

слідчому отримати дані, необхідні для формування доказової бази кримінального провадження, встановлення ознак кримінального правопорушення, виявлення та викриття осіб, причетних до його вчинення, належної кваліфікації їх дій та формулювання підозри, висунення та перевірки версій, проведення слідчих дій, а також визначення розміру завданої шкоди.

Для кримінальних правопорушень за фактом викрадання нафтопродуктів основним видом судової експертизи є дослідження нафтопродуктів та паливно-мастильних матеріалів. Також можуть бути призначені дактилоскопічна, трасологічна, техніко-криміналістична експертиза документів, почеркознавча, ґрунтознавча, судово-біологічна, ботанічна види судових експертиз.

Література:

1. Левченко Ю.О. Запобігання злочинам, що вчиняються у нафтогазовому комплексі України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 «Кримінальне право та криминологія; кримінально-виконавче право». К., 2008. 18 с.

2. Котовенко О.М. Кримінальна відповідальність за пошкодження об'єктів магістральних нафто-, газо- та нафтопродуктопроводів : автореф. дис... канд. юрид. наук: 12.00.08. Харків, 2002. 20 с.

3. Кудінов А.С. Особливості початкового етапу розслідування крадіжок нафти та нафтопродуктів із магістральних трубопроводів: дис. ... канд. юрид. наук: 12.00.09. Запоріжжя, 2013. 240 с.

DOI <https://doi.org/10.36059/978-966-397-357-9-26>

ДО ПИТАННЯ ЕВОЛЮЦІЇ ЗАСОБІВ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Недохлебов І. І.

*здобувач кафедри конституційного та адміністративного права
Запорізький національний університет
м. Запоріжжя, Україна*

Правове забезпечення інформаційної безпеки України має розглядатися як комплексне явище, що окрім законодавчих і підзаконних актів, які регламентують питання захисту інформаційних інтересів держави, включає в себе законодавство, яке визначає порядок функціонування окремих сфер

інформаційної діяльності (сфера медіа, сфера надання інформаційних послуг, видавнича та архівна справи тощо). Слід припустити, що за таких умов система правового забезпечення інформаційної безпеки повинна розглядатися у якості багаторівневої системи, яка включає в себе різні нормативно-правові акти.

Необхідно констатувати, що роль правового забезпечення інформаційної безпеки полягає у тому, щоб: 1) систематизувати перелік внутрішніх і зовнішніх загроз, які присутні в інформаційній сфері; 2) визначити пріоритетні напрями державної політики у сфері інформаційної безпеки; 3) регламентувати механізми забезпечення інформаційної безпеки та відповідний правовий статус спеціальних суб'єктів. Тобто, правове забезпечення, у даному випадку, відіграє основоположну роль, адже в ньому розкриваються як ідеологічні, так і процедурні питання захисту національних інтересів в інформаційній сфері.

В. М. Богущ до числа проблем побудови законодавства у сфері інформаційної безпеки відносить: неузгодженість в процесі формалізації загроз інформаційній безпеці в різних нормативно-правових актах; відсутність дієвих механізмів забезпечення інформаційної безпеки; відсутність практики постійного моніторингу та корегування загроз і викликів в інформаційній сфері; неналежне фінансування механізмів правового забезпечення інформаційної безпеки [1, с. 102].

Досліджуючи питання інформаційної безпеки М. В. Баран наголошує, що правове регулювання інформаційної безпеки повинно відбуватися в нерозривному зв'язку з урахуванням науково-технічного прогресу. До числа проблем правового забезпечення інформаційної безпеки дослідниця відносить: відсутність вичерпного збалансованого переліку видів даних, що становлять таємницю; недосконалість механізмів реалізації права на інформацію; недостатній рівень застосування інформаційних технологій в публічному управлінні [2, с. 133].

А. Ю. Нашинець-Наумова стверджує, що правове забезпечення є найважливішим елементом інформаційної безпеки. Його сутністю є здійснюване державою за допомогою системи правових засобів упорядкування суспільних відносин у цій сфері, їх юридичне закріплення та охорона, а його механізмом – система таких правових засобів. Відповідно, завданням правового забезпечення інформаційної безпеки є створення досконалої правової основи та системи контролю за інформаційною діяльністю з метою забезпечення стабільності інформаційної системи, попередження, виявлення та припинення правопорушень суб'єктами інформаційного права [3, с. 53].

О. Г. Ярема зазначає, що структура законодавства у сфері інформаційної безпеки багато в чому визначається основними напрямками захисту об'єктів інформаційної сфери, до числа яких слід

віднести: захист інформаційних права і свободи; захист інформації, інформаційних ресурсів та інформаційних систем від неправомірного впливу сторонніх осіб; захист інтересів особи, суспільства та держави від впливу шкідливої, небезпечної, недоброякісної інформації [4, с. 250]. Ця теза розкриває механізми формування системи правового забезпечення інформаційної безпеки, в основі яких є узгодження з ключовими сферами інформаційної діяльності.

Так, І. О. Валюшко розглядаючи проблеми трансформації законодавства в умовах російського вторгнення, акцентує увагу на тому, що система правового забезпечення інформаційної безпеки у поєднанні із реструктуризацією системи національної безпеки, дозволять створити потужний механізм стримування зовнішньої інформаційної агресії. Разом з тим науковець підкреслює, що побудова законодавства у такій важливій сфері як інформаційна безпека відбувається за принципом надолуження згаяного. Важливого значення набуває й контроль держави щодо виконання вже прийнятих юридичних норм, повне фінансове й кадрове забезпечення структур пов'язаних із системою інформаційної безпеки, активізація інституційних реформ, які відповідають нагальним потребам у зазначеній сфері [5, с. 40].

І. В. Олефір зазначає, що в Україні на певному рівні створена необхідна законодавча база для побудови та розвитку інформаційного суспільства. Однак, реалізація національних інтересів відповідно до програм розвитку інформаційного суспільства залежить від усвідомленого політичного та суспільного вибору акторів міжнародних відносин у геополітиці, наявності відповідної інфраструктури та психологічної готовності суспільства до змін [6, с. 28]. Означена теза доволі вдало окреслює ключові чинники, які впливають на процес еволюції засобів правового забезпечення інформаційної безпеки.

В Аналітичній записці «Проблеми нормативно-правового забезпечення інформаційної безпеки», підготовленої Національним інститутом стратегічних досліджень у 2014 році систематизовані наступні умови еволюції законодавства в зазначеній сфері: деформування інформаційного суверенітету України; зміни в середовищі, в рамках якого формується система інформаційної безпеки держави; необхідність створення нормативно-правових передумов зростання окремих сфер інформаційної діяльності; стрімке зростання залежності України від ефективності функціонування ключових інформаційних систем [7].

Г. Я. Аніловська пропонуємо визначати еволюцію правового забезпечення інформаційної безпеки через основні етапи розвитку інформаційних правовідносин. З огляду на це, дослідниця виділяє наступні етапи:

1) до початку XIX століття (в цей період основним завданням інформаційної безпеки був захист відомостей про події, факти, майно, місцезнаходження й інші дані, що мали для людини особисто або соціуму, до якого вона належала, життєве значення);

2) від 1816 до 1935 року (з розвитком технологій передачі інформації, почали розвиватись технології її захисту та відповідне законодавство);

3) від 1935 до 1946 року (основним способом забезпечення інформаційної безпеки в цей період було поєднання організаційних і технічних заходів, спрямованих на підвищення захищеності інформації);

4) середина XX століття (на цьому етапі завдання інформаційної безпеки вирішувались методами і способами обмеження фізичного доступу до устаткування засобів добування, перероблення й передачі інформації);

5) 1960-ті – 1970-ті роки (на цьому етапі з'явилися нові завдання для системи інформаційної безпеки, зокрема необхідність адміністрування й управління доступом до мережесих ресурсів, а також захист інформаційно-комунікаційних систем);

6) до середини 1980-их років (цей етап пов'язаний з використанням надмобільних комунікаційних пристроїв з широким спектром завдань, тобто загрози інформаційній безпеці стали набагато серйознішими);

7) від 1985 року – дотепер (стрімкий розвиток глобальних інформаційно-телекомунікаційних систем, а також широке застосування космічних засобів зв'язку, спонукає до пошуку нових високотехнологічних засобів захисту інформації) [8, с. 270].

Таким чином пропонуємо до числа чинників, які вплинули на еволюцію засобів правового забезпечення інформаційної безпеки віднести: 1) зміни у політичному контексті розбудови інформаційного суспільства; 2) низький рівень міжнародної інформаційної співпраці; 3) недостатній рівень розвитку інформаційної інфраструктури; 4) деформування інформаційного суверенітету України; 5) зростання ролі окремих сфер інформаційної діяльності; 6) зростання залежності України від ефективності функціонування ключових інформаційних систем; 7) стрімка глобалізація інформаційного простору; 8) поява нових загроз та викликів, зумовлених збройним конфліктом та тимчасовою окупацією окремих українських територій; 9) євроінтеграційна політика держави.

Література:

1. Богуш В. М. Інформаційна безпека держави: навч. посібник Київ: Видавництво МК-Пресс 2006. 432 с.
2. Баран М. В. Принципи правового регулювання інституту інформаційної безпеки. *Наук. вісник Ужгородського нац. ун-ту*. 2021. № 66. С. 129–134.

3. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.

4. Ярема О. Г. Предмет правового забезпечення інформаційної безпеки в інформаційному праві. *Науковий вісник Львівського державного університету внутрішніх справ*. 2016. № 2. С. 244–252.

5. Валюшко І. О. Інформаційна безпека України: трансформація після російського вторгнення. *Історико-політичні студії*. 2017. № 2 (8). С. 30–43.

6. Олефір І. В. Еволюція інформаційного суспільства в Україні. *S.P.A.C.E.* 2017. № 6. С. 26–29.

7. Проблеми нормативно-правового забезпечення інформаційної безпеки: Аналітична записка підготовлена Національним інститутом стратегічних досліджень у 2014 році. URL: <https://niss.gov.ua/doslidzhennya/informaciyni-strategii/problemi-normativno-pravovogo-zabezpechennya-informaciynogo> (дата звернення: 24.10.2023).

8. Аніловська Г. Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій: *Науковий вісник НЛТУ України*. 2008. № 18 (9). С. 267–280.

DOI <https://doi.org/10.36059/978-966-397-357-9-27>

КРИМІНАЛЬНО-ПРАВОВА ХАРАКТЕРИСТИКА ТА ЗАПОБІГАННЯ ПІРАТСТВУ НА МОРІ

Осадця Р. О.

*здобувач II курсу третього (освітньо-наукового) рівня
вищої освіти ступеня доктора філософії
за спеціальністю 081 – Право
кафедри кримінального права, процесу та криміналістики
Міжнародний гуманітарний університет
Науковий керівник: **Загороднюк С. О.**
кандидат юридичних наук, доцент
Міжнародний гуманітарний університет
м. Одеса, Україна*

Кримінально-правова характеристика піратства на морі визначається різними міжнародними конвенціями та національним законодавством країн. Основна міжнародна конвенція, яка регулює питання піратства, – це Конвенція Організації Об'єднаних Націй з морського права