаются на конференции, актуальны сегодня, как никогда. Как известно из истории, тот, кто владеет информацией, тот владеет миром. И этот факт уже давно стал аксиомой, которая не требует дополнительного обоснования.

Все большую роль в нашей жизни начинают играть коммуникации. Все большее число людей могут с уверенностью заявить, что 21 век – век информационных технологий, потому что эти самые технологии не отпускают их в реальную жизнь. Ведь они целиком и полностью живут в интернете: у них виртуальная дружба, знакомства, любовь, и даже свои эмоции, настроение и чувства они выражают электронным языком – смайлами. Расстояния не имеют того значения, что прежде, мир становится теснее.

Сеть Интернет – это особая сфера жизнедеятельности, в которой существуют определенные отношения, Интернет - отношения. Они аналогичны реальным отношениям, складывающимся в обычной жизни. Следовательно, и неправомерные действия лиц в сети Интернет, подпадающие, например, под нормы уголовного права будут регулироваться уголовным правом, имущественные отношения – гражданским правом, административные – административным правом.

Сейчас доступ к интернету есть практически у любого жителя планеты, за исключением бедствующих слоев населения. Интернет является гигантской глобальной сетью. Его предназначение – это обеспечение любому человеку постоянного доступа к любой информации. Современные интернет-технологии позволяют быстро и легко копировать, публиковать, перепечатывать и распространять практически любую информацию. Очень часто такая легкость приводит к нарушению авторских прав создателей произведений. Объектами нарушений авторских прав становятся фильмы, музыкальные произведения, компьютерные программы, литературные и другие произведения, которые размещаются, копируются или распространяются в сети Интернет без согласия их авторов и без выплаты им какого-либо вознаграждения. В результате авторы этих произведений недополучают прибыль, а иногда (например, по причине плагиата) даже не получают известности.

Поэтому, если вовремя не позаботиться о защите авторских прав, за нас этого никто не сделает. Авторское право – один из самых сложных и деликатных вопросов юриспруденции. Отстоять свое авторство не всегда бывает просто, а иногда и вовсе невозможно. Интернет – это свобода, авторское право – это запрет. Все проблемы истекают из этого фундаментального противоречия.

Наше общество в большинстве своем совершенно безразлично относится к авторскому праву как таковому. Привычка доступа к определенным информационным благам без оплаты глубоко укоренилась в сознании наших граждан, она живет, и умирать, похоже, не намерена — достаточно посмотреть на обилие пиратских CD в торговых точках и плагиата в Интернете. Это и неудивительно. Совсем недавно, во времена Советского Союза, проблема авторства волновала у нас разве что одних авторов, а остальные жили по принципу "все вокруг народное — все вокруг мое". Это изречение как нельзя более точно описывает положение дел в сети Интернет. Тот, кто выкладывает любой чужой контент без согласия автора, нарушает закон. Это всем понятно, и в то же время, мы все ищем в сети БЕСПЛАТНОЕ программное обеспечение, уроки, тексты, аудио и видео для собственных нужд. Тот, кто скажет, что ему все равно: стоит программа денег или нет, главное – качество, – заведомо покривит душой.

Известный немецкий продюсер Карл Фрёлик как-то сказал: «Тот несчастный, которому обычный путь к прибыли кажется слишком долгим и слишком трудным, ворует или просит милостыню». Понятное дело, что просить Вас подарить кому-то свое произведение вряд ли кто станет, а вот то, что его могут украсть – вполне вероятно [1].

Бороться с этими нарушениями достаточно тяжело в виду их массовости и неконтролируемости. Тем не менее, законодательство и практика его толкования высшими судебными инстанциями позволяют привлечь особо злостных нарушителей, действующих в сети Интернет, к ответственности за нарушение авторских прав.

Нарушение авторских прав можно разделить на два вида:

1. Нарушение неимущественных прав – плагиат.

2. Нарушение имущественных прав – пиратство и контрафакция.

Плагиат – это присвоение авторства на чужое произведение науки, литературы, искусства или на чужое открытие, изобретение или рационализаторское предложение, а также использование в своих трудах чужого произведения без ссылки на автора. Плагиат может являться нарушением патентного законодательства или авторско-правового законодательства и влечет юридическую ответственность.

Контрафакция (пиратство) – незаконное умышленное использование объекта интеллектуальной собственности с целью получения материальной выгоды. За нарушение авторского права в Украине предусмотрена административная и уголовная ответственность [2].

Административная ответственность за нарушение авторского права – предусмотрена ст. 51-2 Кодекса Украины об административных правонарушениях. Согласно данному документу за незаконное использование объекта прав интеллектуальной собственности на нарушителя налагается штраф от десяти до двухсот необлагаемых минимумов доходов граждан с конфискацией незаконно изготовленной продукции, оборудования и материалов, которые предназначены для ее использования.

Уголовная ответственность за нарушение авторских прав – предусмотрена ст. 176 Уголовного кодекса Украины. Согласно данной статье незаконное воспроизведение, распространение произведений науки, литературы, искусства, компьютерных программ и баз данных, а равно незаконное воспроизведение, распространение исполнений, фонограмм и программ вещания, их незаконное тиражирование и распространение на аудио - и видеокассетах, дискетах, других носителях информации, а также иное использование чужих произведений, компьютерных программ и баз данных, объектов смежных прав без разрешения лиц, имеющих авторское право или смежные права, если эти действия причинили материальный

ущерб в крупном размере, - наказываются штрафом от ста до четырехсот необлагаемых минимумов доходов граждан или исправительными работами на срок до двух лет, с конфискацией всех экземпляров произведений, материальных носителей компьютерных программ, баз данных, исполнений, фонограмм, программ вещания, оборудования и материалов, предназначенных для их изготовления и воспроизведения.

Те же действия, если они совершены повторно или причинили материальный ущерб в особо крупном размере, - наказываются штрафом от двухсот до восьмисот необлагаемых минимумов доходов граждан или исправительными работами на срок до двух лет, или лишением свободы на тот же срок, с конфискацией всех экземпляров, материальных носителей компьютерных программ, баз данных, исполнений, фонограмм, программ вещания, аудио - и видеокассет, дискет, других носителей информации, оборудования и материалов, предназначенных для их изготовления и воспроизведения.

Действия, предусмотренные частями первой или второй настоящей статьи, совершенные должностным лицом с использованием служебного положения в отношении подчиненного лица, - наказываются штрафом от пятисот до тысячи необлагаемых минимумов доходов граждан или арестом на срок до шести месяцев или ограничением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Важным вопросом остается доказывание виновности конкретного субъекта, совершившего правонарушение в сфере авторских прав через Интернет. Ведь даже зафиксировав IP-адрес, с которого совершено распространение произведения либо скачивание (тиражирование), сложно установить конкретно лицо, которое это совершило. Факт принадлежности компьютера конкретному лицу не свидетельствует о его вине. К примеру, Шевченковский районный суд в постановлении от 20.10.2010 г. по делу № 1-107/2010 о распространении порнографических материалов на

файлообменнике Infostore указал, что «так и остались не установленными ай-пи адреса, с которых были загружены файлы порнографического характера на сайт Infostore и на страницы пользователей «QuQ» и «W.Blake», и принадлежат ли данные ай-пи адреса ЛИЦУ_3 и ЛИЦУ_4, а также не получены у интернет-провайдеров «логи» (текстовые истории активности) пользователей с вышеустановленными ай-пи адресами. Дело было отправлено на дополнительное расследование. Окончательное решение суда по этому делу до сегодняшнего дня не вынесено. В связи с этим практически сложно привлечь к ответственности пользователей файлообменников. [3].

Ответственность за нарушение авторских прав в Интернете несут лица, незаконно выкладывающие контент, и лица, скачивающие такой контент. Файлообменники и их должностные лица могут нести ответственность только в том случае, если они игнорировали требования правообладателей о прекращении нарушения авторских прав.

На наш взгляд, борьба с нарушениями авторских прав, равно как и с нарушениями любых других прав, предоставленных человеку законом, несомненно, явление очень нужное и положительное, которое требует к себе пристального внимания со стороны структур, призванных по роду своей деятельности способствовать полному и качественному расследованию и пресечению преступлений указанного рода, кроме того, необходимо принять меры нормотворческого характера в целях устранения имеющихся недостатков в существующем законодательстве.

Мы считаем, что проблема защиты авторского права невозможна без хотя бы мало-мальски пристойного законодательного вмешательства и рождаемой на этом основании практики защиты на уровне государственных судебных инстанций.

Литература:

1. Регистрация авторских прав [Электронный ресурс]. – Режим доступа: http://vepol.ua/catalog/intellektualnaya_sobstvennost/registratsiya_avtorskikh_prav/

2. Нарушение авторских прав [Электронный ресурс]. – Режим доступа: http://arifmetova.com.ua/index.php?nid=21&p=news&sub=more
3. Ответственность за нарушение авторских прав в Интернете[Электронный ресурс]. – Режим доступа:http://jurliga.ligazakon.ua/news/58422

----------***----------

Драчук С. М.
к.ю.н., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України,
Хлань В. Г.
к.т.н., с.н.с., головний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України,

ОСОБЛИВОСТІ ПРАВОВОГО ЗАХИСТУ ГЕНЕТИЧНИХ ДАНИХ ЛЮДИНИ ВІД ПРАВОПОРУШЕНЬ В ІНФОРМАЦІЙНІЙ СФЕРІ

За міжнародним правом генетичні дані людини це - інформація про спадкові характеристики окремих осіб, що отримана шляхом аналізу нуклеїнових кислот або шляхом іншого наукового аналізу.

Відповідно до норм міжнародного та національного права генетичні дані людини мають особливий статус, у зв’язку з чим може йти мова і про особливості їх правового захисту. Перш за все, відповідна увага має приділятися конфіденційному характеру генетичних даних людини з встановленням відповідного рівня захисту цих даних.

Особливість (конфіденційність) генетичних даних людини полягає в наступному:

- вони можуть вказувати на вияв генетичної схильності відповідної особи;
- вони можуть суттєво впливати протягом декількох поколінь на родину та нащадків, а в деяких випадках – на цілу групу, до якої належить відповідна особа;

- вони можуть вміщувати інформацію, про значення якої може бути не відомо під час збирання біологічних зразків;
- вони можуть мати культурне значення для окремих осіб або груп осіб.

Узагальнення цих особливостей наштовхує нас на думку про те, що система інформаційних правовідносин де об'єктом виступають генетичні дані людини може стосуватися не лише прав людини, а й прав суспільства та держави. Цей факт, в свою чергу, також може розглядатися як особливість генетичних даних людини, що має бути враховано при розробці відповідного механізму їх правового захисту.

За своїми ознаками генетичні дані людини безумовно відносяться до інформації про фізичну особу (персональні дані) оскільки вміщують - відомості про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Сам процес ідентифікації особи за допомогою молекулярно-генетичних досліджень в останні роки набуває широкого застосування. Розробка молекулярно-діагностичних технологій, наукові досягнення медичної генетики та молекулярної біології, підвищили використання їх можливостей як в медицині так і в правоохоронній діяльності. Проте, сучасний стан використання молекулярно-діагностичних технологій потребує вдосконалення механізму захисту генетичних даних людини.

Дослідження проблеми правового захисту генетичних даних людини потребує з'ясування суті цього поняття. Вимушені констатувати, що в національному законодавстві відсутнє визначення поняття «генетичні дані людини», що може розглядатися як визначальна особливість з огляду на розробку дієвого механізму їх правового захисту. Натомість, є суміжне поняття «генетичний матеріал» - будь-який матеріал рослинного, тваринного, мікробного або іншого походження, який містить функціональні одиниці спадковості. Через дотичний термін «геном» визначається поняття «генетична безпека» - стан середовища життєдіяльності людини, при якому відсутній будь-який неприродній вплив на людський геном, відсутній будь-

який неприродній вплив на геном об'єктів біосфери, а також відсутній неконтрольований вплив на геном сільськогосподарських рослин і тварин, промислових мікроорганізмів, який призводить до появи у них негативних та/або небажаних властивостей.

Правові відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту генетичних даних людини тісно пов'язані з медичною практикою, для якої актуальним є конституційне положення про те, що жодна людина без її вільної згоди не може бути піддана медичним, науковим чи іншим дослідам. Також на законодавчому рівні заборонено медичне втручання, яке може викликати розлад генетичного апарату людини. Збирання, обробка, використання і зберігання генетичних даних людини мають важливе значення для прогресу науки про життя та медицини та практичного використання їх здобутків, а також для використання таких даних у немедичних цілях.

Так, при збиранні генетичних даних людини у судово - медичних цілях або в межах судочинства у цивільних, кримінальних та інших справах, зокрема встановлення батьківства, збирання біологічних зразків *in vivo* або *post mortem*, повинно здійснюватися лише на підставі внутрішнього права, що має бути узгодженим з міжнародним правом у сфері захисту прав людини. Державам слід як на національному так і на міжнародному рівні вживати заходів для боротьби з біотероризмом та незаконним обігом генетичних ресурсів та генетичних матеріалів. Також державам варто забезпечити захист прав окремих осіб на приватне життя та конфіденційність генетичних даних особи, родини або у відповідних випадках групи, яка підлягає ідентифікації, відповідно до внутрішнього законодавства або відповідного міжнародного права у сфері прав людини.

У національній правовій системі на законодавчому рівні закріплені особливі вимоги до обробки персональних даних що стосуються генетичних даних, а саме заборона щодо їх обробки та передбачені випадки коли ця норма не застосовується. В МВС України на сьогодні врегульовано певні

особливості функціонування системи обліку генетичних ознак людини (ДНК профілів) як одного з різновиду криміналістичних обліків. Під час наповнення баз (банків) даних поліція забезпечує збирання, накопичення зразків ДНК лише щодо осіб, затриманих за підозрою у вчиненні правопорушень.

На сьогодні генетичні дані людини як персональні дані або конфіденційна інформація прямо захищені нормами Кримінального кодексу України (стаття 182. порушення недоторканності приватного життя) та Кодексу України про адміністративні правопорушення (стаття 188-39 порушення законодавства у сфері захисту персональних даних). Опосередковане відношення до захисту генетичних даних мають й інші статті означених кодексів, зокрема, 132, 168, 164-3.

Як зазначалося вище інформація, що міститься в ДНК людини є конфіденційною, оскільки вона є унікальним ідентифікатором. В тих країнах, де внутрішнє законодавство дозволяє використовувати ДНК – аналізи, зокрема, з метою забезпечення правопорядку (Україна в цьому сенсі не є виключенням) в більшості випадків було прийнято спеціальне законодавство про захист зібраної генетичної інформації.

У такому законодавстві мають бути передбачені такі положення як, наприклад:

генетичні дані людини та біологічні зразки, що належать особі яка може бути ідентифікована не мають розкриватися або ставати доступними для третіх сторін, за виключенням випадків, пов’язаних з важливими суспільними інтересами чітко визначеними у внутрішньому законодавстві;

генетичні дані людини та біологічні зразки, що зібрані з науковою метою, як правило, не повинні пов’язуватися з особою яка може бути ідентифікована у якості їх носія;

генетичні дані людини та біологічні зразки не повинні зберігатися у формі, яка дозволяє суб’єкту даних бути ідентифікованим протягом більшого

часу, ніж це необхідно для досягнення мети, з якою здійснювався їх збір та послідуюча обробка.

В інтересах збереження генофонду народу України, забезпечення здоров'я майбутніх поколінь держава здійснює комплекс заходів, спрямованих на усунення факторів, що шкідливо впливають на генетичний апарат людини, а також створює систему державного генетичного моніторингу, організує медико-генетичну допомогу населенню, сприяє збагаченню і поширенню наукових знань в сфері генетики.

При проведенні генетичних досліджень мають дотримуватися правила біоетики і деонтології. Наприклад, інформація про спадковий характер захворювання у пробанда, чи у родині, яка є конфіденційною надається безпосередньо особі пробанду. У випадку встановлення носійства мутантного гена чи структурної перебудови хромосом у одного із членів подружжя, інформація про виявлені зміни у генетичному апараті надається у письмовій формі пацієнту (носію). Медичними спеціалістами забезпечується право пацієнта щодо необхідності інформування інших членів родини про виявлену патологію. У випадку, коли пробандом виступає дитина або людина зі зниженим розумовим розвитком, результати генетичних досліджень у вигляді висновку видаються батькам, або особам, що їх замінюють, відповідно до чинного законодавства. У посадових інструкціях лікарів-генетиків як правило серед обов’язків зазначається необхідність дотримуватись конфіденційності результатів генетичних досліджень та встановленого діагнозу спадкової патології у межах діючого законодавства, а в правах - використовувати для встановлення діагнозу спадкової патології медичну документацію інших закладів охорони здоров'я та конфіденційну інформацію щодо біологічних батьків досліджуваної особи.

За даними МКЧХ в більшості країн законодавство не встигає своєчасно реагувати на прогрес у сфері ДНК –аналізу, що використовується, зокрема, і в інтересах криміналістики. На сьогоднішній день в Україні є нагальна потреба у законодавчому врегулюванні питання щодо ведення баз даних

генетичних ознак людини та організації функціонування Національної бази даних ДНК.

Питання створення та функціонування баз даних ДНК безпосередньо пов’язано з такою проблемою як захист персональних даних, зокрема генетичних даних людини.

Ґрунтовний аналіз наявних у національному праві визначень поняття «база даних» свідчить по те, що жодне з них повною мірою не відповідає сутності цього поняття або через застарілість внаслідок еволюції юридичної науки, або через порушення правил логіки. Водночас до суттєвих ознак цього поняття можна віднести наступні:

- сукупність даних;
- упорядкованість даних;
- іменований характер даних;
- визначена предметна область;
- відносність даних до стану об'єктів, явищ, процесів;
- відношення між об'єктами, явищами, процесами.

Таким чином база даних ДНК може розглядатися як іменована сукупність упорядкованих генетичних даних (у цифрових, текстових файлах тощо), що відображає стан об'єктів, явищ, процесів та їх відношень у визначеній предметній області.

На сьогодні вчені дійшли до висновку про можливість підробки зразку ДНК конкретної людини навіть не маючи зразку біологічного матеріалу з його тіла, зрештою, лише на підставі інформації генетичного профілю цієї людини з бази даних. Зазначене свідчить про необхідність удосконалення існуючого устаткування криміналістичних лабораторій, які б були здатні виявити різницю між дійсним та підробленим ДНК.

Існує нагальна потреба у розробці національних законодавчих норм та правил у сфері біоетики, зокрема у формі національних кодексів поведінки та керівних принципів.

Загалом, при подальшій розробці та вдосконаленні вітчизняного законодавства у сфері захисту генетичних даних людини слід враховувати міжнародну практику, що закріплена в таких документах як: Загальноприйнята декларація про геном людини і права людини від 11 листопада 1997 р., Міжнародна декларація про генетичні дані людини від 16 жовтня 2003 р., резолюція Генеральної Асамблеї ООН 30 С/23 від 16 листопада 1999 р., резолюції № 2001/39 та №2003/232 Економічної та Соціальної Ради ООН про генетичну конфіденційність та недискримінацію, відповідно від 26 липня 2001 р. та від 22 липня 2003 р., Конвенція Ради Європи Про права людини та біомедицину та додаткові протоколи до неї, Хельсинська декларація Всесвітньої медичної асоціації Про етичні принципи проведення медичних дослідів, об'єктом яких є людина від 1964 р., з змінами, внесеними в 1975 р., 1989 р., 1996 р. та 2000 р., Міжнародні керівні принципи етики для біомедичних дослідів на людині, прийнятих Радою міжнародних науково-медичних організацій у 1982 р., зі змінами, внесеними у 1993 та 2002 роках та інші міжнародні документи з прав людини, що прийняті ООН та спеціалізованими установами системи ООН. Корисним також є можливе запозичення позитивного досвіду діяльності Міжнародного комітету червоного хреста, Міжнародної організації з пошуку безвісти зниклих, Міжурядового комітету з біоетики та Міжнародного комітету з біоетики та інших впливових міжнародних організацій.

Література:

1. ЮНЕСКО: Международнаядекларацияогенетическихданныхчеловека(2003 р.), Всеобщаядекларацияогеномечеловекаиправахчеловека (1997 р.). - [Еэлектронный ресурс] – Режим доступа:http//portal.unesco.org.
2. МККК: «The Missing: Action to resolve the problem of people unaccounted for as a result of armed conflict or internal violence and to assist their families, The legal protection of personal data and human remains», Geneva, 2003. («Действия по решению проблемы людей, пропавших без вести в результате военного конфликта или внутреннего насилия. Правовая защита данных личного характера и человеческих останков». - [Еэлектронный ресурс] – Режим доступа:

http://www.icrc.org/Web/eng/siteeng0.nsf/htmlall/5CALLJ/$File/ICRC_TheMissing_072002_EN_1.pdf..
3. Пособие по передовому опыту работы в условиях вооруженных конфликтов и других ситуаций вооруженного насилия. Второе издание. Пропавшие без вести, ДНК-анализ и идентификация останков/ Сост. Международный комитет красного креста.- М., 2009.- 48 с.
4. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI- [Еэлектронный ресурс] – Режим доступа: http://www.zakon.rada.gov.ua;
5. Закон України «Про Національну поліцію» від 02.07.2015 № 580-VIII- [Еэлектронный ресурс] – Режим доступа: http://www.zakon.rada.gov.ua;
6. Закон України «Про інформацію» від 02.10.1992 № 2657-XII (електронний ресурс) – Режим доступу http://www.zakon.rada.gov.ua;
7. Закон України «Про державну систему біобезпеки при створенні, випробуванні, транспортуванні та використанні генетично модифікованих організмів» від 31.05.2007 № 1103-V (електронний ресурс) – Режим доступу http://www.zakon.rada.gov.ua;
8. Кримінальний кодекс України від 05.04.2001 № 2341-III (електронний ресурс) – Режим доступу http://www.zakon.rada.gov.ua;
9. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X (електронний ресурс) – Режим доступу http://www.zakon.rada.gov.ua;
10. Наказ Міністерства охорони здоров'я України «Про удосконалення медико-генетичної допомоги в Україні» від 31.12.2003 № 641/84 (електронний ресурс) – Режим доступу http://www.zakon.rada.gov.ua;
11. Наказ Міністерства внутрішніх справ України «Про затвердження Інструкції з організації функціонування криміналістичних обліків експертної служби МВС» від 10.09.2009 № 390 (електронний ресурс) – Режим доступу http://www.zakon.rada.gov.ua.

----------***----------

Ю. Г.Грибенюк,
аспірант Науково-дослідного інституту інформатики і права Національної академії правових наук України

ПРАВОВИЙ ПОРЯДОК ПОШИРЕННЯ КУЛЬТУРНО-МИСТЕЦЬКОЇ ТА МУЗЕЙНОЇ ІНФОРМАЦІЇ ТА ВІДПОВІДАЛЬНІСТЬ ЗА НЕПРАВОМІРНЕ ЇЇ ВИКОРИСТАННЯ

Правовий порядок поширення інформаційних ресурсів культурно-мистецькими та музейними комплексами значною мірою залежить від особливостей тих завдань і функцій, які на них покладає держава, як на

державні підприємства, які здійснюють власну господарську діяльність у сфері культурно-мистецьких послуг. Зміст і характер цієї політики обумовлений метою держави в умовах формування та становлення інформаційного суспільства, задовольнити потреби суспільства в інформації та реалізувати права громадян у сфері культури як стратегічному ресурсі його розвитку.

У статті 11 Конституції України визначено, що держава сприяє консолідації та розвиткові української нації, її історичної свідомості, традицій і культури, а також розвиткові етнічної, культурної, мовної та релігійної самобутності всіх корінних народів і національних меншин України.

На сучасному етапі концепція повноти прав громадян у сфері культури деталізована у ст. ст. 6-10 Закону України «Про культуру». Одним з таких прав, які гарантуються державою є також і доступ до культурних цінностей, культурної спадщини і культурних благ.

Роз'яснення способів реалізації права громадян на доступ до культурних цінностей та культурних благ міститься у правовій нормі, передбаченій ст. 8 Закону України «Про культуру».

Зокрема, право на доступ до культурних цінностей реалізується шляхом утримання або надання закладам культури державної підтримки з державного та місцевих бюджетів для забезпечення їх функціонування та доступності їх послуг для різних категорій населення.

Так, громадяни мають право на доступ до культурних цінностей шляхом:

- ✓ користування документами Національного архівного фонду України або їх копіями;
- ✓ ознайомлення з музейними колекціями, що належать до державної частини Музейного фонду України;
- ✓ користування фондами бібліотек, що належать до Державного бібліотечного фонду України.

Реалізація права громадян на ознайомлення із музейними колекціями ставить перед культурно-мистецькими та музейними інституціями питання порядку поширення культурно-мистецької та музейної інформації.

Відповідно до ст. 7 ЗУ «Про музеї та музейну справу» музеї можуть засновуватися на будь-яких формах власності, передбачених законами. Засновниками музеїв можуть бути відповідні органи виконавчої влади, органи місцевого самоврядування, юридичні та фізичні особи. При цьому музеї можуть створюватись і діяти в усіх організаційно-правових формах.

Відповідно до ст. 1 ЗУ «Про культуру» заклад культури - юридична особа, основною діяльністю якої є діяльність у сфері культури, або структурний підрозділ юридичної особи, функції якого полягають у провадженні діяльності у сфері культури;

Згідно ст. 15 ЗУ «Про культуру» заклади та працівники культури вільно розповсюджують та популяризують з дотриманням вимог законодавства твори літератури і мистецтва, самостійно визначають репертуар, програми, зміст і форми гастрольно-концертної, виставкової, бібліотечно-інформаційної та іншої діяльності у сфері культури.

Розпорядженням Кабінету міністрів України від 01.02.2016 р. № 119-р було затверджено Довгострокову стратегію розвитку української культури - стратегії реформ (далі – Довгострокова стратегія).

Забезпечення доступу до культури через традиційні та нові форми культурної діяльності - один із стратегічних напрямків реформ, передбачених Довгостроковою стратегією.

Цей нормативно-правовий акт передбачає операційні цілі щодо музейної діяльності, зокрема:

- ✓ впровадження сучасних інформаційних та інтелектуальних технологій у музейну діяльність, в тому числі створення системи електронного обліку музейних предметів, цифрового реєстру музеїв і закладів музейного типу України з актуальною інформацією для їх популяризації та управління;

✓ системне реформування музейної діяльності з метою перетворення музеїв та заповідників на відкритий універсальний простір, який об’єднує минуле, сучасне та майбутнє, шляхом виконання основних функцій за такими напрямами діяльності, як науково-дослідна, культурно-освітня діяльність, комплектування музейних зібрань, експозиційна, фондова, видавнича, реставраційна, виставкова, пам’ятко-охоронна робота, а також діяльність, пов’язана з науковою атрибуцією, експертизою, класифікацією, державною реєстрацією та всіма видами оцінки предметів, які можуть бути визначеними як культурні цінності.

Музейні установи України в умовах задекларованого державою євроінтеграційного курсу не мають права існувати й розвиватися поза спільноєвропейським інформаційно-культурним простором.

Діюча мережа державних і комунальних закладів культури повинна бути наповнена новим змістом, новими можливостями та знаннями, щоб ефективно надавати гарантовані Конституцією України послуги та забезпечувати реалізацію права громадян на доступ до культури та участь у культурному житті. Сучасні технології мають стати невід’ємним атрибутом діяльності закладів культури.

Нові інформаційні технології забезпечують музеям низку стратегічних переваг, які значно розширюють можливості музеїв в процесі поширення культурно-мистецької та музейної інформації.

Зокрема забезпечується:

1. Створення комп'ютерних систем музейного обліку забезпечує контроль за станом колекцій як з боку органів управління, самих музеїв, так і з боку громадянського суспільства.

2. Інформаційні канатики комунікацій забезпечують ефективний інструмент пошуку партнерів і взаємодії з ними в рамках спільних музейних програм і проектів.

3. Наявність web-сайту, сторінки музею у соціальних мережах – додаткова можливість надання платних пошукових інформаційно-консультативних та експертних послуг.

4. Електронні каталоги і бази зображень музейних предметів дозволяють вирішувати багато дослідницьких і наукових завдань.

5. Практика on-line бронювання квитків та продажу музейного продукту.

6. Розширення віртуальної аудиторії музею, заїх допомогою відвідувач може оперативно отримувати інформацію про нові події та музейні акції, про експоновані предмети та їх каталоги, зробити віртуальну екскурсію музеєм за допомогою електронного путівника тощо.

Розширення можливостей музеїв у процесі поширення культурної та мистецької інформації ставить перед культурними закладами і проблемні питання порушення авторських прав споживачами інформації і питання відповідальності за неправомірне використання культурної та мистецької інформації користувачами такої інформації.

Зокрема, розміщення власних колекцій музеями у мережі Інтернет може розглядатись не лише як можливість розширення доступу споживачів до культурних надбань, а й як можливість порушення майнових авторських прав музеїв.

Чинне законодавство не містить правового порядку, який б регламентував можливості культурно-мистецьких та музейних установ забороняти чи дозволяти використання експонатів, які знаходяться у їх колекціях, із комерційною чи некомерційною метою, для виготовлення сувенірної, друкованої, рекламної продукції тощо.

Відповідно до п. 46 Положення про Музейний фонд України передбачено, що виготовлення образотворчої, друкованої, сувенірної продукції з використанням зображень музейних предметів здійснюється відповідно до вимог законодавства у сфері авторського права та з письмового дозволу музеїв, у яких вони зберігаються. Однак порядок отримання такого

дозволу ані зазначеним нормативно-правовим актом, ані іншими актами не регламентований, що, в свою чергу робить неможливим використання такої норми на практиці та доводить її недієздатність у реальному житті.

Не дає відповіді на питання - яким чином захистити власні колекції від порушення авторських майнових прав у випадку їх розміщення у мережі Інтернет - ні глава 36 Цивільного кодексу України, яка містить основні положення захисту авторських прав, ані спеціальні закони «Про авторські майнові і суміжні права» та «Про музеї та музейну справу».

Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», в рамках законодавчого розвитку інформаційного суспільства, в тому числі і з метою вирішення цієї проблеми, пропонує підготувати та прийняти Інформаційний кодекс України, включивши до нього розділи, зокрема щодо удосконалення захисту прав інтелектуальної власності, в тому числі авторського права при розміщенні та використанні творів у мережі Інтернет тощо.

Враховуючи вищевикладене, можна стверджувати, що правовий порядок доступу до культурно-мистецької та музейної інформації та відповідальність за її неправомірне використання є предметом окремого інформаційно-правового забезпечення та розгляду.

Література:

1. Конституція України від 28.06.1996 р. // Відомості Верховної Ради України 1996 р. - № 30. – ст. 141.
2. Цивільний кодекс України 16 січня 2003 року № 435-IV //Офіційний вісник України. - 2003 р., № 11, стор. 7, ст. 461.
3. Закон України «Про культуру» від 14.12.2010 р. № 2778-VI // Офіційний вісник України. - 2011 р., № 2, стор. 13, ст. 91.
4. Закон України «Про музеї та музейну справу» від 29.06.1995 № 249/95-ВР // Відомості Верховної Ради України. - 1995. — № 25. – ст. 191.
5. Закон України «Про авторське право і суміжні права» від 23.12.1993 року № 3792-XII //Відомості Верховної Ради. - 1994 р. - № 13, - ст. 64.
6. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 № 537-V// Відомості Верховної Ради України. - 2007. — № 12. – ст.102.
7. Закон України «Про інформацію» від 02 жовтня 1992 р. № 2657-XII//

Відомості Верховної Ради. – 1992. – № 48. – ст. 650.
8. Розпорядження Кабінету Міністрів України «Про схвалення Довгострокової стратегії розвитку української культури - стратегії реформ» від 01.02.2016 р. № 119-р. // Офіційний вісник України. - 2016 р. - № 18, стор. 472, ст. 745.
9. Постанова Кабінету Міністрів України «Про затвердження Положення про Музейний фонд України» від 20.07.2000 р. N 1147// Офіційний вісник України. - 2000 р. - № 30, стор. 84, ст. 1268.

----------***----------

Т.А. Переймивовк,
к.е.н., головний судовий експерт
ЛЕД Київського НДІСЕ МЮ України
М.О. Полєнніков,
судовий експерт
ЛЕД Київського НДІСЕ МЮ України

ЕЛЕКТРОННИЙ ДОКУМЕНТ ЯК ОБ'ЄКТ ДОСЛІДЖЕННЯ СУДОВО - ЕКОНОМІЧНОЇ ЕКСПЕРТИЗИ

Відповідно до ст.1 Закону України «Про судову експертизу» від 25.02.1994 № 4038-XII, судова експертиза - це дослідження експертом на основі спеціальних знань матеріальних об'єктів, явищ і процесів, які містять інформацію про обставини справи, що перебуває у провадженні органів досудового розслідування чи суду.

Впровадження інформаційних технологій ініціювало дискусії та дослідження концепції електронного документу, його відмінностей та особливостей порівняно з традиційним документом на паперовому носії.

На відміну від звичайних документів, характеристики та просторові межі яких ми звикли бачити, електронні документи мають зовсім іншу природу. Інформація, яка становить суть електронного документа, має особливі віртуальними межами, які обмежені поняттям "файл", під яким в науковій літературі розуміється «сукупність обмежених за обсягом відомостей, записаних на машинному носії, що становлять єдине ціле з

інформаційного значенням». При цьому електронний документ може існувати як у формі одного файлу, так і у вигляді сукупності файлів.

Згідно ст.99 Кримінально процесуального кодексу України від 13.04.2012 № 4651-VI, документом є спеціально створений з метою збереження інформації матеріальний об’єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження (у тому числі електронні).

Законі України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV зазначено, що електронний документ (ЕД) - це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму.

Оскільки об'єктом судової економічної експертизи документів є матеріальний (матеріалізований) документ, то для класифікації електронних документів, як об'єктів економічної експертизи, важливим є тип його носія: внутрішній (пам'ять ПК) і зовнішній (диски, карти флеш пам'яті, хмарні сервіси, папір, інше).

За стадіями виготовлення документи, в тому числі і електронні, діляться на оригінали, дублікати, копії і виписки. Для електронного документа такі поняття, як «оригінал», «дублікат», «копія» є умовними, оскільки у всіх цих випадках електронний документ залишається оригіналом.

Досліджуючи електронний документ як об'єкт економічної експертизи, слід більше уваги приділяти його зовнішньою формою. Зовнішня форма розмежовує документи за способом фіксації та подання. Важливим є розмежування документів на рукописні і виготовлені за допомогою технічних засобів. Якщо виготовлення документів з використанням технічних засобів вже стало звичним, то рукописна форма електронного

документа - явище досить нове. Рукописна форма введення інформації в комп'ютер з'явилася, практично одночасно з появою сенсорних панелей і планшетів. В експертній практиці ще не зустрічалися випадки дослідження електронних документів, виготовлених рукописним способом. Не виключено, що такі документи в найблищому майбутньому можуть стати об'єктами економічного дослідження.

Також, для того щоб виділити електронний документ з маси всіх інших електронних документів, він повинен бути певним чином персоніфікований, тобто наділений особливими атрибутами, за якими в подальшому може бути здійснена його ідентифікація. Роль персоніфікуючих атрибутів електронного документа виконують його реквізити, до яких відносяться: 1) ім'я файлу, яке присвоюється йому цілеспрямовано творцем інформації або автоматично без його волі; 2) формат файлу, який визначається програмним забезпеченням, за допомогою якого він був створений або збережений; 3) розмір файлу, який представляє собою обсяг пам'яті машинного носія, який займає файл; 4) дата і час створення або редагування файлу.

Крім персоніфікуючих реквізитів, електронний документ може містити захисні або посвідчувальні реквізити. Наприклад, одним з факультативних реквізитів електронного документа, який одночасно є персоніфікуючим і захисним, можна назвати електронний підпис (електронний цифровий підпис). Відповідно до Закону України «Про електронний цифровий підпис» від 22.05.2003 № 852-IV, під ЕЦП розуміється «вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа».

Електронний документ не може існувати без носія інформації. При цьому, мають значення ідентифікуючі ознаки носія інформації, які

включають найменування типу, марки, моделі, індивідуального серійного номера і т.п. машинного носія, на якому записаний файл.

Важливе значення при дослідженні електронних документів має проблема встановлення достовірності електронних доказів і забезпечення їх доказової сили. На сьогоднішній день в процесуальному законодавстві не передбачені конкретні критерії достовірності електронних доказів.

Одним із способів встановлення достовірності походження електронного документа є електронний підпис, про яку говорилося вище. Недолік даного способу полягає в тому, що далеко не кожен електронний документ захищається електронним підписом.

В якості ще одного рішення проблеми забезпечення достовірності електронних документів вчені пропонує використовувати інститут забезпечення інформації, що міститься на електронних носіях і в мережі Інтернет, нотаріусами.

В даний час на практиці склалися деякі правила забезпечення достовірності електронних доказів і пред'явлення їх в суді: 1) якщо електронний документ містить в собі графічну або текстову інформацію, то роздруковується його паперова копія, яка оформлюється і завіряється уповноваженою особою; така копія долучається до справи і досліджується як звичайний письмовий документ; 2) якщо операції, що документально підтверджуються електронним документом (електронний документ підписаний ЕЦП), а сторони оспорюють надання послуг, що підтверджуються цим документом, то призначається комплексна експертиза, де економічна експертиза проводиться вже за даними щодо автентичності ЕЦП; 3) якщо електронний документ являє собою сторінку в мережі Інтернет, то така сторінка за умови посилання роздруковується на папері, оформляється і завіряється як копія веб-сторінки при зверненні зацікавленої особи або до власника сервера, на якому розміщений сайт, або до нотаріуса; завірена роздруківка сторінки сайту долучається до справи і досліджується в процесі; 4) якщо електронний документ несе в собі аудіо- або

відеоінформацію, то, як правило, робиться копіювання таких файлів на окремий переносний електронний носій, який долучається до справи і досліджується за допомогою спеціальних технічних засобів.

Для ідентифікації автора електронного документа відповідно до чинного законодавства може використовуватися електронний підпис. Постає питання: чи можна брати до уваги документ, якщо в ньому немає підпису особи, повноважної на його створення?

Отже, для того щоб визнати електронні документи в якості повноцінних достовірних доказів, необхідно суворо дотримуватися правил процесуального законодавства, а також стандартних прийомів і методик збирання, оцінки, дослідження та використання електронних доказів. Тільки в цьому випадку зацікавлена особа зможе розраховувати на прийняття судом та, в свою чергу, експертом - економістом до уваги подібних документів, до яких досі, на жаль, проявляється недовіра з боку правоохоронних і судових органів.

Література:

1. Кримінальний процесуальний кодекс України від 13.04.2012р. №4651-VI (зі змінами і доповненнями).
2. Закон України «Про судову експертизу» від 25.02.1994р. №4038-VII (зі змінами і доповненнями).
3. Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852-IV (зі змінами і доповненнями).
4. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV (зі змінами і доповненнями).

----------***----------

УДК 930

Ю.Б. Форис,
научный сотрудникКНИИСЭ МЮ Украины
Е.Г. Ефремова,
начальник отдела Центральный государственный архив высших органов власти и управления Украины

ДОКУМЕНТ О СОЗДАНИИ ХАРЬКОВСКОГО НАУЧНО-ИССЛЕДОВАТЕЛЬСКОГО ИНСТИТУТА СУДЕБНЫХ ЭКСПЕРТИЗ

Хотелось бы развеять некоторые мифы касательно создания Киевского и Харьковского научно-исследовательских институтов судебных экспертиз: который создан раньше, который – позже.

Так, в литературе встречаются следующие данные:

«В 1912 М. Бокариус организовал кабинет научно-судебной экспертизы в Харькове. В 1923 кабинет возобновил работу после перерыва на то время он состоял из отделов физических и химических, судебно-медицинских, макро- и микроскопических исследований, идентификации лиц»[1].

«С принятием в 1922 году Уголовно-процессуального кодекса в Украине, органам предварительного расследования и судам при принятии решений в уголовных делах возникла задача полного и всестороннего исследования всех доказательств с помощью научно-технических знаний, в связи с чем, по ходатайству выдающегося судебного медика и криминалиста Николая Сергеевича Бокариуса, Правительство Украины своим постановлением от 10 июля 1923 года создает в системе Народного комиссариата юстиции (НКЮ) областные кабинеты научно-судебных экспертиз в городах Харькове, Киеве и Одессе и утверждает положение о них. Цель создания Кабинетов сформулирована очень кратко – «для производства разного рода научно-технических исследований по судебным делам». С того времени начинается славная история института» [2].

В результате проведенной в государственных архивах Украины кропотливой работы по воссозданию истории Киевского научно-исследовательского института судебных экспертиз, были обнаружены документы, касающиеся истории и других научно-исследовательских институтов судебных экспертиз. Так, в деле Народного Комиссариата Юстиции УССР (далее – НКЮ) был обнаружен документ, адресованный профессором Н. Бокариусом в Наркомат Юстиции и подписанный 23 октября 1923 года. Мы считаем необходимым привести из него выдержки.

«Уже приблизительно около года тому назад начали поступать во вверенный мне Институт суд. Медиц. веществ. доказат. при сопроводительных бумагах, адресованных в Кабинет Научной экспертизы для соответствующего исследования этих объектов: частью судеб.- химич., частью микроскоп. и микрохим. исследования. Кроме того, в последние месяцы (приблизительно около ½-угода уже) поступают ко мне вещественные доказательства по окончании дел для составления коллекций предполагаемого при кабинете научно-Судебной экспертизы учебно-показательного музея. Прислана даже инвентарная книга для записи этих предметов.

Учреждение Каб. Науч. экспертизы прошло уже законодательным порядком, а работа в нем выдвигается запросами и требованиями самой жизни.

Слияние Каб. Научн. экспертизы и Института судебной медицины, в смысле совмещения их, как учреждений, и их работа в последнем из названных учреждений желательна.

Сооружение специального здания для Каб. Научн. экспертизы и даже обособление для него отдельных помещений, а равно и особенно оборудование таковых специальной аппаратурой для НКЮ едва-ли возможно; между тем, открытие кабинета Научн. экспертизы может состояться и быть проведено в жизнь (красной ручкой сверху строки дописано «теперь же», прим. авт.) в жизнь, ввиду того, что институт

Судебной Медицины располагает соответствующими учреждениями и аппаратурой, которые могли бы обслуживать в большей части и нужды Кабинета Научной экспертизы, так как собственно, как выше упомянуто, поручаемые Кабинету работы, исполняются мною в заведуемом мною Институте Судебной Медицины. … (выпускаем часть текста, касающегося оборудования Института и возможностей введения в работу секций, прим. авт.)

Что касается штата, то в целях желательности скорейшего открытия Кабинета Научной экспертизы в Харькове, впредь до введения полной нормы штатов его, в настоящее время секция 5-ая – исследования мертвого тела человека могла бы быть обслужена силами вверенного мне Института Судебной Медицины без включения их в штат Кабинета Научной экспертизы. … (выпускаем часть текста, касающегося предложений по поводу штата Кабинета, прим. авт.)

Все переговоры с Отд. Мед. Обр. при Н.К.Прос’’е и с Правлением Мед. Института я мог бы взять на себя, имея ввиду, что огромное значение учреждения Кабинета Научн. экспертизы в тесном сближении с Институтом Судебной Медицины, какое таковое обстоятельство приобретает в целях более широкого освещения и оживления преподавательской и учебной работ связью их с материалами и моментами из практики судебно-медицинских исследований. …(выпускаем часть текста, касающегося расходов на первое время, прим. авт.)»[3].

В левом верхнем углу первой страницы документа находится рукописная резолюция от 27.X.23г., текст которой мы приводим так, как нам удалось его разобрать: «…ыть 6 …риуса договорись … использовании оборудова… Института суд. медицины (слово «только» зачеркнуто) Кабинетом научной экспертизы по совместимости … назначить проф. Бокариуса с 1го ноября с. г. (слово «директором» зачеркнуто) Заведующим Харьковским Кабинетом Научн. экспертизы. … в соглашении НКФ об

обращении ассигнований по Кабинету по (на?) которым приб… на приобретение оборудования (Подпись неразборчиво, читается «НРи…»)».

Таким образом, Н. С. Бокариус действительно ходатайствовал в пользу Харьковского кабинета, но ПОСЛЕ официального учреждения советской властью 3-х кабинетов в 1923 году. При этом учреждение Киевского и Одесского кабинетов состоялось ранее, в 1913 году, а в 1923 году их «учредили» ПОВТОРНО.

Так, Одобренный Государственным Советом и Государственной Думой Закон «Об учреждении кабинетов научно-судебной экспертизы в городах Москве, Киеве и Одессе» был подписан «Быть по сему» Царем Николаем II на рейде и яхте «Штандарт» 4 июля 1913 года [4].

Литература:

1. Биленчук П.Д. Современное состояние и перспективы развития криминалистики в Украине // Электронный ресурс; режим доступа: http://orbook.ru/index-5962.htm.
2. Выдержка из истории Харьковского НИИСЭ, изложенная на официальном сайте этого института // Электронный ресурс; режим доступа: http://www.hniise.gov.ua/page/4.html.
3. ЦГАВО Украины, Ф. 8, оп. 1, д. 1309, 114 стр., стр. 56, 56 об., 57.
4. РГИА Фонд 1329 Оп. 1. Дело 999. Л. 42.