УДК 340:659.4.327.88 (477)

Лисенко Сергій Олексійович,
кандидат юридичних наук, доцент, доцент кафедри управління безпекою, правоохоронної та антикорупційної діяльності, Міжрегіональна Академія управління персоналом, 03039, м. Київ, вул. Фрометівська, 2, тел.: (044) 490 95 00, e-mail: crimeconsult@ukr.net

ORCID: 0000-0002-7050-5536

Лысенко Сергей Алексеевич,
кандидат юридических наук, доцент, доцент кафедры управления безопасностью, правоохранительной и антикоррупционной деятельности, Межрегиональная Академия управления персоналом, 03039, г. Киев, ул. Фрометовская, 2, тел.: (044) 490 95 00, e-mail: crimeconsult@ukr.net

ORCID: 0000-0002-7050-5536

Lysenko Serhii Oleksiiovych,
PhD in Law, Associate professor, Associate professor of the Department of Security Management and Law Enforcement and Anti-Corruption Activities, Interregional Academy of Personnel Management, 03039, Kyiv, st. Frometovskaya, 2, (044) 490 95 00, e-mail: crimeconsult@ukr.net

ORCID: 0000-0002-7050-5536

МЕТОДОЛОГІЧНІ ПІДХОДИ ДО РОЗУМІННЯ КАТЕГОРІЇ “СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ” З ТОЧКИ ЗОРУ ГЕРМЕНЕВТИКИ У ПРАВІ

Анотація. У статті розглядаються питання щодо дослідження та визначення основних методологічних підходів щодо розуміння категорії “система інформаційної безпеки підприємства” з точки зору герменевтики у праві. Досліджуються основні погляди щодо визначення поняття “герменевтика” у праві та надається авторське визначення цього поняття.

Ключові слова: інформаційне право, інформаційна безпека, герменевтика, право, система інформаційної безпеки підприємств.

МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ К ПОНИМАНИЮ КАТЕГОРИИ "СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ" С ТОЧКИ ЗРЕНИЯ ГЕРМЕНЕВТИКИ В ПРАВЕ

Аннотация. В статье рассматриваются вопросы исследования и определения основных методологических подходов к пониманию категории "система информационной безопасности предприятия" с точки зрения герменевтики в праве. Исследуются основные взгляды относительно определения понятия "герменевтика" в праве и предоставляется авторское определение данного понятия.

Ключевые слова: информационное право, информационная безопасность, герменевтика, право, система информационной безопасности предприятий.

METHODOLOGICAL APPROACHES TO UNDERSTANDING THE CATEGORY OF "ENTERPRISE INFORMATION SECURITY SYSTEM" FROM THE PERSPECTIVE OF LEGAL HERMENEUTICS

Abstract. The paper deals with issues related to studying and defining the basic methodological approaches to understanding the category of "enterprise information system security" from the perspective of legal hermeneutics. It also examines the basic views on definition of the concept of legal "hermeneutics" and gives a definition the author suggests for this concept.

Keywords: information law, information security, hermeneutics, law, and enterprise information security system.

Постановка проблеми. Процес забезпечення інформаційної безпеки організацій будується згідно з чинним законодавством і корпоративними нормативними актами. Будь-який аналогічний процес пов'язаний з суб'єктивним сприйняттям і тлумаченням правових норм, що регулюють ці відносини, самими суб'єктами діяльності. Відносини виникають у сфері забезпечення інформаційної безпеки організацій, регулюються насамперед Конституцією України ст. 17. Так само регулювання відбувається відповідно до Законів України "Про інформацію", "Про Національну програму інформатизації", а в завершенні Накази та Інструкції щодо організації, закріплені в статутах або у протоколах зборів засновників. При таких регулюючих нормах нерідкі випадки різного трактування одних і тих самих правил по-різному. Питання розуміння процесів забезпечення інформаційної безпеки організацій, найкраще розглядаються з точки зору герменевтики у правовій науці.

Аналіз останніх публікацій за проблематикою. Питання про основні методологічні підходи до розуміння категорії "система інформаційної безпеки підприємства", з точки зору герменевтики у праві, розгля-

дали у своїх працях Х.-Г. Гадамер, В. Г. Кузнецов, В. П. Плавич, П. Рікер, В. В. Суслов та ін.

Мета статті — дослідження методологічних підходів щодо розуміння категорії "система інформаційної безпеки підприємств" з точки зору герменевтики у праві

Виклад основного матеріалу. Герменевтика, в наш час, є напрямом новітньої філософії. Предметами сучасної герменевтики є питання соціального пізнання і його методів. У методології герменевтики центральним питанням є те, як зрозуміти людям сенси сущного і належного, і які існують межі інтерпретаційної свободи. Г.-Г. Гадамер висловив її суть так: "Герменевтика — це практика ... Фундаментальна істина герменевтики така: істину не може пізнати і повідомити хтось один. Всіляко підтримувати діалог, давати можливість сказати своє слово й інакомислячим, вміти засвоювати промовлене ними — ось у чому душа герменевтики" [7].

Нині герменевтика у праві і філософії трактується як наука про розуміння сенсу тексту, і має різні ступені розвитку. Термін "герменевтика" вживається також і в теоретичному сенсі: герменевтика — це теорія розуміння, осягнення сенсу [8].

Виходячи з викладеного, можемо вивести визначення. Герменевтика у праві — це розуміння, тлумачення змісту, закладеного законодавцем в текст нормативно-правового акта. Завдання герменевтики у праві — методологічно забезпечити перехід від розуміння змісту норми права до правильного тлумачення його сутності.

Такий перехід є процесом пізнання, результатом якого є знаходження єдиного правильного варіанта тлумачення правових приписів щодо конкретної правової ситуації.

Специфіка герменевтики у праві пов'язана з існуванням різних правових культур, в тому числі української національної правової культури, з власним баченням проблеми прав людини, правової держави, питань поділу влади, місцевого самоврядування тощо, нашим правовим звичаям.

Які б сфери права ми не розглядали, вони складаються з сукупності різноманітних тлумачних розрахунків. У цьому сенсі право є за своєю природою суто герменевтичним явищем.

Найбільш цікаву методологію герменевтичного аналізу правових текстів розробив італійський філософ і юрист Е. Бетті. Він говорив, що існує світ об'єктивного духу, фактів і людських подій, вчинків, жестів, думок і проектів, слідів і свідоцтв ідей, ідеалів і реалізацій. Весь цей світ підлягає інтерпретації. Коментар представляється як процес і мета, адекватний результат якого — розуміння. Коментатор повинен ретроспективно відтворити реальний процес створення тексту шляхом реконструкції послання і об'єктивації намірів автора тексту [9].

Бетті сформулював чотири герменевтичних канони, які активно використовуються у правознавстві:

1. Канон іманентності герменевтичного масштабу. Реконструкція тексту повинна відповідати точці зору автора. Коментатор нічого не повинен привносити ззовні; йому нале-

жить шукати сенс тексту, поважаючи несхожість і герменевтичну автономію об'єкта.

2. Канон тотальності герменевтичного розгляду. Зміст його полягає в тому, що єдність цілого прояснюється через окремі частини, а сенс окремих частин прояснюється через єдність цілого "герменевтичного кола".

3. Канон актуальності розуміння. Коментатор не може зняти свою суб'єктивність до кінця. Щоб реконструювати чужі думки, твори минулого, щоб повернути у справжню, життєву дійсність чужі переживання, — потрібно співвіднести їх з власним "духовним обрієм".

4. Канон смислової адекватності розуміння є вимогою до коментатора тексту. Зрозуміти один одного автор і коментатор можуть, якщо вони конгеніальні і знаходяться на одному рівні. Цей канон передбачає також уміння коментатора прийняти цілі об'єкта інтерпретації, як свої, в самому безпосередньому сенсі слова.

Герменевтика у праві покликана спростити діалог правових точок зору, оскільки правові поняття і категорії такі, наприклад, як свобода, демократія, відповідальність, мають різне значення в різних правових системах [9].

Сучасна юридична наука почала розуміти перспективи герменевтичного підходу до аналізу законодавчих текстів. Цілком логічно стало застосування герменевтики для тлумачення норм інформаційного права та інформаційної безпеки.

Спробуємо застосувати герменевтичний підхід до тлумачення понять систем інформаційної безпеки організацій. Будь-яка норма, яка регулює відносини, що забезпечують інформаційну безпеку є результатом творіння її автора, зміст якого повинен бути встановлений виконавцями або суб'єктами інформаційної безпеки. За буквальним змістом норми завжди ховається другий ситуативний сенс, без адекватного розуміння якого неможливе правильне розуміння сенсу всієї норми. В англійських юристів є приказка: "У законі присутня тільки одна половина змісту, інша прихована, а ідеї знаходяться всередині". Аналогічно, розглядаючи будь-які норми, зазначимо, що для правильного застосування закону у процесі тлумачення необхідно відшукати цю приховану ідею. Герменевтичне тлумачення норм і понять інформаційної безпеки є саме тим інструментом, за допомогою якого може бути вирішена проблема подвійного сенсу, оскільки герменевтика крім дешифрування буквального сенсу тексту, що здійснюється лінгвістичним тлумаченням, дає можливість розкрити зміст правового контексту.

У своїх роботах П. Рікер зазначає, що герменевтичний аналіз правового тексту включає в себе ряд обов'язкових процедур. Визнаним вважається поділ на розуміння, тлумачення і застосування [11; 12].

Розумінням є мистецтво осягнення знаків, що передаються однією свідомістю і сприймаються іншою через їх зовнішнє вираження (насамперед мовне).

Виявлено єдність понять "розуміти" і "тлумачити". Тлумачення — це не просто деякий процес, окремим числом і при нагоді воно доповнює розуміння; розуміння завжди є тлумаченням, а це останнє, відповідно,

суть експліцитна форма розуміння. У розумінні завжди має місце щось на зразок застосування належного розумінню тексту, в якому знаходиться інтерпретатор.

Застосування є такою ж інтегральною частиною герменевтичного процесу, як розуміння і тлумачення. Для юридичної герменевтики конституючим є напруга, яка існує між цим законом, з одного боку, і тим змістом, який він отримає в результаті його застосування в конкретній ситуації, з іншого. Закон зовсім не претендує бути зрозумілим історично, але повинен бути шляхом тлумачення конкретизований у своїй правовій значущості [11; 12].

В. В. Суслов зазначає, що юридична свідомість подібна з історичним, тобто юрист повинен дослідити передісторію факту, що інтерпретується. Щоправда, він підкреслює особливу актуальність зазначеного підходу стосовно процесу доказування. Однак зі змісту зазначеної статті та логічного висновку, створюється враження, що кінцевою метою герменевтичного тлумачення є з'ясування волі законодавця [14]. В. В. Суслов визнає багатозначність юридичних тестів і актуальність ситуативного сенсу, прихованого за буквальним, проте зводить герменевтику до її історичного прийому тлумачення [15].

Звернемося до проблеми розуміння системи інформаційної безпеки організацій по аналогії з історичною герменевтикою. Розглянемо підхід історика і суб'єкта забезпечення інформаційної безпеки до одного й того самого чинного законодавчого акта.

Існують очевидні відмінності. Суб'єкт осягає сенс норми інформаційного права з точки зору конкретного випадку і для певної мети. У історика немає конкретного випадку, який він би розглядав. Він прагне визначити зміст норми інформаційного права, моделюючи і охоплюючи єдиним поглядом сферу його застосування цілком. Розуміння права конкретизується ним лише завдяки всім випадкам його застосування. Історик не може задовольнятися початковим застосуванням норми інформаційного права для визначення її сенсу. Будучи істориком, він повинен врахувати історичні зміни, через які пройшла норма інформаційного права, він повинен визначити своє завдання з точки зору моделювання початкового змісту. Одночасно не можна сформулювати і завдання суб'єкта як приведення норм інформаційного права відповідно до актуального поточного моменту. Якщо дехто прагне привести сенс норм інформаційного права відповідно до поточного моменту, насамперед повинен знати його первісний зміст, тобто він має мислити як історик. І сенс полягає в тому, що історичне розуміння служить йому для досягнення певної мети. Ми переконані, що правовий зміст тієї чи іншої діючої норми інформаційного права цілком однозначний і що сучасна юридична практика просто дотримується його споконвічного змісту. Якби це було так, то стиль юридичного та історичного мислення був би тотожний, то і мета герменевтики зводилася б лише до встановлення початкового сенсу закону і подальшого його застосування в цьому первісному сенсі як правильного. Подібно до висловленої думки, саме розуміння

положень системи інформаційної безпеки організацій не повинно виявляти ніякої проблеми в тому, що суб'єкт забезпечення інформаційної безпеки повинен поставити себе в умови початкового творця цих положень, ігноруючи суперечності, що існують між початковим і практичним юридичним змістом цих норм і положень. Те, що це — юридична помилка, стало очевидним нещодавно.

В. Цимбалюк у своїй публікації зазначив, що з юридичних мотивів випливає необхідність рефлексії з приводу історичних змін, в силу яких початковий сенс закону і сенс, застосовуваний на практиці, відокремлюються один від одного. Юрист-практик, він же суб'єкт забезпечення інформаційної безпеки, завжди має на увазі сам нормативний акт (положення). Однак його зміст має бути визначено з урахуванням того випадку, до якого його слід застосувати. Для того, щоб точно встановити зміст положень системи інформаційної безпеки організацій, потрібне історичне знання їх первісного змісту, і лише заради цього останнього суб'єкт приймає до уваги історичне значення, що повідомляється самою нормою (положенням). Суб'єкт не може, покладатися виключно на те, що відомо йому про наміри і цілі тих, хто розробляв ці норми і положення, протоколи і статути. Навпаки, він повинен зрозуміти зміни, що відбулися в системі інформаційної безпеки організації і заново визначити функцію норм і положень [16].

Суб'єкт, який користується положеннями системи інформаційної безпеки організацій, що дійшли до нього з минулого, до своїх сучасних потреб, прагне вирішити практичне завдання. І це не означає, що він його довільно коментує. Зрозуміти і прокоментувати, означає, що потрібно пізнати і визнати діючий сенс зазначених норм. Суб'єкт прагне дотримуватися основного змісту положень системи інформаційної безпеки, перекладаючи їх на сучасний лад. Він прагне пізнати саме правове значення норм і положень всієї системи, а не історичне їх значення, для якого вся система була впроваджена в дію, або, наприклад, будь-якого випадку її застосування.

Тлумачення норм і положень системи інформаційної безпеки організацій має відбуватися шляхом звернення до власної історії їх створення, але інтерпретуючи на сучасний манер. Той, хто розуміє, не вибирає свою суб'єктивну точку зору, а знаходить сенс, даний заздалегідь. Для самоздійснення герменевтики у праві важливим є те, що закон обов'язковий для всіх членів організації. Там, де це правило порушено, наприклад в патологічних авторитарних організаціях, герменевтика у праві неможлива. Лідер має можливість, ігноруючи придумані ним же норми, не здійснюючи жодних зусиль у їх тлумаченні, домогтися будь-якого рішення, яке вважатиме правильним. Завдання розуміння і тлумачення варто лише там, де законодавчі положення вважаються загальнообов'язковими [11].

Висновки та рекомендації. Застосування норм системи інформаційної безпеки здійснюється суб'єктом, на якого ці норми поширюються так само, як і на будь-якого іншого члена організації. Ідея забезпечення інфор-

маційної безпеки організацій передбачає, що управлінське рішення, повинно базуватися не на свавіллі, а на адекватній (справедливій) оцінці всієї ситуації. На такий справедливий розгляд здатний кожен член організації, який конкретно поглибиться в певну ситуацію. Саме тому в організації з налагодженою системою інформаційної безпеки, як у правовій державі, існує гарантія обов'язковості виконання своїх обов'язків всіма суб'єктами, кожен знає, що він повинен робити і на що він може розраховувати. Будь-який співробітник на своєму місці має принципову можливість дати правильне тлумачення, тобто вірно передбачити правове рішення на основі діючих норм і положень. Щоб винести правильне в конкретному випадку рішення, потрібно враховувати попередню практику і не тільки власну. Для цього достатньо мати можливість обміну інформацією та досвідом з аналогічними суб'єктами забезпечення інформаційної безпеки. Завжди відкрита можливість врахувати весь існуючий досвід, а це дає можливість догматично обробити будь-яку ситуацію і прийняти оптимальне управлінське рішення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Конституція* України: Закон України від 28.06.1996 р. № 254к/96-ВР // Відомості Верховної Ради України. — 1996. — № 30. — С. 141.
2. *Декларація* про державний суверенітет України від 16.07.1990 р. № 55-XII // Відомості Верховної Ради УРСР. — 1990. — № 31. — С. 429.
3. *Виноградова Г. В.* Інформаційне право України: навч. посіб. — К.: МАУП, 2006. — 144 с.
4. *Закон* України "Про інформацію" від 02.10.1992 р. № 2657-XII // Відомості Верховної Ради України. — 1992. — № 48. — Ст. 650.
5. *Закон* України "Про Національну програму інформатизації" від 04.02.1998 р. № 74/98-ВР // Відомості Верховної Ради України. — 1998. — № 27–28. — С. 181.
6. *Закон* України "Про Концепцію Національної програми інформатизації" від 04.02.1998 р. № 74/98-ВР // Відомості Верховної Ради України. — 1998. — № 27–28. — С. 182.
7. *Гадамер Г. Г.* Актуальность прекрасного. — М., 1991. — С. 7–8.
8. *Гадамер Г. Г.* Истина и метод: основы философской герменевтики. — М., 1988.
9. *Кузнецов В. Г.* Герменевтика и гуманитарное познание. — М., 2005.
10. *Плавич В. П.* Архитепические прафеномены права и его структура // Держава і право: зб. наук. пр. "Юрид. і політ. науки". — Вип. 24. — К., 2004.
11. *Рикер П.* Герменевтика. Этика. Политика: московские лекции и интервью. — М., 1995.
12. *Рикер П.* Конфликт интерпретаций: очерки по герменевтике. — М., 1995.
13. *Рикер П.* Торжество языка над насилием: герменевтический подход к философии права // Вопросы философии. — 1995. — № 4. — С. 27–34.
14. *Суслов В. В.* Герменевтика и юридическое толкование // Государство и право. — 1997. — № 6. — С. 116.
15. *Суслов В. В.* Герменевтический аспект законодательного толкования // Правоведение. — 1997. — № 1. — С. 88.
16. *Цимбалюк В.* Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2004. — № 8. — С. 30–33.