очевидним для службової особи і чи усвідомлювала вона протиправність своєї поведінки [3].

Отже, у всіх випадках реалізації Пенсійним фондом України тих чи інших заходів запобіжного характеру, його посадові особи маю чітко дотримуватись змісту принципу законності у своїй діяльності.

Список використаних джерел

1. Теорія держави і права : підручник для студ. юрид. навч. закл./ за ред. О. В. Петришина. Харків: Право, 2014. 368 с.

2. Про застосування Конституції України при здійсненні правосуддя : постанова Пленуму Верховного Суду України від 01.11.1996 № 9. Постанови Пленуму Верховного Суду України в кримінальних справах (упоряд. В. В. Рожнова, А. С. Сизоненко, Л. Д. Удалова. Київ : ПАЛИВОДА А. В., 2011. С. 136-141.

3. Про судову практику у справах про перевищення влади або службових повноважень. Постанова Пленуму Верховного Суду України від 26.12.2003 №15. Режим доступу: https://zakon.rada.gov.ua/laws/show/v0015700-03.

Колб Роксолана Олегівна,
спеціаліст АТ КБ «Приватбанк», кандидат юридичних наук
Пирожик Олександр Веніамінович,
депутат Волинської обласної ради, уповноважений з антикорупційної діяльності комунального підприємства «Волинський обласний фтизіопульмонологічний медичний центр» Волинської обласної ради

ПРОБЛЕМИ КРИМІНАЛЬНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ У СУЧАСНИХ УМОВАХ

У чинному законодавстві України, включаючи Кримінальних кодекс (КК) (розділ XVI Особливої частини), передбачені відповідні правові механізми забезпечення інформаційної діяльності в нашій державі [1, с. 846-859].

Поряд з цим, торкаючись питання вибудови системи забезпечення інформаційної безпеки в Україні, неможливо обійти увагою зарубіжний досвід країн НАТО, які мають у цій сфері ту ж системну проблему, що й Україна, – необхідність запобігання та протидії інформаційній агресії та інформаційним війнам зі сторони Російської Федерації (РФ). При цьому, результати проведеного аналізу наукових та інших джерел свідчить про те, що навіть в одного з фундаторів НАТО – Сполучених Штатів Америки (США) – ця

проблема ставиться на друге місце після тероризму і розглядається як серйозна загроза національній безпеці нації.

Загалом, інформаційна безпека – це поняття, яке введене у науковий обіг досить давно, проте особливої актуальності воно набуло із розвитком технологій. Якщо в цілому узагальнити доктринальні підходи з означеного питання, то можна зробити висновок, що поняття «інформаційна безпека» слід розглядати на основі комплексного або інтегрального підходу як стан та процес захищеності життєво важливих інтересів особи, суспільства та держави, при якому вона, з одного боку, здатна ефективно протистояти дестабілізуючому та неправомірному впливу зовнішніх і внутрішніх інформаційних загроз, а з іншого – її постійне функціонування не створює інформаційних загроз для елементів самої системи і зовнішнього середовища. Відтак, можна констатувати, що інформаційна безпека – це стан захищеності інформації в системах і додатках, при якому зберігається цілісність та конфіденційність даних, їх стійкість до зовнішнього впливу.

Зазначений висновок ґрунтується на тому, що на початку 21 століття у США та розвинутих країнах Європи ввели у вжиток тезу про міжнародну інформаційну безпеку, визнавши, що незахищеність інформаційних ресурсів становить загрозу всьому світу. При цьому на Заході під цим розуміють стан, що забезпечується загальновизнаними і спеціальними принципами та нормами міжнародного права, який включає порушення міжнародного миру і безпеки у сфері інформації та комунікації як окремих держав, так і світового співтовариства в цілому [2].

Виходячи з цього та враховуючи сучасні проблеми, що склалися в Україні у зв’язку з гідридною війною РФ та масовим використанням «інформаційної зброї» з деструктивними проросійськими наративами та застосуванням проти Української держави «інформаційного тероризму» [3, с. 78-115], слід визнати, що їх вирішення неможливе без урахування позитивного досвіду забезпечення інформаційної безпеки країн НАТО, зокрема, на прикладі США – як одного із фундаторів цього Північноатлантичного блоку.

Список використаних джерел

1. Науково-практичний коментар Кримінального кодексу України. 2-ге вид., перероб. і допов./ за заг.ред. О. М. Джужі, А.В. Савченка та В. В. Чернєя. Київ: Юрінком Інтер, 2018. 1104 с.

2. Грицун О. О. Міжнародно-правове забезпечення міжнародної інформаційної безпеки. Дис. на здоб. наук, ступеня к.ю.н., спец. 12.00.11.КНУ імені Тараса Шевченка. Київ, 2016. 233 с.

3. Колб О. Г., Пирожик О. В., Дучимінська Л. М., Колб Р. О., Кухарчук Д. С.. Про зміст і соціально-правову природу деяких джерел, що посягають на національну безпеку України. *Ділектологія:*

монографія. Під заг. ред. І. М. Копотуна, С. В. Пєткова, P. Polian. Куновіце: Академія ГУСПОЛ: 2020, Т. 3. С. 78-115.

Конопельський Віктор Ярославович,
доктор юридичних наук, професор, завідувач кафедри кримінального права та кримінології Одеського державного університету внутрішніх справ
Дмитрієнко Юлія Сергіївна,
аспірант кафедри кримінального права та кримінології Одеського державного університету внутрішніх справ

ДЖЕРЕЛА КРИМІНОЛОГІЧНОЇ ІНФОРМАЦІЇ, ЯКІ ВИКОРИСТОВУЮТЬСЯ ДЛЯ ЗАПОБІГАННЯ ЗЛОЧИНАМ У СФЕРІ ВИКОНАННЯ ПОКАРАНЬ

Як показує вивчення архівних кримінальних проваджень, а також наукової літератури [1, с. 22-28], однією з детермінант, що сприяє вчиненню кримінальних правопорушень у сфері виконання покарань України, є неналежне використання існуючих на практиці джерел кримінологічної інформації щодо особи злочинця та причин і умов, які сформували та дали можливість у подальшому реалізувати її протиправну поведінку у процесі виконання-відбування покарань.

До таких джерел, зокрема, відносяться:

1. Кримінологічна інформація, що міститься в особових справах засуджених [2].
2. Така ж інформація, яка розміщена в інформаційно-пошукових системах правоохоронних органів [3].
3. Інформація, яка є лежить в основі індивідуальних програм соціально-виховної роботи із засудженими (ст. ст. 95-98 Кримінально-виконавчого кодексу (КВК)).
4. Інформація, яка отримана у результаті оперативно-розшукової діяльності в установах виконання покарань (ст. 104 КВК та Закон України «Про оперативно-розшукову діяльність»).
5. Інформація, яка стала наслідком реалізації заходів так званої слідчої профілактики (шляхом проведення негласних слідчих (розшукових) дій (ст. ст. 246-275 Кримінального процесуального кодексу (КПК)); здійснення інших слідчих (розшукових) дій; використання юридично значущої інформації, отриманої в порядку взаємодії з іншими правоохоронними органами).
6. Інша кримінологічна інформація, яка використовується учасниками сторони обвинувачення у кримінальному провадженні як докази та для встановлення обставин, які підлягають доказуванню (ст. ст. 84-94 КПК).