DOI: https://doi.org/10.37634/efp.2024.5.1
УДК 343.3/.7

Андрій Павлович ***КОЛЕСНІКОВ***
к.е.н., доцент, Західноукраїнський національний університет
ORCID: https://orcid.org/0000-0003-3064-4133
e-mail: kole.ua@gmail.com

ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В ДІЯЛЬНОСТІ ОРГАНІВ ЗДІЙСНЕННЯ ПРАВОСУДДЯ

У статті досліджено дефініцію категорії «інформація» в наукових працях та законодавстві України та окреслено необхідність урахування галузевого аспекту при її трактуванні. Визначено об'єкти правового захисту вважаємо у сфері роботи з інформацією та доведено необхідність зарахування до них відомості про суб'єктів, що мають доступ до роботи з інформаційними ресурсами та інформаційними системами. Окреслено нові виклики у сфері захисту інформації, що виникли під час військового вторгнення росії. Обґрунтовано необхідність застосування системного підходу до забезпечення інформаційної безпеки в судовій системі. Звернено увагу на проблему недотримання посадовими особами елементарних правил інформаційної гігієни, а також на роль окремих спеціалізованих структурних підрозділів Вищої ради правосуддя в забезпеченні інформаційної безпеки у судовій системі. Окреслено особливість підходу до захисту персональних даних учасників судового процесу.

Ключові слова: *суд, правосуддя, інформаційне забезпечення здійснення правосуддя, захист інформації в судових органах, об'єкти правового захисту, захист персональних даних суб'єктів судової влади*

ВСТУП

Сприйняття інформації як одного з визначальних ресурсів розвитку суспільства є загальновизнаним фактом. Від якості її оброблення, своєчасності та повноти отримання та фаховості використання значно залежить ефективність прийняття рішень. Водночас досягнення зазначених результатів потребує формування і реалізацію надійних механізмів захисту інформації. Захист інформації в діяльності органів здійснення правосуддя є критично важливим аспектом, особливо у зв'язку з розвитком цифрових технологій. Важливим тут є забезпечення конфіденційності та цілісності даних, що сприятиме зростанню довіри до судової системи і забезпеченню прав і свобод людини.

Питання захисту інформації, зокрема в діяльності органів здійснення правосуддя, неодноразово ставали об'єктом наукових досліджень. С. Демченко у праці [8] та С. Банах у праці [9] розглядали інформацію як теоретичну категорію, роблячи акцент на її застосуванні у праві. Правові аспекти захисту інформації в Єдиній судовій інформаційно-телекомунікаційній системі розглядали В. Теремецький та Є. Дуліба у праці [10], а також Ю. Георгієвський у праці [11]. М. Шепітько у праці [12] робить правовий аналіз захисту інформації у здійсненні правосуддя й окреслює загрози впливу застосування штучного інтелекту в системі захисту інформації. Водночас подальшого дослідження потребує вивчення об'єктів захисту інформації та загроз її порушення.

МАТЕРІАЛИ ТА МЕТОДИ

Для дослідження та узагальнення теоретичних положень у статті застосовано теоретичний аналіз. Аналіз нормативно-правових актів проведено із застосуванням формально-юридичного методу. Крім того, у статті застосовано комплекс загальнонаукових та конкретно-наукових методів дослідження, таких як логічний, метод аналогій та узагальнення.

МЕТА статті – дослідження особливостей захисту інформації в діяльності органів здійснення правосуддя.

РЕЗУЛЬТАТИ

Термін «інформація» є похідним від латинського *informatio,* що тлумачиться як роз'яснення (викладення). Вважаємо, що у загальносвітоглядному розумінні інформацію варто розглядати у двох вимірах: кількісному та якісному. Перший проявляється в її сприйнятті у матеріальній формі (число, слово, звук тощо), другий – як спосіб передачі корисних відомостей. В контексті цього дослідження обидва прояви можуть бути об'єктами правового захисту.

Закон України «Про інформацію» визначає останню як «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [3]. Водночас об'єктом інформаційних відносин (а отже, й захисту) Закон визначає інформацію. Однак ці положення може бути уточнено та адаптовано відповідно до контексту їх застосування. Множинність законодавчих визначень можна прослідкувати зі сторінки «Законодавство України» офіційного сайту Верховної ради України. Застосувавши функцію пошуку термінології законодавства, визначення категорії «інформація» знайдено в 32 документах. Проаналізувавши ці документи автором ідентифіковано 17 різних визначень, окремі з яких адаптовано під галузеві особливості нормативного акта.

Змістовним є дослідження С. Демченко, яка розглядає кібернетичний, філософський та правовий аспекти категорії «інформація», та обґрунтовує необхідність диверсифікації даної категорії залежно від галузевої спрямованості [8].

Вирішення питань захисту інформації передбачає визначення об'єктів, на яких цей захист буде спрямовано. З одного боку, об'єктом правового захисту є інформація, що міститься в правових реєстрах і базах даних з обмеженим доступом, з іншого – це інформація про суб'єктів здійснення правосуддя.

Основи правового захисту інформації, що розміщена у формі реєстрів закладено в Законі України «Про захист інформації в інформаційно-комунікаційних сис-

 © А.П. КОЛЕСНІКОВ, 2024

темах». Відповідно до нього доступ до інформації визначається наданням користувачу можливості її обробляти, а будь-які дії, що вчиняються з порушенням встановленого порядку доступу до цієї інформації визначаються як несанкціоновані, і такі, що порушують її цілісність. Також в Законі визначається окремо визначається категорія оброблення інформації, як «збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів» [2]. Так, бачимо наявність додаткового чинника роботи з інформацією, яка може бути здійснена як автоматизовано, так і за участю людини. У цьому контексті звернемо увагу на ст. 2 цього ж Закону, де об'єктами захисту інформації в системі визначено «інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації» [2]. Вважаємо, що в статтю 2 Закону потрібно внести зміни, надавши їй аспекту суб'єктності, тобто до об'єктів захисту додати методи та алгоритми роботи з інформацією.

Враховуючи це, об'єктами правового захисту у сфері роботи з інформацією вважаємо:

1. Інформаційні ресурси – це сукупність даних, зібраних у різних формах представлення, таких як реєстри, бази даних, системи та інші цифрові чи паперові джерела. Вони можуть містити конфіденційну інформацію, персональні дані, комерційну таємницю чи інші відомості, що потребують захисту від несанкціонованого доступу, модифікації або розголошення.

Приклади інформаційних ресурсів: реєстри (державні, реєстри у сфері права, реєстри майна тощо); бази даних (клієнтські, наукові, юридичні тощо); цифрові архіви та сховища (бібліотеки, наукові репозиторії тощо); паперові документи (договори, звіти, облікові книги тощо).

2. Інформаційні системи (організаційно-технічна система, в якій реалізується технологія оброблення інформації із застосуванням технічних і програмних засобів [2]).

Приклади інформаційних систем: системи електронного документообігу; системи управління базами даних; системи електронної комерції; системи контролю доступу та безпеки.

3. Відомості про суб'єктів, що мають доступ до роботи з інформаційними ресурсами та інформаційними системами. Важливим аспектом захисту інформації є контроль доступу до інформаційних ресурсів та систем. Тому необхідно мати чіткі відомості про суб'єктів, які мають право працювати з такими ресурсами та системами, а також визначити їхні повноваження та обмеження.

Приклади відомостей про суб'єктів доступу: облікові дані користувачів (імена, паролі, посади, рівні доступу); політики та процедури доступу до інформаційних ресурсів та систем; журнали реєстрації дій користувачів (аудит доступу та змін); списки осіб, уповноважених на управління інформаційними ресурсами та системами.

Вторгнення російської федерації в Україну 24 лютого 2022 р. показало якісно нові вимоги до підходів захисту інформації. Результатом розуміння глобальності викликів стало закриття в перші дні вторгнення фактично всіх реєстрів. Також відповідно до Рішення Ради суддів України № 11 від 25 березня 2022 р. зазначено, що право особи на доступ до інформації, гарантоване ст. 34 Конституції України, не є абсолютним і може підлягати обмеженням. Такі обмеження мають бути винятками, які передбачені законом, переслідувати одну або декілька законних цілей і бути необхідними у демократичному суспільстві [4]. Так, Рада суддів України вказує на актуальність більш жорсткого застосування норми ч. 2 ст. 6 Закону України «Про до публічної інформації» про те, що обмеження доступу до публічної інформації можливе: в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи кримінальним правопорушенням, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя; розголошення інформації може завдати істотної шкоди цим інтересам; шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні [5]. Військове вторгнення зробило цю норму Закону як ніколи актуальною.

У зв'язку зі значним зростанням ролі органів забезпечення правопорядку в умовах необхідності розслідування воєнних злочинів і забезпечення невідворотності покарання за колабораційну діяльність, розголошення інформації про діяльність державних органів, зокрема судів, може піддавати ризику життя та здоров'я їхніх представників. До того ж збір відповідної інформації під час конфлікту може мати ознаки диверсійної діяльності, спрямованої проти України. У світлі такого розуміння прийнято рішення, відповідно до якого у разі отримання запитів на надання будь-якої публічної інформації про діяльність судів та інших установ системи правосуддя, копії таких запитів слід негайно направляти до Служби безпеки України для ретельної перевірки осіб, які збирають цю інформацію, та їхніх мотивів.

Потреба у зміцненні заходів захисту інформації в державних установах підтверджується великою кількістю кібератак з боку росії. За даними Урядової групи реагування на комп'ютерні надзвичайні події України CERT-UA, що функціонує у структурі Держспецзв'язку, такі напади відбуваються систематично і часто зумовлені порушенням простих правил інформаційної безпеки.

Фахівці відзначають, що здебільшого несанкціонований доступ до інформаційних комп'ютерних систем об'єкта атаки здійснювався заздалегідь, часто за рік або й більше. Крім того, для проникнення до мережі зловмисники застосовували облікові записи VPN, а також експлуатували вразливості програмного забезпечення та недоліки у налаштуваннях публічно доступних інформаційних систем. Успішність багатьох кібератак часто зумовлено недбалістю керівників та виконавців на місцях, які ігнорують інформацію про поточні кіберзагрози. Водночас власники системи роблять одні й ті ж помилки: не застосовують двофакторну автентифікацію, не забезпечують сегментацію мережі, особливо стосовно обмеження адміністративного доступу, та не контролюють поверхню атаки, такі як вразливе програмне забезпечення, «відкриті порти» тощо [6].

Тимчасове повне закриття реєстрів у сфері забезпечення здійснення правосуддя стало викликом для за-

безпечення прозорості судочинства та забезпечення права на доступ до публічної інформації. Ця ситуація підкреслила необхідність підвищення стійкості інформаційних систем органів правосуддя до кібератак та витоків даних. Наявна система захисту виявилася недостатньо надійною в умовах військової агресії.

Для вирішення цієї проблеми потрібно системно підходити до питання інформаційної безпеки в судовій системі.

По-перше, необхідно посилити технічний захист реєстрів та інших баз даних шляхом застосування сучасних методів кібербезпеки, застосування ефективних протоколів шифрування та регулярного резервного копіювання.

По-друге, необхідно вдосконалити законодавство та розробити чіткі процедури, щоб забезпечити баланс між захистом даних та правом на інформацію в надзвичайних ситуаціях, таких як війна або кібератаки. Має бути передбачено механізми селективного обмеження доступу до чутливої інформації без необхідності повного закриття реєстрів.

По-третє, надзвичайно важливо навчити та підвищити обізнаність персоналу судів та правоохоронних органів у питаннях кібергігієни та безпеки інформації.

Отже, з досвіду закриття реєстрів на початку вторгнення стало очевидним, що в цій діяльності органів здійснення правосуддя виявлено системні прогалини у сфері захисту інформації. Щоб уникнути подібних проблем у майбутньому, необхідно вжити комплексних заходів технічного, законодавчого та освітнього характеру в цій життєво важливій сфері.

Вирішенням завдань захисту інформації в органах здійснення правосуддя займаються окремі структурні підрозділи. Зокрема, у структурі Вищої ради правосуддя функціонує Управління інформаційних технологій та захисту інформації, в межах якого діють підрозділи**:** Управління інформаційних технологій та захисту інформації; Відділ технічного забезпечення та захисту інформації від витоку технічними каналами; Відділ адміністрування та захисту інформації в автоматизованих системах; Відділ з питань функціонування Єдиної судової інформаційної (автоматизованої) системи. До завдань Управління серед інших відносяться:

− забезпечення конфіденційності, цілісності, доступності та спостережливості інформації, вимога до захисту якої регламентується наявним законодавством України у сфері захисту інформації;

− дослідження технології оброблення інформації, що становить інформацію з обмеженим доступом в АС з метою виявлення можливих каналів витоку та інших загроз для безпеки інформації;

− визначення заходів, спрямованих на реалізацію політики безпеки;

− підтримка необхідного рівня захищеності інформації, ресурсів і технологій в АС;

− формування у користувачів АС розуміння необхідності виконання вимог нормативно-правових актів, розпорядчих документів, що стосуються захисту інформації;

− організація і забезпечення захисту інформації баз даних у роботі з Інтернет та електронною поштою.

Питання оброблення персональних даних осіб суб'єктів судової влади є важливим та потребує уважного підходу з урахуванням необхідності забезпечення балансу між правом на приватність та принципом прозорості в діяльності державних органів. З одного боку, особи, що займають публічні посади, повинні розуміти, що їхній спеціальний статус передбачає певний рівень відкритості та відповідно обмежену сферу особистого життя, а з іншого − це не означає, що їхні особисті дані може бути використано та поширено без обмежень.

У своєму рішенні від 20 січня 2012 р. Конституційний Суд України зазначив, що публічний характер органів державної влади та їхніх посадових осіб потребує оприлюднення певної інформації для забезпечення довіри суспільства та підтримки авторитету влади. Однак персональні дані можуть включати не лише інформацію про самих посадовців, але й про членів їхніх сімей, які мають гарантоване Конституцією право на захист приватного та сімейного життя. Так, в кожному окремому разі потрібно знайти рівновагу та вирішити, коли розголошення персональних даних є важливим для суспільного інтересу, а коли воно може порушувати права людини [8].

Інформація про суддів та працівників суду, включаючи їхні персональні дані, може містити конфіденційну і надзвичайно чутливу інформацію, таку як дані про етнічне походження, політичні переконання, релігійні уподобання, стан здоров'я тощо. Розголошення цієї інформації може становити серйозну загрозу безпеці, незалежності та об'єктивності суддів у процесі вирішення справ. Тому важливо забезпечити ефективний захист цих даних від несанкціонованого доступу, витоку або неправомірного використання.

Законодавство України встановлює конкретні вимоги та обмеження до оприлюднення персональних даних осіб, які займають посади в судовій системі. Наприклад, персональні дані фізичних осіб, які претендують на виборні посади або вже займають посади державних службовців першої категорії, зазвичай не вважаються обмежено доступною інформацією за винятком тих даних, які закон визначає як конфіденційні. Водночас персональні дані членів родини суддів та працівників судів зазвичай підлягають захисту від незаконного розголошення. Крім того, законодавство України передбачає, що декларації про доходи осіб, які претендують на посади в судових органах або вже їх займають, не вважаються конфіденційною інформацією, а також їхні персональні дані, за винятком тих, які закон визначає як обмежено доступну інформацію. Це означає, що певний обсяг персональних даних посадових осіб має бути доступним для загального ознайомлення з метою забезпечення прозорості та відповідальності влади.

Водночас оброблення особистих даних осіб, які мають владні повноваження, а також всіх інших фізичних осіб, повинно відбуватися відповідно до принципів та вимог законодавства про захист персональних даних. Органи влади мають чітко визначені цілі для оброблення таких даних, а також встановлені процедури їх збору, зберігання, використання та утилізації. Важливо чітко відокремлювати загальні персональні дані від тих, які відносяться до особливих категорій, оскільки останні потребують додаткових заходів безпеки. Суди повинні публікувати достатньо інформації про свою діяльність та прийняті рішення, щоб громадськість могла здійснювати необхідний нагляд за їхньою роботою. Водно-

час ця інформація повинна бути деперсоналізована для захисту персональних даних учасників судових процесів.

Важливо також забезпечити належний контроль за доступом до персональних даних суб'єктів судової влади, щоб унеможливити їх несанкціоноване чи протиправне використання. Кожна посадова особа, що працює з персональними даними, повинна дотримуватись інструкцій, визначених внутрішніми розпорядчими документами.

Дотримуючись принципів законності, обґрунтованості цілей, міри необхідності й пропорційності, органи державної влади мають забезпечити прозорість своєї діяльності, не порушуючи одночасно право на приватність посадових осіб та членів їхніх сімей. Лише комплексні заходи організаційного, технічного та правового характеру здатні забезпечити належний рівень захисту конфіденційних даних, не порушуючи заразом принципи відкритості та підзвітності судової системи.

ВИСНОВКИ

Захист інформації в діяльності органів здійснення правосуддя є важливим інструментом дієвості судової системи, тому чітке визначення об'єктів захисту дасть змогу оптимізувати дієвість інструментів його забезпечення. Важливим тут є захист не лише ресурсів та інформаційних систем, але й відомостей про осіб, які мають доступ до роботи з інформаційними ресурсами та інформаційними системами. Водночас важливим є не лише забезпечення процедурних аспектів, але й дотримання базових методів інформаційної гігієни. Досягнення цього передбачає реалізацію системного підходу до питання інформаційної безпеки в судовій системі.

Список використаних джерел

1. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник. Харків, 2020. 162 с.

2. Про захист інформації в інформаційно-комунікаційних системах. Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

3. Про інформацію. Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

4. Рішення Ради суддів України від 25 березня 2022 року № 11. URL: https://rsu.gov.ua/uploads/news/richenarsu11250322-f68cadf705.pdf

5. Про доступ до публічної інформації. Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

6. Щодо обстановки в сфері кібер на 23-24 лютого 2024 року. URL: https://cert.gov.ua/article/6277822

7. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України. URL: http://zakon2.rada.gov.ua/laws/show/v002p710-12

8. Демченко С. Підходи до змісту поняття «інформація»: кібернетичний, філософський, правовий. *Jurnalul juridic national: teorie şi practică*. 2016. № 1/2 (17) С.35-38.

9. Банах С. Поняття та особливості інформації як теоретичної категорії. *Актуальні проблеми правознавства*. 2019. №4 (20). С. 226-231.

10. Теремецький В.І., Дуліба Є.В. Особливості впровадження та функціонування єдиної судової інформаційно-телекомунікаційної системи як інструмента електронного правосуддя. *Форум права*. 2023. № 75 (2). С. 130-143.

11. Георгієвський Ю.В. Пропозиції щодо правового забезпечення захисту інформації у Єдиній судовій інформаційно-телекомунікаційні системі. *Юридичний науковий електронний журнал*. 2020. № 3. С. 204–208.

12. Шепітько М. Кримінально-правова охорона інформаційної безпеки під час здійснення правосуддя. *Питання боротьби зі злочинністю*. 2022. Вип. 4. С. 69-75.

References

1. Manzhai O.V., Manzhai I.A. Legal principles of information protection. Kharkiv, 2020. 162 p. (in Ukrainian).

2. On the Protection of Information in Information and Communication Systems. The Law of Ukraine of 05.07.1994 № 80/94-BP. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (in Ukrainian).

3. On information. The Law of Ukraine of 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (in Ukrainian).

4. Decision of the Council of Judges of Ukraine of 25 March 2022 No. 11. URL: https://rsu.gov.ua/uploads/news/richenarsu11250322-f68cadf705.pdf (in Ukrainian).

5. On access to public information. The Law of Ukraine of 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (in Ukrainian).

6. On the situation in the cyber sector as at February 23–24, 2024. URL: https https://cert.gov.ua/article/6277840

7. Decision of the Constitutional Court of Ukraine in the case on the constitutional petition of the Zhashkiv District Council of Cherkasy Region regarding the official interpretation of the provisions of parts one, two of Article 32, parts two, three of Article 34 of the Constitution of Ukraine. URL: http://zakon2.rada.gov.ua/laws/show/v002p710-12 (in Ukrainian).

8. Demchenko S. Approaches to the content of the concept of "information": cybernetic, philosophical, legal. *Jurnalul juridic national: teorie şi practică*. 2016. № 1/2 (17). pp. 35-38. (in Ukrainian).

9. Banakh S. The concept and features of information as a theoretical category. *Actual problems of law*. 2019. № 4 (20). pp. 226-231. (in Ukrainian).

10. Teremetskyi V.I., Duliba Ye.V. Peculiarities of Implementation and Functioning of the Unified Judicial Information and Telecommunication System as an E-Justice Tool. *Law forum*. 2023. № 75 (2). pp. 130-143. (in Ukrainian).

11. Heorhiievskyi Yu.V. Proposals for Legal Support of Information Protection in the Unified Judicial Information and Telecommunication System. *Legal scientific electronic journal*. 2020. № 3. pp. 204-208. (in Ukrainian).

12. Shepitko M. Criminal law protection of information security in the administration of justice. *The issue of fighting crime*. 2022. № 4. pp. 69-75. (in Ukrainian).

Andrii KOLESNIKOV
PhD in Economics, Associate Professor, West Ukrainian National University
ORCID: https://orcid.org/0000-0003-3064-4133
e-mail: kole.ua@gmail.com

FEATURES OF INFORMATION PROTECTION IN THE ACTIVITY OF JUSTICE ENFORCEMENT BODIES

Introduction. *The perception of information as one of the key resources for the development of society is a widely recognised fact. The quality of its processing, timeliness and completeness of its receipt and professional use largely determine the effectiveness of decision-making. At the same time, achieving these results requires the development and implementation of reliable information protection mechanisms. Protection of information in the activities of the judiciary is a critical aspect, especially in connection with the development of digital technologies. It is important to ensure the confidentiality and integrity of data, which will help to increase trust in the judicial system and ensure human rights and freedoms.*

The purpose of the paper *is to study the peculiarities of information protection in the activities of the judiciary.*

Results. *The paper examines the definition of the category "information" in scientific works and legislation of Ukraine and outlines the need to take into account the sectoral aspect in its interpretation. The author identifies the objects of legal protection in the field of information and proves the need to include information about subjects who have access to information resources and information systems. The author outlines new challenges in the field of information protection which arose during the military invasion of the Russian Federation. Attention is drawn to the problem of non-compliance by officials with the basic rules of information hygiene. The author substantiates the need for a systematic approach to ensuring information security in the judicial system. Attention is drawn to the role of certain specialised structural subdivisions of the High Council of Justice in ensuring information security in the judicial system. The author outlines the peculiarity of the approach to the protection of personal data of participants to the judicial process.*

Conclusion. *Protection of information in the activities of the judiciary is an important tool for the effectiveness of the judicial system, so a clear definition of the objects of protection will optimise the effectiveness of the tools to ensure it. It is important to protect not only resources and information systems, but also information about persons who have access to information resources and information systems. It is important not only to ensure procedural aspects, but also to comply with basic information hygiene methods. Achieving this requires a systematic approach to information security in the judiciary.*

Keywords: *court, justice, information support for the administration of justice, protection of information in judicial authorities, objects of legal protection, protection of personal data of judicial authorities*