АДМІНІСТРАТИВНЕ ПРАВО

УДК 34.07

О. А. Марущак, к. ю. н., доцент,
К. Л. Стеченко, студентка

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРАВООХОРОННИХ ОРГАНІВ

Анотація. *Статтю присвячено дослідженню інформаційної безпеки правоохоронних органів. Визначається зміст та форми її забезпечення, розглядається діяльність провідних правоохоронних органів, що протидіють широкому колу загроз інформаційній безпеці України. Проаналізовано офіційні статистичні показники динаміки вчинення кіберзлочинів за останні роки.*

Ключові слова: *інформація; правоохоронні органи; інформаційна безпека; інформаційні ресурси; система захисту інформації; комп'ютерні кримінальні правопорушення (кіберзлочини).*

А. А. Марущак, к. ю. н., доцент,
Е. Л. Стеченко, студентка

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Аннотация. *Статья посвящена исследованию информационной безопасности правоохранительных органов. Определяется содержание и формы её обеспечения, рассматривается деятельность ведущих правоохранительных органов, противодействующих широкому кругу угроз информационной безопасности Украины. Проанализированы официальные статистические показатели динамики совершения киберпреступлений за последние годы.*

Ключевые слова: *информация; правоохранительные органы; информационная безопасность; информационные ресурсы; система защиты информации; компьютерные уголовные правонарушения (киберпреступления).*

O. A. Marushchak, Candidate of Legal Sciences,
Associate Professor,
K. L. Stechenko, Student

LEGAL PROVISION OF INFORMATION SECURITY OF LAW ENFORCEMENT AUTHORITIES

Abstract. *The article is devoted to the study of information security of law enforcement authorities. The content and forms of such support are determined, the activity of the leading law enforcement authorities that counteract a wide range of threats to information security of Ukraine is considered. The official statistical indicators of the dynamics of cybercrime for last years are analyzed.*

Keywords: *information; law enforcement authorities; information security; information resources; information security system; computer criminal offences (cybercrimes).*

Актуальність теми дослідження. Внаслідок надзвичайно широкого розповсюдження різноманітних систем обробки інформації та розширення локальних і глобальних комп'ютерних мереж, якими безпосередньо передається велика кількість інформації державного, комерційного, приватного характеру (в тому числі таємна інформація і службові відомості) виникає необхідність гарантування високого рівня інформаційної безпеки правоохоронних органів, адже неналежний рівень захищеності інформації завдає збитків як конкретній фізичній особі, так і є джерелом серйозних та непоправних загроз для розвитку держави і суспільства.

АДМІНІСТРАТИВНЕ ПРАВО

Постановка проблеми. XXI століття гордо назване «ерою інформаційних технологій». Саме тому вислів Уїнстона Черчіля «хто володіє інформацією, той володіє світом» стає все актуальнішим з кожним днем, адже нині інформація є силою та цінним стратегічним ресурсом, що потребує належного захисту. Із появою та стрімким розвитком глобальної мережі Інтернет індустрія обробки інформації та організації доступу до неї досягла величезних масштабів. З огляду на це, важливого значення набуває забезпечення інформаційної безпеки вітчизняних державних інституцій, зокрема її правоохоронних органів в аспекті захисту таємної інформації і відомостей службового характеру від незаконного доступу та неправомірного використання.

Аналіз останніх досліджень і публікацій. Забезпечення інформаційної безпеки у напрямку реалізації державної інформаційної політики в діяльності правоохоронних органів України розглядалось у наукових працях Д. О. Беззубова, О. В. Бойченка, Ю. Ф. Кравченка, Д. О. Красікова, О. В. Олійника, Ю. А. Родичева, О. В. Руснака, А. І. Суббота, Г. М. Шорохової та інших.

Виділення недосліджених частин загальної проблеми. Наразі науковцями майже не проводились комплексні дослідження щодо форм, способів, особливостей та принципів забезпечення інформаційної безпеки правоохоронних органів. Вважаємо, що необхідною є розробка та прийняття Закону України «Про інформаційну безпеку правоохоронних органів», який, з одного боку, внесе ясність у дане питання, а з іншого – послугує стимулюючим фактором для дискусій у наукових колах.

Постановка завдання. У цій роботі маємо на меті здійснити ґрунтовний аналіз змісту інформаційної безпеки правоохоронних органів, її правового забезпечення, а також дослідити її нинішній стан.

Виклад основного матеріалу. Сучасний процес бурхливого розвитку інформаційних технологій призвів не тільки до якісної зміни способів зберігання і обробки інформації, а й поставив ряд серйозних соціальних, політичних, економічних та правових проблем для держави й суспільства. Разом з тим, активне застосування інформаційних технологій у всіх сферах життя істотно вплинуло на діяльність правоохоронних органів – важливих установ та організацій державного апарату, які здійснюють захист національної безпеки, забезпечують стан законності й правопорядку, захищають права, свободи та інтереси громадян. На передній план висувається проблема їхньої інформаційної безпеки як самостійного і стрижневого складника національної безпеки України, адже ненадійний захист інформації може не лише завдати збитків конкретній фізичній особі в разі незаконного доступу до персональних даних про неї, їх використання чи поширення, а й бути джерелом серйозних та непоправних загроз для розвитку держави і суспільства. Ще одним показником важливості гарантування інформаційної безпеки для людини, держави і суспільства виступає закріплення у ст. 17 Конституції України положення про те, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [1].

Поняття «інформаційної безпеки» тлумачиться у спеціальних нормативно-правових актах, наукових дослідженнях та розкривається у практичній діяльності органів державного апарату, зокрема правоохоронних.

Так, на міжнародному рівні зазначене поняття розуміється як «стан захищеності інформаційної сфери суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій, держави» [2].

Власне українське законодавство тлумачить поняття інформаційної безпеки ширше, визначаючи її як «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [3]. На нашу думку, зазначена дефініція дає досить повну характеристику досліджуваного нами поняття, фіксуючи

при цьому конкретні приклади порушення інформаційної безпеки та посилаючись на якісні властивості інформації в цілому – її цілісність, конфіденційність та доступність.

Зокрема, цілісністю є властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення; конфіденційністю виступає властивість інформації бути захищеною від несанкціонованого ознайомлення; доступність визначається як властивість інформації бути захищеною від несанкціонованого блокування [4].

Формування нової, цілісної та науково обґрунтованої системи гарантування інформаційної безпеки має забезпечуватись не лише на державному рівні, а й на основі поєднання законодавчої, виконавчої, судової, контрольної та, зокрема правоохоронної, форм діяльності усіх державних органів у взаємодії з органами місцевого самоврядування, організаціями, установами та громадянами. Адже, неможливо уявити діяльність правоохоронних органів без збору, обробки та використання інформації, її накопичення й систематизації в базах даних.

Досліджуючи дане питання, А. І. Суббот зазначає, що інформаційна безпека правоохоронних органів – це «спроможність їхніх працівників убезпечити інформаційні ресурси від несанкціонованого доступу до них» [5, с. 21]. Д. О. Беззубов розглядає інформаційну безпеку правоохоронних органів як «стан інформації щодо діяльності правоохоронних органів, при якому з нею ознайомлені лише суб'єкти, які передбачені чинним законодавством та виключено можливість надходження інформації до третіх осіб» [6, с. 18].

Найбільш повним, на нашу думку, є визначення О. В. Бойченка, який вважає, що інформаційна безпека правоохоронних органів полягає у колегіальному обговоренні й документальному закріпленні основних напрямів адміністративної діяльності, пов'язаної з процесами інформатизації правоохоронних органів, захистом відомчої інформації, а також профілактикою і боротьбою з правопорушеннями, що вчиняються з використанням інформаційних технологій – комп'ютерними кримінальними правопорушеннями [7, с. 9].

Особливим правоохоронним органом, який служить суспільству шляхом забезпечення публічної безпеки й порядку, боротьби зі злочинністю, охорони прав і свобод людини, інтересів суспільства й держави та протидіє широкому колу загроз інформаційної безпеки, виступає Департамент кіберполіції як структурний підрозділ Національної поліції України. Він спеціалізується на:

- запобіганні кіберзлочинності (попередженні, виявленні, розкритті кримінальних правопорушень, вчинених з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних інтернет-мереж і систем);
- завчасному інформуванні населення про кіберзлочинців та появу нових видів кіберзлочинів;
- впровадженні програмних засобів для систематизації кіберінцидентів.

За вчинення «комп'ютерних» кримінальних правопорушень (кіберзлочинів) в Україні передбачена кримінальна відповідальність, яка регламентована розділом XVI Кримінального кодексу України (далі – КК України). «Комп'ютерні» кримінальні правопорушення вчиняються з використанням різноманітних схем протиправної діяльності, у тому числі через незаконне заволодіння інформацією та проникнення в державні інформаційні системи та бази даних. Отримавши цю інформацію, зловмисники використовують її для вчинення інших протиправних дій та правопорушень. На сьогоднішній день, масового поширення у цій сфері досягли такі протиправні діяння, як: несанкціоноване втручання в роботу автоматизованих систем та збут інформації з обмеженим доступом, створення і розповсюдження комп'ютерних вірусів тощо.

Проаналізувавши офіційні статистичні показники за 2015-2019 роки [8-12], можна цілісно й аргументовано дослідити динаміку вчинення кіберзлочинів та встановити чіткі результати діяльності Департаменту кіберполіції України (Табл. 1).

Як бачимо, статистичні показники вказують як на підвищення рівня криміналізації інформаційно-телекомунікаційної сфери, так і на адекватне реагування Департаменту кіберполіції України щодо забезпечення інформаційної безпеки та мінімізацію загроз шляхом виявлення, попередження та розкриття комп'ютерних кримінальних правопорушень.

Ще одним із провідних органів спеціального призначення із правоохоронними функціями, який спрямовує свою діяльність на забезпечення інформаційної безпеки як вагомого елементу

національної безпеки України, є – Служба безпеки України. Саме Служба безпеки України, відповідно до ч. 1 ст. 19 Закону України «Про національну безпеку України», є спеціальним уповноваженим органом державної влади у сфері забезпечення охорони державної таємниці. Так, державна таємниця (секретна інформація) – це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України [13].

Таблиця 1

Види «комп'ютерних» кримінальних правопорушень та кількість осіб, притягнутих до кримінальної відповідальності за них

Кримінальне правопорушення	2015 рік	2016 рік	2017 рік	2018 рік	2019 рік
Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України)	24	25	40	38	32
Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1 КК України)	2	2	2	8	18
Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК України)	3	3	3	3	10
Несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України)	8	4	11	21	7
УСЬОГО:	37	34	56	70	67

Ще одним із провідних органів спеціального призначення із правоохоронними функціями, який спрямовує свою діяльність на забезпечення інформаційної безпеки як вагомого елементу національної безпеки України, є – Служба безпеки України. Саме Служба безпеки України, відповідно до ч. 1 ст. 19 Закону України «Про національну безпеку України», є спеціальним уповноваженим органом державної влади у сфері забезпечення охорони державної таємниці. Так, державна таємниця (секретна інформація) – це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України [13].

Головним завданням Служби безпеки України для забезпечення належного рівня інформаційної безпеки є усунення таких негативних факторів як:

- посилення негативного впливу на інформаційний простір України, що загрожує розмиванням суспільних цінностей і національної ідентичності;
- недостатні обсяги вироблення конкурентоспроможного національного інформаційного продукту;
- наближений до критичного стан безпеки інформаційно-комп'ютерних систем в галузі державного управління, фінансової та банківської сфери, енергетики, транспорту, внутрішніх і міжнародних комунікацій тощо [14, с. 75].

Безсумнівно, на ефективність забезпечення інформаційної безпеки правоохоронних органів впливає діюча нормативно-правова база у цій сфері, а також сучасні напрями і форми такого забезпечення. Оцінюючи нинішній стан правового забезпечення інформаційної безпеки правоохоронних органів України, А. І. Суббот розмежовує законодавчу і технічну форми її гарантування. Перша, у свою чергу, здійснюється шляхом ухвалення нормативно-правових актів, які встановлюють чіткі правила використання й обробки інформації, доступ до якої обмежено, та визначають ступінь відповідальності за порушення цих правил, а друга – через регулювання доступу до всіх ресурсів інформаційної системи, регламентацію порядку роботи

користувачів і персоналу та обмеження права доступу до певних файлів [5, с. 22]. Ми погоджуємось з висновком Д. О. Красікова, що інформаційна безпека правоохоронних органів забезпечується в організаційній та правовій формах [15, с. 11-15]. Отож, організаційна форма передбачає налагодження роботи правоохоронних органів, пов'язаної з обігом, збиранням, обробкою та використанням інформації щодо забезпечення інформаційної безпеки, а правова форма представлена виданням законів та підзаконних нормативно-правових актів (наказів, розпоряджень, інструкцій, положень, планів) з цього питання.

Основними нормативно-правовими актами, які регламентують забезпечення інформаційної безпеки правоохоронних органів є Конституція України, Закони України «Про національну безпеку України», «Про інформацію», «Про національну програму інформатизації», «Про захист інформації в автоматизованих системах», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про Національну поліцію України», «Про Службу безпеки України»; Кримінальний кодекс України (розділ XVI), постанова Кабінету Міністрів України «Про деякі питання захисту інформації, охорона якої забезпечується державою», укази Президента України «Про Доктрину інформаційної безпеки України», «Про Положення про технічний захист інформації в Україні» та інші спеціальні нормативно-правові акти, які регламентують діяльність державних органів, установ та організацій у цій сфері, а також встановлюють їхні повноваження щодо забезпечення інформаційної безпеки.

Висновки. Стрімке впровадження комп'ютерних технологій в повсякденне життя випереджає темпи розвитку соціальних і правових відносин в інформаційному суспільстві та зумовлює появу нових проблем, пов'язаних із кіберзлочинністю та посяганням на інформаційну безпеку. Інформаційна безпека являє собою стан захищеності інформації, при якому гарантується її захищеність від загроз несанкціонованого доступу, а її використання є раціональним і результативним для розвитку суспільства та усіх його складових.

На жаль, нині норми чинного вітчизняного законодавства повністю не визначають вимоги і стандарти, заходи та способи забезпечення інформаційної безпеки діяльності правоохоронних органів. З огляду на це, виникає потреба в реалізації системного підходу, що включає в себе: по-перше, поліпшення правового забезпечення інформаційної безпеки правоохоронних органів на державному рівні; по-друге, удосконалення діяльності правоохоронних органів щодо гарантування власної інформаційної безпеки зсередини із обов'язковим законодавчим закріпленням відповідальності службових осіб за недотримання вимог інформаційної безпеки. Оскільки, саме ефективна нормативно-правова база, яка спрямована на регулювання відносин у всіх сферах інформаційного суспільства, виступає дієвим засобом нейтралізації значної частини внутрішніх і зовнішніх загроз інформаційній безпеці як самостійного елемента національної безпеки України.

Список використаних джерел:

1. Конституція України: Закон України від 28 червня 1996 року № 254к/96-ВР / Верховна Рада України // Офіційний веб-портал. - URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#n4976 (дата звернення: 15.11.2020).

2. Угода про вільний доступ і порядок обміну відкритою науково-технічною інформацією держав-учасниць СНД: Угода від 11 вересня 1998 року № 997_889 / Верховна Рада України // Офіційний веб-портал. URL: https://zakon.rada.gov.ua/laws/show/997_889/conv#Text (дата звернення: 15.11.2020).

3. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09 січня 2007 року № 537-V / Верховна Рада України // Офіційний веб-портал. - URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення: 15.11.2020).

4. Про Положення про технічний захист інформації в Україні: Указ Президента України від 27 вересня 1999 року № 1229/99. / Верховна Рада України // Офіційний веб-портал. - URL: https://zakon.rada.gov.ua/laws/show/1229/99#top (дата звернення: 15.11.2020).

5. Суббот, А. І. Інформаційна безпека діяльності працівників правоохоронних органів / А. Суббот // Віче. - 2014. - № 22. - С. 19-22.

6. Беззубов, Д. О. Інформаційна безпека органів внутрішніх справ у системі координації діяльності правоохоронних структур України / Д. О. Беззубов // Міліція України. - 2012. - № 5/6. - С. 18-19.

7. Бойченко, О. В. Інформаційна безпека в органах внутрішніх справ України (організаційно-правові засади): монографія / О. В. Бойченко. - Сімферополь: ВАТ «Сімферопольська міська друкарня», 2009. - 288 с.

8. Звіт про кількість засуджених, виправданих, справи щодо яких закрито, неосудних, до яких застосовано примусові заходи медичного характеру та види кримінального покарання за 2015 рік. Судова статистика. Форма № 6. / Судова влада України. - URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2015 (дата звернення: 15.11.2020).

АДМІНІСТРАТИВНЕ ПРАВО

9. Звіт про кількість засуджених, виправданих, справи щодо яких закрито, неосудних, до яких застосовано примусові заходи медичного характеру та види кримінального покарання за 2016 рік. Судова статистика. Форма № 6. / Судова влада України. - URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2016 (дата звернення: 15.11.2020).

10. Звіт про кількість засуджених, виправданих, справи щодо яких закрито, неосудних, до яких застосовано примусові заходи медичного характеру та види кримінального покарання за 2017 рік. Судова статистика. Форма № 6. / Судова влада України. - URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2017 (дата звернення: 15.11.2020).

11. Звіт про осіб притягнутих до кримінальної відповідальності та види кримінального покарання за 2018 рік. Судова статистика. Форма № 6. / Судова влада України. - URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2018 (дата звернення: 15.11.2020).

12. Звіт про осіб притягнутих до кримінальної відповідальності та види кримінального покарання за 2019 рік. Судова статистика. Форма № 6. / Судова влада України. - URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2019 (дата звернення: 15.11.2020).

13. Про державну таємницю: Закон України від 21 січня 1994 року № 3855-XII. / Верховна Рада України // Офіційний веб-портал. - URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 15.11.2020).

14. Руснак, О. В. Національна безпека в інформаційній сфері: повноваження правоохоронних органів в її забезпеченні / О. В. Руснак // Правова інформатика. - 2013. - № 4 (40). - С. 72-78.

15. Красіков, Д. О. Правове забезпечення інформаційної безпеки в діяльності органів внутрішніх справ України : автореф. дис. канд. юрид. наук: 12.00.07 / О. Д. Красіков. - Київ, 2012. - 20 с.

Надійшла 18.11.2020

Бібліографічний опис для цитування :

Марущак, О. А. Правове забезпечення інформаційної безпеки правоохоронних органів / О. А. Марущак, К. Л. Стеченко // Актуальні проблеми юридичної науки та практики. – 2020. – № 1 (6). – С. 31-36.