Науково-дослідний інститут інформатики і права
Національної академії правових наук України

Національна бібліотека України ім. В.І. Вернадського
Національної академії наук України

Відкритий міжнародний університет розвитку людини "Україна"

ISSN 2616-6798

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 1(24)

2018

Зареєстрований Міністерством юстиції України
(Свідоцтво про державну реєстрацію друкованого засобу масової інформації:
Серія КВ № 20117-9917ПР від 05.07.13 р.)

Згідно з Наказом МОН України від 11.07.16 р. № 820 (додаток 12)
у журналі можуть публікуватися матеріали стосовно дисертаційних робіт
на здобуття наукових ступенів доктора і кандидата наук у галузі юридичних наук

м. Київ

УДК 002:340+316.4+338.46

* * * * * * * * * * *

З М І С Т

Інформаційне право

Правова інформатика

Інформаційна і національна безпека

Інформація в інших галузях права

До відома читачів

Наукове редагування, створення оригінал-макета та дизайн – Брижко В.М.
Граматичне коректування – Майстренко І.А. (укр., англ.).

Формат 70 х 108/16. Спосіб друку – різографія. Ум. друк. арк. 15.8. Тираж 100 прим.
Виготовлено з оригінал-макета в друкарні ТОВ “Видавничий дім “АртЕк”.
04050, м. Київ, вул. Мельникова, буд. 63.
Свідоцтво про внесення суб’єкта видавничої справи до державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції – серія № ДК № 4779 від 15.10.14 р.

Рекомендовано до друку Вченою радою НДІ інформатики і права
Національної академії правових наук України, протокол № 3 від 27.03.18 р.

Інформаційне право

УДК 340.115.3

ДЗЬОБАНЬ О.П., *доктор філософських наук, професор,* головний науковий співробітник НДІ інформатики і права Національної академії правових наук України
ЯРОЦЬКИЙ В.Л., *доктор юридичних наук, професор,* завідувач кафедри цивільного права № 2 Національного юридичного університету імені Ярослава Мудрого

СОЦІОЛОГІЧНИЙ ТА АКСІОЛОГІЧНИЙ НАПРЯМКИ СУЧАСНИХ ПРАВОВИХ ДОСЛІДЖЕНЬ: ЗАГАЛЬНЕ БАЧЕННЯ

Анотація. *Показано, що розширення меж використання у правових дослідженнях нового й уточненого евристичного інструментарію, призначення якого обумовлюється філософськими і природничими трактуваннями сутнісних та системно-структурних властивостей сфери цивільно-правового регулювання, дозволяє розкрити необмежений потенціал кожного досліджуваного феномена в органічному поєднанні як його статичних, так і динамічних характеристик.*

Ключові слова: *методи правового дослідження, спостереження, системний підхід, правова рефлексія.*

Summary. *It is shown that the expansion of the boundaries of using new and revised heuristic tools in civil law studies, the purpose of which is determined by the philosophical and natural interpretations of intrinsic and systemic-structural properties of the sphere of civil law regulation, allows to explore the unlimited potential of each of the studied phenomenon in organic combination both of its static and dynamic characteristics.*

Keywords: *methods of legal research, monitoring, system approach, legal reflection.*

Аннотация. *Показано, что расширение границ использования в правовых исследованиях нового и уточненного эвристического инструментария, назначение которого определяется философскими и естественными трактовками сущностных и системно-структурных свойств сферы гражданско-правового регулирования, позволяет раскрыть неограниченный потенциал каждого исследуемого феномена в органическом сочетании как его статических, так и динамических характеристик.*

Ключевые слова: *методы правового исследования, наблюдение, системный поход, правовая рефлексия.*

Постановка проблеми. В інформаційну епоху, коли наука стала безпосередньою продуктивною силою, а науково-технічна революція набуває неймовірно широкого розмаху, розробка проблем методології та логіки наукового дослідження усіх без винятку галузей науки стає одним з найактуальніших завдань.

Безперервний і постійно збільшуваний потік наукових досліджень у сфері правознавства, помітне зростання числа людей, які займаються правовою наукою, зокрема цивілістикою – усе це не тільки стимулює загальний інтерес до проблем наукового пізнання цивільного права, а й вимагає аналізу й розробки адекватних сучасним потребам методів дослідження, які використовуються у сучасній цивілістиці. Від застосовуваних методів дослідження в їх взаємодоповнюваності залежить якість одержуваного наукового результату, його достовірність і корисність для вирішення

практичних завдань. Тому сучасна розробка й уточнення правової методології – найважливіше наукове завдання, вирішення якого дозволяє отримувати якісно нові наукові результати в ході пізнання.

Продовжуючи наукову дискусію, розпочату авторами на сторінках журналу “Інформація і право” [1], вважаємо за доцільне, крім догматичного рівня наукових досліджень у цивілістиці, звернути увагу на соціологічний та філософський (аксіологічний) рівні.

Результати аналізу наукових публікацій і практика науково-дослідної діяльності свідчать про те, що сучасні дослідження у сфері права та законодавства постійно поповнюються новими теоретичними даними, які далеко не завжди корелюють з усталеними цивілістичними постулатами та вивіреними підходами загальної (інструментальної) теорії права. Методологічний інструментарій пізнання правових явищ в сучасних умовах постійно вдосконалюється, зазнаючи кількісної та якісної трансформації. Крім того, постійно проявляється необхідність рефлексивного перегляду методологічного інструментарію цивілістичної науки, приведення його у відповідність з сучасними соціокультурними реаліями.

Метою статті є спроба уточнити соціологічний та філософський рівні правових досліджень з урахуванням сучасної динаміки правової реальності.

Виклад основного матеріалу. Систематика цивілістичної науки за рівнями пізнання аналогічна за складом будь-якій науковій сфері. Як доводилося раніше [1], дослідження у галузевих юридичних науках взагалі й цивілістиці зокрема можуть здійснюватися на декількох взаємопов’язаних, але все ж окремих рівнях – догматичному, соціологічному та аксіологічному. У межах даної статті сконцентруємося на соціологічному та аксіологічному рівнях цивілістичних досліджень.

Для соціологічного рівня цивілістичних досліджень предметом вивчення є правова діяльність – середовище впровадження юридичних конструкцій у межах людської взаємодії, де використовуються відповідні засоби правової регуляції (правові засоби в широкому розумінні), а методи їх дослідження повинні відповідати методам соціологічного дослідження. Методами дослідження є спостереження (зовнішнє і включене), інтерв’ювання, опитування тощо. Допоміжне значення для соціологічного напрямку цивілістичного дослідження може мати і метод герменевтики, у тих випадках, коли проводиться опосередковане спостереження і досліднику потрібно проаналізувати текстуальний вираз результату спостереження, зафіксований у письмовому документі (протокол засідання), або в інших випадках, коли сліди правової діяльності відображені в письмових документах (претензії, акти, листування). У цих випадках герменевтичний метод застосовується у тому ж порядку, як було описано вище.

Спостереження – основний метод пізнання ще з часів Демокріта й Аристотеля, суть якого полягає у сприйнятті того, що відбувається. Спостереження як метод може поєднуватися лише з уявним експериментом і уявним моделюванням. Основним недоліком спостереження як методу пізнання є найсильніша залежність результату його використання від особистості спостерігача, оскільки єдиним “вимірювальним приладом” виявляється сам спостерігач, який здійснює процес спостереження, будучи обтяженим власним неявним знанням. Подібна залежність від особистості дослідника була показана раніше, при описі методу правової герменевтики і його використання при дослідженні юридичного тексту. Крім того, спостереження і опис побаченого самі по собі не становлять ніякої цінності. “Не поверхневі описи спостережуваних явищ, а достовірне осмислення фактів, встановлення необхідних зв’язків, певних закономірностей у

досліджуваній царині дійсності” [2, с. 13] є наукою. Внаслідок цього, спостереження й описання хоча і є методами пізнання, але аж ніяк не методами наукового осмислення.

Незважаючи на те, що спостереження не може бути основним методом дослідження, все ж без його проведення не може обійтися жодне дослідження, у тому числі й у цивілістиці. Невірно проведене спостереження призводить до недоліків збору матеріалу, який у подальшому піддається осмисленню і оцінюванню, а значить, – до недостовірності отриманих результатів наукових досліджень.

Спостереження як метод юридичного дослідження передбачає збір первинної та подальшої інформації про досліджуваний об’єкт шляхом цілеспрямованого організованого безпосереднього сприйняття і прямої фіксації спостережуваних явищ і процесів.

Спостереження можна вести безпосередньо – будучи присутнім при проведенні певної ситуації, або опосередковано – шляхом ознайомлення з документами, складеними при проведенні даного заходу (стенограми, протоколи та ін.). Сама процедура ведення протоколу різних юридично значущих дій являє собою фіксацію безпосереднього спостереження, а дослідження протоколу – опосередкованим спостереженням. Для подальшого наукового дослідження обидва методи представляють цінність. Відмінності полягають у тому, що опосередковане спостереження не дозволяє вивчати невербальну частину спостережуваної події, яка здійснює відчутно значний вплив на саму процедуру і її результат. Спостереження як метод має суттєве значення і для правильного правозастосування. Отримані дані повинні бути враховані при регулюванні відповідних відносин як за допомогою нормативних правових актів, так і актами саморегуляції.

У даний час через поширення використання можливостей телекомунікаційних систем (наприклад, для ведення переговорів) розширюються можливості безпосереднього спостереження – коли суб’єкт може в режимі он-лайн бути присутнім при проведенні спостережуваного правового явища. Разом з тим, для правового дослідження опосередковане спостереження – через дослідження зафіксованих результатів спостереження інших осіб – представляє основний вид спостереження. Велика частина правових ситуацій (укладання договорів, проведення переговорів, проведення загальних зборів акціонерів, засідань рад директорів, врегулювання претензій в процесі переговорів тощо) оцінюється за допомогою опосередкованого спостереження, у зв’язку з чим доводиться докладати спеціальних зусиль для нівелювання впливу неточностей у фіксації спостережуваного явища.

Отримані у процесі спостереження дані залежать від установки спостерігача. Незважаючи на те, що спостереження призначене для збору максимально об’єктивних даних про ситуацію, спостерігач має власну правосвідомість, правову культуру і уявлення про ситуацію, у зв’язку з цим, спостерігаючи її, він порівнює об’єкт, що спостерігається, зі своїми уявленнями, що в результаті спотворює сприйняття. Про ці особливості ми писали вище, стосовно до герменевтики. Їх же можна буде виявити у всіх інших методах пізнання, які використовуються в наукових дослідженнях.

Ситуація очевидно посилюється при опосередкованому спостереженні, оскільки у цьому випадку між ситуацією, яка спостерігається, і результатом спостереження стоять два спостерігачі – безпосередній (секретар, який веде протокол або стенограму) і опосередкований – дослідник, який пов’язаний вже не лише власною правосвідомістю, а й інтерпретацією безпосереднього спостерігача.

Спостерігач впливає на об’єкт спостереження. Безпосереднє спостереження соціальної ситуації (а більша частина ситуацій у соціологічній частині юриспруденції передбачає спостереження саме соціальної ситуації) може призводити до включення спостерігача в неї (наприклад, до його думки апелюють сторони при виникненні спору).

Сама присутність у соціальній ситуації сторонньої особи змінює відносини, які спостерігаються. Для безпосереднього спостереження як методу правового дослідження така властивість спостереження є його істотним дефектом. І в цьому сенсі опосередковане спостереження виявляється переважним, вивільняючи опосередкованого спостерігача від впливу на перебіг ситуації, яка спостерігається.

Об’єкт спостереження впливає на спостерігача. За загальним правилом, спостерігач повинен бути поза ситуацією спостереження, оцінюючи її і виділяючи істотні властивості. Однак виділяють особливий різновид спостереження – включене спостереження, при якому спостерігач сам є учасником ситуації, що спостерігається. У правових дослідженнях це проявляється у посиланнях на “особисті архіви автора” при описі конкретних правових ситуацій. Правова позиція спостерігача, його висновки та умовиводи, узагальнення, покладені в основу його подальших наукових розробок, у такому випадку деформуються під впливом об’єкта спостереження. Це викликає певні сумніви у достовірності даних, отриманих в результаті безпосереднього включеного спостереження, які відображаються, наприклад, у публікаціях суддів за матеріалами розглянутих ними судових справ, адвокатів, юрисконсультів та інших осіб, що здійснюють правову допомогу одній із сторін конфлікту, що дають правовий висновок у справі тощо. У спостереженні, при якому спостерігач не є учасником ситуації, що спостерігається, подібне трапляється рідше, але все ж можливо.

Поряд зі спостереженням, у сучасних цивілістичних дослідженнях досить широко застосовуються методи інтерв’ювання та опитування [1; 3 – 4].

Аксіологічний (філософський) рівень правових досліджень передбачає вивчення найбільш загальних засад і мети регулювання відносин. У будь-якому явищі, досліджуваному цивілістикою, є два рівня мети – мета регуляції, поставлена суб’єктом правотворчої діяльності при формуванні позитивного права і мета суб’єктів правової діяльності, що змушує їх вступати у правовий зв’язок (правовідносини). Розуміння правової догми і правової діяльності передбачає розуміння мети того й іншого. Спеціальних методів виявлення і дослідження мети і цінності в даний час не вироблено.

У даний час єдиним найбільш науково розробленим механізмом об’єднання в цілісну картину світу знань, отриманих різними галузями науки, з використанням різних підходів, і знань про різні предмети (які, безумовно, знаходяться при цьому в межах одного об’єкта пізнання) є системний підхід. З його допомогою і відбувається так зване розпредметнення, тобто безпосереднє звернення до об’єкта з підсумовуванням знань, отриманих про різні предмети всередині одного об’єкта.

Основи системних досліджень можна виявити ще в далекій давнині – стародавні греки розглядали світ як дещо єдине (космоцентризм). Однак як міждисциплінарний філософсько-методологічний напрям системний підхід став формуватися порівняно недавно – починаючи з середини XX ст. В даний час існують два основних напрямки системного підходу: онтологічний, відповідно до якого ознаки системи, системність притаманні самим об’єктам дійсності, і епістемологічний, відповідно до якого системність розглядається як невіддільний від спостерігача спосіб вивчення явища, його здатність сконструювати предмет дослідження як системний.

Евристичний потенціал цього методу наукового пізнання приватно-правової сфери досить великий. Зокрема, він дозволяє виявити такі властивості правових явищ, які вислизають від спостерігача при вивченні їх виключно з позицій формально-логічного аналізу, структурного дослідження або, тим більше, за допомогою спостереження чи рефлексії, дозволяючи інтегрувати знання, отримані про різні предмети, в межах одного об’єкта пізнання.

До проведення системних досліджень висувається низка методологічних вимог: опис кожного елемента має супроводжуватися з’ясуванням його місця й функцій у системі, один і той же елемент повинен розглядатися як такий, що володіє безліччю властивостей і функцій, які проявляються по-різному відповідно до місця в ієрархії і етапу розвитку системи. При дослідженні систем слід враховувати дуже важливу їх властивість – наявність у них протилежних процесів – в яких і міститься основа для їх розвитку. Про цю неодмінну особливість систем писали практично всі дослідники даної проблеми.

Зауважимо, що системний підхід, згідно з яким пропонується розглядати явище як цілісність, яка не зводиться до простої механічної сукупності елементів, динамічну, мінливу в своєму розвитку, не тотожну собі самій в різних стадіях, а тому таку, яка лише умовно розчленовується на елементи, співіснує одночасно з іншими підходами. Йдеться про аналітичний, структурно-функціональний та інші подібні наукові підходи, в основу яких покладено ідею про більш ретельне виявлення всіх частин досліджуваного явища і виявлення всіх функцій кожного з елементів, сукупність яких і дасть уявлення про властивості досліджуваного предмета [5, с. 20-24]. На слушне міркування Е. Юдіна, “...навіть у дослідженні, яке без будь-яких застережень можна назвати системним, системна постановка проблеми зазвичай знаходить подальший розвиток в опорі на неспецифічні ...несистемні засоби дослідження ... Системний підхід, як, утім, і будь-який методологічний напрямок, не виступає і, мабуть, не може виступати в чистому вигляді, але завжди доповнюється іншими методологічними ідеями й засобами” [5, с. 140].

У літературі виділяють наступні принципи системного дослідження, які повинні обов’язково враховуватися при проведенні наукових досліджень у правознавстві взагалі й у цивілістиці зокрема [5 – 7]:

- уявлення про цілісність досліджуваної системи, яке включає в себе протиставлення системи і навколишнього середовища, розчленовування системи на певні елементи з власними функціями і місцем у системі;
- між елементами системи є зв’язок двох і більше типів (наприклад, просторових, функціональних, генетичних);
- система є впорядкованим (організованим) феноменом;
- будова системи є ієрархічною, структура системи може мати різні рівні та ієрархії;
- специфічним способом регулювання багаторівневої ієрархії є управління;
- при дослідженні систем необхідним є вивчення проблеми мети і доцільного характеру “поведінки” системи. При цьому відзначається неузгодженість локальних цілей окремих підсистем, кооперування і конфлікт цих локальних цілей;
- джерело перетворення системи знаходиться у самій системі (вона самоорганізується);
- системне дослідження має виявляти співвідношення функціонування і розвитку системи для отримання повного знання про неї.

Звернемо увагу на дуже важливу особливість системного підходу, яка, на жаль, залишається поза увагою вчених-юристів в їх спробах застосування системного підходу у своїх наукових дослідженнях. Практично всі автори, які здійснювали розробку цього методологічного спрямування, відзначали, що в принципі як систему можна розглянути абсолютно будь-який об’єкт (у даному випадку ми ведемо мову про епістемологічний напрямок системного підходу). Взагалі навіть сама назва наукової теорії “Загальна

теорія систем” (Людвіг фон Берталанфі) включає в себе вказівку на її загальність. В.Артюхов підкреслює, що системою є будь-який об’єкт матеріальної або ідеальної дійсності. Між первинними (неподільними) елементами цієї системи існують певні відносини, які не можуть бути будь-якими: вони обмежені певними умовами або правилами. Таким чином можуть бути виділені абсолютно будь-які системи і в кожній з них обов’язково виявляться системоутворюючі атрибути [7, с. 13].

Разом з тим, за зазначеною загальністю системного підходу криється і його недолік, який є, як справедливо стверджує С. Філіппова, продовженням переваг [8, с. 56]. Застосування системного аналізу в науковому дослідженні повинне обґрунтовуватися, причому зовсім не наявністю системних властивостей у явища, які є завжди, а тими функціональними й евристичними можливостями, які з’являються при розгляді явища як системи.

Важливою властивістю системного підходу є надана ним можливість урахування розвитку системи, в цьому, як уявляється, полягає його основне позитивне начало. У найзагальнішому вигляді теорія систем виходить з існування трьох варіантів взаємодії між елементами системи: прагнення елементів до асоціації, прагнення їх до дисоціації і збереження (нестійка форма взаємодії). Відносини між елементами можуть бути несуперечливими одна одній – виражатися в узгодженому або неузгодженому, але не протилежному відношенні, або суперечливими – виражатися в дисоціації [7, с. 20]. Загальний висновок, що лежить в основі системного підходу, звучить так: “Світ влаштований так, що в ньому є в наявності два типи природних законів – такі що організують і дезорганізують матерію” [7, с. 30].

Незважаючи на очевидний суттєвий евристичний потенціал системного підходу як методологічного напрямку, все ж існують межі його використання для дослідження правових явищ. Іноді в науковій літературі з’являються деякі скептичні оцінки можливості його безпосереднього застосування для вирішення конкретних наукових, зокрема юридичних завдань. Так, наприклад, один з основоположників системного підходу однозначно зауважив, що “системний підхід являє собою методологічний напрям наукового пізнання..., сам по собі системний підхід не вирішує і не може вирішувати змістовних наукових завдань” [5, с. 143]. Основними його завданнями є постановка проблеми та оцінювання результатів застосування інших методів. Системний підхід перестав бути якимось трафаретом (калькою), приклавши який на будь-яке явище (виходячи з фактично загальновизнаного вже універсального характеру загальної теорії систем), можна отримати якийсь результат. Він за своїми функціональними можливостями є лише способом апробації, верифікації отриманих знань, а також певним ракурсом дослідження, який змушує вченого шукати все нові й нові варіанти рішень. І взагалі, варіативність є однією з найбільш значних “знахідок” системного аналізу. Саме тому, як справедливо вказує С. Філіппова, застосування системного підходу можливе тільки після вже проведеного дослідження об’єкта за допомогою інших методів для отримання комплексного знання [8, с. 57].

Системний підхід, застосований до обробки результатів цивілістичних досліджень, повинен дати на виході нове знання про досліджуване правове явище, що об’єднує у собі і знання про норму права, і знання про людську діяльність, до якої така норма повинна бути застосована зі збереженням при цьому загальних ідей про сутність цивільного права і його значення для правового регулювання особистих немайнових та майнових відносин. Незважаючи на повсюдне згадування системного підходу як методології своїх досліджень у багатьох роботах у сфері юриспруденції, у сучасній цивілістиці дійсно системних досліджень правових явищ проводиться дуже мало.

Це пов’язано з тим, що завдання системного підходу реалізується тільки при визначенні одного об’єкта, дослідженого з різних сторін (предметів). Як правильно зауважує В. Бєлов, критично оцінюючи результати застосування системного підходу в юриспруденції, “предметом системного вивчення повинно бути не право, а щось інше” [9, с. 167].

В результаті інтеграції наукових знань за допомогою системного аналізу отриманий результат повинен бути осмислений на філософському рівні методології [10, с. 457]. Основним методом дослідження на даній стадії цивілістичного дослідження є правова рефлексія – осмислення, усвідомлення відомостей про норми права і факти правової дійсності. Правова рефлексія включає в себе процес заломлення спостережуваних даних правової дійсності крізь призму правосвідомості дослідника і вбудовування їх в існуючу правову парадигму за допомогою в тому числі інтуїтивного відчуття сутності спостережуваного явища правової дійсності.

У правовій рефлексії найбільш яскраво проявляється творче начало наукової діяльності, що додає їй характеру постійного пошуку нових підходів, висновків, і саме в ній виявляються прогностичні можливості юридичних досліджень у сфері цивілістики.

За хронологією проведення, правова рефлексія є завершальним етапом розумової діяльності правника, що обіймає собою всі факти, отримані в ході спостереження і герменевтичного аналізу юридичних текстів, виявлення закономірностей розвитку досліджуваних явищ правової дійсності в рамках системного підходу і правового моделювання. Осмислення отриманих даних, співвіднесення їх з власними знаннями і переконаннями вченого і являє собою правову рефлексію.

Правова рефлексія є різновидом наукової рефлексії, в ході якої знання про факти, отримані із застосуванням інших методів, повинні бути узагальнені і зібрані в єдину концепцію. При вербалізації результатів правової рефлексії знання повинно бути максимально очищене від неявного, від припущень, тощо, що при описаних властивостях правової рефлексії виявляється у великій мірі ускладненим. Сама рефлексія, будучи актом виключно суб’єктивним, привносить у знання власні припущення дослідника, ідеалізації та абстрагування від певних властивостей досліджуваного явища. Отриманий у першу чергу інтуїтивно висновок, повинен послідовно бути вивільнений від більшої частини своєї основи. Припущення, апріорні знання повинні бути усвідомлені дослідником і перевірені (доведені).

В епістемології склалося два основних підходи до діяльності вченого. Відповідно до першого з них – науковий результат діяльності вченого складається з суми знань, отриманих попередниками, будучи її підсумком. Відповідно до другого підходу вчений-дослідник – це виняткова людина, що володіє специфічними особистісними якостями, наділена інтуїцією, здатна інакше дивитися на світ. В юридичній науці взагалі й в цивілістиці, зокрема, в даний час склалося упереджене ставлення до інтуїції як способу отримання нового знання. Загальна тенденція зводиться до того, що правильна організація процесу вивчення правової дійсності неминуче повинна приводити до отримання істинного нового знання про неї. При цьому особисті якості, і тим більше, інтуїція вченого-правознавця, як правило, не береться до уваги.

У зв’язку з цим відзначимо, що в сучасних умовах дедалі більше правників визнають фундаментальну роль інтуїтивних суджень нарівні з логікою. Ця обставина пов’язується, зокрема, з розвитком комп’ютеризації науки, в якій велику частину логічних операцій може виконувати машина (комп’ютер). Звільнена ж від рутини логіки наука “в залишку” має саме цю креативність, засновану на інтуїції [11, с. 78], і в цій частині людину на сьогодні замінити ніким.

Дедалі більшого поширення набувають методики кооперативного мислення з розподілом технічних (формально обґрунтованих логічних прийомів) і креативних (евристичних) дій між машиною (комп’ютером) і людиною. У такій ситуації прагнення виробити формально-логічний апарат юридичної науки таким, що максимально виключає особистість вченого-юриста з процесу пізнання, перетворює його в машину, видається дещо невчасним. Об’єктивне дослідження цифр і аналіз статистики може зробити і комп’ютер, але побачити сенс за цими цифрами може лише людина.

Висновки.

Соціологічний рівень охоплює дослідження динаміки правових зв’язків між самими учасниками особистих немайнових та майнових відносин, що взаємодіють між собою на підставі діалектично пов’язаних сил кооперації й конфлікту, за допомогою методів спостереження, опитування, інтерв’ювання тощо.

Філософський рівень забезпечує дослідження найбільш загальних цілей упорядкування суспільних відносин, виходячи з аксіологічних особливостей сфери дії механізму правового регулювання.

Результати досліджень вказаних рівнів пізнання (включаючи й догматичний [1]) підлягають об’єднанню за допомогою системного аналізу і далі осмислюються за допомогою методу правової рефлексії.

На кожному рівні наукового дослідження підлягають врахуванню об’єктивні й суб’єктивні чинники, що впливають на кінцевий науковий результат. До останніх відносяться неявні знання правника, засновані на системі його установок і цінностей, рівні та якості його освіти, прихильності до певної наукової школи, правосвідомості, правовій культурі, вихованні, загальній ерудиції та інших чинниках. Внаслідок цього можливе існування безлічі альтернативних подібно обґрунтованих пояснень явищ у сфері права, відповідно – безлічі різних варіантів рекомендацій щодо вдосконалення законодавства, правозастосовчої практики та правореалізаційної діяльності.

Розширення меж використання у законодавстві нового евристичного інструментарію, призначення якого обумовлюється філософськими і природничими трактуваннями сутнісних та системно-структурних властивостей сфери правового регулювання, дозволяє розкрити необмежений потенціал кожного досліджуваного феномена в органічному поєднанні як його статичних, так і, головним чином, динамічних характеристик.

Таким чином, методологія правового дослідження є продуктом переходу з абстрактно-гносеологічного рівня, який виступає “робочим майданчиком” для методології теоретико-правового аналізу, на рівень пізнання конкретного, з урахуванням апробованої галузевої специфіки дослідження відповідних явищ. В силу особливостей дії та застосування норм права та позанормативних регуляторів особистих немайнових та майнових відносин, методологія рухається у бік інструменталізації як матеріальних, так і процесуальних аспектів всебічного пізнання об’єкта наукового дослідження. Крім цього, для сучасної нормативно-правової методології характерна тенденція до встановлення стійкого кореляційного зв’язку між цими аспектами з метою всебічного пізнання конкретного явища правової дійсності і продуктивної практичної апробації отриманих теоретичних результатів у вигляді обґрунтованих рекомендацій щодо подальшого вдосконалення приписів чинних актів законодавства України.

Аналіз проблем правової науки з урахуванням новітніх методологічних підходів, його просторово-часових характеристик, діалектичного розвитку, категоріально-понятійного апарату, загальної систематики може істотно поповнити скарбницю фундаментальних наукоємних досліджень. Крім того, розширення меж застосування у

цивілістиці апробованого у інших галузевих науках сучасного методологічного інструментарію допоможе вивести наші уявлення про сутність сфери правового регулювання на новий, більш високий рівень, що матиме потужний теоретичний і методологічний ефект, об’єднуючи на єдиних засадах праворозуміння правову науку, законодавство і юридичну практику.

Використана література

1. Дзьобань О.П., Яроцький В.Л.. Герменевтичний метод у сучасних цивілістичних дослідженнях: до питання про доцільність застосування. // Інформація і право. – № 2(21)/2017. – С. 5-12.

2. Пугинский Б.И. Методологические вопросы правоведения // Правоведение. – 2010. – № 1. – С. 6-19.

3. Данильян О.Г. Методи правового дослідження / О.Г. Данильян, О.П. Дзьобань / Велика українська юридична енциклопедія : у 20 т. – Т. 2 : Філософія права ; редкол. : С.І. Максимов (голова) та ін. – Х. : Право, 2017. – С. 456-459.

4. Дзебань А.П. Общеметодологические и эвристические аспекты современных цивилистических исследований / А.П. Дзебань, В.Л. Яроцкий : сб. ст. посвящ. памяти проф. А.А. Пушкина [“Методология исследования проблем цивилистики”] ; под ред. Ю.М. Жорнокуя и С.А.Слипченко. – Х. : Право, 2017. – С. 176-205.

5. Юдин Э.Г. Системный подход и принцип деятельности / Э.Г. Юдин. – М. : Наука, 1978. – 391 с.

6. Садовский В.Н. Основания общей теории систем / В.Н. Садовский. – М. : Наука, 1974. – 280 с.

7. Артюхов В.В. Общая теория систем : самоорганизация, устойчивость, разнообразие, кризисы / В.В. Артюхов. – М. : Книжный дом “ЛИБРАКОМ”, 2009. – 224 с.

8. Филиппова С.Ю. Инструментальная методология цивилистического исследования : дис. на соискание науч. степени д-ра юрид. наук: 12.00.03 / С.Ю.Филиппова. – М., 2016. – 481 с.

9. Белов В.А. Наука гражданского права как система / В.А. Белов / Гражданское право : актуальные проблемы теории и практики ; под общ. ред. В.А.Белова. – М. : Юрайт-Издат, 2007. – С. 161-197.

10. Данильян О.Г. Методи правового дослідження / О.Г. Данильян, О.П. Дзьобань / Велика українська юридична енциклопедія : у 20 т. – Т. 2 : Філософія права ; редкол. : С.І. Максимов (голова) та ін. – Х. : Право, 2017. – С. 456-459.

11. Ельчанинов В.А. Логика и методология научного исследования : монография / В.А. Ельчанинов. – Барнаул : Изд-во Алтайского гос. ун-та, 2009. – 147 с.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

УДК 342.52

КОРЖ І.Ф., *доктор юридичних наук,* завідувач науковою лабораторією
НДІ інформатики і права НАПрН України

ВІЛЬНИЙ ДОСТУП ГРОМАДЯН ДО ПРАВОВОЇ ІНФОРМАЦІЇ – ЗАСАДНИЧА ОЗНАКА ЗАБЕЗПЕЧЕННЯ ПРАВОВОЇ БЕЗПЕКИ ДЕРЖАВИ

Анотація. *В даній статті досліджується питання правового регулювання доступу громадян України до правової інформації, як різновиду публічної інформації; аналізується ефективність дії законодавства у даній сфері, а також відповідність його міжнародно-правовим актам, що регулюють дане питання; здійснюється аналіз міжнародних статистичних даних, що досліджують питання стану доступу громадян України до згаданої інформації; аргументується співвідношення стану доступу до правової інформації зі станом правової безпеки держави.*

Ключові слова: *взаємодія влади і суспільства; доступ до правової інформації; консультації; правова безпека; правова інформація; управління державними справами.*

Summary. *This article explores the question of legal regulation of access of Ukrainian citizens to legal information, as a type of public information; analyzes the effectiveness of the legislation in this area, as well as its compliance with international legal acts governing this issue; an analysis of international statistical data that examines the state of access of Ukrainian citizens to the said information; the balance of the state of access to legal information with the state of legal security of the state is argued.*

Keywords: *interaction of power and society; access to legal information; consultations; legal security; legal information; management of public affairs.*

Аннотация. *В данной статье исследуется вопрос правового регулирования доступа граждан Украины к правовой информации, как разновидности публичной информации; анализируется эффективность действия законодательства в данной сфере, а также соответствие его международно-правовым актам, регулирующим данный вопрос; осуществляется анализ международных статистических данных, которые исследуют вопрос состояния доступа граждан Украины к упомянутой информации; аргументируется соотношение состояния доступа к правовой информации с состоянием правовой безопасности государства.*

Ключевые слова: *взаимодействие власти и общества; доступ к правовой информации; консультации; правовая безопасность; правовая информация; управление государственными делами.*

Постановка проблеми. Відповідно до статті 34 Конституції України, кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб. Здійснення цих прав може бути обмежене законом. А згідно зі статтею 57 Конституції України, кожному гарантується право знати свої права і обов’язки. Закони та інші нормативно-правові акти, що визначають права і обов’язки громадян, мають бути доведені до відома населення у порядку, встановленому законом. Закони та інші нормативно-правові акти, що визначають права і обов’язки громадян, не доведені до відома населення у порядку, встановленому законом, є нечинними.

Таким чином правова інформація, яка міститься у відповідних актах та документах органів державної влади, як різновид публічної інформації (оскільки вона стосується діяльності публічних органів держави, визначає права і свободи суб’єктів суспільних відносин), має бути доступною для громадськості. Зазначене питання регулюється

відповідними законами [9, с. 18] і має усі підстави для відкритості і доступності. Також, актуальність зазначеного обумовлено тим, що в демократичній державі влада не може ефективно функціонувати без взаєморозуміння і конструктивної взаємодії з громадянським суспільством, яке являє собою множинність самодіяльних, незалежних від держави соціальних груп та індивідів, які самостійно захищають свої інтереси.

Наукові розвідки з питань доступу до правової інформації, регулювання суспільних відносин між державними органами, органами місцевого самоврядування, територіальними органами, установами, підвідомчими державними органам та фізичними і юридичними особами в сфері отримання та поширення інформації є надзвичайно корисними в сучасний період розвитку української держави. Фактично, право на інформацію є одним за найважливіших здобутків громади на шляху до становлення демократичної держави, де реалізується ефективна участь громадян в управлінні країною і існує справжня підзвітність уряду. ЗМІ наводять безліч прикладів, коли право на інформацію вже стало інструментом виявлення випадків корупції у багатьох державних органів. Слід також мати на увазі, що законодавство про доступ до інформації здатне забезпечити важливі соціальні переваги. Воно встановлює способи і порядок отримання і поширення публічної інформації, визначає права і обов’язки користувачів і власників інформацією, забезпечує гарантії реалізації прав користувачів інформацією на вільне одержання та поширення публічної інформації.

Як показує світова практика, за умови належно організованої взаємодії влади і громадськості, у державі набагато ефективніше вирішуються проблемні питання. Наразі можна стверджувати, що в Україні є серйозний прогрес із забезпечення громадян можливістю контролювати державні органи, ознайомлюватись з національним законодавством, постановами регіональних державних органів тощо. В той же самий час у порівнянні з більш розвиненими країнами світу Україна все ще відстає в даній сфері.

Метою статті є аналіз стану доступу громадян до правової інформації в Україні, як конституційного права громадян, зазначивши існуючі проблеми щодо доступу до правової інформації та причини їх виникнення; визначення співвідношення стану реалізації згаданого права з такою правовою категорією як “правова безпека”; розкриття наслідки впливу негативних чинників на стан демократичних свобод у державі.

Виклад основного матеріалу. Успішна реформа державної влади, місцевого самоврядування та суспільного життя в Україні, і як результат зазначеного –відповідність рівня основних національних стандартів (соціальних, правових, політичних тощо) стандартам передових європейських країн – саме цього очікує українське суспільство від провідників зазначених змін в Україні. Люди очікують впровадження у життя саме європейських демократичних цінностей та наповнення свого життя реальним змістом. Розглянемо базові європейські цінності, відповідність яким прагнуть мати українці.

Базові загальні цінності, на яких побудований Європейський Союз, закріплені у другому параграфі Європейського договору від 07 лютого 1992 р. [1]. Цими принципами є: шана до людської гідності та до прав людини, включаючи права осіб, що належать до меншин; засадничі свободи та демократія; рівність; верховенство права. Ці цінності є загальними для держав-членів у суспільстві, де переважають плюралізм, недискримінація, толерантність, справедливість, солідарність та рівність жінок і чоловіків. В основі цих цінностей лежить:

– гуманістичне мислення, згідно з яким у центрі усіх подій знаходиться людина, тобто “humanitas” (лат. – людяність);

– раціональність, тобто раціональне мислення визначається розумом як єдиним джерелом пізнання;

– секулярність – відокремлення держави і церкви, політики і релігії, політичних організацій і релігійних;

– правова держава, що включає в себе основні права, поділ влади, прогнозованість діяльності держави, наявність механізмів безпеки;

– демократія, за якої встановлюється такий політичний порядок, за якого влада спирається на волю народу і підзвітна йому;

– права людини, як найбільше досягнення розвитку людства, які забезпечуються усім.

У 1993 році на засіданні Європейської Ради в Копенгагені були прийняті Копенгагенські критерії – критерії вступу країн в Європейський Союз, і підтверджені в грудні 1995 року на засіданні Європейської Ради в Мадриді [2]. Наведемо лише Політичні критерії, які зазначають, що членство в ЄС під кутом зору політичних стандартів вимагає від країни-кандидата стабільності інститутів, що гарантують демократію, верховенство права, повагу і захист меншин. Статтею 6 Договору про Європейський союз закріплено, що “Союз базується на принципах свободи, демократії, поваги до прав людини і основних свобод та верховенства права”.

Країни, які бажають стати членами ЄС, повинні не лише закріпити принципи демократії і верховенства права у своїх конституціях, але й втілювати їх у повсякденне життя. Конституції країн-заявників мають гарантувати демократичні свободи, включаючи політичний плюралізм, свободу слова і свободу совісті. Вони встановлюють демократичні інститути та незалежні органи правосуддя, органи конституційної юрисдикції, що створює умови для нормального функціонування державних установ, проведення вільних і справедливих виборів, періодичної зміни правлячої парламентської більшості, а також визнання важливої ролі опозиції у політичному житті.

З метою оцінки виконання країнами-кандидатами умов членства Європейська Комісія (далі – ЄК) у кожному своєму Висновку виходить за межі формального опису політичних інститутів і відносин між ними. На основі ряду детальних критеріїв вона оцінює, чи має демократія реальний характер. При цьому перевіряється, як захищаються конституційні права і свободи, зокрема, свобода слова в процесі діяльності політичних партій, неурядових організацій і засобів масової інформації.

Згідно з рішенням Європейської Ради у Люксембурзі в 1997 р., ЄК було запропоновано подавати щорічні звіти про досягнутий прогрес країн-кандидатів у процесі приєднання з відповідними висновками. У них ЄК аналізує відповідність реформ, що проводяться у країнах-кандидатах з 1997 р., Копенгагенським критеріям. При цьому беруться до уваги лише вжиті заходи, а не ті, що готуються. Це є універсальним методом, який дає можливість на основі об’єктивного підходу порівняти й оцінити реальний прогрес країн на шляху вступу до ЄС.

Оцінка реального прогресу проводиться на підставі різних джерел інформації:

- інформації, наданої країнами-кандидатами з метою внесення коректив до Висновків ЄК;

- інформації, отриманої під час зустрічей у рамках Європейських угод і перевірки адаптації законодавства;

- звітів Європейського Парламенту, оцінок держав-членів, роботи міжнародних організацій, зокрема Ради Європи і ОБСЄ, міжнародних фінансових інститутів і неурядових організацій.

Таким чином, перед країнами-кандидатами стоять досить складні завдання, швидкість вирішення яких залежить від ефективності засобів їх розв’язання. Центральні органи ЄС не тільки контролюють процес досягнення відповідності критеріям вступу,

але й намагаються розробляти ефективні програми для цих цілей. Підготовлені на основі згаданого аналізу Висновки щодо поданих країнами-кандидатами заяв на членство в ЄС відображають їх прогрес у досягненні відповідності Копенгагенським критеріям.

Згадані засадничі цінності отримали свій розвиток в проголошеній на засіданні Європейської Ради в Ніцці 7 грудня 2000 року Хартії Європейського Союзу про основні права [3]. У Хартії основою класифікації обрані не вид або сфера застосування права, а цінності, на яких вони базуються та які вони захищають, – *людська гідність, свобода, рівність, солідарність*.

Так, Розділ I ***“Гідність”*** (статті 1 – 5), крім, власне, права на людську гідність, закріплює права та гарантії, які забезпечують гідне існування людської особистості в суспільстві: право на життя, заборона тортур, рабства тощо.

У розділі II ***“Свободи”*** (статті 6 – 19) зосереджено увагу на фундаментальних громадянських та політичних свободах, закріплених в Європейській Конвенції з прав людини [4], яка, у свою чергу, базується на Загальній декларації прав людини ООН [5]: право на свободу та особисту недоторканність, на повагу приватного та сімейного життя, на захист інформації особистого характеру, на укладення шлюбу та створення сім’ї, свободу думки, совісті та віросповідання, свободу мистецтва та науки тощо.

Розділ V ***“Права громадян”*** (статті 39 – 46) включає права, користування якими, як правило, пов’язане із наявністю в особи громадянства ЄС. До цього Розділу були включені деякі права, про які йдеться в інших положеннях Договору про ЄС, зокрема, право на доступ до документів (ст. 15 ДФЄС). Крім того, передбачається право подання скарги на порушення прав людини до Омбудсмена ЄС, а також подання петиції до Європарламенту.

Відповідно до зазначених цінностей, лише вільні люди, які поважають один одного, дотримуються права і гідності інших людей, спроможні побудувати суспільство, в якому зможе вижити будь-яка людина. Тому можна стверджувати, що сьогодні здійснюється трансформація держави з пост-радянським укладом до соціально-орієнтованого суспільства з прозорою демократією. Йде зміна кількох ціннісних систем, які були надбанні нашими пращурами за багаторічну історію та формується нова система, яка передбачає чітку орієнтацію на європейську шкалу цінностей, на значні ціннісні досягнення українського народу, на моральне оздоровлення суспільства, зростання значення культури громадянського суспільства.

Прозорий контроль за державою з боку громадянського суспільства може забезпечити оздоровлення держави та державного управління, позбавлення від такого важкого тягаря нації – корупційних проявів. Ми вважаємо, що в сучасній українській державі потрібні зміни в акцентах виховання людини. Нині слід формувати не лише сентиментального патріота, а й дієвого громадянина, який любить свою Батьківщину й бере активну участь у модернізації суспільства і держави. Насамперед, зазначене стосується реального доступу громадянина до управління державою, до участі у напрацюванні та прийнятті органами державної влади та органами місцевого самоврядування відповідних рішень.

Зазначене може бути реалізовано лише за умови гарантованого доступу громадян до правової інформації, як це передбачено статтею 34 Конституції України [6] *“Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, 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”. Ця норма Конституції відповідає головним міжнародно-правовим стандартам у галузі прав людини, яким є комплексний акт, розроблений в рамках ООН і відомий як ***Хартія про права людини***. Ця Хартія складається: із ***Загальної декларації прав людини***, що затверджена і проголошена Генеральною Асамблеєю ООН 10 грудня 1948 р. і норми якої не є формально обов’язковими для дотримання членами ООН; ***Міжнародного пакту про економічні, соціальні і культурні права*** та ***Міжнародного пакту про громадянські та політичні права*** [7], який набув чинності, в тому числі для України, 23 березня 1976 року. Норми, що закріплені у пактах, прирівнюються до міжнародних договорів і вважаються обов’язковими для дотримання державами, які до цих Пактів приєдналися. Україною ратифіковано всі документи, що складають Хартію прав людини.

Відповідно до положень статті 19 цього Пакту: *“*2) *кожна людина має право на вільне вираження свого погляду; це право включає свободу шукати, діставати і поширювати будь-яку інформацію та ідеї, незалежно від державних кордонів, усно, письмово чи за допомогою друку або художніх форм вираження чи іншими способами на свій вибір. Користування передбаченими в пункті (2) цієї Статті правами накладає особливі обов’язки й особливу відповідальність. Воно може бути, отже, пов’язане з певними обмеженнями, які, однак, мають встановлюватися законом і бути необхідними: b) для охорони державної безпеки, громадського порядку, здоров’я чи моральності населення”*.

Реалізація права на доступ до інформації, яка знаходиться в розпорядженні органів державної влади та місцевого самоврядування, підтримується також конституційним правом на звернення, яке гарантується статтею 40 Конституції. Ця стаття зобов’язує органи державної влади та місцевого самоврядування, їхніх посадових та службових осіб розглядати усні чи письмові звернення, індивідуальні або колективні, і давати обґрунтовану відповідь у встановлений законом термін.

Чому так багато уваги приділяється інформації? Тому що інформація – це повітря демократії. Лише обізнане суспільство може здійснити контроль за діяльністю влади, щоб примусити її служити громадським інтересам. І навпаки, погана влада потребує таємності, щоб поховати власну неефективність, марнотратство і корупцію. Звідси відкритість влади, оприлюднення інформації про те, що саме і як вона засекречує, є завжди актуальним політичним питанням, лакмусовим папірцем, що свідчить про її реальні наміри і плани [8].

Інформація є засобом комунікації людей, а також є об’єктом їх діяльності. Без застосування інформації у різних її формах і проявах неможлива еволюція людини, розвиток суспільства і держави. Інформаційні потреби є одним з різновидів нематеріальних потреб людини, які виникають через брак інформації для здійснення людської діяльності і є характерною особливістю, притаманною людині, що відрізняє її від решти живих організмів, які хоч і відчувають потребу в інформації, але виключно для задоволення відносно простих вітальних потреб. Інформація в житті суспільства настільки ж необхідний ресурс, як сировинні, енергетичні, фінансові та інші. Більше того, інформація – тепер об’єкт купівлі та продажу. Інформаційний продукт – ресурс суспільного надбання. Це ресурс вічний.

В демократичних суспільствах важливе значення має вільний доступ громадян до такого різновиду інформації, як правова інформація. У науковій літературі під правовою інформацією розуміють сукупність документованих або публічно оголошених

відомостей про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення тощо. До неї відносять всю інформацію, яка пов’язана з правом, тобто з матеріалами про правову освіту, про розробку наукових концепцій розвитку права, а також з матеріалами підготовки нормативно-правових актів, їх обговоренням і впорядкуванням, тлумаченням і реалізацією правових норм, вивчення практики їх застосування. Існує законодавче визначення зазначеного терміну: ***правова інформація*** *– будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо* [9].

З метою забезпечення доступу до законодавчих та інших нормативних актів фізичним та юридичним особам держава забезпечує офіційне видання цих актів масовими тиражами у найкоротші строки після їх прийняття.

До основних видів правової інформації відносяться нормативна і ненормативна правова інформація. Нормативно-правова інформація складає основу правової інформації і являє собою сукупність нормативно-правових актів (далі – НПА) в усьому їх різноманітті і динаміці, тобто включає в себе нормативно-правові акти та інформацію про їхні розробку, обговорення та прийняття, про їхню дію, про внесені зміни до них, про колізію норм, прогалини та недоліки дії.

З метою забезпечення конституційного права громадян на доступ до правової інформації та створення належних умов користування чинними актами законодавства, на Міністерство юстиції України покладено функції офіційного видавця збірників актів законодавства України, а також їх оновлення. Необхідно пам’ятати, що громадяни, державні органи, підприємства, установи, організації під час здійснення своїх прав і обов’язків мають застосовувати закони України, інші акти Верховної Ради України, акти Президента України і Кабінету Міністрів України, опубліковані в офіційних друкованих виданнях або одержані у встановленому порядку від органу, який їх видав.

Необхідно зазначити, що рівень інформатизації українського суспільства постійно зростає, що вимагає швидкого доступу до актуальних текстів нормативно-правової інформації, забезпечуючи тим самим конституційне право громадян на участь в управління державними справами, в реалізації своїх прав і свобод. Державна влада в останні десять років багато зробила для того, щоб громадяни держави мали можливість брати участь в управлінні державними справами, напрацюванні та прийнятті рішень органами державної влади. Це особливо помітно стало в період підготовки до вступу України до Євросоюзу. Державна влада усвідомлює, що розвинуте демократичне та громадянське суспільство можна побудувати лише в державі, де громадяни є активними учасниками процесу формування та реалізації державної політики. З цією метою розробляються та здійснюються заходи, що сприятимуть становленню громадянського суспільства, підвищується рівень правової культури громадян, створюються умови для ширшої обізнаності громадян під час проведення діалогу з владою.

З метою залучення громадян до участі у формуванні та реалізації державної політики, Уряд України запроваджує проведення консультацій з громадськістю з найбільш важливих для суспільства питань. Зазначений спосіб участі громадян в управлінні державними справами передбачений Порядком проведення консультацій з громадськістю з питань формування та реалізації державної політики, затвердженим постановою Кабінету Міністрів України від 03.11.10 р. № 996 [10]. Цей Порядок визначає основні вимоги до організації і проведення органами виконавчої влади консультацій з громадськістю з питань формування та реалізації державної політики. Мета їх проведення – залучення громадян до участі в управлінні державними справами,

надання можливості для їх вільного доступу до інформації про діяльність органів виконавчої влади, а також забезпечення гласності, відкритості та прозорості діяльності зазначених органів.

Проведення консультацій з громадськістю має сприяти налагодженню системного діалогу органів виконавчої влади з громадськістю, підвищенню якості підготовки рішень з важливих питань державного і суспільного життя з урахуванням громадської думки, створенню умов для участі громадян у розробленні проектів таких рішень. Консультації з громадськістю проводяться з питань, що стосуються суспільно-економічного розвитку держави, реалізації та захисту прав і свобод громадян, задоволення їх політичних, економічних, соціальних, культурних та інших інтересів. Результати проведення консультацій з громадськістю враховуються органом виконавчої влади під час прийняття остаточного рішення або в подальшій його роботі. Консультації з громадськістю організовує і проводить орган виконавчої влади, який є головним розробником проекту нормативно-правового акту або готує пропозиції щодо реалізації державної політики у відповідній сфері державного і суспільного життя.

Органи виконавчої влади щороку мають складати орієнтовний план проведення консультацій з громадськістю з урахуванням основних завдань, визначених Програмою діяльності Кабінету Міністрів України, Державною програмою економічного і соціального розвитку України, планом законопроектних робіт та іншими документами, а також результатів проведення попередніх консультацій з громадськістю. Орієнтовний план затверджується до початку року, оприлюднюється на офіційному веб-сайті органу виконавчої влади та в інший прийнятний спосіб.

Громадські об’єднання, релігійні, благодійні організації, творчі спілки, професійні спілки та їх об’єднання, асоціації, організації роботодавців та їх об’єднання, органи самоорганізації населення, недержавні засоби масової інформації, інші непідприємницькі товариства та установи, легалізовані відповідно до законодавства, можуть ініціювати проведення консультацій з громадськістю з питань, не включених до орієнтовного плану, шляхом подання відповідних пропозицій громадській раді або безпосередньо органу виконавчої влади. У разі коли пропозиція щодо проведення консультацій з громадськістю з одного питання надійшла не менше ніж від трьох інститутів громадянського суспільства, такі консультації проводяться обов’язково.

Консультації з громадськістю проводяться у формі публічного громадського обговорення, електронних консультацій з громадськістю (безпосередні форми) та вивчення громадської думки (опосередкована форма) або одночасно у трьох цих формах.

В обов’язковому порядку проводяться консультації з громадськістю у формі публічного громадського обговорення та/або електронних консультацій з громадськістю щодо проектів нормативно-правових актів, які:

– стосуються конституційних прав, свобод та обов’язків громадян;

– стосуються життєвих інтересів громадян, у тому числі впливають на стан навколишнього природного середовища;

– передбачають провадження регуляторної діяльності у певній сфері;

– визначають стратегічні цілі, пріоритети і завдання у відповідній сфері державного управління (у тому числі проекти державних і регіональних програм економічного, соціального і культурного розвитку, рішення стосовно їх виконання);

– стосуються інтересів територіальних громад, здійснення повноважень місцевого самоврядування, делегованих органам виконавчої влади відповідними радами;

– визначають порядок надання адміністративних послуг;

– стосуються правового статусу громадських об’єднань, їх фінансування та діяльності;

– передбачають надання пільг чи встановлення обмежень для суб’єктів господарювання та інститутів громадянського суспільства;

– стосуються присвоєння юридичним особам та об’єктам права власності, які за ними закріплені, об’єктам права власності, які належать фізичним особам, імен (псевдонімів) фізичних осіб, ювілейних та святкових дат, назв і дат історичних подій;

– стосуються витрачання бюджетних коштів (звіти головних розпорядників бюджетних коштів за минулий рік).

Строк проведення таких консультацій з громадськістю визначається органом виконавчої влади і повинен становити не менш як 15 календарних днів.

Необхідно зазначити, що публічне громадське обговорення передбачає організацію і проведення публічних заходів:

– конференцій, форумів, громадських слухань, засідань за круглим столом, зборів, зустрічей (нарад) з громадськістю;

– Інтернет-конференцій, відео-конференцій.

Згаданою Постановою рекомендовано органам місцевого самоврядування під час проведення консультацій з громадськістю та утворення громадських рад при органах місцевого самоврядування керуватися затвердженими цією постановою Порядком і Типовим положенням про громадську раду.

Таким чином, є очевидним, що сильна держава неможлива без розвиненого громадянського суспільства, яке стає дієвим чинником державотворення за умови конструктивного та соціально відповідального діалогу з державою в межах правового поля. Саме громадянське суспільство активно сприяє процесам політичної демократизації, набуття державою ознак правової, відстоюючи матеріальну і духовну незалежність людини від держави, домагаючись правової гарантії такої незалежності, захисту приватних і суспільних інтересів людей. Разом з тим, має бути зворотний зв’язок державних інститутів з громадськістю, оскільки правова держава має реагувати на запити і потреби асоційованого громадянства, видавати відповідні законодавчі акти та слідкувати за їх виконанням. Іншими словами, вона повинна створити ситуацію правової захищеності громадян, сформувати сприятливе правове поле для діяльності створюваних ними громадських інститутів. Тому особливого значення набуває проблема взаємодії інститутів громадянського суспільства з органами державної влади України. І саме така форма взаємодії, як участь інституту громадянського суспільства у нормотворчій діяльності держави, яка має забезпечуватися участю у розробленні та обговоренні проектів нормативно-правових актів. Участь у правотворчій діяльності є найпоширенішою формою участі громадських організацій у державному управлінні у правових, демократичних державах.

В правовій державі громадське обговорення проектів нормативних актів має бути обов’язковим етапом нормотворчого процесу в системі органів виконавчої влади. Консультації з громадськістю в нормотворчому процесі мають проводитися з метою залучення громадян до участі в управлінні державними справами, надання можливості для їх вільного доступу до інформації про діяльність органів виконавчої влади, а також забезпечення гласності, відкритості та прозорості в діяльності цих органів. Проведення консультацій з громадськістю має також сприяти налагодженню системного діалогу органів виконавчої влади і громадськості, підвищенню якості підготовки та прийняття рішень з важливих питань державного і суспільного життя з урахуванням думки громадськості, створенню умов для участі громадян у розробленні проектів таких рішень.

Необхідно зазначити, що проблема взаємодії влади і суспільства була завжди актуальною, оскільки полягає у складності інформування усього населення про

діяльність влади, а також в отриманні зворотного зв’язку від населення щодо проблем, які існують у суспільстві. У процесі функціонування органів державної влади, коли інформаційний супровід їх діяльності не завжди є відкритим, питання зворотного зв’язку між владою і суспільством набуло актуальності, що і стало одною із підстав для реформ, здійснюваних нині в Україні. Зазначене потребує від органів державної влади підвищення своєї відкритості і легітимності, а також більш оперативно здійснювати комунікації з суспільством для вирішення проблем, що виникають у суспільстві. Таким чином, ефективна комунікація – це взаємодія, що передбачає зворотній зв’язок та дозволяє підтримувати інтерес і довіру населення до діяльності влади. Вона направлена на формування довготривалого лояльного відношення до законодавчої та виконавчої влади, органів місцевого самоврядування.

У сучасній демократичній державі, в якому інститути громадянського суспільства функціонують достатньо ефективно, державно-владні структури не можуть встановлювати так звані “власні правила гри” у відносинах з громадськістю, оскільки в такому разі будь-які рішення, навіть досить ефективні і такі, що відповідають інтересам громадськості, не будуть мати легітимності. Основним критерієм ефективності функціонування відносин влади з громадськістю є створення умов для вільного схвалення громадянами дій органів влади, прийнятих ними рішень. Тому саме у формі двостороннього, збалансованого зв’язку суспільства та влади створюються найбільш оптимальні умови для ефективного функціонування суб’єктів зазначених відносин оскільки це передбачає:

– відкритість інформаційних потоків у поясненні змісту державної політики, що гарантує максимальну свободу в обговоренні суспільних проблем;

– сприяння розумінню громадянами діяльності органів державної влади, доцільності прийняття ними відповідних рішень;

– активну участь громадськості в управлінні державою, яка супроводжується систематичним залученням її до вирішення соціально значущих проблем;

– організацію та підтримку владою соціальних дискусій шляхом залучення громадськості до процесів творення та реалізації державної політики [11, с. 11].

А чи усе робиться в Україні для того, щоб громадянське суспільство країни ефективно використовувало свій потенціал в управлінні державними справами? На жаль для оптимістичної упевненості у цьому недостатньо підстав. Якщо Українським парламентом, судовою владою, Президентом України здійснюються заходи щодо залучення громадян до вирішення актуальних проблем, то виконавча гілка влади страждає старою хворобою – працювати непрозоро, а це негативно впливає на стан свободи у країні.

У 2018 році Фрідом Хаус (анг. Freedom House – “дім свободи”), міжнародною правозахисною неурядовою організацією, яка займається підтримкою та дослідженням стану демократії, політичних свобод і дотримання прав людини, опубліковано звіт “Свобода в світі 2018” [12] з оцінкою ступеня демократичних свобод, свободи преси та свободи в інтернетмережі по кожній країні світу, і в якому зазначено, що демократія зіткнулася з її найбільш серйозною кризою протягом десятиліть в 2017 році, оскільки її основні положення були піддані нападу у всьому світі. Щодо України, то в ньому зазначено, що зволікання у судовому переслідуванні високопосадових корупціонерів підірвало популярність Уряду. Його прозорість роботи складає 50 %. У сфері громадянських свобод відзначався політичний тиск та напади на журналістів, що створює загрози свободі преси, свобода преси недостатньо ефективна, преса вільна на 50 %.

Відзначено також, що, незважаючи на сильний тиск з боку громадянського суспільства, серйозною проблемою є невелика політична воля для боротьби з корупцією. Громадянські свободи складають біля 60 %. В цілому Україна віднесена до

напіввільних держав, маючи оцінку 62 зі 100, фактично знаходячись на одному рівні з такими країнами, як: Молдавія, Киргизія, країни колишньої Югославії та ряд африканських та латино-американських країн.

За іншим дослідженням Україна зайняла 83-тю позицію зі 167-ми у рейтингу Democracy Index 2017, підготованому фахівцями групи Intelligent Unit журналу The Economist. В оприлюдненому минулого тижня звіті Україна має загальний бал 5,69, інформує видання. Найменше балів Україна отримала за показником “функціонування влади” – лише 3,21.

При визначенні балу враховувалося 5 аспектів – виборчий процес та плюралізм, громадянські свободи, функціонування влади, політична участь і політична культура. Виходячи з балів за 60-ма показниками в межах цих категорій, кожна держава класифікується як один із чотирьох типів режиму: повна демократія, недосконала демократія, гібридний режим і авторитарний режим. У рейтингу світових демократій Україна класифікована як держава з “гібридним режимом” [13].

За ще одним оцінюванням світового рейтингу рівня життя, проведеного британським аналітичним центром The Legatum Institute, Україна зайняла 112 місце зі 148, втративши 5 позицій в порівнянні з 2016 роком. Починаючи з 2006 року, коли був опублікований перший Індекс процвітання, Україна опустилась на 17 позицій. Оцінка здійснювалася за результатами опитування громадян країн за 8 категоріями: стан економіки, соціальна сфера, діяльність влади, підприємництво, охорона здоров’я і персональної свободи громадян. За діяльністю влади Україна зайняла 130 місце, гірше лише охорона здоров’я – 135 місце [14].

Нагадаємо, що Україна зайняла останнє, 44 місце у Європі, і 150 місце у світі серед 186 країн світу в рейтингу економічної свободи американського аналітичного центру Heritage Foundation [14].

Зазначене свідчить, що незважаючи на відповідні запевнення представників державної вади про невідворотність демократичного європейського поступу України, про прозорість діяльності державної влади, реальність далека від зазначених запевнень. Для підтвердження можна навести приклад дії представників Міністерства соціальної політики України щодо їхнього прагнення здійснити так зване реформування пенсійного забезпечення військовослужбовців та деяких інших осіб. Ламаючи перевірену роками концепцію нарахування і перерахування пенсії військовослужбовцям, з її простими, прозорими і зрозумілими механізмами, керівництво міністерства намагається всупереч положенням зазначених вище міжнародних угод, внутрішнього законодавства і Конституції України (ст. Регламенту Кабінету Міністрів України – § 3. Взаємодія з громадськістю) [15], всупереч консолідованій думці громадських і ветеранських організацій, керівництва військових формувань держави, “підкилимно”, без громадського обговорення “проштовхнути” законопроект, яким запроваджується механізм нерівного пенсійного забезпечення в залежності від року виходу на пенсію, а фактично запроваджується диспропорція у пенсійному забезпеченні. Крім того, надаються великі преференції військовослужбовцям, які перебували в АТО і які проходили військову службу у зазначений період, а іншим військовим пенсіонерам мінімізується рівень пенсійного нарахування та перерахування за 3-ма складовими – посадовий оклад, оклад за військовим званням та розмір за вислугу років (на сьогоднішній день враховуються усі складові грошового забезпечення). Зазначене може викликати антагоністичні відносини в середовищі військових пенсіонерів, як і серед самих військовослужбовців, чого ні в якому разі не можна допускати, враховуючи сьогоднішню ситуацію, пов’язану із агресією Росії щодо України. Захисників Вітчизни

не можна “стравлювати” один з одним – це підрив засад національної безпеки. Умисно це робиться, чи внаслідок недалекоглядного підходу, це мають визначити керівники держави, однак їм потрібно пам’ятати, що запропоновані преференції у пенсійному забезпеченні можуть викликати відтік досвідчених, високопрофесійних офіцерів з військової служби, що, у свою чергу, може призвести до підриву обороноспроможності держави та її безпеки.

Другим негативним прикладом слугує ситуація з наданням та припиненням українського громадянства громадянина Саакашвілі Міхеіла. Оскільки Указ Президента про прийняття до громадянства України згаданого громадянина відбулося було підписано прозоро, з публікацією акту [16], то не відповідає положенням Закону України “Про доступ до публічної інформації” утаємничення Указу Президента про припинення українського громадянства щодо громадянина Сакаашвілі М., відмова громадянину Олександру Павліченку [17] у наданні інформації за таких підстав як: “Запитувана інформація про припинення громадянства України є конфіденційною і стосується прав та охоронюваних законом інтересів іншої особи, однак письмовий дозвіл на доступ до такої інформації відповідно до статті 7 закону України “Про доступ до публічної інформації” не надано”. В даному випадку не реалізується принцип забезпечення доступу до публічної інформації, передбачений ст. 4 Закону [18], щодо “вільного отримання, поширення та будь-якого іншого використання інформації, що була надана або оприлюднена відповідно до цього Закону, крім обмежень, встановлених законом”.

Зазначена негативна ситуація з правом та непрозора діяльність Уряду та Президента України, недотримання положень згаданих вище правових актів – все це створює загрози правовій безпеці держави, яка має потребу в розробці конституційно-правового поняття національної безпеки, правової охорони Конституції, підвищення ефективності законотворчого процесу, вдосконалення механізму впровадження принципу верховенства права [19, с. 178].

Як зазначає Добродумов О. П. – “…постановка питання про правову безпеку має два аспекти. Перший з них полягає в забезпеченні захищеності самої правової системи і спрямований на її вдосконалення і подальший розвиток. Інший полягає в тому, що в рамках правової системи шляхом правового регулювання суспільних відносин здійснюються заходи безпеки в різних сферах: економічній, екологічній, воєнній тощо. Отже, правова безпека покликана забезпечити захищеність національних інтересів, які відбиваються в процесі правового регулювання суспільних відносин, опосередкувати всі види безпеки. Усе це визначає роль і значення правової безпеки в охороні національних інтересів України та її провідне місце серед інших видів безпеки в регулюванні суспільних відносин в різних сферах”. За допомогою права усуваються загрози, спрямовані на будь-які обмеження. Національні інтереси у сфері економіки, екології, оборонній та інших сферах забезпечуються за допомогою права, дії правової системи. Отже, забезпечення всіх інших видів безпеки за допомогою права свідчить про необхідність всебічної охорони самого права, яке виступає гарантом безпеки в рамках діючої правової системи [19, с. 178-179].

Мета, зміст, характер правової безпеки обумовлені можливостями права захистити суспільні відносини від порушень. Саме недосконаліть законодавства, його недотримання і відповідно неефективність регулювання суспільних відносин і справляють негативний вплив на захист як інтересів суспільства і людини, так і національних інтересів. На стан правової системи, результативність її дії значний вплив чинять також правосвідомість, правова культура, ставлення до права у суспільстві.

Фактором, який безпосередньо впливає на правову систему, є правовий нігілізм, що втілює низький рівень правової культури. Невиконання закону, безвідповідальність, незастосування санкцій породжують незахищеність національних інтересів і виступають як негативні фактори впливу на правову систему. І головне полягає в тому, що за скоєння подібних дій (чи бездіяльності), які по суті представляють загрозу національній безпеці, відповідальність, в основному не несеться. Найбільша міра відповідальності – зняття з посади, переведення на іншу роботу.

Негативно впливати на правову систему, її функціонування можуть і не відображені в законодавстві інтереси особи, суспільства, держави. У них відсутня правова охорона, а отже, ці інтереси не реалізуються, не знаходять правового регулювання в рамках суспільних відносин тощо.

Для подолання правового нігілізму, невиконання законів та інших правових актів необхідна не тільки пропаганда права, але й насамперед видання правових законів, справедливих за своєю сутністю, які б повною мірою відображали потреби й інтереси громадян.

Дотримання прав і свобод, їх гарантованість є пріоритетом для будь-якої демократичної держави. Правова система держави є основним механізмом, який має гарантувати та забезпечувати права і свободи громадян України, а також їх поновлювати у випадку порушення. Саме в цьому і полягає авторитетність права, тобто його спроможність втілюватися в систему суспільних відносин, створюючи правопорядок. Право авторитетне у суспільстві, якщо воно є: надійною опорою безпеки особи і майна; гарантією спокійної праці і побуту; загальнодоступним способом цивілізованого вирішення спорів і конфліктів. Найбільше його авторитетність визначається станом правопорядку – реальною можливістю здійснення прав і законних інтересів членів суспільства, їх захисту від злочинних посягань, об’єктивним, законним вирішенням правових спорів у судах, а за необхідності – примусовим виконанням невиконаних зобов’язань, усуненням протиправних станів, поновленням порушених прав [20].

Міцність правопорядку, авторитетність права значною мірою залежать від спроможності законодавця своєчасно враховувати відносини, що виникають і породжують спори, конфлікти, які потребують юридичного регулювання і захисту і які, насамперед, знаходять відображення в правозастосовній (судовій та адміністративній) практиці. Саме стабільна, авторитетна, динамічна правова система, яка забезпечена відповідним їй апаратом судової влади та правоохоронних органів – є найбільш ефективною формою упорядкування і динаміки суспільних відносин [20, с.70].

Існують наступні визначення: ***правова безпека*** *– це спроможність суб’єктів права держави реалізувати та забезпечити свої життєво важливі інтереси за допомоги суспільних відносин, які охоронювані та захищені сукупністю здійснюваних в правовій системі держави і за допомогою права заходів, засобів і способів правового регулювання* [21]. Враховуючи зазначене та викладене вище, можна констатувати, що в Україні склалася ситуація, за якої продукуються загрози належному функціонуванню правової системи держави, тобто, існують реальні загрози правовій безпеці держави.

Висновки.

На підставі проведеного дослідження можна зробити висновок про те, що непрозорість функціонування органів державної влади, обмеження доступу громадян до правової інформації і, як наслідок, фактична заміна демократичних принципів в частині доступу громадян до інформації на авторитарні, коли органи влади самі вирішують, допускати громадян до правової інформації, чи ні – саме ці фактори створюють реальні загрози правовій системі держави. Як свідчать численні факти, органи державної влади

нині у своїй діяльності поширюють практику дистанціювання від громадськості зокрема та суспільства в цілому.

Статистичні дослідження таких відомих зарубіжних центрів, як Фрідом Хаус, Intelligent Unit журналу The Economist, The Legatum Institute, Heritage Foundation підтверджують, що структури державної влади України за рейтингами прозорості функціонування, за ступенем забезпечення демократичних свобод, свободи преси та свободи в інтернет-мережі пасуть задніх. Україна визнана напів-вільною, напів-демократичною, з існуванням гібридного режиму країною. Органи державної влади продовжують погіршувати зазначені показники, оскільки, як показує реальна дійсність, замість демократизації суспільного життя, нехтуючи об’єктивними потребами щодо розвитку громадянського суспільства і реального виконання взятих на себе міжнародних зобов’язань, керівництво держави часто ігнорує суспільні потреби і піклується про примноження своїх особистих статків. Зазначене підтверджується тим, що владою не беруться до уваги і не сприймаються відповідні наукові напрацювання, а впроваджуються у практику вузькокорпоративні інтереси, насамперед інтереси заможних представників істеблішменту.

Для зміни такої ситуації потрібні кардинальні зміни в системі формування державної влади, а також посилення міжнародного контролю у даній царині.

Використана література

1. Consolidated version of the Treaty on European Union, Title I, Common provisions. – Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex: 12012M002#document1

2. Копенгагенські критерії членства в Європейському Союзі. – Режим доступу : http://mfa.gov.ua/ua/page/open/id/774

3. Хартія основних прав Європейського Союзу 2000. – Режим доступу : https://constituanta.blogspot.de/2011/03/2000.html

4. Конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 року. – Режим доступу : http://www.echr.coe.int/Documents/Convention_ukr.pdf

5. Загальна декларація прав людини від 10 грудня 1948 року. – Режим доступу : http://www.irs.in.ua/index.php?option=com_content&view=article&id=82&catid=47&Itemid=74&lang=ru

6. Конституція України : Закон України від 28.06.96 р. // Відомості Верховної Ради України (ВВР). – 1996. – № 30. – Ст. 141.

7. Міжнародний Пакт про громадянські та політичні права від 16 грудня 1966 року. – Режим доступу : http://search.ligazakon.ua/l_doc2.nsf/link1/MU66003U.html#

8. Права людини в Україні – 2004. Право на доступ до інформації. – Режим доступу : http://stop-x-files-ua.org/права-людини-в-україні-2004-viii-право-на-дост

9. Про інформацію : Закон України від 02.10.92 р. // Відомості Верховної Ради України (ВВР). – 1992. – № 48. – Ст. 650.

10. Про забезпечення участі громадськості у формуванні та реалізації державної політики : Постанова Кабінету Міністрів України від 3.11.10 р. № 996 // Офіційний вісник України. – 2010. – № 84. – Ст. 2945.

11. Афонін Е.А. Громадська участь у творенні та здійсненні державної політики / Е.А. Афонін, Л.В. Гонюкова, Р.В. Войтович. – К. : Центр сприяння інституц. розвитку держ. служби, 2006. – 160 с.

12. Freedom in the World - 2018. Democracy in Crisis. – Режим доступу : https://freedom house.org/report/freedom-world/freedom-world-2018

13. Україна “пасе задніх” у світовому рейтингу процвітання. – Режим доступу : https://www.epravda.com.ua/news/2018/02/5/633749

14. Democracy Index 2017. – Режим доступу : https://www.eiu.com/topic/ democracy-index

15. Про Регламент Кабінету Міністрів України : Постанова Кабінету Міністрів України від 18.07.07 р. № 950 // Офіційний вісник України. – 2007. – № 54. – Ст. 2180.

16. Про прийняття до громадянства України Саакашвілі М. як особи, прийняття якої до громадянства України становить державний інтерес для України : Указ Президента України від 29.05.15 р. № 301/2015. – Режим доступу : http://www.president.gov.ua/documents/3012015-19079

17. Указ по Саакашвілі і таємниця Адміністрації Президента. – Режим доступу : https://www.pravda.com.ua/columns/2018/02/8/7170970

18. Про доступ до публічної інформації : Закон України від 13.01.11 р. // Відомості Верховної Ради України (ВВР). – 2011. – № 32. – Ст. 314.

19. Добродумов О.П. Правова безпека як складова національної безпеки. – (Національна безпека України : стан, кризові явища та шляхи їх подолання). – К. : Національна академія управління, Центр перспективних соціальних досліджень, 2005. – 400 с.

20. Общая теория государства и права : академический курс : в 3 т. – [3-е изд., перераб. и доп.]. – Т. 2. ; отв. ред. М.Н. Марченко. – М. : Норма, 2007. – 802 с.

21. Корж І. Політична корупція та правова безпека // Право України. – 2009. – № 6. – С. 55-60.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

УДК 342.951:351.82

ТАРАСЮК А.В., аспірант Національного університету
біоресурсів і природокористування України

ВПЛИВ ЗАГАЛЬНОГО РЕГУЛЮВАННЯ ЗАХИСТУ ДАНИХ НА КОНТРОЛЕРІВ ТА ПРОЦЕСОРІВ ПЕРСОНАЛЬНИХ ДАНИХ – РЕЗИДЕНТІВ УКРАЇНИ

Анотація. *Стаття присвячується правовим аспектам та проблемам застосування загального регулювання захисту даних до контролерів та процесорів персональних даних – резидентів України, в контексті обробки останніми персональних даних в рамках законодавства Європейського Союзу.*

Ключові слова: *захист персональних даних, інформаційні відносини, інформаційне право*

Summary. *The article is dedicated to the legal aspects and problems of application of the general adjusting of data protection to the inspectors and processors of the personal information – residents of Ukraine, in the context of the personal data handling carried out by them within the framework of legislation of European Union.*

Keywords: *personal data protection, informative relations, informative right.*

Аннотация. *Статья посвящается правовым аспектам и проблемам применения общей регуляции защиты данных к контролерам и процессорам персональных данных – резидентов Украины, в контексте обработки последними персональных данных в рамках законодательства Европейского Союза.*

Ключевые слова: *защита персональных данных, информационные отношения, информационное право.*

Постановка проблеми. В умовах поширення застосування технологій Великих даних, персональні дані фактично стають сировиною для володільців баз даних і забезпечують можливість прийняття компаніями рішень, в основі яких лежить прогноз можливої поведінки конкурентів в рамках конкретних ресурсів в мережі Інтернет. Межа між законною обробкою таких даних та втручанням у приватне життя надзвичайно тонка.

Законодавства про захист персональних даних різняться в залежності від юрисдикції, але з прийняттям у 2016 році Європейським Парламентом і Радою Регламенту (ЄС) 2016/679 від 27.04.16 р. – “Загальне регулювання захисту даних” (General data protection regulation) (далі – GDPR) [1], вимоги до регулювання інформаційних відносин в сфері захисту персональних даних стають уніфікованими для всіх “контролерів” та “процесорів” персональних даних (далі – контролер та процесор відповідно), якщо вказані суб’єкти мають зв’язки з державами-членами Європейського Союзу.

Регламент GDPR вступає в силу в травні 2018 року і відповідне регулювання застосовуватиметься і до контролерів та процесорів – резидентів України. Оскільки зміни є значущими і положення вказаного Регламенту значно відрізняються від норм, які застосовувались до цього, а також від норм вітчизняного законодавства, що регулює умови обробки персональних даних, для українських контролерів та процесорів є проблемним розуміння нових правил та, відповідно, впровадження відповідних правових процедур у свою діяльність. Одним з завдань вітчизняної правової науки є вирішення питання можливості такої адаптації та розробки відповідної дорожньої карти для дотримання вказаними суб’єктами норм GDPR, що будуть застосовані до регулювання їх діяльності.

Результати аналізу наукових публікацій. Визначення та вирішення проблем правових основ у створенні нормативно-правової системи та механізмів захисту персональних даних в Україні, а також – загальної систематизації суспільних відносин в сфері інформаційного права було детально розглянута у роботах Брижко В.М., зокрема у [2; 3]. Значній вклад в удосконалення нормативно-правового регулювання інформаційних відносин в сфері захисту персональних даних було здійснено Барановим О.А., зокрема у [5; 6], Пилипчуком В.Г. [4; 5], Мельником К.С. [5; 7; 8] та іншими українськими вченими. Серед них можливо виділити праці таких, як Кохановська М.Ю. [9], Боєр В.М. та Павельева О.Г. [10], які займалися проблемами цивільно-правових відносин в інформаційній сфері. Іншими українськими вченими, зокрема, такими як Серьогін С.А., досліджувалась тематика – Великі дані, як загроза приватному життю [11].

Проте, питання практичного застосування нових приписів Європейського Союзу для сфери захисту персональних даних стосовно Регламенту GDPR залишаються дискусійними та знаходяться на початковому етапі пошуку шляхів їх вирішення.

Метою статті є визначення ключових правових вимог, які стосуються українських контролерів та процесорів в контексті Регламенту GDPR та створення базової дорожньої карти для адаптації відповідних суб’єктів під нові вимоги законодавства Європейського Союзу.

Виклад основного матеріалу. Регулювання питання законності обробки персональних даних варіюється в залежності від юрисдикцій. Основним законом, який регулює це питання на території України, є Закон України “Про захист персональних даних” [12]. Цей Закон регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних. В епоху інформатизації та великих даних, правовідносини виникають на перетині юрисдикцій і персональні дані певної особи, громадянина України, можуть оброблюватись компаніями з США або країн західної Європи в режимі реального часу і відповідно до законів цих країн.

Так само, компанії-резиденти України, надаючи послуги з використанням мережі Інтернет суб’єктам персональних даних з держав-члены Європейського Союзу, можуть оброблювати персональні дані таких осіб на умовах відповідної згоди від вказаних суб’єктів та імперативних норм відповідного правопорядку. Концептуальним є питання вибору вказаного правопорядку. Зазвичай, компанії, які оброблюють персональні дані та надають відповідні шаблони згод на обробку таких даних, визначають право країни, результатом якої вони є, як таке, що застосовується, у тому числі, до питання обробки персональних даних.

Мотивація вибору правопорядку проста – на веб-портал компанії можуть зайти фізичні особи з будь-якої точки світу і на стадії, поки такі особи не сповістили інформацію про себе шляхом заповнення відповідних форм, для компанії не є зрозумілим, резидентами якої країни є такі користувачі. Більш того, технічними засобами не завжди можливо встановити, на території якої країни перебуває фізична особа-користувач, який може не завжди вводити точні дані або не вводити їх взагалі. Таким чином, на сьогодні склалася практика, коли саме володільці персональних даних (контролери) визначають умови згоди на обробку персональних даних, а користувачі погоджуються з такими умовами, або не використовують певний сервіс взагалі. Одним з ключових аспектів в розрізі даної проблематики буде визначення місця надання конкретної послуги – його зазвичай визначає компанія, яка такі послуги надає, у

відповідній публічній оферті. При цьому, така дефініція має відбуватись з урахуванням імперативних норм держави, резидентом якої є компанія і від цього і залежить можливість вибору конкретного правопорядку і відповідних норм.

З іншого боку, деякі країни встановлюють спеціальні захисні норми, які мають бути враховані при обробці персональних даних громадян таких країн та націленості певної послуги саме на ринок відповідної країни. Як приклад, вимоги статті частини 5 статті 18 Закону Російської Федерації “Про персональні дані”, відповідно до положень якої, на оператора персональних даних, під час їх збирання, покладається вимога забезпечити запис, систематизацію, накопичення, зберігання, уточнення (оновлення, зміну), виїмку персональних даних громадян Російської Федерації з використанням баз даних, що знаходяться на території РФ [13]. В контексті застосування вказаних вимог до операторів персональних даних – вони будуть застосовуватись лише до суб’єктів, чиї веб-сайти, в рамках яких відбувається обробка персональних даних користувачів, направлені на територію РФ, та які не підпадають під виключення, що встановлені законом. Як ключові індикатори “направленості” визначаються – пропонування товарів та послуг російською мовою, можливість придбання та прямого отримання товару чи послуги на території РФ та можливість сплати в російських рублях [14].

Таким чином, деякі країни, прагнучі додатково захистити персональні дані осіб, що перебувають на їх території та/або своїх громадян, встановлюють імперативні норми, які розповсюджуються і на іноземних суб’єктів, чия діяльність націлена на відповідний ринок.

Як вже зазначалося раніше, в квітні 2016 року було прийнято Регламент (ЄС) 2016/679 “Про захист фізичних осіб при обробці персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС” (GDPR) [1]. Регламент вступає в силу 24 травня 2018 року та визначає нові умови обробки персональних даних у Європейському Союзі.

Регламент GDPR має екстериторіальну дію, що означає, що його положення застосовуються не лише до компаній-резидентів ЄС, але і до контролерів та процесорів, які оброблюють персональні дані в Євросоюзі, навіть, якщо вони є резидентами інших країн, за умов, які прямо передбачені положеннями GDPR, зокрема, якщо обробка персональних даних пов’язана з пропонуванням товарів або послуг (навіть безкоштовно) суб’єктам персональних даних в ЄС або моніторингу поведінки таких суб’єктів. При цьому наявні окремі спеціальні вимоги як до контролерів, так і до процесорів [1]. Таким чином, компанії-резиденти України підпадатимуть під регулювання GDPR, перебуваючи у статусі контролера або процесора, як це визначено в самому GDPR за умов, що вказані вище.

В рамках GDPR значно розширене саме поняття “персональні дані” в контексті можливих ідентифікаторів та інформації, яка може бути віднесена до персональних даних, а суб’єкти персональних даних отримали більше реальних важелів впливу на контролерів та процесорів в контексті реалізації своїх прав, перелік яких також значно розширений. У зв’язку з цим виникає необхідність проаналізувати ключові нововведення GDPR в контексті моделювання їх застосування до контролерів та процесорів персональних даних – резидентів України.

В статті 4 GDPR визначені ключові поняття, зокрема: персональні дані означають будь-яку інформацію, що стосується ідентифікованої чи такої, що ідентифікується фізичної особи (“суб’єкта даних”), а фізичною особою, яка ідентифікується, визначається особа, яка може бути ідентифікована безпосередньо чи опосередковано, зокрема шляхом посилання на такий ідентифікатор, як ім’я, ідентифікаційний номер, дані про місцезнаходження, он-лайн – ідентифікатор або один чи більше факторів,

характерних для фізичної, фізіологічної, генетичної, психічної, економічної, культурної, або соціальної ідентичності цієї фізичної особи [1]. Поняття “контролер” та “процесор”, як вони визначені в GDPR можна за аналогією порівняти з поняттями “володілець персональних даних” та “розпорядник персональних даних”, як вони визначені в Законі України “Про захист персональних даних”. Зокрема, для “контролера” і “володільця персональних даних” ключовим є встановлення мети та засобів (способів) обробки персональних даних, а для “процесора” та “розпорядника персональних даних” ключовим є те, що вони є суб’єктами, яким надано право обробляти персональні дані від імені “процесора” та “володільця персональних даних” відповідно.

В рамках GDPR вводиться також багато нових термінів, які використовуються в регулюванні персональних даних. Одним з таких термінів, який, можливо, в майбутньому, буде доданий і до українського законодавства в сфері персональних даних є поняття “профілювання”.

Зокрема, профілювання означає будь-яку автоматичну обробку персональних даних, що полягає у використанні персональних даних для оцінки певних особистих аспектів, пов’язаних з фізичною особою, зокрема для аналізу та прогнозування аспектів, що стосуються результатів діяльності фізичної особи на роботі, економічної ситуації, здоров’я, особистих уподобань, інтересів, надійності, поведінки, місцезнаходження або переміщень [1].

При застосуванні технологій Великих Даних персональні дані певною мірою можна вважати матеріалом, який після автоматичної обробки перетворюється на інсайти – інформацію, що дозволяє автоматизоване прийняття рішень на основі первинної інформації. Це можуть бути пропозиції реклами певних товарів або послуг, в яких особа може бути зацікавлена виходячи з даних аналізу. Стаття 22 GDPR передбачає право суб’єкта персональних даних заборонити контролеру приймати щодо такого суб’єкта рішення, що засновані виключно на автоматичній обробці, включаючи профілювання, якщо такі рішення мають юридичні наслідки. Як можливий приклад такого автоматичного рішення – рішення фінансової установи про видачу чи не видачу кредиту особі в режимі он-лайн, виходячи з даних анкети, що була нею заповнена або інші види послуг, в рамках яких відбувається так званий “скоринг” або оцінка клієнта як потенційного контрагента за допомогою автоматичних систем. Ще одним прикладом може бути сфера онлайн – рекрутингу (підбору персоналу), в рамках якої можуть мати місце автоматичні рішення про можливість пропонування роботи чи відхилення кандидатури певного суб’єкта персональних даних.

В GDPR визначено ряд прав для суб’єкта персональних даних, зокрема: право на зрозумілу та доступну інформацію, право бути забутим, право на мобільність даних, право заборони використання автоматизованих рішень, заснованих на профілюванні щодо себе, право отримувати інформацію про порушення правил безпеки зберігання даних.

Одним з найбільш цікавих з правової точки зору є право суб’єкта персональних даних “бути забутим”, яке передбачене статтею 17 GDPR. Однією з підстав реалізації цього права суб’єктом персональних даних може бути відкликання ним згоди на обробку персональних даних.

Право на мобільність даних, що передбачене статтею 20 GDPR надає право суб’єкту персональних даних вимагати у контролера свої персональні дані, які були йому надані таким суб’єктом у зручному, структурованому та такому, що може бути зчитаний комп’ютером, вигляді.

Одним з важливих аспектів GDPR, який необхідно враховувати контролерам-резидентам України, є необхідність збереження підтвердження факту надання згоди від

суб’єкта персональних даних та можливості демонстрації факту такої згоди за запитом. В рамках GDPR згода повинна бути однозначною та бути виражена чіткою заявою або дією. Цікавим є те, що в рамках GDPR прямо заборонена можливість отримувати згоду шляхом представлення для користувача вже заповнених полів з відповідними пташечками. Стаття 7 GDPR встановлює особливі вимоги до згоди. Зокрема, у випадку, якщо згода надається разом з іншою інформацією або завіренням, сам бланк згоди має бути таким, що є вільно відділений від іншої частини документу. Також, відповідно до норм вищевказаної статті, суб’єкт персональних даних має бути повідомлений про своє право відкликати свою згоду у будь-який момент і це буде зробити легко [1].

Стаття 8 Закону України “Про захист персональних даних” [10] також передбачає право суб’єкта персональних даних відкликати свою згоду на обробку персональних даних. На практиці реалізація цього права ускладняються тим, що персональні дані особи могли бути передані іншим володільцям персональних даних в рамках досить широких та розмитих умов згоди, на яку погодився суб’єкт персональних даних, фактично не маючи іншого виходу, адже прийняття відповідних умов згоди було єдино можливим варіантом для отримання відповідної послуги таким суб’єктом. При цьому суб’єкт персональних даних може навіть не знати, кому були передані його персональні дані, адже в умовах згоди було сказано “іншим третім особам, на розсуд володільця персональних даних для реалізації цілей надання цієї згоди”. При цьому, самі цілі згоди часто прописуються максимально широко та в незрозумілому ключі і в результаті – відкликання своєї згоди для суб’єкта персональних даних стає максимально складним.

Прийняття GDPR покликане уникнути таких ситуацій для суб’єктів персональних даних з Євросоюзу, адже встановлює чіткі вимоги не лише до формату згоди, а і до побудови процесів управління вже отриманими згодами. Зокрема, ICO (Information Commissioner’s Office), в своїх рекомендаціях щодо управління згодами, що будуть отримані в рамках GDPR, зазначає наступне (невиключний перелік):

- запит на отримання згоди варто робити виразним, стислим, відокремленим від інших умов і простим для розуміння;
- варто включити назву організації та будь-яких контролерів-третіх сторін, які будуть спиратися на згоду, пояснити, навіщо потрібна інформація, які дії будуть проводитись з інформацію, і наявність у суб’єкта персональних даних права на відкликання згоди;
- згода має бути надана в активній формі (без авто-заповнених полів анкет чи за замовчуванням);
- за можливості варто надавати можливість детального вибору умов згоди для різних цілей різних видів обробки;
- варто зберігати підтвердження факту надання згоди – суб’єкт, який надав згоду, час надання, спосіб та що було повідомлено суб’єкту перед наданням такої згоди;
- варто робити простою можливість відкликати надану згоду та розглянути можливість використання інструменту вибору преференцій;
- варто тримати отримані згоди під контролем та оновлювати їх у випадку змін, а також зробити це частиною власних бізнес-процесів [15].

Таким чином, згоди стають певним матеріально вираженим об’єктом, що в більшості випадків буде існувати в електронному режимі. Кожна відповідна згода, як об’єкт, буде свідчити про факт надання права певному контролеру використовувати персональні дані на умовах, що визначені в такій згоді. Управління масивом таких згод є

завданням контролера, який оброблює відповідні персональні дані і, відповідно, є відповідальним за додержання всіх принципів обробки таких даних, як це визначено в статті 5 GDPR.

Ключовим для українських контролерів в рамках GDPR є умови трансферу персональних даних суб’єктів з Євросоюзу в інші країни. Такий трансфер можливий на умовах, що визначені в GDPR, і однією з відповідних підстав є явна згода суб’єкта персональних даних на запропонований трансфер після того, як він був поінформований про відповідні ризики та відсутність умов, що визначені в статті 49 GDPR. Таким чином, для передачі персональних даних в Україну, суб’єкт персональних даних повинен буде прямо погодитись на такий трансфер і відповідна компанія має зберігати таку його згоду.

GDPR визначає як загальні правила, що застосовуються до будь-якої обробки персональних даних, так і спеціальні правила, що застосовуються до обробки спеціальних категорій персональних даних, таких як дані про стан здоров’я, що відбуваються в контексті наукових досліджень, включаючи клінічні та трансляційні дослідження [16]. В GDPR мають місце розділи, присвячені особливим категоріям персональних даних, щодо обробки яких встановлюються додаткові вимоги.

Ще одним важливим нюансом для контролерів та процесорів – резидентів України, які підпадають під регулювання GDPR (згідно частини 2 статті 3 GDPR) буде необхідність призначення представника на території Європейського Союзу, як це визначено в п. 27 GDPR.

Стаття 28 визначає основні вимоги до процесорів, під які підпадають і компанії процесори – резиденти України, якщо персональні дані, які вони оброблюють від імені контролера, були отримані з Європейського Союзу.

Діяльність процесорів у тому числі визначається відповідним договором з контролером. В обов’язках процесора має бути зазначено тривалість, природу та мету обробки, типи даних, що оброблюються та права і обов’язки контролера [17].

Таким чином, компанії-резиденти України мають бути готові до нових реалій захисту персональних даних згідно нових приписів законодавства Європейського Союзу.

Висновки.

Українським компаніям, що орієнтуються на ринок держав-членів Європейського Союзу, необхідно проаналізувати, чи підпадають вони під регулювання положень Регламенту GDPR і якщо так – прийняти міри для дотримання відповідних вимог.

Ключовими індикаторами для визначення, чи підпадає організація під таке регулювання, є наступні:

а) контролер чи процесор засновані в державах-членах Європейського Союзу;

б) факт пропонування товарів чи послуг на ринок Європейського Союзу або моніторинг за поведінки суб’єктів персональних даних в Європейському Союзі на умовах, визначених в Регламенті GDPR.

Враховуючи неймовірну новизну багатьох положень та концепцій GDPR порівняно з регулюванням захисту персональних даних українським законодавством, компаніям-резидентам України, діяльність яких підпадає під регулювання GDPR необхідно якомога раніше починати підготовку до адаптування своїх бізнес-процесів під нові вимоги а також розпочинати розробку відповідних політик, форматів згод на обробку персональних даних та інших документів.

Основною особливістю для українських компаній в рамках виконання умов GDPR є також необхідність;

а) призначення свого представника для комунікації з відповідними уповноваженими органами Європейського Союзу;

б) наявність явної та недвозначної згоди від суб’єкта персональних даних на передачу своїх персональних даних на територію України, якщо такими є плановані бізнес-процеси.

Питання впливу GDPR на контролерів та процесорів резидентів України є новим та малодослідженим. Наступні наукові дослідження у цьому напрямку зможуть допомогти у розробці певної дорожньої карти, яка зможе зробити процес адаптації вказаних компаній до нових вимог європейського законодавства з захисту персональних даних зрозумілим та однозначним.

Використана література

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). – Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from= EN

2. Брижко В.М. Організаційно-правові питання захисту персональних даних : дис. на здобуття наук. ступеня. канд. юрид. наук : спец. 12.00.07 – теорія управління ; адміністративне право і процес ; фінансове право ; інформаційне право / В.М. Брижко. – (НДЦПІ АПрН України, НАДПС України). – К.- Ірпінь, 2004, – 251 с.

3. Брижко В.М. Основи систематизації інформаційного законодавства : теоретичні та правові засади : монографія / В.М. Брижко. – К. : ТОВ “ПанТот”, 2012 р. – 304 с.

4. Pylypchuk, Volodymyr; Bryzhko, Valery, 2016. PRIVACY AND HUMAN SECURITY IN THE PROTECTION OF PERSONAL DATA (Приватність та безпека людини у сфері захисту персональних даних) // Social and Human Sciences. Polish-Ukrainian scientific journal, 04 (12). – Available at : http://sp-sciences.io.ua/s2596466/pylypchuk_volodymyr_bryzhko_valery_2016_privacy_and_human_security_in_the_protection_of_personal_data_social_and_human_sciences._polish-ukrainian_scientific_journal_04_12_ (accessed 08 January 2017).

5. Становлення і розвиток правових основ та системи захисту персональних даних в Україні : монографія / [В.Г. Пилипчук, В.М. Брижко, О.А. Баранов, К.С. Мельник] ; за ред. В.М. Брижка, В.Г. Пилипчука. – К. : ТОВ “Видавничий дім “АртЕк”, 2017. – 226 с.

6. Баранов О.А. Напрями перспективних досліджень у галузі інформаційного права // Інформація і право. – 2(17)/2016. – Режим доступу : http://ippi.org.ua/baranov-oa-napryami-perspektivnikh-doslidzhen-u-galuzi-informatsiinogo-prava-stor-15-31

7. Мельник К.С. Іноземний та вітчизняний досвід становлення інституту захисту персональних даних // Інформаційна безпека людини, суспільства, держави. – 2013. – № 2. – С. 97-103. – Режим доступу : http://nbuv.gov.ua/UJRN/iblsd_2013_2_18

8. Мельник К.С. Правові та організаційні основи захисту персональних даних в Європейському Союзі та в Україні : дис. на здобуття наук. ступеня. канд. юрид. наук : спец. 12.00.07 – теорія управління ; адміністративне право і процес ; фінансове право ; інформаційне право / К.С. Мельник. – (НДЦПІ АПрН України). – К., 2015, – 269 с.

9. Кохановська О.В. Інформація як об’єкт правовідносин. – Режим доступу : http://papers.univ.kiev.ua/1/jurydychni_nauky/articles/kokhanovska-o-information-as-an-object-of-legal-relations_18016.pdf

10. Боер В.М. Информационное право / В.М. Боер, О.Г. Павельева. – Ч. 1. – СПб. : ГУАП, 2006. – 116 с.

11. Серёгин В.А. BIG DATA : новая угроза для прайвеси в условиях информационного общества // Науковий вісник Ужгородського національного університету. – (Серія Право). – 2015. – № 35. – Ч. 1. – Т. 1. – С. 93-97.

12. Про захист персональних даних : Закон України від 01.06.10 р. № 2297-VI. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2297-17

13. О персональных данных : Закон Російської Федерації від 27.07.06 г. № 152-ФЗ : ред. от 29.07.17 г. – Режим доступу : http://www.consultant.ru/document/cons_doc_LAW_61801

14. О обработке и сохранении персональных данных : разъяснение Минкомсвязи России от 01.09.15 г. – Режим доступу : http://minsvyaz.ru/ru/personaldata

15. Рекомендації Информационного Комиссара (ICO). – Режим доступу : https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-bases-for-processing/co nsent

16. Gauthier Chassang,. The impact of the EU general data protection regulation on scientific research. – Режим доступу : http://ecancer.org/journal/11/full/709-the-impact-of-the-eu-general-data-protection-regulation-on-scientific-research.php

17. Debbie Heywood : Obligations on data processors under the GDPR. – Режим доступу : https://united-kingdom.taylorwessing.com/globaldatahub/article-obligations-on-data-processors-under-gdpr.html

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 341: 316.774: 070.13

ЗАБАРА І.М., *кандидат юридичних наук, доцент*,
кафедра міжнародного права Інституту міжнародних відносин
Київського національного університету імені Тараса Шевченка

ДИСТАНЦІЙНЕ ЗОНДУВАННЯ ЗЕМЛІ: МИНУЛЕ І СУЧАСНЕ МІЖНАРОДНО-ПРАВОВОГО РЕГУЛЮВАННЯ ОТРИМАННЯ І ВИКОРИСТАННЯ ІНФОРМАЦІЇ

***Анотація**. У статті досліджуються питання міжнародно-правового регулювання діяльності з дистанційного зондування Землі з космосу. Автор акцентує увагу на інформаційній складовій міжнародно-правової проблематики діяльності суб'єктів з дистанційного зондування. У статті аналізуються проблемні питання базових засад міжнародно-правового режиму сучасних міжнародних інформаційних відносин в сфері використання інформації, що отримується в результаті діяльності з дистанційного зондування Землі з космосу.*

***Ключові слова**: дистанційне зондування, дані дистанційного зондування, інформація, міжнародно-правовий режим, міжнародно-правові відносини.*

***Summary.** The article deals with the issues of international legal regulation of the remote sensing of the Earth from outer space. The author focuses on the information component of the international legal issues of the activities of subjects of remote sensing. The article analyzes the problematic issues of the basic principles of the international legal regime of modern international information relations in the sphere of the use of information obtained as a result of remote sensing of the Earth from space.*

***Keywords:** remote sensing, remote sensing data, information, international legal regime, international legal relations.*

***Аннотация**. В статье исследуются вопросы международно-правового регулирования деятельности по дистанционному зондированию Земли из космоса. Автор акцентирует внимание на информационной составляющей международно-правовой проблематики деятельности субъектов по дистанционному зондированию. В статье рассматриваются проблемные вопросы базовых основ международно-правового режима современных международных отношений в сфере использования информации, получаемой в результате деятельности по дистанционному зондированию Земли из космоса.*

***Ключевые слова:** дистанционное зондирование, данные дистанционного зондирования, информация, международно-правовой режим, международно-правовые отношения.*

Постановка проблеми. Широкий і масштабний розвиток інформаційно-комунікаційних технологій у поєднанні з сучасною космічною технікою надають широкі можливості для подальшої діяльності у сфері дистанційного зондування Землі з космосу. Разом з новими напрямами їх практичного використання, а також тенденціями щодо комерціалізації цієї діяльності та участі приватних осіб, вони висувають до міжнародного співтовариства нові вимоги, завдання і пріоритети. Важливим також є визначення і узагальнення базових засад міжнародно-правового режиму сучасних міжнародних інформаційних відносин в сфері використання інформації, отриманої в результаті дистанційного зондування Землі з космосу.

Варто було б і приділити увага розбіжностям у концептуальних підходах держав як принципових питань, пов'язаних як з категорією інформації, так і до правових режимів, що встановлюються на міжнародному і національному рівнях для діяльності з дистанційного зондування Землі, відмінності між якими, із її прогресивним розвитком, зростають.

Результати аналізу наукових публікацій свідчать про те, що коло проблемних питань, висвітлених у роботах А.А. Абдураімова, М. Адхикарі, Дж. Барбоса, В.Д. Бордунова, В.С Верещетіна, Р. Вільямсона, І. Габриновича, Б. Едельмана, Ф. Дунка, Г.П. Жукова, А. Іто, С. Краффта, Ю.М. Колосова, А.С. Конюхової, А. Кеннета, В. Леістера, В.Н. Маркова, В. Манна, О. Огунбанво, Р.Е. Пасєчніка, В.М. Постишева, Б. Сайфулає, Р. Сзафарса, П. Томпсона, М. Ферраззані, Ф. Фйоріо, Ч. Хенлі, Н.С. Хосенболла, С. Христола, Б. Шмідт-Теда та багатьох інших вчених, є доволі широким. Серед розглянутих авторами – питання міжнародно-правового режиму діяльності з дистанційного зондування Землі, дотримання принципів і норм міжнародного права і суверенних прав держав при здійсненні цієї діяльності, історичних, економічних, інформаційних аспектів формування міжнародно-правових позицій держав, її комерціалізації. Разом з тим, враховуючи різноманітність розглянутої авторами тематики, вартими окремого розгляду є і питання щодо сучасних підходів до інформаційних аспектів регулювання, зокрема на тлі достатньо широкого кола наукових робіт щодо “космічного сегменту” діяльності з дистанційного зондування та методів дистанційного зондування.

Метою статті є визначення і узагальнення базових засад міжнародно-правового режиму сучасних інформаційних відносин в сфері використання інформації, отриманої в результаті дистанційного зондування Землі з космосу.

Виклад основного матеріалу. В рамках дистанційного зондування поверхні Землі з космосу (далі – ДЗЗ) свою діяльність ведуть понад два десятки держав. Методи дистанційного зондування використовуються ними у геології, землекористуванні, гідрології, океанології, метеорології, лісовому і сільському господарствах, картографуванні та у інших сферах діяльності.

Діяльність з ДЗЗ стала предметом теоретичних та науково-практичних досліджень в багатьох науках. Разом з тим, використання даних отриманих шляхом ДЗЗ, дало поштовх у розвитку багатьох наук.

Низка держав запровадила програми супутникових спостережень, у яких беруть участь понад двадцять п’ять держав. Свої програми здійснюють і окремі міжнародні організації.

У зв’язку з широким спектром можливостей використання, ще на початковому періоді діяльності держав з дистанційного зондування Землі з космосу, виникали питання щодо її належного міжнародно-правового регулювання, вирішення яких не тільки сприяло б широкому співробітництву між державами, але виключало б можливість використання отриманих даних та інформації про природні ресурси іноземних держав на шкоду суверенним правам цих держав, їх економічним і оборонним інтересам [1].

Комітет ООН з використання космічного простору у мирних цілях, до компетенції якого були віднесені ці питання, вперше розпочав роботи з проблематики дистанційного зондування Землі у 1969 р. Тільки після п’ятнадцятирічної тривалої, складної і клопіткої роботи у 1986 р. було завершено роботу і погоджено шляхом консенсусу між державами “Принципи, що стосуються дистанційного зондування Землі з космічного простору” (далі – Принципи ДЗЗ 1986 р.). Потім, теж шляхом консенсусу, їх було схвалено самим Комітетом ООН з космосу і врешті, 3 грудня 1986 р. – Генеральною Асамблеєю ООН (Резолюція 41/65) [2].

Прийнятий ГА ООН акт включає п’ятнадцять принципів, які відображають доволі складний шлях і крихкий компроміс, що підкреслюється позиціями тринадцяти держав, які зробили застереження або заяви про власне тлумачення окремих положень.

Важливим стало те, що сторони погодились здійснювати свою діяльність з дистанційного зондування Землі згідно з міжнародним правом (Принцип III) [2].

Принципи ДЗЗ 1986 р. визначили основні міжнародно-правові засади діяльності з ДЗЗ, і стали основою для багатьох подальших наукових розробок, що були зосереджені на проблемних міжнародно-правових питаннях, переважно пов’язаних із космічною тематикою, міжнародно-правовим режимом діяльності з дистанційного зондування Землі і, у цьому контексті – використанням отриманих даних і інформації. Отже, для подальшого розгляду базових засад міжнародно-правового режиму сучасних міжнародних інформаційних відносин в сфері використання інформації, отриманої в результаті дистанційного зондування Землі з космосу вартим, на нашу думку, є стисле узагальнення їх положень.

Важливим є те, що Принципи ДЗЗ 1986 р., для характеристики правовідносин, визначили поняття “дистанційне зондування” та “діяльність з дистанційного зондування”. Так, “дистанційне зондування” означає зондування поверхні Землі з космосу з використанням властивостей електромагнітних хвиль, які випромінюються, відбиваються або розсіюються зондованими об’єктами, з метою кращого розпорядження природними ресурсами, вдосконалення землекористування та охорони навколишнього середовища (Принцип I). З визначення випливає, що сфера дії Принципів охоплює діяльність, що здійснюється певними засобами, з певною метою і спрямовується тільки на мирні цілі їх використання. Ця діяльність не охоплює спостереження з космосу, що провадяться з військовими (розвідувальними, моніторинговими, контрольними) цілями.

“Діяльність з дистанційного зондування” означає експлуатацію космічних систем дистанційного зондування, станцій по прийманню і накопиченню первісних даних і діяльність щодо опрацювання, інтерпретації та розповсюдження опрацьованих даних. (Принцип I). Цим положенням принципово розподілена діяльність, що здійснюється як безпосередньо у космосі, так і безпосередньо наземними станціями. Це надає можливість не тільки визначати і розмежувати поняття “первісні дані”, “опрацьовані дані”, “проаналізована інформація”, але й зменшити розбіжності у поглядах між різними групами держав на порядок отримання і поширення даних зондування.

Принципи ДЗЗ 1986 р особливо підкреслюють характер діяльності держав з дистанційного зондування Землі, зазначаючи, що вона:

- здійснюється “заради добробуту і в інтересах усіх країн, незалежно від рівня їх економічного, соціального чи науково-технічного розвитку та з особливим врахуванням потреб країн, що розвиваються” (Принцип II);
- сприяє міжнародному співробітництву шляхом співучасті у діяльності інших держав, на справедливих і взаємовигідних умовах (Принципи V, VI, VII, XII, XIII);
- здійснюється “на основі поваги до принципу повного і постійного суверенітету всіх держав і народів над своїми багатствами і природними ресурсами з належним врахуванням прав та інтересів інших держав і організацій” (Принцип IV);
- здійснюється за сприяння ООН і відповідних установ системи ООН (Принцип VIII);
- здійснюється за умов інформування ООН та інших держав і разі проведення програми дистанційного зондування (Принцип IX);
- має сприяти охороні природного середовища Землі, а також захисту людства від стихійного лиха (Принципи X, XI).

У зв’язку із появою та масштабним використанням інформаційно-комунікаційних технологій, розвитком інформаційного суспільства, і як наслідок, підвищенням уваги до категорії інформації і інформаційної діяльності, набуває нового бачення, наповнення і

розуміння проблематика з дистанційного зондування Землі. Зокрема, в рамках міжнародно-правового регулювання інформаційної діяльності, пов’язаної із забезпеченням її передачі, можна виокремити наступні проблемні питання:

- визначення і класифікації інформації з ДЗЗ;
- поширення даних і інформації з ДЗЗ;
- розширення цілей і сфер використання ДЗЗ та видів інформації;
- розширення проблематики відповідальності суб’єктів за ДЗЗ.

Отже, варто надати стислий аналіз зазначеним проблемним питанням.

1. Визначення і класифікації інформації з ДЗЗ.

Питання визначення і класифікації інформації, отриманої в результаті діяльності з дистанційного зондування Землі з космосу виступило одним із важливих і принципових.

У рамках діяльності Комітету ООН з використання космічного простору у мирних цілях (далі – Комітет ООН з космосу), до компетенції якого були віднесені питання діяльності з ДЗЗ, було запропоновано дві концепції класифікації інформації. Зокрема, концепція поділу інформації ДЗЗ на певні категорії у залежності від ступеню їх просторової роздільності. Пропонувалось дані високої якості роздільності поширювати тільки за згодою держави, територія якої зондується. Інші дані надавались би у вільне користування. Положення цієї концепції знайшли втілення у *Конвенції про передачу і використання даних дистанційного зондування Землі з космосу 1978 р*. [3] (прийнята і ратифікована десятьма державами; набула чинності 21 серпня 1979 р., термін дії – 5 років; *de jure* не була відмінена, *de facto* вона припинила діяти) [4, с. 86].

Іншою була концепція поділу інформації ДЗЗ у залежності від факту її надання державі, територія якої зондується. Факт надання визначав правомірність подальшого поширення інформації ДЗЗ у міждержавних відносинах. Положення цієї концепції були сполучені із вимогами держав, що розвиваються, про надання їм пільг у доступі до супутникової інформації.

У результаті погоджень, як компроміс, враховуючи, що діяльність з ДЗЗ була фактично розмежована на космічну і наземну, було запропоновано використання наступних термінів: “первісні дані”, “опрацьовані дані” і “проаналізована інформація”.

У якості “первісних даних” ДЗЗ розглядалась одна з категорій інформації, яку отримують за допомогою супутників, космічних апаратів. До цієї категорії пропонувалось віднести дані, що безпосередньо отримані за допомогою спеціальних засобів космічних апаратів і які є основою для отримання у подальшому опрацьованих даних та проаналізованої інформації.

Принципи ДЗЗ 1986 р. визначили – термін “первісні дані” означає неопрацьовані дані, які одержують за допомогою апаратури дистанційного зондування, встановленої на борту космічного об’єкта, які передаються або доставляються на Землю з космосу через телеметрію і у вигляді електромагнітних сигналів, фотоплівки, магнітної стрічки або будь-якими іншими способами (Принцип I).

Відмінністю їх правового режиму, визначеного Принципами ДЗЗ 1986 р. стало те, що “первісні дані” не були віднесені до тієї категорії супутникової інформації, що надається відповідним державам в найкоротші строки у разі стихійного лиха або загрози від стихійного лиха (Принцип XI). В якості необхідної інформації в цьому випадку були визначені такі категорії як “опрацьовані дані” та “проаналізована інформація”.

“Опрацьовані дані”, згідно з Принципами ДЗЗ 1986 р., визначені як матеріали, одержані в результаті такого опрацювання первісних даних, яке необхідне для забезпечення можливості користуватися цими даними (Принцип I).

У якості категорії “проаналізована інформація” розглядалась інформація, що є кінцевим результатом діяльності з дистанційного зондування Землі з космосу у поєднанні з іншими даними, повідомленнями і інформацією, що отримана з інших джерел (авіаційних та ін.). Для отримання проаналізованої інформації додатково використовуються дані та інформація з геології, біології, статистики та інших галузей науки, в залежності від мети зондування. Принципи ДЗЗ 1986 р. надають лаконічне визначення – термін “проаналізована інформація” означає інформацію, одержану в результаті інтерпретації опрацьованих даних, додатково введених даних і відомостей з інших джерел (Принцип I). Особливою умовою її надання є те, що “проаналізована інформація”, яка здатна запобігти будь-якому шкідливому для природного середовища Землі явищу, сповіщається відповідним державам (Принцип X).

Особливістю правового режиму категорій “опрацьовані дані” та “проаналізована інформація” є наступне:

а) “опрацьовані дані” та “проаналізована інформація” надаються державам які постраждали від стихійного лиха або зазнають загрози від стихійного лиха, що насувається, за можливістю в найкоротші строки (Принцип XI);

б) “опрацьовані дані” та “проаналізована інформація”, як результат діяльності з ДЗЗ, не можуть використовуватись на шкоду законним правам і інтересам держави, територія якої зондується (Принципи I та IV).

Враховуючи масштаби діяльності держав з дистанційного зондування Землі з космосу, технічні особливості систем зондування, варто зазначити, що прийняті низкою держав національні акти мають певні термінологічні особливості у характеристиці як визначення, так і класифікації інформації; відповідно визначається і правовий режим доступу і поширення для таких даних і інформації.

2. Поширення даних і інформації з ДЗЗ.

Доступ до даних і інформації з дистанційного зондування Землі був одним з найбільш гострих питань під час дискусій у Комітеті ООН з космосу. Зокрема, одними з важливих постали питання щодо міжнародно-правового регулювання отримання і передачі первісних і опрацьованих даних та проаналізованої інформації від (космічного) дистанційного зондування Землі, а також правових наслідків їх отримання і передачі.

Проблема полягала у тому, що існуючі концепції використання інформації з ДЗЗ визначались двома принциповими підходами до проблем отримання і поширення інформації у міждержавних відносинах. Прихильники першої концепції (США, Японія та ін.) наполягали на застосуванні до даних і інформації від ДЗЗ принципу вільного потоку інформації та виступали за вільну торгівлю супутниковою інформацією на світовому ринку. Прихильники другої концепції (Франція та ін.) виходили з тієї позиції, що держави мають суверенні права на інформацію, отриману за допомогою ДЗЗ з територій, що знаходяться під їх суверенітетом і, відповідно, можуть контролювати її використання. З часом була висловлена і компромісна позиція щодо дозвільного порядку поширення інформації ДЗЗ у міждержавних відносинах.

Разом з тим, окремими державами були запропоновані і здійснені практичні кроки – проекти угод. Перші проекти міжнародних угод, що були представлені Аргентиною (1970 р.), Бразилією (1973 р.), спільним аргентино-бразильським проектом (1974 р.), до якого приєднались інші члени Комітету ООН з космосу (Венесуела, Мексика, Чилі). Вони виходили з того, що держава, територія якої зондується, має суверенні права на супутникову інформацію, що стосується території, яка знаходиться під її юрисдикцією і може повністю розпоряджатись нею.

Пізніше, у проектах угод, представлених Мексикою (1981 р.) і Чилі (1984 р.), були запропоновані положення щодо надання державі, територія якої зондується, права на першочерговий доступ до відповідної інформації. Низка окремих держав (Еквадор та ін.) досить тривалий час вимагала безкоштовного доступу до супутникової інформації. Такі вимоги не враховували значних витрат держав, що здійснювали дистанційне зондування, на створення відповідної техніки, проведення робіт, отримання, обробку і інтерпретацію даних. Вони не були сприйняті членами Комітету ООН з космосу.

У той же час, у *Принципах, що стосуються дистанційного зондування Землі 1986 р*., прийнятих Резолюцією 41/65 ГА ООН, були визначені положення щодо доступу держави, територія якої зондується, до відповідних даних і інформації. Зокрема, у результаті компромісу, були зазначені положення щодо доступу держави, територія якої зондується, до “первісних даних” і “опрацьованих даних” з території, яка знаходиться під її юрисдикцією, на недискримінаційній основі і на розумних умовах оплати. До того ж було зазначено, що державі, територія якої зондується, надається також доступ до “проаналізованої інформації” на тій же основі і тих самих умовах, особливо беручи до уваги потреби та інтереси країн, що розвиваються (Принцип XII).

На нашу думку, головною серед інших, залишається проблема безконтрольного поширення даних і інформації ДЗЗ, яка може заподіяти шкоди економічним, військовим та іншим життєво важливим інтересам держав. Таке бачення випливає з позицій окремих держав, що закріпили у своєму національному законодавстві положення щодо вільного доступу користувачів до цифрових даних зондування. До цього варто додати, що нове бачення проблеми викликано і кількома чинниками, зокрема: а) масовими запусками супутників, що здійснюють зондування; б) фактичним розширенням початкової мети ДЗЗ (відповідно і кола задач, що вирішується сучасними технологіями ДЗЗ); в) використанням, крім зазначених у Принципах ДЗЗ 1986 р., ще і інших технологій збирання даних; г) можливістю подальшого поширення (передачі) даних і інформації третім особам (державам, міжнародним організаціям та ін.).

3. Розширення цілей і сфер використання ДЗЗ та видів інформації

Діяльність з дистанційного зондування, відповідно до положень Принципів ДЗЗ 1986 р., має здійснюватись у кількох визначених сферах. Зокрема, 1) розпорядження природними ресурсами, 2) вдосконалення землекористування, 3) охорона навколишнього середовища (Принципи I). Вона має сприяти: 4) охороні природного середовища Землі та 5) захисту людства від стихійного лиха (Принципи X та XI). Відповідно, тематика отриманих видів даних і інформації повинна бути зосереджена на зазначених сферах.

У той же час, держави, майже з самого початку своєї діяльності з дистанційного зондування, почали розширювати сферу її використання, ставлячи за мету отримання і інших даних та інформації, що відповідала б їх інтересам. Так, за допомогою дистанційного зондування були розширені теоретичні і практичні можливості метеорології, геодезії, геології, гідрології, океанології, землезнавства та інших напрямків. Це також дало поштовх у розвитку і наукових сфер (зокрема космічної метеорології, космічної геодезії, космічної гідрології, космічної океанології, космічного землезнавства та ін.). Отримання відповідних даних і інформації стало надавати більше можливостей державам для кращого розпорядження власними ресурсами та спостереження за різними природними процесами.

Разом з тим, була висловлена позиція щодо розширення діяльності з ДЗЗ на військову сферу, що власне практично здійснюється державами і окремими міжнародними організаціями, проте є несумісною з метою Принципів ДЗЗ 1986 р.

Водночас, на нашу думку, треба звернути увагу і на нові види інформації, що включаються сторонами до правовідносин. Зокрема, дані і інформація, що отримуються шляхом дистанційного зондування Землі, охоплюють низку сфер і, відповідно, можуть бути класифіковані за видами (метеорологічні дані і інформація, геологічні, геодезичні, гідрологічні та ін.). Разом з тим, у сучасній договірній практиці держав і міжнародних організацій спостерігається тенденція укладати міжнародні угоди з окремих видів інформації (екологічна, економічна, правова, освітня, наукова, науково-технічна тощо). Як правило, в угодах щодо таких видів інформації зазначається мета, об’єкт, порядок і умови використання, правовий режим.

Враховуючи розширення сфер дистанційного зондування і появу даних і інформації, які можуть бути використані користувачами інформації (державами, міжнародними організаціями, приватними особами), варто припустити, що подальша договірна практика з укладання міжнародних угод теж буде розширюватись і поширяться на нові дані і інформацію. Логічно припустити і те, що ці угоди щодо надання, обміну, поширення даних і інформації, отриманих шляхом дистанційного зондування Землі, міститимуть відповідні аналогічні умови щодо її використання.

При цьому, форми надання даних і інформації, на нашу думку, можуть бути різними і не обмежуватимуться тільки тими, що зазначені у Принципах ДЗЗ 1986 р.

4. Проблематика відповідальності суб’єктів за ДЗЗ

Проблематика відповідальності за діяльність з дистанційного зондування Землі традиційно розглядалась науковцями і практиками з позицій міжнародного космічного права.

Вважається, що вона, в основному, визначається Принципами ДЗЗ 1986 р. Проте, навіть у свій час, фахівці зауважували, що формулювання Принципу XIV, де йдеться про відповідальність держав за діяльність з ДЗЗ, навряд чи може вважатись задовільною [5].

Суть проблеми міжнародної відповідальності за діяльність з ДЗЗ полягає у тому, що зазначена діяльність представляє собою у функціональному відношенні єдине ціле та разом з тим, за місцем здійснення – вона поділяється на дві складові стадії: космічну і наземну.

Космічна (відповідно до Принципу I) – це “експлуатація космічних систем дистанційного зондування”) беззаперечно підпадає під дію принципів і норм міжнародного космічного права, яке встановлює пряму відповідальності держав за будь-яку діяльність, незалежно від того, ким така діяльність проводиться (*Принцип XIV; Договір про принципи діяльності держав по дослідженню і використанню космічного простору, включаючи Місяць та інші небесні тіла 1966 р., Конвенція про міжнародну відповідальність за збитки, заподіяні космічними об’єктами 1971 р.*).

Наземна (відповідно до Принципу I) – це діяльність “станцій по прийманню і накопиченню первісних даних і опрацювання, інтерпретації та розповсюдження опрацьованих даних”, що відповідно до Принципу XIV – під зазначене не підпадає, оскільки її “не торкається застосування норм міжнародного права про відповідальність держав у тому, що стосується діяльності з дистанційного зондування” і фактично, за таких умов, залишається невизначеною.

Варто констатувати, що Принципи ДЗЗ 1986 р. не визначають питання відповідальності за міжнародну інформаційну діяльність суб’єктів.

Разом з тим, ситуація на сьогодні, на нашу думку, дещо змінилась. Суб’єкти міжнародного права – держави і міжнародні організації – активно продовжують інформаційну діяльність і є учасниками численних міжнародних інформаційних

правовідносин, у тому числі з даними і інформацією, отриманою від діяльності з дистанційного зондування Землі з космосу.

У зв’язку з прийняттям ГА ООН нових міжнародних актів, зокрема – Статей про відповідальність держав 2001 р. та Статей про відповідальність міжнародних організацій 2011 р., що охопили загальну проблематику відповідальності цих суб’єктів у міжнародному праві, питання щодо відповідальності за протиправні діяння, у тому числі і в інформаційній сфері, набувають сенсу і виступають предметом окремого наукового дослідження.

Висновки.

Таким чином, розглянувши питання, пов’язані із визначення і узагальнення базових засад міжнародно-правового режиму сучасних інформаційних відносин в сфері використання інформації, отриманої в результаті дистанційного зондування Землі з космосу, варто зазначити наступне:

- проблематика діяльності з дистанційного зондування Землі з космосу набуває нового бачення, наповнення і розуміння у зв’язку із появою та масштабним використанням інформаційно-комунікаційних технологій, розвитком інформаційного суспільства і, як наслідок, підвищенням уваги до категорії інформації і інформаційної діяльності;
- у рамках міжнародно-правового регулювання інформаційної діяльності, пов’язаної із дистанційним зондуванням Землі з космосу, виокремлюються наступні проблемні питання, що підлягають подальшому науковому осмисленню і обґрунтуванню:

а) визначення і класифікація інформації, отриманої з дистанційного зондування;

б) поширення даних і інформації, отриманої з дистанційного зондування;

в) розширення цілей і сфер використання дистанційного зондування та видів інформації;

г) розширення проблематики відповідальності суб’єктів за діяльність з дистанційного зондування.

Використана література

1. Бордунов В.Д. Космос. Земля. Право. / В.Д. Бордунов, В.Н. Марков. – М. : Междунар. отношения, 1978. – 136 с.

2. Принципи, що стосуються дистанційного зондування Землі з космічного простору : Резолюція 41/65 Генеральної Асамблеї ООН від 3 грудня 1986 року. – Режим доступу : http://zakon0.rada.gov.ua./laws/show/995_596.

3. Про передачу та використання даних дистанційного зондування Землі з космосу : Конвенція ООН від 19 травня 1978 року. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/995_498

4. Словарь международного космического права / [Л.А. Афанасьева, В.С. Верещетин, С.В. Виноградов, Г.М. Даниленко и др.] ; под ред. В.С. Верещетин. – М. : Междунар. отношения, 1992. – 296 с.

5. Верещетин В.С., Постышев В.М. Международная ответственность государств за деятельность по дистанционному зондированию Земли из космического пространства // Сов. государство и право. – 1986. – № 5. – С. 103-108.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

Правова інформатика

УДК 007.51 (477)

ЖИЛЯЄВ І.Б., *доктор економічних наук, с.н.с.*
СЕМЕНЧЕНКО А.І., *доктор наук з державного управління, професор*
ФУРАШЕВ В.М., *кандидат технічних наук, доцент, с.н.с.*

ІНСТРУМЕНТИ ДЕРЖАВНОГО СТРАТЕГІЧНОГО УПРАВЛІННЯ: НАЦІОНАЛЬНА ПРОГРАМА ІНФОРМАТИЗАЦІЇ

Анотація. *У статті, на прикладі 20-ти річного досвіду реалізації Національної програми інформатизації, розглянуто основні проблеми, підходи, пріоритетні напрями удосконалення стратегічного управління сферою інформаційно-комунікаційних технологій, його організаційно-правового забезпечення, науково-обґрунтовані рекомендації органам публічної влади щодо адаптації організаційно-правових механізмів стратегічного програмування у цій сфері до сучасних реалій.*

Ключові слова: *національна програма інформатизації, стратегічне управління, організаційні та правові механізми, суб’єкти інформатизації, об’єкти інформатизації.*

Summary. *The article examines on the example of the 20 years of experience in implementing the National Program of Informatization, the main problems, approaches, priority directions of improvement of strategic management of the field of information and communication technologies, its organizational and legal support, scientifically substantiated recommendations to public authorities regarding the adaptation of organizational and legal mechanisms of strategic programming in this area to modern realities.*

Keywords: *national program of informatization, strategic management, organizational and legal mechanisms, subjects of informatization, objects of informatization.*

Аннотация. *В статье, на примере 20-ти годового опыта реализации Национальной программы информатизации, рассмотрены основные проблемы, подходы, приоритетные направления усовершенствования стратегического управления сферой информационно-коммуникационных технологий, его организационно-правового обеспечения, научно-обоснованные рекомендации органам публичной власти относительно адаптации организационно-правовых механизмов стратегического программирования в этой сфере к современным реалиям.*

Ключевые слова: *национальная программа информатизации, стратегическое управление, организационные и правовые механизмы, субъекты информатизации, объекты информатизации.*

Постановка проблеми. Особливостями сучасного суспільно-політичного та соціально-економічного розвитку є його значний динамізм, багатовекторність, невизначеність, глобальність та суперечливість, що значно ускладнює процеси управління цим розвитком. Традиційні підходи та методи публічного управління та адміністрування виявилися недостатньо спроможними ефективно розв’язувати значну кількість сучасних проблем, які стає дедалі важче прогнозувати. Однак, збільшення кількості, масштабів та рівня загроз та ризиків (див. [1]) для громадян, суспільства та держави актуалізує необхідність посилення впливу інститутів громадянського суспільства на формування та реалізацію публічної політики, яка легітимізується у відповідних стратегічних актах: зокрема, в Стратегії соціально-економічного розвитку Європейського Союзу на період до 2020 року “Європа 2020” [2], а також в національному законодавстві в таких стратегічних документах як Стратегія сталого

розвитку “Україна – 2020” [3], Стратегія реформування державного управління України на 2016 – 2020 роки [4], Програма діяльності Кабінету Міністрів України [5], Концепція розвитку цифрової економіки та суспільства України на 2018 – 2020 роки [6] тощо. Згідно зі статтею 2 Закону України “Про Національну програму інформатизації” Національна програма інформатизації (далі – НПІ) [7] визначає стратегію розв’язання проблеми забезпечення інформаційних потреб та інформаційної підтримки соціально-економічної, екологічної, науково-технічної, оборонної, національно-культурної та іншої діяльності у сферах загальнодержавного значення і тому обґрунтовано відноситься до стратегічних документів. Її механізм формування та виконання було запроваджено 20 років тому у вигляді Законів України “Про Концепцію національної програми інформатизації” [8] та “Про Національну програму інформатизації” [7], “Про завдання національної програми інформатизації на 1998 – 2000 роки” [9] і цілої низки підзаконних актів. Враховуючи багаторічний досвід реалізації НПІ, актуальною є проблема аналізу та оцінки її організаційно-правових механізмів публічного управління, визначення основних факторів впливу (позитивних та негативних) на НПІ та формування пропозицій щодо їх удосконалення.

Результати аналізу наукових публікацій. Проблемі інформатизації суспільства, окремих галузей економіки, культури, освіти тощо науковцями та фахівцями приділяється достатньо уваги [10 – 13], у тому числі й проблемам стратегічного управління в цій сфері [14]. В той же час, на сьогодні відсутня комплексна оцінка результатів виконання НПІ та перспектив її подальшого розвитку.

Метою статті є оцінка організаційно-правових механізмів стратегічного управління цифровою економікою та суспільством[1] на прикладі Національної програми інформатизації в контексті основних тенденцій світового розвитку, здійснення порівняльного аналізу з кращими міжнародними практиками в цій сфері, а також формування науково-обґрунтованих пропозицій органам влади щодо удосконалення цих механізмів.

Виклад основного матеріалу. Відставання в сфері інформатизації загрожує перетворенню країни на сировинний придаток розвинутих країн. Світовий досвід показує, що більшість країн, як правило, мають окремі національні програми інформатизації з урахуванням місцевих особливостей та умов [15]. Але при цьому необхідно мати на увазі, що некоректна програма або її недостатній динамізм та мобільність можуть бути джерелом загроз та ризиків для громадян, суспільства та держави.

В залежності від ступеня досяжності кінцевих та проміжних цілей в інформатизації фахівці виокремлюють три етапи її розвитку:

- створення політичних, організаційних, законодавчих, соціальних, економічних та технічних умов формування та початкового задоволення інформаційних потреб громадян, суспільства та держави;
- розвиток інформаційної інфраструктури та забезпечення умов для її включення у світову;
- повне та якісне забезпечення інформаційних потреб громадян, суспільства, держави та бізнесу [16].

В Україні перший етап реалізації інформатизації формально розпочався у 1993 – 1994 роках, коли Кібернетичним центром НАНУ було розроблено проект НПІ, якій у 1995 р. було передано для подальшого опрацювання до Національного агентства з питань інформатизації при Президентові України – першого центрального органу

[1] З 2014 року ЄС широко використовує назву “Digital Economy and Society”.

виконавчої влади, визначеного відповідальним за інформатизацію в Україні. Йому передувала у 1989 – 1990 роках в Радянському Союзі розробка та прийняття Концепції розвитку інформатизації [17]. Отриманий досвід програмного управління НПІ був врахований при розробці Закону України “Про державні цільові програми”, прийнятому 2004 році. Формальним підтвердженням актуальності проблеми є наявність в базі даних “Законодавство України” 2949 документів з словом “інформатизація” з загальної їх кількості 224637, а також те, на що на початок 2017 р. на розгляді лише в профільному Комітеті Верховної Ради України з питань інформатизації та зв’язку знаходилось 128 законопроектів [18].

До її особливостей слід віднести довготривалість, масштабність, комплексність, системність поставлених цілей та завдань, гнучкість, прозорість та значною мірою демократичність її процедур. Окрім того, передбачалось підвищити рівень ефективного використання обмежених ресурсів, вводячи такий інструмент публічного управління, як НПІ, спрямована на подолання т.з. “провалів ринку” (фіаско ринку – англ. market failures). В свій час НПІ була однією з перших в світі програм такого типу у цій сфері.

За цей час отримано як значний міжнародний досвід в стратегічному управлінні електронним (цифровим) розвитком, так і національний (зокрема – в реалізації самої НПІ), якій доцільно проаналізувати з точки зору організаційно-правових механізмів стратегічного управління та врахувати його в інтересах її удосконалення.

Так, наприклад, в США була розроблена та впроваджена перша серед західних країн національна програма інформатизації, основним змістом якої було створення Національної інформаційної інфраструктури та в подальшому цифрової економіки. У 1995 – 1996 роках були прийняті закони “Про зниження паперового документообігу” та “Про реформу використання інформаційних технологій”, створення в рамках Адміністративно-бюджетного управління Управління з питань інформації та регулювання для безпосереднього впровадження політики керівництва всьома процесами збору, обробки, захисту та розповсюдження інформації, а також питань щодо закупівлі та використання інформаційних технологій. Уніфікація політики та практики дозволили американському Уряду реалізувати такі масштабні та складні проекти як створення федеральної інфраструктури публічних ключів та системи авторизації доступу, загальнодержавної системи федеральних форм, системи пошуку документів по усіх державних установах, федеральна система державних закупівель тощо [19].

У 2000 році Європейська Комісія прийняла програму “Електронна Європа”, основними завданнями якої були**:**

- створення інформаційно-комунікаційної інфраструктури і рівний доступ до неї усіх надавачів послуг;
- чітке законодавче оформлення таких сфер як мультимедійні комунікації та електронна комерція;
- принципове нове, високоякісне наповнення нових інтерактивних послуг та ефективний електронний уряд;
- кваліфіковані кадри;
- глобальне покриття мережами усієї території ЄС тощо [20].

Поряд з Європейськими програмами в цей час були розроблені та реалізовані національні програми інформатизації окремих країн: Великої Британії, Франції, тощо, а також в колишніх республіках СРСР, наприклад, в Республіках Білорусь, Казахстан, Молдова та Узбекистан [21; 22].

Таким чином НПІ повністю відповідала сучасним світовим трендам розвитку інформаційно-комунікаційних технологій (далі – ІКТ) та загальним підходам до управління сферою інформатизації.

Стратегія реформування державного управління України одним з своїх головних напрямів визначає: формування і координацію державної політики (стратегічне планування державної політики, якість нормативно-правової бази та державної політики в цілому, включаючи вимоги щодо формування політики на основі ґрунтовного аналізу та участь громадськості), акцентуючи увагу на таких проблемах стратегічних засад реформування державного управління та формування і координації державної політики як:

- відсутність потужного політичного лідерства та недостатній рівень координації реформування державного управління на політичному рівні;
- недостатня спроможність органів державної влади щодо проведення комплексного реформування державного управління;
- недостатня спроможність Кабінету Міністрів України до стратегічного планування;
- недостатній рівень якості державної політики у різних сферах, законодавчої та нормативної бази;
- відсутність системи середньострокового бюджетного планування, пов’язаного із стратегічним плануванням політики [4].

Зазначені проблеми повною мірою стосуються сфери інформатизації, розвитку ІКТ та інформаційного (цифрового) суспільства в цілому.

В документі серед основних завдань пріоритетного напряму “Стратегічне планування, формування і координація політики” також зазначається необхідність удосконалення системи стратегічного планування, проведення його моніторингу та оцінки, включаючи засади оцінювання результативності діяльності міністерств та інших державних органів. Так система стратегічного планування, моніторингу та аналізу передбачає наявність системи взаємопов’язаних і взаємоузгоджених програмних і стратегічних документів державної політики. Чинні процедури підготовки програмних і стратегічних документів державної політики, передбачені в нормативно-правових актах, потребують перегляду та систематизації. Необхідно визначити чіткі, єдині вимоги і методологію підготовки програмних і стратегічних документів державної політики (аналіз стану справ, визначення проблем, що потребують розв’язання, підготовка альтернативних варіантів розв’язання проблем, оцінки впливу, визначення критеріїв ефективності, консультації із громадськістю та заінтересованими сторонами, визначення строків звітування, процедура оновлення).

З точки зору кількості та якості отриманих за 20 років позитивних результатів НПІ не можна вважати успішною. Так, майже не були досягнуті її цілі, що були визначені як в її концептуальній частині, так і в переліках завдань. Деякі з її складових, а саме програми та проекти інформатизації органів місцевого самоврядування так і не були впроваджені, більша кількість проектів та завдань з інформатизації виконувались поза межами НПІ, вона не стала обов’язковою і для більшості регіонів України, втрачена актуальність її Концепції та деяких процедур, а найголовніше – довіра до неї як з боку органів влади, так і з боку громадян та бізнесу, насамперед щодо її ефективності та результативності.

Протягом останніх років визначились негативні тенденції в механізмах формування та реалізації НПІ:

зменшення її координуючого впливу на процеси інформатизації і, як наслідок, зменшення її організаційного, кадрового та фінансового забезпечення, всупереч

зростаючій динаміці впровадження ІКТ в усі сфери життєдіяльності суспільства, людини та держави;

зменшення ролі впливу громадськості, бізнесу та науки на формування та виконання НПІ (виключення Науково-технічної ради НПІ з числа суб’єктів управління, фактична ліквідація Консультативної ради з питань інформатизації при Верховній Раді України, скасування такого інструменту публічного управління, як щорічні звіти Уряду перед Парламентом та громадськістю про стан розвитку інформаційного суспільства та інформатизації), що суперечить політиці демократизації влади та суспільства;

хронічне незастосування програм та проектів інформатизації органів місцевого самоврядування та обмежена кількість діючих регіональних програм інформатизації.

Тому актуалізується альтернатива: або закриття НПІ і заміна її новим інструментом або її модернізація з урахуванням світових тенденцій та особливостей розвитку України. Концепцією розвитку електронного урядування [23] в рамках пріоритетного напряму “Підвищення ефективності управління розвитком електронного урядування” було обрано другий шлях, а саме визначено завдання “модернізація і забезпечення виконання Національної програми інформатизації та регіональних програм інформатизації”. Таким чином у 2017 році Уряд визначився з подальшим майбутнім цієї НПІ і розробив проект Закону України “Про внесення змін до Закону України “Про Національну програму інформатизації” [24].

Серед основних недоліків існуючої НПІ фахівці також відзначають такі:

обмеженість в основному розвитком інфраструктурної складової органів публічної влади та проведенням нечисельних з обмеженим значенням НДДКР;

негнучність, надмірна забюрократизованість та неузгодженість з іншими механізмами публічного управління та адміністрування;

незабезпеченність необхідним статусом та повноваженнями Генерального державного замовника НПІ;

неорієнтованість на споживачів публічних послуг;

значна затримка затвердження переліку щорічних завдань (проектів) у часі;

певна “відстороненість” від нових світових трендів: не враховує особливості розвитку цифрової економіки, електронного та Відкритого уряду, електронної демократії, електронної комерції інших сучасних ІКТ, а також механізмів державно-приватного та державно-громадського партнерства;

неузгодженість з сучасними політичними процесами децентралізації, деконцентрації, дерегуляції, демократизації влади;

фактична відсутність необхідного наукового, інформаційно-аналітичного, організаційного та фінансового забезпечення, останнє робить НПІ декларативною;

моральна застарілість, у тому числі, категорійно-понятійного апарату;

низька імплементація правових норм НПІ [13].

При прийнятті Урядом рішення щодо майбутнього оновлення законодавчого забезпечення НПІ було враховано такі її позитивні якості:

20-річний досвід застосування та необмеженість у часі;

достатньо конкретний, детальний, прозорий та відкритий механізм формування та виконання НПІ, який передбачає участь громадськості, експертів та бізнесу у формуванні публічної політики у сфері інформатизації та її реалізації;

законодавчо продуману організаційну структуру управління НПІ, що включає: Генерального державного замовника, який підпорядкований безпосередньо голові Уряду, державних замовників завдань (проектів), Керівника НПІ та керівників галузевих (регіональних) програм (проектів) інформатизації;

створено мережу підрозділів в органах влади, що відповідають за інформатизацію;

визначено основні об’єкти НПІ та відповідні механізми управління ними: сукупність державних програм з інформатизації; галузеві та регіональні програми та проекти інформатизації; програми та проекти інформатизації органів місцевого самоврядування;

нормативно-правова база НПІ є розвинутою, системною та ієрархічною і в цілому відповідає розвитку цієї сфери;

успішність реалізації деяких регіональних програм інформатизації, наприклад, Волинської та Дніпропетровської, та відпрацювання механізму їх взаємодії з програмами інформатизації органів місцевого самоврядування, який доцільно впровадити в масштабі всієї країни.

В той же час однією з головних організаційних проблем НПІ залишається некоординованість дій органів публічної влади в цій сфері, коли створюються державні органи з дублюючими завданнями та функціями, розробляються та приймаються неузгоджені між собою програмні та планові документи, не забезпечується необхідний статус Генерального державного замовника НПІ, як “головного координатора”, порушуються зв’язки та управлінська вертикаль між суб’єктами управління, що призводить до конкуренції органів влади між собою за вплив на сферу, неефективного витрачення бюджетних коштів, втрати довіри та іміджу влади [25].

Двадцятирічний досвід реалізації НПІ демонструє, що у багатьох випадках органи публічного управління “наштовхуються” на проблеми із запровадженням ІКТ у певну сферу суспільно-політичного та економічного життя, розуміють складнощі із їх вирішенням на всьому українському просторі, враховують обмеженість ресурсного забезпечення тощо. Зазначене призводить до прагнення вирішити ці проблеми локально, запровадивши нові механізми у визначеній сфері[2]. На це також впливає критичне відношення до самої НПІ, прагнення оцінити її результативність на короткому проміжку часу (часто прив’язаному до фінансового року). Іншим фактором недооцінки необхідності цілісного стратегічного управління сферою ІКТ є “тиск” лобіювання новітніх міжнародних концепцій, які часто динамічно змінюють одне одну.

Незважаючи на це, на сьогодні НПІ залишається єдиним “системним інтегратором”, який став своєрідним “стрижнем” інформатизації, яка включає певну кількість організаційно-правових інструментів публічного управління національним розвитком із застосуванням ІКТ, зафіксованих у стратегічних документах щодо:

Національної програми інформатизації (з 1998 р.);

державних цільових програм щодо галузевої комп’ютеризації, запровадженню ІКТ, формування комунікаційних систем та мереж тощо (з 2004 р.);

розвитку інформаційного суспільства (з 2007 р.);

розвитку електронного урядування (з 2010-2015 рр., з 2017 р.);

розвитку електронної демократії (з 2017 р.);

---

[2] Всесвітній банк зазначав, що “прийняти” і реалізувати “ефективні” заходи політики часто непросто, оскільки певні суспільні групи, яким вигідний існуючий стан речей, можуть володіти достатнім впливом для перешкоджання необхідному реформуванню. Тому успішні реформи – це не тільки “оптимальна практика”. Вони вимагають впровадження та коригування інституцій, з тим щоб вирішити проблеми, що перешкоджають подальшому розвитку, які пов’язані зі слабкою політичною волею і недостатніми спільними діями”. Див.: World Bank. 2017. World Development Report 2017: Governance and the Law. Washington, DC : World Bank. – Режим доступу : http://www.worldbank.org/en/publication/wdr2017

міжнародної ініціативи “Відкритий Уряд” (з 2012 р.);

Стратегії кібербезпеки та Доктрини інформаційної безпеки (з 2016 та 2017 років відповідно);

Концепції розвитку цифрової економіки та суспільства України на 2018 – 2020 роки (з 2018 р.) та Плану заходів з її реалізації;

Міжвідомчої ради з питань розвитку електронного урядування (з 2009 р., перше засідання – 2015 р.);

Консультаційної ради з питань розвитку інформаційного суспільства при Верховній Раді України (2015 р.);

Стратегії реформ сталого розвитку “Україна – 2020”, Програми діяльності Кабінету Міністрів України, Середньострокового та Короткострокового планів пріоритетних заходів Уряду;

Стратегії реформування державного управління України на 2016 – 2020 рр.;

Зеленої та Білої книги з розвитку електронного урядування (з 2014 р.);

Рекомендацій парламентських слухань за цією тематикою тощо.

В цих стратегічних документах ставляться відмінні цілі та завдання, суб’єктами управління, як правило, виступають різні державні органи, а об’єкти управління неузгоджені між собою та лише частково стосуються проблем інформатизації, самі акти часто “не виходять за рамки концепцій (доктрин)”, мають декларативний характер, не підтримані організаційно та ресурсно [3]. Ситуація погіршується перманентними реформами ЦОВВ з змінами їх структури, завдань та функцій. Так, наприклад, схвалена Урядом Концепція розвитку цифрової економіки та суспільства України на 2018 – 2020 роки та План заходів з її реалізації (головний державний орган з їх координації – Міністерство економічного розвитку і торгівлі) включають такі пріоритетні напрямки, які стосуються і розвитку сфери інформатизації:

- подолання цифрового розриву шляхом розвитку цифрових інфраструктур (“твердих” та “м’яких”), у тому числі, інфраструктури електронного урядування та електронної демократії, електронної комерції, кібербезпеки, широкосмугової та мобільної телекомунікаційної інфраструктури тощо;
- розвиток цифрових компетенцій;
- впровадження концепції цифрових робочих;
- цифровізація реального сектору економіки, головної складової цифрової економіки;
- цифровізація реального сектору економіки;
- реалізація проектів цифрових трансформацій;

[3] Всесвітній банк зазначав, що “…країнам Європи і Центральної Азії, що розвиваються, доведеться не тільки провести реформи, покликані поліпшити доступ до Інтернету, а й зосередити увагу на “аналоговому фундаменті» цифрової економіки, а саме – на навичках, інститутах і нормативно-правовій базі”. …“Цифровий економіці також необхідний міцний аналоговий фундамент, який складається з *нормативно-правової бази*, яка створює динамічне ділове середовище і дозволяє фірмам повною мірою використовувати ІКТ для конкуренції та інновацій; *навичок*, що дозволяють працівникам, підприємцям і державним службовцям використовувати нові можливості, що відкриваються в цифровому світі; підзвітних *інститутів*, що використовують Інтернет для розширення прав і можливостей громадян. Її довготривалий вплив на розвиток зовсім не стійкий, оскільки він визначається безперервним впливом технічного прогресу та вибраних країною принципів організації економічного та соціального розвитку і державного управління”. Див.: World Bank. 2016. World Development Report 2016: Digital Dividends. Washington, DC: World Bank. – Режим доступу : http://documents.Worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf

- гармонізація з європейськими цифровими та науковими ініціативами [6].

В вищезазначених документах, як правило, відсутнє будь яке посилання на НПІ та не визначено відповідного механізму їх взаємодії.

Можливим варіантом такої взаємодії могла б стати заміна Закону України “Про Концепцію національної програми інформатизації” законом щодо розвитку цифрової економіки та суспільства України (Концепція) з чітким розподілом повноважень між Мінекономрозвитку та Державним агентством з питань електронного урядування стосовно сфери інформатизації, або спільна їх робота над новою редакцією проекту Закону України “Про Національну програму інформатизації”, який би врахував особливості всіх перелічених вище ініціатив у сфері ІКТ-розвитку країни. Позитивним прикладом такої взаємодії між цими державними органами є розмежування їх прав та обов’язків щодо надання електронних послуг, а також застосування узгоджувального механізму Міжгалузевої ради з питань розвитку електронного урядування [26].

Такий підхід передбачає, насамперед внесення змін до Закону України “Про Національну програму інформатизації”, починаючи від оновлення категорійно-понятійного апарату (терміносистеми), принципів, цілей, пріоритетів, завдань ІКТ-розвитку країни в цілому та його окремих складових; переліку суб’єктів, а також уточненням та конкретизацією особливостей базових регламентів формування та виконання: моніторингу, аналізу, прогнозування, організації, експертизи, контролю, оцінювання результативності, ресурсному, науково-методичному, організаційному забезпеченню НПІ тощо.

“Інтеграційний” підхід, спрямований на підвищення ефективності організаційно-правових механізмів системи державного управління та регулювання в цілому ІТ-галузі, було визначено Парламентом за результатами відповідних парламентських слухань [27], де рекомендовано Уряду: “утворити центральний орган виконавчої влади, що забезпечуватиме формування та/або реалізацію державної політики у сферах ІКТ та зв’язку, розвитку інформаційного суспільства, інформатизації, телекомунікацій, програмування, інформаційної безпеки та кібербезпеки, впровадження технологій електронного урядування, електронного документообігу, електронного підпису тощо та передати зазначеному органу повноваження інших органів виконавчої влади, що стосуються сфери ІКТ та зв’язку, чітко розмежувати повноваження між органами виконавчої влади в зазначених сферах відповідно до законодавства Європейського Союзу”. Але ця рекомендація Парламенту не знайшла практичної імплементації у відповідних рішеннях Уряду.

Інший підхід передбачає розробку та затвердження замість Закону України “Про Концепцію національної програми інформатизації”, так званих, “пріоритетних напрямків Національної програми інформатизації”, що включають: стратегічні цілі інформатизації, її основні принципи, напрямки, очікувані наслідки реалізації цієї НПІ та формуються центральним органом виконавчої влади, який реалізує державну політику у сферах інформатизації, електронного урядування, формування і використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства, і визначаються постановою Кабінету Міністрів України за поданням Генерального державного замовника Національної програми інформатизації, а також у відповідних актах Президента України, Верховної Ради України, Кабінету Міністрів України та центрального органу управління у сфері інформатизації – Генерального державного замовника Національної програми інформатизації [24].

Враховуючи основні тенденції розвитку сфери інформатизації, ІКТ, цифрової економіки, реформ, що відбуваються в Україні, пропонується призначення НПІ

уточнити і сформулювати так: НПІ інформатизації визначає пріоритетні напрямки та стратегію реалізації публічної політики у сфері інформатизації: забезпечення інфраструктурних потреб розвитку інформаційного суспільства та цифрової економіки, формування і використання національних електронних інформаційних ресурсів, впровадження сучасних інформаційно-комунікаційних технологій для підтримки ефективної та результативної діяльності органів публічної влади у всіх сферах життєдіяльності громадянина, суспільства та держави.

Перелік основних завдань НПІ доцільно осучаснити такими стратегічними завданнями як:

забезпечення інтероперабельності державних реєстрів та баз даних;

створення та впровадження стандартів електронного урядування та електронної демократії;

подолання цифрової нерівності;

прискорення процесу розроблення та впровадження сучасних інформаційно-комунікаційних технологій у публічне управління та адміністрування, охорону здоров’я, культуру, освіту, науку, охорону навколишнього природного середовища, бізнес тощо;

підвищення кваліфікації публічних службовців, працівників підприємств та установ, організацій з питань е-врядування та е-демократії;

підвищення якості та доступності електронних послуг, спрощення процедур їх надання і скорочення відповідних витрат, деперсоніфікація надання електронних послуг як інструмент зниження рівня корупції;

організація інформаційної взаємодії органів державної влади та органів місцевого самоврядування на базі електронного документообігу з використанням електронного цифрового підпису;

створення, впровадження та розвиток внутрішньовідомчих систем електронного документообігу;

розвиток інфраструктури електронної комерції, кібербезпеки, широкосмугової та мобільної телекомунікаційної інфраструктури – розвиток цифрових компетенцій;

впровадження концепції цифрових робочих;

реалізація проектів цифрових трансформацій;

гармонізація з європейськими цифровими та науковими ініціативами.

що в цілому буде сприяти взаємоузгодженню механізму публічного управління НПІ з іншими вищевказаними механізмами.

Всі цілі та завдання НПІ повинні бути чітко представлені системою кількісно-якісних індикаторів та показників їх досягнення у часі як основи для застосування ефективних процедур моніторингу, оцінювання, контролю та прогнозування розвитку сфери інформатизації. Але за 20 років НПІ така система показників (критеріїв) так і не була створена та впроваджена, що безумовно негативно вплинуло на Програму.

Тому доцільно доповнити Закон України “Про Національну програму інформатизації” окремою статтею стосовно оцінювання НПІ та стану розвитку сфери: Оцінювання результативності виконання Національної програми інформатизації ґрунтується на результатах реалізації її складових частин та окремих завдань (проектів), позиції України у міжнародних рейтингах, результатах статистичних спостережень Держстату та моніторингу України міжнародними організаціями у сфері інформатизації на основі сучасних загальноприйнятих індикаторів, оцінок громадськості, показників, які демонструють стан розвитку інформатизації.

Стаття враховує як основні суб’єкти моніторингу та оцінювання стану розвитку інформатизації в Україні та НПІ, так і їх комплексне застосування з метою підвищення

рівня об’єктивізації результатів оцінювання, узгодженості з міжнародними системами оцінювання в цій сфері, забезпечення ефективного зворотного зв’язку.

Результати реалізації НПІ мають оформлюватись у вигляді урядової доповіді про поточний стан та перспективи розвитку інформатизації та інформаційного суспільства в Україні (Доповідь), яка має замінити “Доповідь про стан інформатизації в Україні”, передбачену чинним Законом. Зміна назви документу передбачає зміну його змісту, а саме посилення його аналітичної складової за рахунок впровадження результатів короткострокових та середньострокових прогнозів, розширення на сферу інформаційного суспільства та цифрової економіки тощо. Важливо змінити негативну тенденцію останніх років стосовно ігнорування розробки Доповіді Урядом та надання її для розгляду Парламентом, починаючи з 2014 року.

Механізм стратегічного управління НПІ, окрім чіткого визначення цілей, стратегічних завдань, системи індикаторів(показників), критеріїв ефективності (результативності) Програми, повинен чітко визначати суб’єкти та об’єкти НПІ.

Організаційний механізм НПІ включає такі її основні суб’єкти, як:

замовники робіт з інформатизації;

виконавці окремих завдань (проектів) інформатизації;

організації, що здійснюють експертизу окремих завдань та проектів інформатизації;

користувачі автоматизованих та інших інформаційних систем і засобів інформатизації [28].

Сучасні умови розвитку України, у тому числі, такі процеси як децентралізації, деконцентрації, дерегуляції, демократизації управління, а також євроінтеграції та отриманий 20-річний досвід обумовлюють необхідність внесення змін в існуючий організаційний механізм НПІ, у тому числі, стосовно переліку її суб’єктів. В змінах до Закону пропонується такий уточнений перелік її основних суб’єктів:

Генеральний державний замовник Національної програми інформатизації;

керівник Національної програми інформатизації;

Міжгалузева рада з питань розвитку електронного урядування;

Консультативна рада з питань розвитку інформаційного суспільства при Верховній Раді України;

Науково-технічна рада Національної програми інформатизації;

державні замовники завдань (проектів) Національної програми інформатизації;

керівники галузевих, регіональних програм інформатизації, а також програм інформатизації органів місцевого самоврядування та об'єднаних територіальних громад;

виконавці окремих завдань (проектів) Національної програми інформатизації;

організатори та виконавці державної експертизи завдань та проектів Національної програми інформатизації;

користувачі інформаційних систем і засобів інформатизації, створених в результаті виконання завдань (проектів) Національної програми інформатизації.

Враховуючи важливість залучення громадськості, бізнесу, експертного середовища до процесів формування та реалізації державної політики в цій сфері, а також відповідно до таких принципів належного урядування як відкритість, прозорість та участі до суб’єктів НПІ пропонується додати Міжгалузеву раду з питань розвитку електронного урядування та Консультативну раду з питань розвитку інформаційного суспільства при Верховній Раді України, які вже визначені чинним законодавством на рівні постанов Уряду та Парламенту відповідно [26; 29]. Згідно Концепції розвитку електронного урядування в Україні [23] головним призначенням Міжгалузевої ради з питань розвитку

електронного урядування (попередня назва Міжгалузева рада з питань розвитку інформаційного суспільства) є сприяння забезпеченню координації дій органів влади під час реалізації її положень. До складу Міжгалузевої ради в основному включені керівники центральних органів виконавчої влади та незначна кількість представників громадських організацій, не представлені регіональна влада, бізнес та наукове середовище. Відсутність дієвості є головною проблемою цього суб’єкта НПІ, який, починаючи з моменту його створення у 2009 році, майже не працював. Головною метою Консультативної ради з питань розвитку інформаційного суспільства при Верховній Раді України(попередня назва Консультаційна рада з питань розвитку інформатизації при Верховній Раді України) є сприяння Верховній Раді України у виробленні політики в сферах розвитку інформаційного суспільства, інформатизації, електронних комунікацій, високих технологій, при підготовці та затвердженні завдань Національної програми інформатизації, а також при підготовці та прийнятті законів України у цих сферах з урахуванням найновіших досягнень і технологічних рішень. До складу Консультативної ради входять за згодою вчені у галузі інформатики та суміжних галузях, представники підприємств, установ, організацій, які працюють у сфері інформаційних послуг, народні депутати України, представники органів виконавчої влади (на відміну від Міжгалузевої ради в цій Раді більш широко представлені бізнес та наука) [29]. Однак, з 2013 року не відбулося жодного засідання цієї ради. Тому доцільність включення зазначених рад до суб’єктів НПІ насамперед обумовлена гарантуванням їх справжнього функціонування.

Ще один дорадчий консультативний орган НПІ – Науково-технічна рада Національної програми інформатизації при Генеральному державному замовнику НПІ входила до складу її суб’єктів (стаття 12 Закону “Про Національну програму інформатизації”), але у 2012 році її було необґрунтовано виключено на загальнодержавному рівні при збереженні як суб’єкта для галузевих та регіональних програм (проектів) інформатизації. Її повноваження включали:

розроблення пропозицій і рекомендацій щодо формування та реалізації державної політики у сфері інформатизації, а також щодо стратегії розвитку інформаційної інфраструктури;

розроблення пропозицій і рекомендацій щодо проектів нормативно-правових актів із питань інформатизації;

розроблення пропозицій щодо стратегічних цілей, основних принципів та пріоритетних напрямків НПІ, очікуваних результатів її реалізації;

розгляд пропозицій та надання рекомендацій щодо формування нормативно-правових, організаційних, методологічних, методичних, науково-технічних, інструментально-технологічних, економічних і гуманітарних засад підтримки НПІ;

розгляд пропозицій та надання рекомендацій щодо формування завдань (проектів) НПІ на наступні роки;

розгляд проектів галузевих, регіональних та місцевих програм інформатизації, а також частин інших програм, що стосуються питань інформатизації;

розгляд результатів виконання завдань (проектів) НПІ, галузевих, регіональних та місцевих програм інформатизації, а також частин інших програм, що стосуються питань інформатизації;

розгляд проекту щорічної доповіді про стан інформатизації в Україні;

розроблення пропозицій щодо удосконалення механізмів формування та виконання НПІ;

організація взаємодії з керівниками та науково-технічними радами галузевих, регіональних та місцевих програм інформатизації [28].

“Повернення” цього суб’єкта до НПІ буде не тільки сприяти її більшій прозорості, відкритості та обґрунтованості, але й уніфікації процесів її формування та виконання на всіх рівнях: загальнодержавному, галузевому, регіональному та місцевому.

Ефективна робота цих консультативно-дорадчих органів НПІ передбачає, насамперед їх скоординовану діяльність та взаємодію між собою, яка на сьогодні відсутня.

Головним в управлінні Програмою є її Генеральний державний замовник, якого в останні роки безпосередньо підпорядкували Прем’єр-міністру України, збільшивши його реальний вплив як на складові НПІ, так і на її суб’єкти. Його основні повноваження щодо формування та виконання НПІ визначені статтями 13 та 22 Закону та відповідними рішеннями Уряду і включають:

координацію державних, галузевих, регіональних програм та проектів інформатизації, програм та проектів інформатизації органів місцевого самоврядування;

моніторинг у сфері інформатизації;

забезпечення методологічної, нормативно-правової, інформаційної та організаційної підтримки процесів формування і виконання НПІ;

доповідь щорічно Кабінету Міністрів України про стан інформатизації в Україні;

надання щорічно Кабінету Міністрів України завдань НПІ на наступні три роки і проекту програми завдань (робіт) на наступний бюджетний рік;

внесення Кабінету Міністрів України пропозиції щодо змін до НПІ [7].

Ці повноваження, по-перше, доцільно поширити на сферу розвитку інформаційного суспільства, по-друге, додати йому такі повноваження як:

- організація проведення державної експертизи пропозицій завдань (проектів) державних замовників та завдань (проектів) НПІ, та їх погодження за результатами цієї експертизи, а також погодження розрахунків граничних обсягів та індикативних прогнозних показників, які надаються державними замовниками;

- організація обговорення Міжгалузевою радою з питань розвитку електронного урядування завдань (проектів) інформатизації, які виконуються в інтересах кількох органів виконавчої влади або мають загальнонаціональний масштаб;

- оцінювання та прогнозування розвитку інформатизації та інформаційного суспільства.

По-третє, уточнити повноваження Генерального державного замовника НПІ, а саме:

забезпечувати комплексність та узгодженість програм інформатизації з відповідними завданнями (проектами) НПІ;

визначати виконавців завдань (проектів) програм інформатизації відповідно до законодавства про публічні закупівлі;

здійснювати нагляд і контроль за виконанням відповідних завдань (проектів) НПІ, галузевих та регіональних програм інформатизації згідно з укладеними контрактами (договорами);

забезпечувати приймання, впровадження та використання результатів виконання завдань (проектів) Національної програми інформатизації;

розробляти типові завдання (проекти) інформатизації галузевих, регіональних програм інформатизації, програм інформатизації органів місцевого самоврядування та об'єднаних територіальних громад;

подавати Кабінету Міністрів України обґрунтування щодо припинення виконання окремих завдань (проектів) Національної програми інформатизації, галузевих, регіональних програм інформатизації та їх окремих завдань (проектів).

Зазначені уточнення повноважень Генерального державного замовника НПІ мають бути спрямовані на законодавче посилення його координуючої, контролюючої, організуючої, прогностично – аналітичної діяльності, а також на підвищення відкритості, прозорості та ефективності механізмів формування та виконання НПІ і є результатом обговорення проекту Закону [24]**,** розробленого Державним агентством з питань електронного урядування, з центральними та регіональними органами виконавчої влади та громадськістю. При цьому необхідно мати на увазі, що без підтримки вищого політичного керівництва ці та інші зміни Закону не будуть мати успіху і все знов завершиться черговим декларативним документом, який черговий раз не буде імплементовано.

Перелік державних замовників завдань (проектів) НПІ доцільно розширити, у тому числі з урахуванням децентралізації влади, включивши до нього: Апарат Верховної Ради України, Адміністрацію Президента України, Секретаріат Кабінету Міністрів України, державні органи, органи місцевого самоврядування, об’єднані територіальні громади, органи судової влади, органи прокуратури, Національну Академію наук України. Функції державних замовників при їх взаємодії з Генеральним державним замовником пропонується уточнити, додатково включивши такі з них, як:

подавати своєчасно керівникові Національної програми інформатизації пропозиції до переліку завдань (проектів) Національної програми інформатизації;

враховувати при підготовці тендерної документації рекомендації Генерального державного замовника в частині технічних, якісних та кількісних характеристик предмета закупівлі;

звітувати перед Генеральним державним замовником про хід виконання завдань (проектів) Національної програми інформатизації тощо.

Доцільно також оновити категорійно-понятійний апарат НПІ (її терміносистему), структуру її об’єктів та суб’єктів, їх функцій та завдань тощо.

Висновки.

1. У 1998 році в Україні було створено один з перших у світі механізмів стратегічного управління розвитком інформатизації, який охоплював майже всі сфери політичного, соціально-економічного та культурного життя. Однак внаслідок сукупності негативних факторів, насамперед таких як недостатня координації, розпорошеність та обмеженість ресурсів, НПІ за 20 років лише частково реалізувала планові завдання, перетворилася значною мірою на декларативну, мало демократичну, негнучку бюрократичну структуру. В той же час, незважаючи на всі ці недоліки, НПІ все ж залишається єдиним реально діючим інструментом стратегічного управління з розвитку ІКТ, яка за останні роки певною мірою підвищила результативність, що обумовлено, насамперед, організаційними змінами та підходами до ресурсного забезпечення НПІ.

2. Актуальною залишається проблема збереження генеральної спрямованості розвитку країни на широке запровадження ІКТ у всі сфери соціального та економічного життя, забезпечення синергії державних рішень щодо реалізації окремих концепцій: інформаційного суспільства, відкритого уряду, е-урядування та е-демократії, інформаційної та кібербезпеки тощо.

3. З двох варіантів розв’язання накопичених проблем публічного управління розвитком країни на основі запровадження ІКТ: 1) припинити Національну програму інформатизації, замінивши її іншим інструментом стратегічного управління – зокрема Концепцією розвитку

цифрової економіки та суспільства, 2) адаптувати (осучаснити) її до завдань політичного та соціально-економічного розвитку України та світу, більш перспективним та раціональним є другий, оскільки він відповідає світовим тенденціям, дозволяє більш ефективно використовувати ресурси, враховує отриманий за 20 років досвід.

4. Реалії сучасного розвитку, накопичений український та світовий досвід застосування різних інструментів публічного управління запровадженням ІКТ дозволив обґрунтувати надані пропозиції щодо необхідності модернізації організаційно-правового механізму НПІ, основні зміни щодо складу її суб’єктів, державних замовників, об’єктів, їх функцій та завдань, спрямованих на усунення існуючих недоліків та на підвищення рівня демократичності, гнучкості, ефективності, результативності та відповідності міжнародних механізмів.

Використана література

1. У 13-тій черговій доповіді “The Global Risks Report 2018”, опублікованій до Всесвітнього економічного форуму 2018 року, суттєво переглянуто перелік та визначено нові глобальні майбутні ризики за групами: “Економічні” (9 позицій); “Екологічні” (5); “Геополітичні” (6); “Соціоетальні” (6) та “Технологічні” (5). Серед технологічних глобальних ризиків визначено: 1) негативні наслідки технічного прогресу, таких як штучний інтелект, геоінженерна та синтетична біологія (передбачувані або непередбачені), що спричиняє людський, екологічний та економічний збиток; 2) підвищення вразливості з відключення важливої інформаційної інфраструктури (наприклад, Інтернету, супутників тощо) та мереж (злам); 3) великомасштабні кібератаки або зловмисне програмне забезпечення, що спричиняють великі економічні збитки, геополітичну напруженість або втрату довіри до Інтернету; 4) масові випадки шахрайства, крадіжки даних, наслідком яких є безпрецедентне неправомірне використання приватних чи офіційних даних. – Режим доступу : http://www3.weforum.org/docs/WEF_GRR18 _Report.pdf

2. European Commission. Europe 2020. – Режим доступу : https://ec.europa.eu/info/busin ess-economy-euro/economic-and-fiscal-policy-coordination/eu-economic-governance-monitoring-prevent ion-correction/european-semester_en.

3. Стратегія сталого розвитку “Україна – 2020” : Указ Президента України від 12.01.15 р. № 5/2015. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/5/2015

4. Стратегія реформування державного управління України на 2016 – 2020 роки : Розпорядженя Кабінету Міністрів України від 24.06.16 р. № 474-р. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/474-2016-%D1%80

5. Програма діяльності Кабінету Міністрів України : Постанова Кабінету Міністрів України від 14.04.16 р. № 294. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/294-2016-%D0%BF

6. Концепція розвитку цифрової економіки та суспільства України на 2018 – 2020 роки та план заходів щодо її реалізації : Розпорядженя Кабінету Міністрів України від 17.01.18 р. № 67-р. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/67-2018-р

7. Про Національну програму інформатизації : Закон України. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80

8. Про Концепцію Національної програми інформатизації : Закон України. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80

9. Про затвердження Завдань Національної програми інформатизації на 1998 – 2000 роки : Закон України. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/76/98-%D0% B2%D1%80

10. Грицевич В.С. Інформатизація суспільства, як соціально-географічний виклик XXI століття. – Режим доступу : //geography.lnu.edu.ua

11. Петрова Е.А. Зарубежный опыт информатизации и особенности его реализации в России. – Режим доступу : https://www.fundamental-research.ru/ru/article/view?id=3673

12. Соснін О.В. Інформатизація як феномен та умова інноваційного розвитку України. – Режим доступу : http://uaforeignaffairs.com/ua/ekspertna-dumka/view/article/informatizacija-jak-fenomen-ta-umova-innovaciinogo-roz

13. Яковенко Ю., Шевцов А. Информатизация и Украина : взгляд на проблему. – Режим доступу : //www.db.niss.gov.ua/docs/region/inform_1.htm

14. Сітнікова Н.П. Досвід стратегічного планування сталого розвитку у країнах Європейського Союзу. – Режим доступу : //www.economy.in.ua/pdf/11_2012/ 5.pdf

15. Подболотова М.И. Международная практика реализации стратегий и программ информатизации в области финансовой грамотности детей и молодежи. – Режим доступу : http://journals.rudn.ru/informatization-education/article/download/13237/12667

16 Опыт информатизации и перспективные идеи. – Режим доступу : https://studfiles.net /preview/593899/page:16

17. Концепция информатизации общества (обобщенный вариант) – (Архив академика А.П. Ершова). – Режим доступу : http://ershov-arc.iis.nsk.su/archive/eaindex.asp?lang=1&gid=2367

18. Розвиток інформаційного суспільства в Україні в 2016 році : основні тенденції, фактори впливу та стан ІТ-індустрії : аналітична записка, 2017. – 24 с. – (Національний інститут стратегічних досліджень). – Режим доступу : http://www.niss.gov.ua/articles/2594

19. Береза Н.В. Ринок информационных услуг : современные тенденции и перспективы развития : монография. – М. : Директ-Медиа, 2014. – 180 с.

20. Європейський досвід нормативно-проектного забезпечення розвитку інформаційного суспільства: висновки для України : аналітична доповідь, 76 с. – (Національний інститут стратегічних досліджень). – Режим доступу : http://www.niss.gov.ua/articles/1732

21. Министерство связи и информатизации Республики Беларусь. – Режим доступу : http://www.mpt.gov.by/ru

22. Министерство информации и коммуникаций Республики Казахстан. – Режим доступу : http://mic.gov.kz/ru

23. Концепція розвитку електронного урядування в Україні : Розпорядження Кабінету Міністрів України від 20.09.17 р. № 649-р. – Режим доступу : https://www.kmu.gov.ua/ua/npas/ 250287124

24. Про внесення змін до Закону України “Про Національну програму інформатизації” : проект Закону України. – Режим доступу : http://dknii.gov.ua/content/zakon-ukrayiny-pro-vnesennya-zmin-do-zakonu-ukrayiny-pro-nacionalnu-programu-informatyzaciyi

25. Семенченко А.І. Методологічні підходи до формування організаційно-правових механізмів державного управління та регулювання розвитком інформаційної інфраструктури // Вісник НАДУ.– 2014. – № 3. – С.43-52.

26. Про утворення Міжгалузевої ради з питань розвитку електронного урядування : Постанова Кабінету Міністрів України від 14.01.09 р. № 4. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/4-2009-%D0%BF

27 Про Рекомендації парламентських слухань на тему: “Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України” : Постанова Верховної Ради України від 31.03.16 р. № 1073-VIII. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/1073-19

28. Наказ Міністерства транспорту та зв’язку України від 10.04.07 р. № 324. – Режим доступу : http://kved.ukrstat.gov.ua/KVED2010/62/KVED10_62_02.html

29. Консультативна рада з питань розвитку інформаційного суспільства при Верховній Раді України : Постанова Верховної Ради України від 4.02.98 р. № 77/98-ВР. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/77/98-%D0%B2%D1%80

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 002.6:004:340.1+316.329.8

БАРАНОВ О.А., *доктор юридичних наук, с.н.с.,*
керівник Центру теоретико-правових проблем інформаційної сфери
НДІ інформатики і права НАПрН України

ІНТЕРНЕТ РЕЧЕЙ (IoT) І БЛОКЧЕЙН

Анотація. *Аналізуються методологічні причини доцільності використання технології блокчейн в сфері Інтернету речей. Класифіковані види транзакційних зв'язків в умовах застосування технологій Інтернету речей. Пояснюється значення довіри для здійснення таких зв'язків. Дається обґрунтування доцільності організації розподілених систем довіри в умовах використання мережі Інтернет. Показані специфічні властивості технології блокчейн як потенційного технологічного способу побудови розподілених систем довіри в певних сферах діяльності. Сформульовано правові проблеми теоретичного і практичного спрямування, які є бар'єром на шляху впровадження технології блокчейн в умовах використання технологій Інтернету речей.*

Ключові слова: *блокчейн, транзакція, довіра, Інтернет речей, правове регулювання.*

Summary*. The methodological reasons for the expediency of using blockchain technology in the sphere of Internet of Things are analyzed. Types of transactional relations in the conditions of application of Internet of Things technologies are classified. The importance of trust for the implementation of such relations is explained. The rationale for the organization of distributed systems of trust in the conditions of using the Internet is given. The specific properties of blockchain technology as a potential technological method for constructing distributed trust systems in certain spheres of activity are shown. Legal problems of the theoretical and practical directions are formulated, which are a barrier to the introduction of blocking technology in conditions of using Internet of things technologies.*

Keywords: *blockage, transaction, trust, Internet of things, legal regulation.*

Аннотация. *Анализируются методологические причины целесообразности использования технологии блокчейн в сфере Интернета вещей. Классифицированы виды транзакционных связей в условиях применения технологий Интернета вещей. Поясняется значение доверия для осуществления таких связей. Дается обоснование целесообразности организации распределенных систем доверия в условиях использования сети Интернет. Показаны специфические свойства технологии блокчейн как потенциального технологического способа построения распределенных систем доверия в определенных сферах деятельности. Сформулированы правовые проблемы теоретического и практического направления, которые являются барьером на пути внедрения технологии блокчейн в условиях использования технологий Интернета вещей.*

Ключевые слова: *блокчейн, транзакция, доверие, Интернет вещей, правовое регулирование.*

Постановка проблеми. В останні кілька років раптом бурхливо стартувало обговорення використання технологій блокчейн в самих різних сферах, в тому числі, з’являються перші роботи, присвячені аналізу перспектив їх використання в сфері технологій Інтернету речей (далі – ІР).

Практично з самого початку масового використання Інтернет-технологій виникли проблеми, пов’язані з особливостями мережі Інтернет: потенційна анонімність суб’єктів відносин, невизначеність їх юрисдикції, часу здійснення транзакцій і достовірності отриманої інформації та ряд інших [1]. Для нейтралізації негативних наслідків проявуцих особливостей як національні правові системи, так і міжнародне право відреагували появою певних нормативно-правових актів з метою забезпечення довіри в процесі здійснення різних транзакцій, заснованих на використанні Інтернет-технологій.

Вирішенню проблем довіри до Інтернету як до відкритого середовища присвячено ряд міжнародних документів: Доповідь Генерального секретаря ООН [2], аналітичний огляд ISOC “Рамки політики для відкритого і надійного Інтернету” [3], Глобальний звіт ISOC “Економіка побудови довіри в Інтернеті: запобігання спотворенню даних” [4] і багато інших. Квінтесенція цих підходів полягає в наступній думці: Інтернет потребує надійного фундаменту довіри, щоб повністю реалізувати його потенціал [5].

В якості одного з інструментів підвищення довіри між суб’єктами, що здійснюють транзакції за допомогою мережі Інтернет, особливо, в умовах зростаючої кількості видів і типів кіберзагроз, пропонується використовувати технології блокчейн [9; 13 – 19].

Цілком очевидно, що більшість проблем, які мають місце при використанні інтернет-технологій, будуть мати місце і у сфері IP, в якій мережа Інтернет є базовою інфраструктурною платформою.

З урахуванням економічної привабливості, передбачуваної безпрецедентності масового використання технологій IP, проблема забезпечення довіри буде набувати все більш важливого значення. Таким чином, дослідження в сфері IP правових методів і механізмів забезпечення довіри, зокрема, з використанням для цього технологій блокчейн, має значну актуальність.

Метою статті є визначення методологічних причин використання технологій блокчейн в сфері IP, а також наявності та змісту правових проблем при їх використанні.

Виклад основного матеріалу. На основі результатів роботи [6], а також проведеного аналізу юридичних і технічних джерел запропонуємо в інтересах цього дослідження наступне визначення: ***Інтернет речей*** – це сукупність взаємодіючих технічних систем і комплексів, що складаються з мікропроцесорів, сенсорів, пристроїв, систем передачі даних, локальних і/або розподілених обчислювальних ресурсів і програмних засобів, в тому числі програм штучного інтелекту, на основі використання величезної кількості даних і мережі Інтернет та призначених для здійснення суспільних відносин, зокрема, пов’язаних з наданням послуг або проведенням робіт за безпосередньою участю або без участі суб’єктів цих відносин (юридичних або фізичних осіб).

Спираючись на базове для інституційної економіки поняття економічної транзакції [7], сформулюємо таке поняття: ***транзакція*** – це добровільна взаємодія (спільна дія в інтересах один одного), що здійснюється за згодою суб’єктів щодо ресурсів або дій (предмета транзакції).

Можна припустити, що феномен IP, його величезні економічні, соціальні та технологічні переваги будуть причиною істотної зміни ландшафту бізнес-моделей в сучасному і майбутньому світі – світі технологій IP.

Сучасні бізнес-моделі взаємодії різних суб’єктів містять елементи ієрархічних зв’язків, які, як правило, обумовлені необхідністю взаємодії з суб’єктами публічної влади. Ця необхідність зумовлена існуючими національними та міжнародними системами сертифікації, ліцензування, квотування, фітосанітарного контролю та переміщення вантажів, платіжними та митними системами тощо. Наявність ієрархічних зв’язків призводить до збільшення непродуктивних транзакційних витрат ведення бізнесу, які значно збільшуються для компаній, розташованих в різних країнах. Так, наприклад, сьогодні реальний час необхідний для здійснення власне угоди купівлі-продажу нерухомого або рухомого майна вже може обчислюватися хвилинами, але підготовка необхідних документів для переоформлення права власності може зайняти кілька днів.

Так як причина збільшення транзакційних витрат (далі – ТВ) – це наявність ієрархічних зв’язків з державними органами, то, природньо, напрошується радикальне

рішення: шлях мінімізації ТВ – це шлях усунення ієрархічних зв’язків. Або, іншими словами, це означає міграцію від ієрархічної структури бізнес відносин до горизонтальної (плоскої) структури. ***Горизонтальні бізнес-відносини*** – це пірингові відносини (peer to peer), тобто однорангові відносини між рівними партнерами без посередників.

В останні роки завдяки використанню мережі Інтернет відносини між різними суб’єктами як національної, так і іноземної юрисдикції активно реалізуються відповідно до горизонтальної моделі взаємодії. Безсумнівно, це повною мірою стосується і випадків використання технологій Інтернету речей. Яскравим прикладом можливостей IP для реалізації піринговых відносин між виробником і споживачем можуть бути відносини, що пов’язані з технологіями 3D-друку. Зростаюча сфера застосування 3D-друку та простота його використання дозволяють припустити, що в майбутньому стане можливою організація масового “виробництва” товарів на дому у споживачів відповідно до їх індивідуальних замовлень. Така “поставка” товарів не потребуватиме ані торгових посередників, ані ієрархічних зв’язків.

Відзначимо кілька системних факторів розвитку світової економіки, які стимулюють перехід до горизонтальних бізнес-моделей:

- глобалізація економічних, виробничих, інформаційних, фінансових та інших відносин;
- зростання конкуренції як на національному, так і на міжнародному рівні;
- зростання міжнародної конкуренції, тобто конкуренції на національних локальних ринках окремих країн гравців локальних ринків з інших країн світу;
- наявність міцного кореляційного зв’язку результатів ведення бізнесу та невизначеності і волатильності попиту на продукцію або послуги;
- необхідність для гравців локальних ринків швидкого освоєння знань про особливості конкретних юрисдикцій не тільки в цілому інших держав, але навіть їх окремих регіонів;
- прискорення темпів протікання і розвитку всіх процесів в соціумі, і, перш за все, в економіці;
- необхідність різкого збільшення швидкості та підвищення якості реакції на виклики.

Таким чином, формування горизонтальних бізнес-відносин на основі Інтернет-технологій створює унікальні передумови для надання послуг і проведення робіт в інтересах суб’єктів (фізичних або юридичних осіб) з мінімальними, іноді, навіть, з нульовими, транзакційними витратами завдяки усуненню ієрархічних зв’язків.

Однак, має місце фундаментальний фактор, який стримує перехід до горизонтальних моделям взаємовідносин – це довіра, вірніше, її відсутність.

Довіра. Словники в основному однаково тлумачать довіру, наприклад, як переконаність в чиїйсь чесності, порядності; віра в щирість і сумлінність будь-кого [8].

Розуміння людством значення фактору довіри в економічній практиці виникає досить давно. Імовірно, з того часу, коли в торгові взаємовідносини стали масово залучатися суб’єкти з невідомою один для одного репутацією, що створювало цілком відчутний фактор ризику реалізації загроз, пов’язаних з недобросовісною поведінкою суб’єкта транзакцій. Заходи, які необхідно було проводити для мінімізації цього ризику, збільшували ТВ, але інакше була реальна ймовірність отримати набагато більші ТВ в разі реалізації загроз.

Таким чином, однією з причин збільшення ТВ була недобросовісна поведінка суб’єктів транзакції [7], яку не можна було заздалегідь виключити через відсутність підстав для безумовної довіри до них.

У даній роботі будуть досліджуватися проблеми мінімізації тільки тих ТВ, наявність яких обумовлено фактором відсутності довіри.

Проблема довіри загострюється тоді, коли в якості еквівалента товару стали масово використовуватися національні “гроші”, специфічні для кожного державного (квазідержавного) утворення. Наявність різних еквівалентів створювало ризики при здійсненні транзакцій, що вимагало формування довірчих механізмів обміну цими еквівалентами. Функцію забезпечення довіри при обміні еквівалентів стали виконувати треті особи – посередники при обміні національних “валют” (міняйли), які обслуговували будь-якого учасника ринку. Природно, за свою послугу міняйли стягували певну плату, що і становило частину ТВ, обумовлених наявністю ієрархічного зв’язку між покупцями (продавцями) і такою інституцією як міняйли.

Назвемо таку систему обміну національними “валютами” – централізованою системою довіри. ***Централізована система довіри*** (далі – ЦСД) – це система, в якій носієм довіри (інформації про довіру) до суб’єктів взаємовідносин є спеціальний центральний (єдиний, загальний) елемент системи, що функціонує в інтересах будь-якого і кожного суб’єкта соціуму. ***Інформація про довіру*** – це достовірна, повна і своєчасна інформація про сумлінному (несумлінному) поведінку суб'єкта.

У своїй статті [9] М. Зейдель вводить поняття розподіленої форми довіри – це коли люди, раніше невідомі один одному, можуть вступати в безпосередні, рівні довірливі стосунки без звернення до якоїсь центральної організації, яка ручається за будь-якого з них [10]. Цілком можна погодитися з таким підходом визначення особливостей довіри у відсутності ЦСД, але слід зауважити, що така форма довіри може охоплювати не тільки тих, хто раніше був невідомий один одному, але також і тих, хто знав один одного раніше. При цьому, необхідно пам’ятати, що така розподілена система довіри створюється на засадах самоорганізації та добровільного приєднання до неї. Для розподіленої системи довіри можуть бути створені і використані різні механізми забезпечення довіри.

Отже, ***розподілена система довіри*** (далі – РСД) – це особливого роду організаційна система, формально чи не формально створена як закрита корпорація, в якій носієм довіри (інформації про довіру) до суб’єктів взаємовідносин є будь-який суб’єкт, але який обов’язково входить до цієї корпорації.

Аналіз функціонування РСД дозволяє виділити основні властивості притаманні саме цій формі довіри:

- зберігання інформації про довіру здійснюється кожним суб’єктом незалежно від інших;
- інформація про довіру не зберігається в централізованому місці (бібліотеці, журналі, реєстрі, базі даних), а зберігається розподілено – кожним суб’єктом;
- вільний доступ або обмін інформацією про довіру до будь-якого суб’єкта для всіх членів РСД;
- розголос виявлених фактів порушення довіри або прояви якимось суб’єктом нечесності, непорядності або несумлінності.

Отже, ми приходимо до розуміння того, що проблема довіри – це проблема створення та функціонування деякої інформаційної системи (централізованої або розподіленої), яка забезпечує збір, накопичення, використання і зберігання достовірної, повної та своєчасної інформації про сумлінну (несумлінну) поведінку суб’єктів взаємовідносин. Тому, завдання створення правових механізмів вирішення проблеми довіри відноситься до завдань інформаційного права.

Таким чином, будемо розуміти ***довіру*** – як наявність своєчасної, повної та достовірної інформації про сумлінну поведінку.

Для майбутнього використання технологій IP завдяки ряду переваг кращими є горизонтальні бізнес відносини, які в свою чергу можуть гуртуватися на стійких або нестійких горизонтальних транзакційних зв’язках.

До типових стійких горизонтальних транзакційних зв’язків можна віднести, наприклад, зв’язки між членами замкнутих професійних корпорацій. Саме наявність корпоративної довіри дозволяє такі стійкі горизонтальні транзакційні зв’язки вважати довірчими. До стійких горизонтальних транзакційних зв’язків умовно можна також віднести зв’язки, що складаються відповідно до договору, укладеного в результаті тривалих переговорів, або багаторазово повторювані зв’язки між одними і тими ж суб’єктами, що власне і формує якусь неформальну квазікорпорацію. Такі стійкі зв’язки супроводжуються накопиченням достовірної та повної інформації про сумлінну (несумлінну) поведінку суб’єктів корпорації. Отже, стійкі горизонтальні транзакційні зв’язки мають високий ступінь довіри, що дозволяє звести до нуля транзакційні витрати усередині корпорації, а іноді і за її межами.

Таким чином, можна дати наступне визначення**:** ***стійкі горизонтальні транзакційні зв’язки*** – це багаторазово повторювані взаємовідносини між відомими один одному суб’єктами з приводу однорідних транзакцій. Однорідність транзакцій означає високу ступінь подібності умов здійснення взаємовідносин, а значить передбачає стабільність (сумлінної чи несумлінної) поведінки суб’єктів.

Антиподом розглянутим зв’язкам є ***нестійкі горизонтальні транзакційні зв’язки*** як разові або нечисленні спорадичні взаємовідносини між відомими або невідомими один одному суб’єктами, які виникають завдяки попиту або потребам, що ситуативно виникли. Спорадичність і нечисленність взаємовідносин не сприяють накопиченню достовірної та повної інформації про сумлінну (несумлінну) поведінку суб’єктів цих відносин. Спорадичні взаємовідносини, як правило, характерні для відкритих систем, тобто систем, відкритих для взаємодії між будь-якими суб’єктами. До таких систем, в першу чергу, можуть бути віднесені ті, які функціонують на базі використання Інтернет-технологій. Це в повною мірою стосується і Інтернету речей.

Отже, в умовах використання технологій IP будуть мати місце переважно нестійкі горизонтальні транзакційні зв’язки, що особливо гостро ставить питання забезпечення довіри.

Традиційно проблема забезпечення довіри вирішувалася шляхом створення деякої третьої сторони – централізованої спеціальної інституції, апріорі такою, що заслуговує на довіру (credible institution), в якій у той чи інший спосіб збиралася інформація про довіру (благонадійність) до можливих суб’єктів суспільних відносин. До недавнього часу вважалося, що централізовані організаційні структури є найкращим способом вирішення проблеми довіри. У разі законодавчого регулювання функціонування централізованої системи довіри, така система може бути використана будь-яким членом соціуму. Як приклад можуть служити банківська система, система нотаріату, офіційні реєстри нерухомого майна чи земельних ділянок, система сертифікації електронно-цифрових підписів тощо. Безсумнівно, необхідність правового регулювання відносин, пов’язаних з ЦСД, і необхідність фінансування її діяльності зумовлює збільшення прямих і непрямих ТВ.

Виходячи з вищесказаного, можемо констатувати наявність для ЦСД наступного протиріччя:

- з одного боку, довіра є необхідною умовою зменшення ТВ;

• з іншого – збільшення ТВ є необхідною умовою для забезпечення довіри (зменшення ступеня ризику) при здійсненні нестійких горизонтальних транзакційних зв’язків.

На думку М. Зейделя, раніше вважалося, що саме організаційні структури забезпечують централізоване джерело легітимності і це є основою розвитку організаційної екології, інституціональної теорії і економічної теорії транзакційних витрат [9]. Іншими словами, це означало, що довіру може бути забезпечено тільки за рахунок введення ЦСД.

Однак, інтерпретація відомої теореми нобелівського лауреата 1991 року з економіки Р. Коуза, говорить про те, що тільки наявність транзакційних витрат у відносинах між економічними агентами призводить до необхідності введення зовнішнього регулювання і, власне, призводить до необхідності появи третіх осіб або іншими словами, до появи спеціалізованих організаційних структур [11; 12]. Але, якщо сформулювати зворотну теорему, то вона зведеться до наступного: мінімізація ТВ економічних агентів при їх взаємодії, що в ідеалі прагнуть до нуля, нівелює роль зовнішнього регулювання, а значить виключає необхідність в створенні якихось спеціалізованих організаційних структур.

У свою чергу, зворотна теорема дозволяє сформулювати гіпотезу про те, що якщо якась система відносин між економічними агентами має нульову вартість транзакцій, то така система не потребує наявності якоїсь централізованої організації для аутентифікації сторін угод і підтвердження довіри.

Іншими словами, приходимо до важливого висновку про те, що система відносин між економічними агентами, в якій є інформація про довіру до кожного, – це система з нульовою вартістю транзакцій.

Одним з факторів, що формує вимоги до систем довіри як до інформаційних систем, є часовий чинник. Транзакції, які здійснюються за допомогою Інтернет-технологій, мають істотні переваги перед іншими способами їх здійснення завдяки високій швидкості їх реалізації. Отже, будь-яка система довіри потенційно повинна мати швидкодію (час) реакції менше часу, необхідного на реалізацію транзакції. В іншому випадку система довіри буде причиною збільшення ТВ. Особливо негативно це може позначитися на каскадних бізнес-процесах, що складаються з великої кількості високоінтегрованих складно організованих горизонтальних транзакційних зв’язків, що як раз і є характерним для технологій IP.

Крім того, проблема забезпечення довіри в останні роки значно загострилася через стрімко прогресуючі методи та засоби реалізації кіберзагроз.

Для бізнес-моделей, що реалізуються в умовах використання технологій IP, найбільш поширеними і масовими будуть нестійкі (випадкові) горизонтальні транзакційні зв’язку, в яких:

• суб’єкти можуть здійснювати транзакції з різних місць і в різний час;

• час отримання об'єктів транзакцій (товарів, послуг, платіжних засобів тощо) для суб’єктів може бути різним;

• суб’єкти можуть не знати не тільки один одного, але й не знати нічого один про одного;

• репутація суб’єктів, в традиційному її розумінні, практично нічого не означає в умовах, коли тимчасові і вартісні витрати на її перевірку істотно збільшують транзакційні витрати в порівнянні з вартістю угоди.

Отже, фактор довіри, тобто методи і способи збору, зберігання і обробки інформації про довіру до суб’єктів транзакцій при використанні технологій IP в умовах формування нестійких горизонтальних бізнес-моделей набуває фундаментальне значення.

Тому тільки динамічна в функціонуванні, максимально економічна для суб’єктів транзакцій, доступна розподілена інформаційна система, що має своєчасну, повну і достовірну інформацію про довіру, може створити умови для реалізації всіх переваг технологій ІР.

Все йде до необхідності відновлення в умовах розвитку технологій Інтернету історично раніше широко розповсюдженого способу здійснення транзакцій – “вдарили по руках” (handshake), коли суб’єкти без складання письмового договору простим рукостисканням здійснювали транзакції на багато мільйонів з практично нульовими ТВ. Настільки велика була сила репутації і довіри. Звичайно, відновлення способу “вдарили по руках” має буде здійснюватися на нових організаційних і технологічних принципах і рішеннях.

Таким чином, одним з можливих варіантів розв’язання проблеми довіри в умовах використання технологій ІР є створення РСД, що потребує широких досліджень в різних галузях знань, в тому числі, і в такій галузі як інформаційне право. Тому дослідження правових проблем, наприклад, пов’язаних з визначенням правових принципів побудови і функціонування РСД як інформаційної системи, визначення правових механізмів збору, використання і зберігання інформації про довіру, взаємодії РСД з іншими системами довіри і розгляду ймовірних спорів є дуже актуальними саме на порозі широкого впровадження технологій ІР.

Блокчейн. Авторитетний вчений Р. Меллон вважає, що технології блокчейн усувають необхідність в звичних економічних, правових і політичних інститутах, які в традиційній економіці виконують роль посередників довіри, оскільки усувають власне необхідність довіри, замінюючи її доказами [13].

На Світовому економічному форумі в Давосі (2015 р.) було дано таке визначення: блокчейн – нова технологія, яка усуває необхідність третіх осіб для забезпечення довіри до фінансових, договірних та виборних дій [14].

Існують інші, більш технократичні визначення, наприклад: блокчейн – це послідовна база даних інформації, яка захищена методами криптографічного доказу і пропонує альтернативу класичним фінансовим книгам [15]. Або, блокчейн – публічна база всіх здійснених транзакцій різного типу в рамках єдиної системи, які шикуються певним чином і з них формується ланцюжок блоків [16].

На думку експертів, блокчейн буде застосовуватися в найрізноманітніших сферах, таких як: грошові перекази, мікроплатежі, розумні контракти (або смарт-контракти), ідентифікація фізичних об’єктів і активів, державне управління, оборона і безпека, міжнародна діяльність тощо. В цілому, передбачається, що в майбутньому технології блокчейн можуть стати драйвером радикальних змін в широкому спектрі галузей, бізнес-моделей, соціальних і операційних процесів [17]. Тестування та впровадження технологій блокчейн розпочали в ряді країн і у багатьох великих корпораціях.

З одного боку, багато дослідників слідом за Д. Тапскоттом [20] підносять трансформаційний потенціал технологій блокчейн не тільки в бізнесі, але в багатьох інших сферах: політичній, державного управління, попередження корупції, освіті та культурі, захисту прав громадян тощо. З іншого боку, існує досить ґрунтовний скепсис щодо можливостей і перспектив використання технологій блокчейн [26]. Цілком очевидно, що крапку над “і” розставить історичний досвід і результати практичного використання цих технологій в різних додатках. Важливу роль в успіху цього досвіду буде відігравати наявність відповідного правового регулювання там, де це буде необхідно, що заздалегідь нівелює можливість виникнення юридичних бар’єрів на шляху використання можливостей технологій блокчейн.

З урахуванням того, що технологія блокчейн реалізується за допомогою комп’ютерних і програмних засобів, а функціонує на базі використання мережі Інтернет, то для нейтралізації можливих атак хакерів або недобросовісних дій з інформацією використовуються криптографічні засоби.

У технологічному сенсі блокчейн – однорангова комп’ютерна мережа, яка функціонує поверх мережі Інтернет, була представлена в жовтні 2008 року в рамках пропозиції щодо біткойну (віртуальної валютної системи), яка не потребувала централізованого управління емісією, юридичної передачі права власності та підтвердження транзакцій [18].

Дуже цікаве і реалістичне обґрунтування появи технологій блокчейн, що практично збігається з викладеним вище баченням про необхідність побудови РСД, викладено в роботі В.П. Купріяновского [19]. Автори вважають, що системи розрахунків в сучасній економіці базуються на ієрархічних кореспондентських відносинах банків з величезним числом посередників (в тому числі і на валютному ринку), що обумовлює:

- імітування інформаційного он-лайну за рахунок досить великого ланцюжка посередників, які страхують ризики один одного;
- високу вартість проведення платежів;
- ризики, пов’язані з поняттям операційного дня і можливими різними датами виконання платежів;
- ризики невиконання або оспорювання сторонами угоди проведених платежів;
- додаткової ліквідності для платіжних систем.

Нейтралізація всіх цих недоліків традиційними методами призводить до необхідності створення кваліфікованого фінансового посередника (довіреної третьої сторони: клірингові системи, депозитарії, системи передачі фінансової інформації типу Reuters або SWIFT). Однак, використання посередників призводить до чергового значного подорожчання і уповільнення розрахунків (міжнародні фінансові транзакції – до семи днів).

Таким чином, в банківській сфері констатуються серйозні протиріччя між сформованим традиційним бізнесом і сучасними інноваційними технологіями.

Вихід з цієї ситуації знайшли у використанні технології блокчейн, яка за визначенням не вимагає третіх осіб для реалізації функції посередника, що підтверджує інформацію про довіру до суб’єкта.

Наведемо опис технології блокчейна з роботи В.П. Купріяновского [19]. Блокчейн – це мережа, що складається з елементів (комп’ютери/суб’єкти), які називаються вузлом, кожен з яких містить (зберігає) ланцюжок блоків (книгу). Кожен блок містить набір транзакцій, здійснених з моменту закінчення формування попереднього блоку мережі до моменту складання цього блоку, розмір якого залежить від того, скільки транзакцій було завершено в заданий інтервал часу. Повідомлення про транзакції включає відомості про публічну адресу одержувача, вартості транзакції і криптографічного цифрового підпису, який доводить справжність транзакції. Вузли мережі, отримавши повідомлення від будь-якого іншого вузла, підтверджують справжність і дійсність повідомлення шляхом дешифрування цифрового підпису. Різні мережі блокчейнів використовують різні методи прийняття рішення про сумлінність транзакції і відсутність шахрайства. Новий блок одним з вузлів в мережі поміщається в оновлену версію книги (реєстру, бази даних), в якій містяться всі попередні блоки. Всі блоки блокчейна криптографічним методом пов’язані один з одним таким чином, що внести зміни в будь-який з них неможливо.

Технології блокчейн мають наступні основні властивості [16] в рамках певної мережі блокчейн, що об’єднує деяку обмежену сукупність суб’єктів:

- можливість зберігання інформації для кожної транзакції суб’єкта у вигляді незалежних записів;
- можливість зберігати для кожної транзакції різноманітну інформацію, наприклад, про права власності, звіти по кредитуванню, якість товарів і так далі;
- реєстр транзакцій не зберігається в певному місці, а розподіляється на тисячі комп’ютерів (суб'єктів) по всьому світу;
- наявність вільного доступу у суб’єктів до всього реєстру (книги) транзакцій.

Таким чином, блокчейн є публічною базою даних всіх транзакцій між суб’єктами мережі блокчейн. Оскільки мережа блокчейна відкрита для вільного приєднання, то публічність даних мережі фактично означає загальнодоступність цих даних.

Що дає технологія блокчейна людству? На думку сина і батька Тапскоттов, авторів фундаментальної роботи [20], вперше в історії дві сторони, які не знають і не довіряють одна одній, можуть безпосередньо вести бізнес та інші будь-які справи, оскільки перевірка особистості та встановлення довіри більше не є правом і привілеєм фінансового посередника. Більш того, в контексті фінансових послуг протокол довіри приймає подвійне значення. Блокчейн також може встановлювати довіру, перевіряючи особистість і потенціал будь-якого контрагента за допомогою комбінації минулої історії транзакцій (за блочним ланцюжком), показників репутації на основі узагальнених оглядів та інших соціально-економічних показників.

Спираючись на результати досліджень І. Марко і К. Лакхані [18], наведемо порівняльні характеристики 4-х фаз інноваційного розвитку використання (додатків) мережі Інтернет та блокчейна.

1. Одиничне застосування – додатки з невисокою новизною (електронна пошта і біткойн). Фактично це реалізація відомих інформаційних технологій на новій технологічній базі. Практична відсутність необхідності в координації.

2. Локалізація – додатки містять відносну новизну, розроблені в інтересах обмеженої кількості користувачів (електронний документообіг та облік поставок). Фактично це реалізація окремих етапів бізнес процесів на новій технологічній базі. Невисокі вимоги до рівня координації.

3. Заміщення – це суперпозиція двох перших фаз (одиничного і локалізованого застосування) і має відповідну технологічну новизну в інтересах необмеженої кількості користувачів (електронна торгівля і криптовалютні системи). Фактично це реалізація нових або модернізація бізнес процесів завдяки використанню нових технологій. Вимагає високого рівня координації, оскільки може охоплювати велику кількість галузей і сфер діяльності.

4. Трансформація – це абсолютно нові додатки, які мають потенціал для змін природи економічних, соціальних і політичних відносин (Інтернет речей і smart-контракти). Фактично це реалізація нових методів і способів системного ведення бізнесу, що повністю базуються на використанні нових технологій. Вимагає не тільки високого рівня координації, а й інституційної угоди щодо стандартів і процесів в економічній, соціальній, правовій та політичних сферах.

В даний час технології блокчейн найбільш широко використовуються в сегменті криптовалют. Аналіз досвіду такого використання дозволив виділити різні бар’єри на шляху застосування технологій блокчейн [17; 21; 22]: технологічні, економічні, соціальні та юридичні.

Передбачається, що один з основних технологічних бар’єрів поширення технологій блокчейн – це труднощі при масштабуванні блоку, пов’язані з тим, що кожен комп’ютер в мережі обробляє кожну транзакцію, буде подолано в найближчому майбутньому і це відкриє перспективи для використання технологій блокчейн в Інтернеті речей [23].

Що стосується юридичних бар’єрів, то в частині вирішення проблеми формування правового забезпечення широкого застосування технологій блокчейн з урахуванням результатів, отриманих в роботі [24] можна сформувати наступні завдання, що стоять перед правовою наукою, зокрема, перед інформаційним правом:

1. Систему правового регулювання застосування технологій блокчейн доцільно розробляти в парадигмі максимальної інтеграції в традиційну національну правову систему.

2. Для низки публічних додатків технологій блокчейн задля зниження ризиків необхідно визначення юридичного статусу мережі блокчейн, її реєстру і записів транзакцій, формування правових вимог до їх форми і змісту.

3. Визначення юрисдикції реєстру мережі блокчейн, в тому числі, при наявності транскордонних транзакцій.

4. Дослідження особливостей правовідносин, пов’язаних з технологіями блокчейн, юридичних прав, обов’язків і відповідальності сторін.

5. Дослідження проблеми визначення юридичних ризиків та обмежень використання технологій блокчейн в різних сферах застосування.

6. Формування правових механізмів нагляду, встановлення відповідальності за порушення прав суб’єктів мережі блокчейн і відшкодування завданих збитків або при наявності помилок в комп’ютерній програмі.

8. Вирішення правовими засобами проблеми наявності неповної спостережливості з боку суб’єктів мережі блокчейн всіх прихованих дій програмного забезпечення, що реалізує ту чи іншу функцію технології блокчейн, що може привести до небажаного збитку.

9. Розробка правових механізмів верифікації суб’єктів мережі блокчейн (в разі необхідності), які здійснюють транзакцію, на момент її здійснення.

10. Вирішення протиріччя між законодавчими вимогами обмеження доступу до персональних даних та іншої чутливої інформації суб’єктів мережі блокчейн, яка може міститися в реєстрі цієї мережі, і відкритістю інформації для всіх суб’єктів по всіх транзакціях та їх зберіганням в кожному вузлі мережі блокчейн.

11. Установити правову регламентацію забезпечення, перевірки і сертифікації (при необхідності) кібербезпеки як програмного забезпечення, що підтримує функціонування мережі блокчейн, так і програмно-апаратних платформ, на яких розміщується це програмне забезпечення.

12. Розробка пропозицій щодо процесуальних особливостей розгляду у суді суперечок, пов’язаних з мережами блокчейн.

Слід зазначити, що вимога практики щодо можливості проведення юридично значимої фіксації дій, пов’язаних з технологією блокчейн, починає враховуватися розробниками такої технології. Одна з компаній повідомляє, що їх блокчейн-середовище має основну відмінність від інших блокчейн-проектів в тому, що вона створювалася спочатку для реального сектора економіки з урахуванням юридично-значимих дій, які будуть визнаватися в судах, а не для тіньового бізнесу і обліку анонімних дій [25].

Спираючись на думку М. Сван [21] зауважимо, що технологія блокчейн на диво своєчасно з’явилася для того, щоб підтримати практичну реалізацію ідеї децентралізації,

втілення якої стало можливим завдяки широкому використанню Інтернет-технологій. Децентралізована модель може бути хорошими ліками від багатьох бід цивілізації, обумовлених надмірною концентрацією і централізацією, звільняючи від “закупорки” соціальні артерії практично в будь-яких сферах діяльності, які базуються на довірі.

Таким чином, сучасні приклади реалізації блокчейн проектів підтверджують принципову можливість технологічного забезпечення доступності, достовірності та своєчасності інформації про сумлінне та чесне здійснення будь-якої конкретної транзакції між будь-якими суб’єктами, що входять в деяку обмежену корпорацію. Однак, необхідно відзначити, що належить виконати ще багато технічної, соціальної і юридичної роботи протягом багатьох років для того, щоб ці технології були швидкодіючими, економічними і надійними в широкому використанні в різних сегментах людської діяльності.

Феноменально багатий емпіричний досвід для проведення аналізу і оцінки переваг і недоліків технологій блокчейн в останні роки дало широке впровадження і активне функціонування різних систем криптовалют, які базуються на використанні цих технологій.

Інтерес до тематики правового регулювання технологій блокчейн різко зростає в останні кілька років. Аналіз тільки однієї бази даних (Google Scholar):

– на кінець січня 2018 року – 16400 наукових досліджень, що містять ключове слово “blockchain”, з них майже 6 500 – за 2017 рік;

– на кінець січня 2018 року – близько 4400 робіт, що містять ключове слово “problems of legal regulation blockchain” (26,8 % від усієї кількості), з них майже 1900 – за 2017 рік (29,2 % від кількості).

Висновки.

1. У всьому світі розвиток технологій IP буде пов’язано з стрімким зростанням кількості нестійких горизонтальних транзакційних зв’язків, які вимагатимуть системи довіри до суб’єктів взаємовідносин.

2. Найбільш економічними, що мінімізують транзакційні витрати і забезпечують суб'єктів взаємовідносин своєчасною, повною та достовірною інформацією є розподілені системи довіри.

3. В даний час технології блокчейн формують найкращі технологічні умови побудови розподілених систем довіри для суб’єктів, що вступають в нестійкі горизонтальні транзакційні зв’язки в сфері IP.

4. Використання в майбутньому технологій блокчейн вимагатимє міждисциплінарних досліджень як власне розвитку та особливостей застосування цих технологій для різних додатків, так і спеціальних питань, пов’язаних з визначенням стратегій і соціальних наслідків їх застосування, цілісністю і повнотою даних, захистом приватності, конфіденційністю, кібербезпекою і багато інших, в тому числі, і досліджень правових проблем.

5. У сфері права застосування як технологій IP, так і технологій блокчейн в публічних або загальносуспільних сферах неминуче спричинить необхідність досліджень, як мінімум, питань встановлення та розподілу юридичної відповідальності у разі настання небажаних наслідків або визначення правових умов недопущення або відновлення порушених прав учасників відповідних суспільних відносин, а також багатьох інших, які неминуче виникнуть при використанні публічних і приватних мереж блокчейн.

6. Найкращою стратегією майбутніх правових досліджень було б орієнтування на створення таких правових конструкцій, які б максимально інтегрувалися в традиційну національну і міжнародну правові системи.

7. Своєчасно вжиті юридичною науковою спільнотою зусилля можуть дозволити отримати попереджувальні наукові результати і практичні рекомендації щодо правового регулювання суспільних відносин, що сприятиме широкому визнанню, швидкому впровадженню і поширенню прогресивних досягнень чергової технологічної революції, в тому числі, технологій Інтернету речей і технологій блокчейн.

Використана література

1. Баранов А.А. Интернет : объект правоотношений и предмет регулирования : монография / А.А. Баранов. – К. : Ред. журн. “Право Украины”, 2013. – 144 с.

2. Прогресс, достигнутый в осуществлении решений и последующей деятельности по итогам Всемирной встречи на высшем уровне по вопросам информационного общества на региональном и международном уровнях : доклад Генерального секретаря ООН. Генеральная Ассамблея. Экономический и Социальный Совет, 28 июля 2016 года – 27 июля 2017 года. – URL : http://unctad.org/en/PublicationsLibrary/a71d67_ru.pdf

3. A policy framework for an open and trusted Internet. An approach for reinforcing trust in an open environment. Internet Society (ISOC), 22 June 2016. – URL : https://www.internetsociety.org/ resources/doc/2016/policy-framework-for-an-open-and-trusted-internet

4. Global Internet Report 2016. The Economics of Building Trust Online: Preventing Data Breaches. Internet Society (ISOC), 2016. – URL : https://www.internetsociety.org/globalinternetreport /2016/#first-d

5. A policy framework for an open and trusted Internet. An approach for reinforcing trust in an open environment. Internet Society, 22 June 2016. – URL : https://www.internetsociety.org/resour ces/doc/2016/policy-framework-for-an-open-and-trusted-internet/

6. Баранов О.А. “Інтернет речей” як правовий термін // Юридична Україна. – 2016. – № 5-6. – С. 96-103. – Режим доступу : http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis _64.exe? C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name= PDF/ur ykr_2016_5-6_16.pdf

7. Ананьин В.И. Трансакционные издержки и информационные технологии / Intelligent Enterprise. – 2002. – № 13. – Режим доступу : https://www.iemag.ru/analitics/detail.php?ID=15908

8. Толковый словарь русского языка ; под ред. Д.Н. Ушакова. – М. : Гос. ин-т “Сов. энцикл.”; ОГИЗ; Гос. изд-во иностр. и нац. слов., 1935-1940. – 4 т. – Режим доступу : https://dic.academic.ru/dic.nsf/ushakov/790118

9. Marc-David L. Seidel. Questioning Centralized Organizations in a Time of Distributed Trust. January 2018. / Journal of Management Inquiry 27(1). – URL : https://www.researchgate.net/public ation/319872986_Questioning_Centralized_Organizations_in_a_Time_of_Distributed_Trust

10. Marc-David L. Seidel. Centralized Organization and Distributed Trust. October 27, 2017. – URL : https://managementink.wordpress.com/2017/10/27/centralized-organization-and-distributed-trust

11. Коуз Р. Природа фирмы ; под ред. О. Уильямсона и С. Уинтера. – М. : Дело, 2001.

12. Капелюшников Р.И. Новая институциональная теория. – Режим доступу : http://www. libertarium.ru/10625.

13. Robert Mellen. Critical review of “The Truth About Blockchain” / Harvard Business Review. Feb. 2017. – URL : https://www.linkedin.com/pulse/critical-review-truth-blockchain-harvard-business -feb-robert-mellen

14. Deep Shift – Technology Tipping Points and Societal Impact (2015) / World Economic Forum Survey Report. – URL : https://www.weforum.org/reports/deep-shift-technology-tipping-points -and-societal-impact

15. David Yermack. Corporate Governance and Blockchains. Review of Finance, Volume 21, Issue 1, 1 March 2017. Pages 7–31. – URL : https://doi.org/10.1093/rof/rfw074

16. Что такое технология блокчейн (Blockchain)? 04.09.2017. – Режим доступу : https://www.allcrypt onews.com/chto-takoe-tehnologiya-blokchejn-blockchain

17. Цветкова Л.А. Перспективы развития технологии блокчейн в России : конкурентные преимущества и барьеры / Экономика науки. – 2017. – Т. 3. – № 4. – С. 275-296. DOI:10.22394 /2410-132X-2017-3-4-275-296

18. Iansiti Marco, Karim R. Lakhani. The Truth about Blockchain /. Harvard Business Review 95, no. 1 (January – February 2017). P. 118-127. – URL : https://hbr.org/2017/01/the-truth-about-blockchain

19. Цифровые цепи поставок и технологии на базе блокчейн в совместной экономике / [В.П. Куприяновский, С.А. Синягов, А.А. Климов, А.В. Петров, Д.Е. Намиот] / International journal of open information technologies. – 2017.– Т. 5. –№ 8. – С 80-95. – URL : http://injoit.org/ index.php/j1/article/download/473/445

20. Tapscott Don, Tapscott Alex. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Portfolio/Penguin, 2016. – 368 p. – URL : http://dontaps cott. com/books/blockchain-revolution

21. Melanie Swan. Blockchain : Blueprint for a New Economy. O'Reilly Media, Inc., 2015. – P. 129. – URL : https://www.twirpx.com/file/1671876

22. Mitsu Fonseca. The impact of blockchain on legal environment. October 16, 2017. – URL : https://irishtechnews.ie/the-impact-of-blockchain-on-legal-environment

23. Vinay Gupta. A Brief History of Blockchain. Harvard Business Review. February 28, 2017. – URL : https://hbr.org/2017/01/the-truth-about-blockchain

24. Баранов О.А. Інтернет речей (IoT) : правові проблеми застосування розумних контрактів // Інформація і право. – № 4(23)/2017. – С. 26-40. – Режим доступу : http://ippi.org.ua/ jpage/76

25. Компания “Aronicle”. 2018. – URL : http://datachains.world/bc3base/index

26. Kai Stinchcombe. Ten years in, nobody has come up with a use for blockchain. Dec 22, 2017. – URL : https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee 98c180100

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

УДК 340.5

КОСТЕНКО О.В., головний науковий співробітник Інституту спеціальної техніки та судових експертиз Служби безпеки України

КОМПРОМЕТАЦІЯ ОСОБИСТОГО КЛЮЧА ЕЛЕКТРОННОГО ПІДПИСУ: ПРАВОВИЙ АСПЕКТ

Анотація. *Статтю присвячено дослідженню поняття компрометації особистого ключа електронного підпису, правовим аспектам компрометації в контексті теорії права. У роботі наведено поняття явної і неявної компрометації та межі їх дії, а також правові наслідки компрометації.*

Ключові слова: *компрометація, особистий ключ, підписувач, електронний підпис.*

Summary. *The article is devoted to the study of the concept of compromising the personal key of digital signature, the legal aspects of compromise in the context of the theory of law. The paper presents the concept of explicit and implicit compromise and the limits of their actions, as well as the legal consequences of compromise.*

Keywords: *compromise, personal key, signer, digital signature.*

Аннотация. *Статья посвящается исследованию понятия компрометации личного ключа электронной подписи, правовым аспектам компрометации в контексте теории права. В работе представлены понятия явной и не явной компрометации, их границы, а так же правовые последствия компрометации.*

Ключевые слова: *компрометация, личный ключ, подписчик, электронная подпись.*

Постановка проблеми. Значущим фактором сьогодення є стрімкий розвиток політичних, економічних, наукових, бізнесових, торгівельних, інформаційних відносин які безпосередньо впливають не тільки на міжнародний стан, а й на відповідні процеси у конкретних країнах, а також на здійснення прав, задоволення інтересів і потреб їх громадян та державних інституцій. Однією з основних вимог при реалізації цих відносин є швидкий обмін інформацією, відображеною в цифровому вигляді, забезпечення її актуальності, надійності, цілісності, оперативності, ідентичності, достовірності і повноти.

Потужні інформаційні комп’ютерні технології створюють нові можливості за рахунок використання цифрової інформації (даних), що, в свою чергу, створює нові суспільні відносини, які виникають між суб’єктами правовідносин під час: електронного обміну інформацією (Electronic Data Interchange); електронного руху капіталу (Electronic Funds Transfer); електронної торгівлі (e-Trade); використання електронних грошей (e-cash); електронного маркетингу (e-market); електронного банкінгу (e-banking); електронної системи здоров’я (e-health) та в інших в сферах. Обмін інформацією здійснюється в процесі електронних транзакцій у формі електронних (цифрових) документів. Надійність інформації під час обміну забезпечується завдяки застосуванню довірчих електронних послуг, а вимоги достовірності і цілісності інформації – завдяки застосуванню алгоритмів цифрового криптографічного захисту із використанням технології електронного підпису. Однак, широке застосування цієї технології водночас виявило й правові проблеми, пов’язані із використанням особистого ключа електронного підпису. Однією із таких проблем є правова невизначеність дефініції “компрометація” особистого ключа електронного підпису.

Якнайшвидше урегулювання проблеми правової невизначеності дефініції “компрометація” та своєчасне реагування права на ризики, які виникають або зумовлені компрометацією особистого ключа електронного підпису, є наразі актуальною проблемою.

Результати аналізу наукових публікацій. Питанням правового регулювання суспільних відносин, пов’язаних з використанням електронного підпису займались такі вітчизняні вчені: Козіел Г., Петрицький А., Плескач В., Пономаренко Л., Шпірко А., Янчева Л., Локшин А. та ін. Серед іноземних вчених дану тему досліджували: Масон С., Тірі А., Венбо М., Петров А., Беззубцев О. За останні роки питання створення надійних механізмів визнання електронних підписів порушували такі науковці: Перевозчикова О.Л., Бєлов С.В., Горбенко І.Д., Потій О.В., Погорелов Б.А., Мелащенко А.О. Проблема компрометації в контексті компрометації особистого ключа електронного підпису в Україні висвітлювалась переважно в технічному аспекті. Так, у статті Бєлова С.В. “Моделі побудови національної інфраструктури центрів сертифікації ключів та їх ризики” висвітлюються виключно наслідки компрометації електронного підпису [1], а в публікації Погорелова Б.А. “Щодо визначення основних криптографічних понять” наголошено на нейтралізації загроз компрометації для системи управління електронними ключами [2].

Разом з тим, на даний час недостатньо теоретичних праць та досліджень в комплексі питань, які визначають дефініцію “компрометація” особистого ключа електронного підпису.

Метою статті є визначення правових проблем, пов’язаних із визначенням дефініції “компрометація”, як елемента понятійного апарату в чинному законодавстві, а також пропозиції щодо формулювання дефініції “компрометація особистого ключа”.

Виклад основного матеріалу. Перш ніж перейти до дослідження дефініції “компрометація особистого ключа” розглянемо історію виникнення самого терміну “компрометація” в правовій моделі суспільно-правових відносин, що регулюють сферу використання підпису.

Розвиток телекомунікаційних технологій сприяв виникненню механізмів обміну між користувачами документами в електронній формі, які мають юридичну значимість. Потреба в використанні та обміні такими документами була настільки високою, що багато країн майже одночасно прийняли спеціальні закони, що регулювали основи електронної торгівлі та застосування електронних підписів. Так, Європейським Парламентом та Радою 13 грудня 1999 року прийнято Директиву “Про систему електронних підписів, що застосовується в межах Співтовариства”, у США введено Закон “Про електронні підписи в глобальній і національній комерції”, Францією затверджено Декрет “Про електронний підпис”, Німеччиною прийнято Федеральний закон “Про цифрові підписи”.

Однак на той час ні в України, ні у більшості країн не було практичного досвіду побудови систем електронних підписів як в організаційному, так і в правовому аспекті. Багато національних законів розроблялись як моделі загальних правил використання електронних підписів. Практичне застосування вказаних законодавчих актів виявило низку неврегульованих нормами права суспільних відносин, пов’язаних з використанням електронного підпису, в тому числі, з відсутністю чіткої дефініції поняття “компрометація особистого ключа”.

Слід зауважити, що необхідність створення нової дефініції “компрометація особистого ключа” зумовлена наявністю таких причин.

По-перше, міжнародні законодавчі норми в галузі електронного підпису не мають чітких, загальноприйнятих визначень поняття “компрометації”. Термін “компрометація”, в контексті “компрометація електронного підпису”, застосовано у Типовому законі

ЮНСІТРАЛ “Про електронні підписи і керівництво із прийняття рішень” [3], прийнятого у Відні 5 липня 2001 року на 34-й сесії ЮНСІТРАЛ, статтею 57 якого поняття “ненадійний сертифікат” трактується як такий, особистий ключ якого “скомпрометовано” в наслідок втрати підписувачем контролю над ним. У США поняття “компрометація” визначено Національним інститутом стандартів і технологій (National Institute of Standards and Technology – NIST) як “неавторизоване розкриття, модифікація, заміщення або використання конфіденційних даних (включаючи криптографічні ключові тексти та інші дані Центру політики безпеки (CSP)” [4] або “неавторизоване розкриття, модифікація, заміщення або використання конфіденційних даних (наприклад, ключів, метаданих та іншої інформації, що стосується безпеки)” [5; 6].

По-друге, вітчизняне законодавство також по-різному трактує дефініцію “компрометація”. Так, пунктом 26 статті 1 Закону України “Про електронні довірчі послуги” визначено, що “компрометація особистого ключа – будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа” [7]. Однак, таке ж саме тлумачення містив і попередній Закон України “Про електронний цифровий підпис”. На жаль, таке визначення з одного боку не надає визначення які саме об’єкти або суб’єкти правових відносин вчиняють вказані вище дії та які саме дії/події призводять до несанкціонованого використання особистого ключа, а з іншого боку невизначеність дефініції створює підстави для довільного трактування вказаної норми закону.

В той же час, українські технічні спеціалісти в галузі захисту інформації запровадили кілька варіантів визначення “компрометація”, як технічного терміну. Так, Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України у 1999 році при створені НД ТЗІ 1.1.-003-99 “Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу“” застосовано термін “компрометація” (compromise) – як порушення політики безпеки; несанкціоноване ознайомлення” [8]. Дане визначення спрямоване на врегулювання деструктивних подій в системі безпеки, пов’язаних із порушенням чітких правил використання цифрових підписів. Проте, таке визначення не поширюється на відносини, що відбуваються із використанням особистого ключа поза межами визначеними політикою безпеки, а самі політики безпеки можуть суттєво різнитися. Також, така дефініція не пояснює визначення “несанкціоноване ознайомлення”.

Крім того, наказом Державної служби спеціального зв’язку та захисту інформації України “Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису” від 20.07.07 р. № 141 визначено більш розширене поняття компрометації – як будь-який випадок (втрата, розголошення, крадіжка, несанкціоноване копіювання тощо) з ключовими документами (ключовими даними) та засобами криптографічного захисту інформації, який призвів (може призвести) до розголошення (витоку) інформації про них, а також інформації, яка обробляється та передається [9]. Без сумніву, це найбільш вдале визначення “компрометації”, яке доцільно покласти в основу дефініції “компрометація особистого ключа” та закріпити на рівні законодавчого акта, що сприятиме чіткому застосуванню норм права.

По-третє, в українському законодавстві склалася ситуація, коли відсутність дефініції “компрометація особистого ключа” в суспільних відносинах, які регулюють сферу використання електронних ключів, позбавила право ясності та конкретики, ускладнивши процес його застосування, що зменшило довіру до електронних

документів та правочинів, які вчинили за допомогою електронних підписів, про що свідчить судова практика.

За останні роки збільшилася кількість правопорушень та злочинів, пов’язаних саме із компрометацією та незаконним використанням особистих ключів електронних підписів. Переважна більшість злочинів із використанням особистого ключа електронного підпису скоєні внаслідок явної компрометації особистого ключа самим підписувачем. Саме підписувачі створюють умови для компрометації особистого ключа й подальшого його незаконного використання. Здебільшого такі злочини здійснюються в банківській сфері, а також в галузі нотаріату та реєстрації юридичних осіб. Прикладом є низка кримінальних справ, фігуранти яких, будучи банківськими працівниками, нехтували правилами політик банківської безпеки, під різними приводами заволодівали особистими ключами цифрових підписів своїх колег або підлеглих та організували схеми незаконного заволодіння коштами клієнтів банків [10; 11]. Має місце практика компрометації особистого ключа нотаріуса або реєстратора під час вчинення правочинів. Так, непоодинокі випадки компрометації через неналежне зберігання та заволодіння особистим ключем нотаріуса або реєстратора, які призводять до незаконного відчуження майна та власності шляхом втручання в роботу Єдиного державного реєстру речових прав на нерухоме майно та Єдиного державного реєстру юридичних осіб та фізичних осіб-підприємців [13]. Також мають місце випадки заволодіння сторонніми особами особистими ключами керівників підприємств та головних бухгалтерів або отримання таких ключів в Акредитованих центрах сертифікації ключів за підробленими довіреностями з подальшим вчиненням фінансових злочинів [14].

По-четверте, специфічні проблеми надання послуг в галузі електронного підпису, пов’язані із компрометацією особистого ключа, полягають у достатньо складній структурі та видах компрометації.

У зв’язку із невизначеністю дефініції пропонується поділяти “компрометацію особистого ключа” на явну та неявну компрометацію.

Розглянемо вказані види компрометації.

Явною компрометацією особистого ключа слід вважати втрату доступу до інформації особистого ключа, що гарантовано підтверджується наявними фактами порушень політики безпеки та несанкціонованого ознайомлення із ключовою інформацією.

В свою чергу, явну компрометацію можливо розподілити на:

− компрометацію, що відбулася за участю або з волі підписувача;

− компрометація, яка здійснена третіми особами без відома підписувача.

Так, до явної компрометації особистого ключа, що відбулася за участю або за волею підписувача, слід віднести наступні фактори:

− втрата (викрадення) ключових носіїв, втрата ключів (кодів) від сейфів у момент зберігання в них ключових носіїв та втрата ключів (кодів) із наступним їх знаходженням;

− свідома або шляхом зловживання довірою передача особистого ключа сторонній особі;

− порушення встановлених в організації правил використання і зберігання особистих ключів, розголошення мережних паролів, паролів криптозахисту, правил зберігання та знищення (після закінчення терміну дії) особистого ключа, а також вимог зберігання пароля або PIN-коду до особистого ключа;

− зберігання особистого ключа у відкритому, незашифрованому вигляді, безпосередньо на HDD ПЕОМ користувача;

− компрометація особистого ключа, яка здійснена третіми особами без відома підписувача та доступ сторонніх осіб до ключової інформації;

− порушення цілісності печаток на сейфах із ключовими носіями у разі якщо застосовується процедура опечатування сейфів;

− доступу до ключових носіїв шляхом несанкціонованого копіювання;

− викрадення особистого ключа внаслідок відповіді на запит, надісланий із ознаками шахрайства або підробки;

− виготовлення особистого ключа за підробленими документами [15; 16].

На відміну від явної компрометації особистого ключа, неявна компрометація базується на припущеннях або версіях подій, що створили або створюють умови компрометації особистого ключа із використанням сторонніми особами технічних засобів, програмного забезпечення тощо. До неявної компрометації можливо віднести:

− виникнення підозри на витік інформації щодо ключових даних;

− випадки, коли неможливо достовірно встановити, що саме відбулося з ключовими носіями (в тому випадку коли ключові носії вийшли з ладу і доказово не спростовують можливість того, що даний факт відбувся в результаті неконтрольованих дій сторонніх осіб);

− будь-які інші події, які дають привід вважати, що ключова інформація стала відома або доступна стороннім особам;

− перехоплення спеціальними технічними засобами звукової інформації, електромагнітного або радіовипромінювання комп’ютерів, на яких оброблюється інформація із застосуванням особистих ключів;

− перехоплення спеціальними технічними засобами, спеціалізованим або шпигунським програмним забезпеченням інформації, яка циркулює в Інтернет або локальній мережі, в яких оброблюється інформація із застосуванням особистих ключів [16; 17].

По-п’яте, неявна компрометація із застосуванням технічних методів та пристроїв несанкціонованого доступу до особистих ключів підписувачів на сьогодні більш обмежена у протиправних можливостях через доволі складний механізм криптозахисту даних. Світове наукове товариство періодично демонструє можливості технічного, знеособленого доступу до ключів особистого електронного підпису. Так, група вчених з Японії, Швейцарії, Нідерландів та США, успішно здійснили технічний доступ до даних, зашифрованих за допомогою криптографічного ключа [18]. Відомий криптограф Аді Шамір розробив метод технічного доступу та відтворення особистого ключа шляхом акустичного криптоаналізу без явного фізичного втручання в телекомунікаційні мережі та системи [19].

По-шосте, проблеми пов’язані із складністю надання правознавцями оцінки правових наслідків компрометації особистого ключа в період між реальним фактом компрометації та фактом її офіційного оголошення, із наступним блокуванням або скасуванням сертифікату особистого ключа. Саме протягом такого періоду існує ймовірність застосування скомпрометованого особистого ключа для вчинення дій, що мають юридичні наслідки.

Розглянемо перебіг подій у часі, який умовно поділимо на п’ять періодів від початку компрометації особистого ключа до усунення наслідків його компрометації.

Перший період – це час коли компрометація особистого ключа відбулася але підписувач не має підозри та фактів явної або неявної компрометації. Цей період найскладніше зафіксувати процесуально і правові наслідки, які створює цей період скомпрометований особистий ключ, мають статус офіційних та таких, що має низьку вірогідність визнання їх в подальшому недійсними, через недостатню доказову базу, яка зазвичай базується на припущеннях [20].

Другий період характерний тим, що у підписувача, за результатом суб’єктивного аналізу певних фактів або подій, формується підозра щодо можливості компрометації особистого ключа.

Наступний період характеризується необхідністю прийняти рішення підписувачем щодо оголошення компрометації особистого ключа. Третій період може тривати від кількох хвилин до кількох діб. Це обумовлено наступними факторами: прийняттям рішення щодо компрометації користувачем, у разі якщо електронний підпис використовувався для роботи з ресурсами, що не несуть юридичних ризиків та потребує незначного часу. Натомість, прийняття рішення щодо компрометації особистого ключа, який постійно використовується для роботи в реєстрах або групи ключів, що забезпечують функціонування інформаційно-обчислювальних систем та мереж установи, потребує аналізу ситуації та розрахунку часу для заміни ключів та відновлення роботи систем. В органах державної влади або місцевого самоврядування прийняття рішення щодо оголошення компрометації особистих ключів може тривати декілька днів.

Оголошення компрометації здійснюється під час четвертого періоду. Законодавство передбачає процедуру оголошення про компрометацію шляхом звернення до Акредитованого центру сертифікації ключів із заявою про компрометацію, яка передається будь-якими технічними засобами комунікацій. Останній період передбачено Законом України “Про довірчі послуги” і він не повинен перевищувати 2 години, протягом яких сертифікат ЕЦП блокується або скасовується [7].

Аналізуючи етапи компрометації від реального факту компрометації та факту офіційного блокування або скасування сертифікату особистого ключа електронного підпису, можемо стверджувати, що найбільшому ризику піддаються дії із особистим ключем, які здійснюються в перший період, оскільки можливість збору доказової бази щодо вчинення суспільно небезпечного діяння із використанням скомпрометованого особистого ключа має низьку вірогідність.

По-сьоме, на сьогодні в законодавстві поняття компрометації особистого колюча електронного підпису фактично не має чіткого визначення та переліку подій або підстав, що дають можливість беззаперечно вважати їх компрометаційними, і, відповідно, базовими “маяками” для правознавців, які сьогодні оцінюють прецеденти порушення законодавства, пов’язані із використанням особистого ключа електронного цифрового підпису виключно в контексті статей 361-363 Кримінального кодексу України. Диспозиції цих статей визначають, що особистий ключ підписувача можливо класифікувати як предмет або знаряддя злочину, як технічний засіб несанкціонованого втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку [21].

В той же час, дії або бездіяльність підписувача, які призвели до компрометації особистого ключа електронного підпису, як і поняття “компрометації особистого ключа”, поки що не знайшли правової оцінки. Відсутність переліку базових ознак компрометації особистого ключа електронного підпису створює неоднозначність трактування правоохоронними органами, судами та адвокатурою ознак злочинів, що вчинені із використанням електронного підпису, що, в свою чергу, створює умови для уникнення від покарання.

Отже, дефініція “компрометація” в нині діючому законодавстві – це фактично розпливчатий термін, для якого можуть виникати пограничні випадки, у яких може бути незрозумілим чи допустиме використання терміну, чи ні. Тому слід розширити встановлену практику використання дефініції “компрометація”, щоб зробити термін

менш розпливчастим та більш інформативним, врахувати поняття явної та неявної компрометації, що сприятиме більш якісному застосуванню норм права.

Без сумніву, існуючі проблеми в правовій моделі суспільно-правових відносин, що регулюють сферу використання електронного підпису, формують в цілому недовіру до законодавства в сфері електронного підпису, пов’язану саме із невизначеністю дефініції “компрометація”, створюють сумнів щодо надійності електронних підписів, цілісності електронних документів, підписаних ними, достовірності правочинів, вчинених нотаріусами та державними реєстраторами в електронному вигляді, незмінності інформації, внесеної в Єдиний державний реєстр речових прав на нерухоме майно та Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців, надійності угод та договорів, укладених в електронній формі тощо.

Зважаючи на наявну неврегульовану нормами права проблему суспільних відносин, пов’язану з використанням електронного підпису, вважається за доцільне запровадити дефініцію “компрометація особистого ключа електронного підпису” та викласти її в наступній редакції:

Компрометація особистого ключа електронного підпису – будь-яка явна або неявна подія та/або дія (втрата, розголошення, крадіжка, несанкціоноване копіювання тощо) з даними особистого ключа електронного підпису та засобами криптографічного захисту інформації, що призвела або може призвести до несанкціонованого розголошення, зміни, знищення, блокування, перехоплення, копіювання та використання особистого ключа електронного підпису, а також інформації, яка обробляється та передається за його допомогою.

Явною компрометацією особистого ключа електронного підпису є втрата доступу до інформації особистого ключа, за участю або бездіяльністю підписувача або третіх осіб без застосування технічних засобів.

Неявною компрометацією особистого ключа електронного підпису є втрата доступу до інформації особистого ключа електронного підпису із застосуванням будь-яких технічних засобів без участі підписувача.

Дане визначення містить загальну норму компрометації та два деталізованих визначення явної та неявної компрометації. Такий підхід дозволить здійснювати більш якісну кваліфікацію суспільно небезпечних протиправних дій із використанням особистого ключа електронного підпису.

Варто зазначити, що злочин, як і будь-яке інше правопорушення, є вчинком людини. Але на відміну від інших вчинків людини злочин за своєю соціальною сутністю є посяганням на ті відносини, що склалися в суспільстві, відображають його найбільш важливі інтереси, внаслідок чого охороняються законом. Компрометацію особистого ключа електронного підпису слід розглядати саме як свідомий вольовий вчинок людини, який виражений у конкретній дії або бездіяльності. Суспільна небезпечність компрометації особистого ключа електронного підпису, як матеріальна ознака злочину полягає в тому, що діяння чи бездіяльність заподіює шкоду відносинам, які охороняються законом, або містить у собі реальну можливість заподіяння такої шкоди. Це – об’єктивна властивість злочину, реальне порушення відносин, що склалися в суспільстві в сфері електронного підпису. Значення суспільної небезпечності компрометації особистого ключа електронного підпису як матеріальної ознаки злочину полягає в тому, що вона, по-перше, є основним об'єктивним критерієм визнання діяння злочином; по-друге, дозволяє дати класифікацію злочинів за ступенем тяжкості; по-третє, визначає межу між злочином та іншими правопорушеннями; по-четверте, є однією з загальних засад індивідуалізації відповідальності і покарання [22].

Крім того, визначення “явна компрометація” сприятиме можливості надання юридичної оцінки вчинкам як підписувача, власника особистого ключа, так і третім особам, які ним заволоділи та несанкціоновано використовують. В той же час, використання поняття “неявна компрометація” дозволить детальніше класифікувати суспільно-небезпечні діяння, які скоюють стосовно особистого ключа підписувача або із його використанням в контексті статей 361-363 Кримінального кодексу України, які регулюють суспільні відносини у сфері інформаційної діяльності, в тому числі і електронного підпису, та окреслюють особливий вид злочинів, пов’язаних із незаконним використанням сучасних інформаційних технологій і засобів комп’ютерної техніки. Компрометацію особистого ключа електронного підпису слід відносити до зазначених в законі наслідків вчинення злочинів, передбачених ст. 361-363 Кримінального кодексу України – витоку, втрати, підроблення, блокування інформації, спотворення процесу її обробки або порушення встановленого порядку її маршрутизації [23].

Пропонуємо дефініцію “компрометація особистого ключа” у запропонованій редакції внести до пункту 26 статті 1 Розділу І Закону України “Про електронні довірчі послуги”.

Висновки.

Враховуючи проаналізовані підходи до визначення компрометації особистого ключа, її види та характерні ознаки, можливо зробити висновок, що відсутність законодавчого врегулювання такого суспільно небезпечного діяння як “компрометація особистого ключа” в сфері права впливає на стабільність інформаційних ресурсів держави та їх безпеку.

Отже, забезпечуючи чіткість законодавчої мови та визначеність правових норм нова законодавча дефініція “компрометація особистого ключа електронного підпису” сприятиме правовому регулюванню суспільних відносин, пов’язаних з використанням електронного цифрового підпису, чіткій класифікації злочинів та правопорушень, вчинених із використанням особистого ключа електронного підпису, а також підвищить довіру до надійності електронних документів підписаних ними, електронних сервісів, угод та договорів, укладених в електронній формі із використанням електронного підпису, стимулюватиме розвиток транскордонної електронної торгівлі та послуг.

Використана література

1. Бєлов С.В., Мартиненко С.В. Моделі побудови національної інфраструктури центрів сертифікації ключів та їх ризики. – Режим доступу : http://www.itsway.kiev.ua/pdf/Model-CA_ Risks.pdf

2. Погорелов Б.А., Черемушкин А.В., Чечета С.И. Об определении основных криптографических понятий : материалы конференции [“Математика и безопасность информационных технологий”], (г. Москва, МаБИТ-03, 23-24 октября 2003 г.). – М. : МГУ, 2003.

3. Типовой закон ЮНСИТРАЛ об электронных подписях. – Режим доступу : http://zakon 0.rada.gov.ua/laws/show/995_937

4. FIPS PUB 140-2. Security Requirements for Cryptographic Modules // Federal Information Processing Standards Publication 140-2, U.S. Department of Commerce, 05/2001.

5. Recommendation for Key Management. Special Publication 800-57, Part 1 Rev. 3, NIST, 05/2014.

6. NIST SP 800-130. A Framework for Designing Cryptographic Key Management Systems. – Режим доступу : http://nvlpubs.nist.gov/nistpubs/SpecialPublications/ NIST.SP.800-130.pdf

7. Про довірчі послуги : Закон України від 05.10.17 р. № 2155-VIII. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2155-19

8. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу : Наказ ДСТСЗІ СБУ від 28.04.99 р. № 22. – Режим доступу : http://www.dsszzi.gov.ua/dsszzi/control/uk/doccatalog/list?currDir=41640

9. Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису : Наказ ДССЗЗІ України від 20.07.07 р. № 141. – (Зареєстрований Міністерством юстиції України від 30.07.07 р. № 862/14129). – Режим доступу : http://zakon2.rada.gov.ua/laws/show/z0862-07

10. Постанова Ленінського районного суду м. Кіровограда від 19.10.11 р. у справі № 1-463/11. – (Єдиний державний реєстр судових рішень). – Режим доступу : http://www.reyestr.court.gov.ua/Review/20422029

11. Розслідування 12016040730000533. – (Єдиний державний реєстр судових рішень). – Режим доступу : http://www.gp.gov.ua/ua/erdr.html

12. Ухвала Івано-Франківського міського суду Івано-Франківської області від 09.03.17 р. у справі № 344/3171/17. – (Єдиний державний реєстр судових рішень). – Режим доступу : http://www.reyestr.court.gov.ua/Review/65214508

13. Ухвала Печерського районного суду м. Києва від 14.03.17 р. у справі № 757/10916/16-к. – (Єдиний державний реєстр судових рішень). – Режим доступу : http://www.reyestr.court.gov.ua/Review/56854252

14. Kleinjung T., Aoki K., Franke J., Lenstra A.K., Thome E., Bos J.W., Gaudry P., Kruppa A., Montgomery P.L., Osvik D.A., H. te Riele, Timofeev A., Zimmermann P. Factorization of a 768-bit RSA modulus, version 1.4, February 18, 2010. – Режим доступу : https://eprint.iacr.org/2010/006.pdf

15. Инструкция по работе со средствами криптографической защиты информации, сертификатами ключей подписи, открытыми и закрытыми ключами электронной подписи. : Приложение № 17 к постановлению администрации Хабаровского муниципального района от 14.04.17 р. № 808. – Режим доступу : khabrayon.ru/sites/default/files/2016/05/808_14.04.2017_p 17.rtf

16. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи. – Режим доступу : www.dsyst.com/files/security-manual.doc

17. Инструкция по обеспечению безопасности эксплуатации сертифицированных средств криптографической защиты информации (СКЗИ). – Режим доступу : www.aksicom.ru/content /istr_skzi.pdf.

18. Pellegrini A., Bertacco V., Austin T. Fault-Based Attack of RSA Authentication. – Режим доступу : https://web.eecs.umich.edu/~taustin/papers/DATE10-rsa.pdf

19. Genkin D., Shamir A., Tromer E. RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. – Режим доступу: http://www.tau.ac.il/~tromer/papers/acoustic-20131218.pdf

20. Mike Just, Paul C. van Oorschot Addressing the Problem of Undetected Signature Key Compromise. – Режим доступу : http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.26.507&rep=rep1&type=pdf

21. Кримінальний кодекс України : Закон України від 05.04.01 р. № 2341-III // Відомості Верховної Ради України (ВВР). – 2001. – № 25-26. – Ст. 131.

22. Кримінальне право України : загальна частина : підручник / [М.І. Бажанов, Ю.В. Баулін, В.І. Борисов та ін.] ; за ред. проф. М.І. Бажанова, В.В. Сташиса, В.Я. Тація. – [2 е вид., перероб. і допов.]. – К. : Юрінком Інтер, 2005. – 480 с.

23. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), автоматизованих систем та комп’ютерних мереж і мереж електрозв’язку. – Режим доступу : http://www.scourt.gov.ua/clients/vsu/vsu.nsf/(documents) /AFB1E90622E4446FC2257B7 C00499C02

~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~

УДК 340:007

РАФАЛ КАНІЯ (Rafał Kania), Ph. D., декан факультету адміністрації,
Коледж університету імені Павла Влодковіца, Плоцк, Польща

РОЗВИТОК ПРАВОВОЇ КІБЕРНЕТИКИ У ПОЛЬЩІ В XX-му СТОРІЧЧІ

Анотація. *У другій половині XX століття активізувались правові дослідження в Польщі. Зокрема, було здійснено спробу використати для вивчення правових проблем інструменти, що надані кібернетикою. Головною метою статті є стисла презентація основних положень та зв'язку між кібернетикою та правом у польській науковій думці. Зокрема, автор робить спробу показати процес еволюції від початків кібернетики права до сучасної юридичної інформатики в Польщі.*

Дослідження у галузі кібернетики права, що здійснювались в Польщі у XX столітті, слід вважати достовірними та творчими. Це підтверджується не тільки розвитком теорії правових інформаційних систем у галузі правової інформатики, але, насамперед, чітким зазначенням обмежень у використанні кібернетичного моделювання в галузі правоих наук. Серед вчених в цій галузі вирізняються Францишек Студницький, Єжи Врублевський, Анджей Малиновський та Єжи Курциш. Результати їх досліджень підтвердили справедливість тези про те, що роль людини не може бути зведена лише до пасивної складової соціального механізму, тоді як суспільство не є аналогом машини і не піддається безапеляційному контролю на розсуд центральної влади. Тому застосування кібернетичного моделювання в юридичних науках має межу, обумовлену специфікою психофізичної побудови людини.

Більш ефективними з точки зору юридичної практики виявилися наукові дослідження в галузі правової інформатики. Вони в кінцевому підсумку призвели до створення правових інформаційних систем. Безсумнівно, це було також зумовлено технологічним прогресом та IT-революцією, яка відбулася наприкінці XX століття. В даний час важко уявити собі роботу юриста без доступу до пошукових систем або використання комерційних програмних баз даних, що містять правові акти, аналітику та правові вчення. (наприклад, в Польщі це Legalis, LexPolonica). У цій перспективі, значним також є вплив кібернетичних досліджень на нормотворчу діяльність у Польщі у XX столітті. Суттєвих змін зазнала також методологія юридичної практики.

Ключові слова: *кібернетика права, правова інформатика, польське право, юриспруденція.*

Summary: *During second part of the XX Century a few interesting researches about law were developed in Poland. One of them was an attempt to use tools that a cybernetics gave to explore a legal problems. The mine subject of article is a short presentation of general assumptions and relation between cybernetics and law in Polish science. Especially, the author tries to show a process of evolution from beginning of cybernetics of law until the contemporary legal informatics in Poland.*

Keywords: *cybernetics of law, legal informatics, Polish law, jurisprudence.*

Аннотация. *Во второй половине XX века активизировались правовые исследования в Польше. В частности, была предпринята попытка использовать инструменты, предоставленные кибернетикой для изучения юридических проблем. Главной целью статьи является краткая презентация основных положений и связи между кибернетикой и правом в польской научной мысли. В частности, автор демонстрирует процесс эволюции от начал кибернетики права до современной юридической информатики в Польше.*

Ключевые слова: *кибернетика права, правовая информатика, польское право, юриспруденция.*

1. The conditioning of the development of judicial cybernetics in Poland.

The term ‘cybernetics’ has a long tradition in Poland. The first one who used this term in 1843 in a sense of governing human collectives was Bronisław Trentowski [1, p. 9-10]. However,

the cybernetics as a science had not started to develop until the mid 20th century. The book *Cybernetics or control and communication in the animal and the machin* [2] written by Norbert Weiner, considered the author of modern cybernetics, was published in Polish translation in the early 1960 [3]. Cybernetics (Greek: *kybernetikos* – the art of steering, the art of governing) as a science studying the processes of steering systems focused on the processes of communication and information [4 – 6] using for that purpose its own conceptual apparatus. The basic ones include such notions as: open and closed systems, steering, steered and control systems, homeostasis, steering, system environment, regulation and feedback[7, 8, 9]. From 1950s to 1980s the science was developing dynamically in Poland. It is proved by a long list of publications whose authors searched for the use of cybernetics to improve the steering of technical, electronic, bionic, linguistic, military, medical, economic, social and psychological systems.

Initially, the USSR authorities, and with them also the Communist parties ruling in other socialist countries, perceived cybernetics negatively. Partially the criticism resulted from new problems that arose in the field of cybernetic exploration. There were considerations to what extent social life and psychological activities of people could be described in the way of cybernetic models, whether the products of technology could be human analogue thinking, and whether it was possible to steer the social system by using appropriate algorithms. Thanks to its broad scope of application, cybernetics began to gradually aspire to be *mathesis universalis* in industrial societies. As a science based on positivistic assumptions it aimed to build universal scientific laws. Practiced on a high level of abstraction, it enabled describing various dynamic systems including human societies. A broad spectrum of applications led to conflict between cybernetics and Marx’s dialectical materialism which aspired to the role of metascience. Finally, the anticybernetic campaign was terminated by the Soviet military officials aware of the practical usefulness of the research findings of the science [10, p. 901-902].

The current legal and political model aided the application of the achievements of cybernetics to organise and control the society through the legal system. Marxism-Leninism accepted the principle of democratic centralism as the basis of the system of the Polish People’s Republic. The model of a single centre of supreme power was introduced to be the political representation of the nation. The postulate of combining the legislative and executive functions was supposed to lead to the situation in which the realisation of power actions would possibly be most closely related to the will of the working class. In legal and structural terms the highest place in the structures of national authorities was taken by the Sejm which was the representative of the nation. Its will was supposed to be put into action by the Council of the State, while the intermediary enabling steering the socio-political system was the Council of Ministers and the state apparatus [13, p. 19].

Marxism assumed the existence of close relationship between the law and the material basis of social existence. The existing economic relationships shaped the legal order. Another determinant of the legal system was politics existing in every element of the superstructure. Each form of public awareness, the state, law, morality, science, art, culture included the political element. Consequently, the government policy had to be reflected also in the law as a tool of the implementation of objectives designated by the authorities. The legal system was *a peculiar form of implementing the working class policy* [15, p. 51]. It was assumed that *socialist law, as a very important element of the superstructure, serves the new socialist economic relations i.e. relations free from exploitation. As a tool of progressive class, the socialist law reflects more or less faithfully the known objective laws of social development* [15, p. 91-92].

2. The Genesis and the Development of Cybernetics of the Law in Poland.

Political and social state of affairs in Poland caused the *Cybernetics of the Law* to become a propitious research area; its scientific potential had been indicated earlier by Wiener [3, p. 51]. The cybernetic approach to legal sciences in Poland dates back to the 1950s. Franciszek Studnicki was a forerunner in this field. Gradually, two main lines of research could be distinguished. The former focused on the application of cybernetic methods in the study of the state legal system and its performance; some other chosen aspects in this field were also taken into account. This research area was conceptualized as *the cybernetic model of analysis*. The latter line of research, defined as *the automation of legislative decisions,* concentrated on exploring the possibilities of algorithmisation of legislative decisions, additionally aided by the use of numerical machines [16, p. 126; 17, p. 195].

The initial assumptions towards the use of cybernetic analysis in the study and the description of the legal structure were based on the general model for the dynamic system of correlated components. The components of the system are provided with inputs and outputs which constitute the means of communication between those elements. The edge areas, additionally distinguished in the system, serve as communication channels linking the system and its surrounding environment. The key premises of cybernetic modelling are based on the feedback linkage, i.e.: the means of paths identification, enabling the individual components to exert influence on the other elements within the system. The character of those feedback linkages determine the performance of the whole system; its state changes, depending on the flow of information. Additionally, the model of a ‘black box’ proved to be applicable as a research mode; it enables analyzing the functioning of the system or its individual components as seen from the outer perspective. That approach resulted in the possibility of focusing on the whole system and the interaction of individual system units, excluding the analysis of its internal parts [16, p. 163-164; 8, p. 38-39].

To recognize the law as the instrument which serves the public authority to administer the social and economic system, the model of management system was of a particular importance. *Controlling,* in terms of cybernetics, may be defined as affecting the state of the system variables. Such an approach requires the control constituent to be distinguished. That constituent specifies the shape of the object and the element being controlled, the state of which is determined by the received control signals. The control process is performed through the inputs and outputs being the part of the individual system elements. Due to deviations in operation, i.e. variations in the functioning of the controlled elements, in the context of expected performance required by the controlling element, a correcting element was distinguished in dynamic systems. The correcting element, through its connections with the controlling and controlled components, enables modification of the system performance by eliminating identified deviations. The correcting element serves as a hemostat in the system [18, p. 100; 19, p. 8; 6, p. 52; 16, p. 164].

In Poland, in the course of the research concerning the application of Cybernetics in jurisprudence, it was quickly noticed that the analogy between the general assumption of cybernetic modelling and the role of the state legal system could be drawn. The legal system constitutes one of the most important instruments of social control [20, p. 129]. However, to meet the expectations of the centre powers, the legislative activity should conform to the conditions of rationality and purposefulness. The support for the legislative process itself was to be the policy of the law. Leon Petrażycki, a prominent lawyer, advocated the law policy to be practiced as early as in the beginning of the 20th century. As being consistent with the assumptions of the theory of Marxism-Leninism, underlying the political control of social systems, his concept had numerous followers in Poland [21, p. 120].

Cybernetics gave the state and the law theoreticians effective instruments to describe the social reality in the realms of establishing and applying the law. In the 1970s, Cybernetics of the Law, as a sub-discipline, finally found its place at the confluence of the Legal Sciences, Social Cybernetics and Cultural Cybernetics [22, p. 11; 23, p. 90]. According to the assumptions of cybernetic models, the legal system was analogous to the control system. A ‘legal norms giver’ played a role of a controlling component i.e. the giver was a subject entitled to create the legal order. In the Polish People’s Republic it was the Polish Parliament and during the intermissions between its sessions – the Council of the State. On the other hand, the whole society or individual addressees of the legal norms played the role of the controlled components of the system. The other option embraced also the cases of individual applications of the law. The institutions dealing with the application and enforcement of the law acted as corrective components of the system in question. They operated in the range of their entitlement to reduce inconsistency between the addressees’ behaviour and the patterns of behaviours specified by the legal standards. Notably, those tasks were fulfilled by the courts of law, the law enforcement and the investigative authorities, the security administration and the state administration [16, p. 164-165].

In accordance with the cybernetic model, drawn up for the description of the law application, the ‘legal norms giver’ (controlling component) creates a specific control signal (legal regulation). Afterwards, by introducing certain provisions, on the grounds of which the norms of behaviour are reconstructed, the addressees receive the message (norms of behaviour) and adjust their conduct, according to the signals of the ‘norm giver’. All that is accompanied by the process of generating new signals which are sent back to the controlling component (norm giver) and the corrective component (e.g. courts of law). The flow of those messages creates a feedback loop containing the information on the status of the applicable law being implemented. In the social control system using the legal one, the special role is performed by its corrective elements, such as: courts, prosecutors, Citizens' Militia, etc. Their task was to respond to cases of violation of the legal order by the addressees of norms and to restore the desired state [24, p. 899; 16, p. 165-166].

Cybernetic analysis of the control system is characterized by a holistic approach. Its individual elements are treated as “black boxes”, that is, their internal structure and rules of functioning are disregarded. Such an approach suffices in physical or organic systems. However, if the cybernetic modelling is to have any sense at the socio-economic and cultural level, it has become necessary to penetrate the internal structure of the “black boxes”. It was necessary because human communities constitute the undetermined systems. The behaviour of individual elements of the system is not only the result of receiving signals sent by the control element. The functioning of society and the economy as well as individual recipients of social norms is also influenced by other stimuli (the effect of the so-called “humanistic coefficient”). The above-mentioned conditions forced Polish researchers to modify the traditional cybernetic approach to the issue of jurisprudence [16, p. 166-167].

The universality of cybernetic instruments in the case of the description of the process of controlling human communities became, in consequence, a weakness of the concept. That was particularly visible in the context of constructing a cybernetic model of the legal system. The essence of each model is to present a simplified or idealized image of reality that exposes the essential features of the original. Researchers realized that achieving the expected effectiveness of social engineering directives requires that the proposed system model faithfully reflected reality in given aspects. The adequacy of the model in relation to the original increases as its complexity grows [25, p. 428-429]. However, on the other hand, the increase in the level of complexity of the model causes a decrease in its usefulness, considering the amount and the

variety of data that needed to be taken into account during its construction. Hence, that particular procedure was necessary to capture the unique specificity of the law [26, p. 39].

Polish legal theorists, investigating the possibility of using cybernetics in jurisprudence, faced a serious problem. To control physical systems (e.g. technical devices) which constitute determinate systems, it was enough to use models that take into account the use of messages created in a formal language. The reference to the formal characteristics of the message was sufficient to program technical devices. On the other hand, it could not serve its intended purpose in managing people [6, p. 91; 18, p. 186-187; 27, p 133]. At the cultural level, the formal properties of the message play only the role of the carrier of the real factor of influence encoded in the semantic meaning of the message. As a recipient of the message, a human reacts not only to his formal aspect, but also thanks to his or her ability to understand, they assign deeper meanings to the message they receive [8, p. 77; 16, p. 167].

The specific properties of the controlled element in the social system (human) forced researchers to cease using solely the language of formal meanings and to move to the transition to the level of language of semantic and pragmatic meaning. At that point, there emerged practical barriers difficult to overcome in the application of cyber cybernetics. Conducting semantic analyses forced the use of conceptual categories, which, in terms of formal language, cannot be attributed to any specific or unique sense. Legal theorists had to recognize the internal states of the elements of the legal system (human motivations, values, etc. encoded in the psyche) as impossible to fully characterize in cybernetic terms. That resulted in the need to leave them outside the analysis area or attempt to enrich the language of cybernetics by introducing the necessary semantic categories. In the former case, that would involve the need to create models that are too general and therefore not very useful to describe the legal reality. However, in the latter one, by moving away from the assumptions of classical cybernetics, it would be possible to create a new research area in which the assumptions of the basic discipline would no longer be applicable [16, p. 168].

The semantic barrier was not the only problem. It was more difficult to describe the pragmatic aspect of the impact of the law using the formal language of cybernetics. Apart from the semantic meaning of the message, in order to properly understand the law, it is necessary to understand the process of the desired effect of the legal norm on the addressee. The motivational dimension of the message sent by the system control element is of crucial importance here. That state of affairs resulted in the prioritization of qualitative analysis before quantitative analysis. Corresponding difficulties occurred during attempts at cybernetic analysis of the behaviour of the control element and the correction element. In that case, the situation was further hindered by the fact that in the legal system their roles were taken not by single people but by institutions i.e. permanent and formalized organizations [8, p. 12; 6, p. 17-19].

The research conducted led to the conclusion that the complexity of legal issues eluded pure cybernetic categories. Researchers took a stance that in the case of law research, the use of a cybernetic perspective precludes the examination of issues beyond the boundaries set by cybernetic conceptual apparatus. Accordingly, further difficulties and limitations appeared along with the progress of detailed research. Finally, it was accepted that the analysis of the legal system using cybernetic modelling could bring limited practical effects in the state of knowledge available at that time [16, p. 170-171].

3. The genesis of legal informatics in Poland.

More satisfying results were yielded by the research on the automation of legal information search through the use of digital machines (computers). The hypothesis was that there is a formal representation of the operation imitating the search and selection of

information used while applying the law. For that purpose, attempts were made to devise appropriate algorithms [16, p. 171].

The direction of scientific research discussed led to the emergence of the new research trend, legal informatics. The term was used for the first time in Polish science by Jerzy Wróblewski [28, p. 639]. The practical aim of developing that direction of cybernetic research was to facilitate the access to the information concerning legal issues. In formal language, that meant the development of procedures enabling the selection, in the searching space composed of texts of legal acts, judicial and administrative decisions as well as the views of doctrine, a subset of elements contained in a given set, meeting the adopted search criteria [29, p. 25-26]. The selection of information in the set required a prior search of the data entered into the memory of a digital machine (computer) arranged according to the adopted earlier code (database).

The improvement of the tools used in legal informatics enabled more advanced search of legal information. Descriptive method was used in addition to full-text information search systems. In place of a simpler required data search method based on the identification of words contained in legal acts, decisions, judgments, etc. the semantic criterion was applied. It allowed the identification of the searched information using the meaning of the content carried by the text [30, p. 64-65].

Along with the development of the field of legal informatics research in Poland, the discipline's aims have also been clarified. The goal was to construct systems for automatic legal decision-making based on the study of legal norms and their intercorrelations, using digital machines to search for legal information [31, p. 18-19]. Building models, in the area of legal informatics as well as using mathematical and logical methods to analyze legal issues took the form of 1) reconstruction models reflecting all aspects of the real system, and 2) idealization models depicting the system in a simplified manner, showing only these aspects of the system which are considered important for the analysis [31, p. 20]. Jerzy Wróblewski’s functional model of imitating the process of the judicial application of the law became one of the more popular cybernetic models [32, p. 25]. In turn, the first Polish computer systems for the search of legal information were created at the turn of the 50s and 60s of the 20th century. Following the Czech researcher, V. Knapp, there began the construction of the foundations of the computer program used while constructing, organizing, applying and interpreting the law [31, p. 24-25].

Eventually, the issue of legal informatics in Poland has been divided into three areas: 1) issues related to computer legal information search systems; 2) problems of constructing factual systems; 3) issues of constructing systems (algorithms) of applying the law. The first two areas have become the space of dynamic development along with the IT progress. The third one has not been developed due to the above mentioned difficulties arising from language barriers between the formal and the semantic meanings of processed legal information, as well as psychological resistance in the Polish society [33, p. 20-21].

Conclusion.

The research in the area of cybernetics of the law conducted in Poland in the 20th century should be considered as reliable and creative. That is proved not only by the evolution of the theory of legal information systems in the area of legal informatics but, above all, by the clear indication of limitations in the use of cybernetic modelling in the area of judicial sciences. Franciszek Studnicki, Jerzy Wróblewski, Andrzej Malinowski and Jerzy Kurcysz are among the scientists with special merits in this field. The findings of their research confirmed the validity of the thesis that a human being cannot be only reduced to the role of a passive component of the social mechanism while the society is not an analogue of the machine and

does not yield to random control in accordance with the will of the centre of power. Therefore, the application of cybernetic modelling in legal sciences found a limit in the form of an impassable barrier determined by the specificity of the psychophysical construction of a human being.

What turned out more efficient from the point of view of legal practice was the scientific exploration conducted in the field of legal informatics. The research in its area eventually led to the creation of legal information systems [8, p. 140, 170]. Undoubtedly, it was also driven by the technological progress and the IT revolution that took place at the late 20th century. Nowadays, it is difficult to imagine the work of a lawyer without access to search engines, for instance, the Internet System of Legal Acts or the use of commercial software databases containing legal acts, case law and legal doctrine views. (e.g. Legalis, LexPolonica). In this respect, the impact of the cybernetic research on law conducted in Poland in the twentieth century has yielded significant achievement which considerably altered the methodology of lawyers’ practice.

References

1. Trentowski B. Stosunek filozofii do cybernetyki, czyli sztuki rządzenia narodem. – Warszawa, 1974. – P. 9-10.

2. Cybernetyka, czyli sterowanie i komunikacja w zwierzęciu i maszynie : The title of the Polish edition, trans. J. Mieścicki. – Warszawa, 1971.

3. Wiener N. Cybernetyka i społeczeństwo, trans. O. Wojtasiewicz. – Warszawa, 1960.

4. Mazur M. Cybernetyka i charakter, ed. 3. – Warszawa, 1999. – P. 16, 45, 61, 91.

5. Pszczołowski T. Mała encyklopedia prakseologii i teorii organizacji. – Ossolineum, 1978. – P. 35-36.

6. Studnicki F. Cybernetyka i prawo. – Warszawa, 1969. – P. 17 et n.

7. Gomółka Z. Cybernetyka w zarządzaniu. Modelowanie cybernetyczne. Sterowanie systemami. – Warszawa, 2001. – P. 11.

8. Malinowski A. Wstęp do badań cybernetycznych w prawoznawstwie. – Warszawa, 1977. – P. 161.

9. Polewoj N.S. Prawowaja informatyka i kibernetyka. – Moskwa, 1993. – P. 24.

10. Kołakowski L. Główne nurty marksizmu. Powstanie-Rozwój-Rozkład. – Warszawa, 1988. – P. 901-902.

11. Janowski J. Cyberkultura prawa. Współczesne problemy filozofii i informatyki prawa. – Warszawa, 2012. – P. 36 et n.

12. Klaus G. Cybernetyka i społeczeństwo, trans. E. Kofler, B. Wojciechowski. – Warszawa, 1970. – P. 23.

13. Burda A. Rozwój ustroju politycznego Polski Ludowej. – Warszawa 1969. – P. 19.

14. Maneli M. (ed.), Zagadnienia ustroju Polsku Ludowej. – Warszawa 1962. – P. 37 et n., 44 et n., 51-52, 55-59.

15. Wiszniewski J. Zarys encyklopedii prawa, ed. 4. Warszawa, 1966. – P. 43-45.

16. Studnicki F. Ujęcia cybernetyczne w dziedzinie prawa in: A. Łopatka (ed.), Metody badania prawa. – Ossolineum, 1973. – P. 162-180.

17. Karsz W. Przesłanki wyodrębnienia cybernetycznej płaszczyzny prawoznawstwa. ZNUŁ, 1971 n. 83. – P. 195.

18. L. Bertalanffy, Ogólna teoria systemów. Podstawy, rozwój, zastosowania, tłum. E. Woydyłło-Woźniak. – Warszawa, 1984. – P. 100.

19. Rassołow M. Problemy uprawlenija i informacji w obłasti prawa. – Moskwa, 1991. – P. 8.

20. Opałek K., Wróblewski J. Zagadnienia teorii prawa. – Warszawa, 1969. – P. 129.

21. Kowalski J., Lamentowicz W., Winczorek P. Teoria państwa i prawa. – Warszawa, 1983. – P. 120.

22. Janowski J., Cyberkultura prawa. Współczesne problemy filozofii i informatyki prawa. –Warszawa, 2012. – P. 11.

23. Kossecki J. Cybernetyka kultury. – Warszawa, 1974. – P. 90.

24. Wróblewski J. Prawo a cybernetyka. Państwo i Prawo, 1968, n. 12. – P. 899.

25. Podgórecki J. (ed.), Socjotechnika. Style działania. – Warszawa, 1972. – P. 428-429.

26. Langer T. O modelach i modelowaniu w naukach prawnych. Państwo i Prawo 1987, n. 9. – P. 39.

27. Rowieński Z., Ujemow A., Ujemowa J. Filozoficzny zarys cybernetyki, trans. M. Niewęgłowski. – Warszawa, 1963. – P. 133.

28. Wróblewski J. Informatyka prawnicza – możliwości zastosowania cybernetyki. PiP, 1971, n. 3-4. – P. 639.

29. Studnicki F. Wprowadzenie do informatyki prawniczej. Zautomatyzowane wyszukiwanie informacji prawnej. – Warszawa, 1978. – P. 25-26.

30. Kurcyusz, Wprowadzenie do nauki o informacji i informatyce prawniczej. – Katowice, 1979. – P. 64-65.

31. Petzel J. Informatyka prawnicza. Zagadnienia teorii i praktyki. – Warszawa, 1999. – P. 18-19.

32. Wróblewski J. (ed.), Wstęp do informatyki prawniczej. – Warszawa, 1985. – P. 25.

33. Wiewiórowski W.R., Wierczyński G. Informatyka prawnicza. Technologia informacyjna dla prawników i administracji publicznej, ed. 2. – Warszawa, 2008. – P. 20-21.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

Інформаційна і національна безпека

УДК 340+35.078.3

ДОВГАНЬ О.Д., *доктор юридичних наук, старший науковий співробітник*,
НДІ інформатики і права НАПрН України
ТКАЧУК Т.Ю., *кандидат юридичних наук, доцент*,
ННІ інформаційної безпеки НА СБ України

СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ: ОНТОЛОГІЧНІ ВИМІРИ

Анотація. *У статті досліджується зміст категорії “система інформаційної безпеки” та визначаються складові відповідної системи, а також обґрунтовується необхідність розмежування системи інформаційної безпеки та системи забезпечення інформаційної безпеки.*

Ключові слова: *інформаційна безпека, забезпечення інформаційної безпеки, національна безпека, система, стан, процес, загроза.*

Summary. *The article explores the content of the category “information security system” and determines the components of this system, and also substantiates the need to delimit the information security system and the information security ensuring system.*

Keywords: *information security, information security ensuring, national security, system, state, process, threat.*

Аннотация. *В статье исследуется содержание категории “система информационной безопасности” и определяются составляющие соответствующей системы, а также обосновывается необходимость размежевания системы информационной безопасности и системы обеспечения информационной безопасности.*

Ключевые слова: *информационная безопасность, обеспечение информационной безопасности, национальная безопасность, система, состояние, процесс, угроза.*

Постановка проблеми. Постійне зростання ролі інформаційних ресурсів у житті сучасного суспільства та значення інформаційного впливу на суспільну свідомість внаслідок небаченого розширення медіа-поля, запровадження новітніх інформаційних технологій, удосконалення інформаційної інфраструктури зумовлює необхідність приділення дедалі більшої уваги проблемі інформаційної безпеки. Інформація стає сьогодні головним ресурсом науково-технічного й соціально-економічного розвитку суспільства, який, на відміну від переважної більшості традиційних ресурсів, не тільки не зменшується внаслідок використання, але й неухильно зростає, забезпечуючи зростання життєвого рівня населення, економічного, оборонного і політичного потенціалу країни. Цілісність світового співтовариства також забезпечується за рахунок інтенсивного інформаційного обміну. У цих умовах інформаційна сфера життєдіяльності суспільства стає дедалі більш уразливою мішенню для інформаційної агресії й тероризму, відтак кожна держава повинна забезпечити в країні відповідний рівень інформаційної безпеки як на національному рівні, так і на рівні організацій і окремих громадян. Системний характер впливу на інформаційну безпеку великої сукупності різнопланових факторів, що мають до того ж різну фізичну природу та переслідують різні цілі, а також викликають різні наслідки, призводить до необхідності комплексного підходу до вирішення цієї проблеми.

На сьогодні в Україні закладена основа правового регулювання забезпечення національної безпеки й інформаційної безпеки зокрема, завдяки чому одержали своє законодавче закріплення основні поняття в області національної безпеки, а також правове обґрунтування системи її забезпечення. Разом з тим, основні нормативно-правові акти у сфері інформаційної безпеки вимагають доопрацювання, зокрема, в аспекті визначення й законодавчого закріплення поняття й змісту категорії “система інформаційної безпеки”, а також розробки теоретичних і правових засад її забезпечення.

Результати аналізу наукових публікацій. Проблематика інформаційної безпеки та її забезпечення у різних аспектах досліджувались у наукових працях Х. Андерсена, О. Баранова, В. Брижка, Н. Влажика, В. Горбуліна, В. Гурковського, О. Дзьобаня, О. Довганя, Г. Ємельянова, Р. Калюжного, Б. Кормича, Дж. Кріка, В. Ліпкана, В. Лопатіна, Р. Максутова, А. Марущака, А. Нашинець-Наумової, М. Ніелса, В. Остроухова, М. Панова, В. Пилипчука, М. Потрубача, Г. Почепцова, М. Присяжнюка А. Прозорова, С. Расторгуєва, В. Рубана, С. Стрельцова, О. Тихомирова, М.-Дж. Шварца та інших вітчизняних та зарубіжних дослідників. Водночас, слід констатувати, що ні в сучасній науковій літературі, ні на законодавчому рівні поки не склалося єдиного підходу до розуміння системи інформаційної безпеки держави. На практиці це призводить не лише до активізації наукової дискусії, але й до неадекватності розуміння змісту тих або інших положень, висновків і рекомендацій, що стосуються сфери інформаційної безпеки України і мають прикладне значення. Зокрема, наразі немає єдиного підходу до визначення системи інформаційної безпеки як на доктринальному, так і на нормативному рівні, що свідчить про актуальність дослідження з відповідної проблематики.

Метою статті є визначення змісту категорії “система інформаційної безпеки” та складових відповідної системи.

Виклад основного матеріалу. Відповідно до ст. 17 Конституції України захист інформаційної безпеки, нарівні із захистом суверенітету та територіальної цілісності України, є найважливішою функцією держави та справою всього Українського народу [1], то ж інформаційна безпека, безперечно, є однією з найважливіших складових національної безпеки України. Оскільки інформаційна сфера має своїм змістом знання про інші сфери життєдіяльності суспільства, вона одночасно існує як самостійно, так і у взаємозв’язку з іншими сферами життєдіяльності суспільства, оскільки здійснює їх “інформаційне обслуговування” за допомогою інформації. Це зумовлює виняткове значення інформаційної сфери та загроз, що на неї спрямовані, адже, як справедливо зазначає Г. Сащук, “…під впливом інформаційних атак може цілеспрямовано змінюватися світогляд та мораль як окремих осіб, так і суспільства в цілому, нав’язуються чужі інтереси, мотиви, спосіб життя” [2], а на думку В. Ліпкана “національні інтереси, загрози їм, управління цими загрозами в усіх галузях національної безпеки знаходять свій вираз, реалізуються через інформацію та інформаційну сферу” [3]. Відтак забезпечення інформаційної безпеки є запорукою забезпечення інших складових національної безпеки, адже всі типи взаємовідносин між суб’єктами інформаційного суспільства ґрунтуються на споживанні й обміні інформацією, а когнітивний простір багато в чому не лише обслуговує й супроводжує, але й підміняє реальний.

Досліджуючи питання системи інформаційної безпеки, передусім слід визначитись із тим, що саме ми розуміємо під інформаційною безпекою, адже наразі з цього приводу наука досі не має єдиної думки. Зокрема, О. Данільян, О. Дзьобань та М. Панов визначають інформаційну безпеку як безпеку об’єкта від інформаційних загроз або негативних впливів, пов’язаних з інформацією, та нерозголошення даних про той чи інший об’єкт, що є державною таємницею [4]. В. Гурковський вважає, що інформаційна

безпека – це суспільні відносини, пов’язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі, що є необхідною умовою збереження та примноження духовних і матеріальних цінностей державоутворюючої нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів [5]. Інша група вчених [6] під інформаційною безпекою розуміють стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни.

В. Ярочкін та Т. Шевцова зазначають, що інформаційна безпека – це проведення правових, організаційних та інженерно-технічних заходів при формуванні та використанні інформаційних технологій, інфраструктури та інформаційних ресурсів, захисті інформації високого значення й прав суб’єктів, що беруть участь в інформаційній діяльності [7]. На думку Р. Калюжного, інформаційна безпека – це вид суспільних інформаційних правовідносин стосовно створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності, спеціальних правовідносин, які пов’язані з створенням, зберіганням, поширенням і використанням інформації [8]. К. Бєляков також зазначає, що під інформаційною безпекою слід розуміти не лише технологічну, але й правову захищеність інформаційної сфери суспільства, що забезпечує її формування та розвиток в інтересах громадян, організацій та держави в цілому [9].

Про інформаційну безпеку, як захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави, говорить Б. Кормич [10].

Ряд вчених [11] розглядають інформаційну безпеку як процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України. Через властивість управління загрозами і небезпеками пропонує розглядати інформаційну безпеку В. Шульга [12]. А. Лукашов в своїй праці [13] запропонував визначати інформаційну безпеку як функціонування системи засобів, що забезпечують захищеність інформаційних систем, котрі являють собою впорядковану сукупність інформаційних ресурсів, інформаційних технологій та комплексу програмно-технічних засобів, якими здійснюються інформаційні процеси в людино-машинному або автоматичному режимі. До цього, В. Брижко вважає, що під інформаційною системою розуміється така система, яка отримує вхідні дані або інформацію, здійснює їх обробку або зміну свого внутрішнього стану (зв’язків) та видає результати обробки для подальших дій [14 , с. 5].

Ю. Фісун характеризує інформаційну безпеку як стан захищеності інформаційного середовища, який відповідає інтересам держави, який забезпечує формування, використання і можливості розвитку незалежно від впливу внутрішніх і зовнішніх інформаційний загроз [15].

За визначенням І. Панаріна, інформаційна безпека – це стан інформаційного середовища суспільства і політичної еліти, що забезпечує її формування і розвиток в інтересах керівництва країни, громадян і суспільства [16, с. 128].

І. Бондар пропонує розглядати національну безпеку України в інформаційній сфері, тобто, інформаційну безпеку, як інтегральну цілісність чотирьох складових – персональної, публічної (суспільної), комерційної (корпоративної) й державної безпеки [17].

І. Громико визначає інформаційну безпеку як захищеність державних інтересів, за

якої забезпечується запобігання, виявлення і нейтралізація внутрішніх та зовнішніх інформаційних загроз, збереження інформаційного суверенітету держави і безпечний розвиток міжнародного інформаційного співробітництва [18, с. 134]

На думку О. Баранова, під інформаційною безпекою слід розуміти такий стан захищеності життєво важливих інтересів особистості, суспільства і держави, при якому зводиться до мінімуму заподіяння шкоди через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [19].

В. Остроухов також визначає інформаційну безпеку як стан захищеності об’єкта (особистості, суспільства, держави, інформаційно-технічної інфраструктури), при якому досягається його нормальне функціонування незалежно від внутрішніх і зовнішніх інформаційних впливів [20, с. 136].

Такі визначення, які можна назвати традиційними, в цілому відображають погляди багатьох інших дослідників та співвідносяться із законодавчим визначенням інформаційної безпеки, що наведене у Законі України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки”. Так, зазначений Закон тлумачить інформаційну безпеку, як “стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається завдання 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” [21].

Наведене визначення, як бачимо, не визначає співвідношення національної та інформаційної безпеки, а також не надає уявлення про систему інформаційної безпеки, так само, як і визначення, які торкаються окремих аспектів інформаційної безпеки, зокрема, інформаційної безпеки телекомунікаційних мереж [22] або кібербезпеки [23].

На доктринальному рівні система інформаційної безпеки вибудовується з використанням доволі широкого спектру критеріїв, що зумовлює диференціацію підходів до змісту поняття “система інформаційної безпеки”.

У зарубіжних наукових джерелах під системою інформаційної безпеки зазвичай розуміють систему безпеки інформації у складі таких структурних елементів, як цілісність, доступність та конфіденційність інформації [24 – 26]. Під цілісністю інформації розуміють її властивість не бути модифікованою неавторизованим користувачем і (або) процесом, тобто, зберігатись у стані, визначеному її створювачем та законним володільцем, в т.ч. й достовірність інформації як її відповідність дійсності в аспекті адекватності відображення. Конфіденційність означає властивість інформації бути недоступною користувачам, які не мають на це права. Ця властивість пов’язана з розмежуванням інформації за режимом доступу. Доступність інформації полягає в тому, що уповноважений користувач може використовувати її відповідно до правил, встановлених політикою безпеки, не очікуючи більше заданого проміжку часу, тобто це властивість інформації знаходиться у необхідному користувачеві вигляді та місці, в той час, коли вона йому необхідна [27, с. 190]. Втім відповідні характеристики не можуть надати уявлення про систему інформаційної безпеки як складової національної безпеки.

Натомість науковці пострадянського простору, в тому числі й вітчизняні вчені, приділяють значну увагу питанням інформаційно-психологічної та державно-ідеологічної складової інформаційної безпеки, існування яких зумовлюється поділом інформаційної сфери на інформаційно-технічну та інформаційно-психологічну [28, с. 62; 29-31]. На підставі критерію функціональності також пропонують визнавати складовими системи

інформаційної безпеки її аспекти: соціальний; нормативно-правовий; економічний; фінансовий; військовий; екологічний; програмно-технічний тощо [32, с. 74].

За твердженням Б. Кормича, інформаційна безпека має суб’єктно-об’єктний склад, відтак з точки зору критерію основного об’єкту система інформаційної безпеки складається з інформаційної безпеки особи, інформаційної безпеки суспільства та інформаційної безпеки держави. Крім того, держава, людина та суспільство одночасно виступають і як суб’єкти інформаційної безпеки, здійснюючи своїми діями захист важливої для них інформації та інформаційних процесів [33, с. 28-32].

О. Довгань розглядає інформаційні структури як компоненти інформаційної безпеки, тобто, як елементи системи інформаційної безпеки [34, с. 110-119], та вважає її об’єктом інформаційний суверенітет [35, с. 109-111]. Також систему інформаційної безпеки характеризують такі поняття, як інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології [36, с. 84].

О. Тихомиров зазначає, що інформаційна безпека – це стан інформаційної системи загалом та її елементів зокрема, що характеризується сукупністю умов оптимального функціонування і розвитку в інформаційній сфері та можливостями їх усвідомлення та контролю [37, с. 74], однак вибудовує систему забезпечення інформаційної безпеки за широким спектром критеріїв, зокрема: за сферами суспільного життя *(забезпечення інформаційної безпеки в економічній, політичній, воєнній, науково-технологічній, екологічній, соціальній сфері тощо)*; за об’єктами національної безпеки *(забезпечення інформаційної безпеки особи, суспільства та держави)*; за сучасними аспектами розуміння інформаційної безпеки *(забезпечення інформаційно-психологічної безпеки, забезпечення інформаційної безпеки у сфері прав і свобод людини та інформаційно-технічної, в т.ч. кібернетичної безпеки)*; за основними видами інформаційної діяльності *(забезпечення законних можливостей створення, збирання, одержання та використання інформації, законного порядку поширення інформації, належного зберігання інформації, охорона та захист інформації, створення і розвиток інформаційних ресурсів тощо)*; за формами державного забезпечення інформаційної безпеки *(забезпечення якісного інформування, процесів інформатизації; правова регламентація сфери інформаційних відносин; боротьба з правопорушеннями в інформаційній сфері*); за напрямами пізнавального процесу в галузі забезпечення інформаційної безпеки *(професійна освіта, наукові дослідження, інформаційно-просвітницька діяльність тощо)*; …за засобами забезпечення інформаційної безпеки: правове забезпечення *(правова регламентація відносин в інформаційній сфері; контрольно-наглядова діяльність, ліцензування, сертифікації, експертизи тощо)*; техніко-технологічне забезпечення; залежно від особливостей забезпечення доступу до інформації *(за правовим режимом доступу до інформації; за заходами із захисту секретної інформації тощо)* [38, с. 67-74].

На відмінності між системою інформаційної безпеки та системою забезпечення інформаційної безпеки можуть бути екстрапольовані відповідні закономірності, виявлені щодо системи національної безпеки та системи забезпечення національної безпеки [39, с. 5-8]. Так, основними елементами системи забезпечення інформаційної безпеки є її суб’єкти і об’єкти, а також прямі та зворотні зв’язки між ними. Основними об‘єктами системи забезпечення інформаційної безпеки як складової національної безпеки є національні цінності, національні цілі та національні інтереси. Розглядаючи національні цінності, національні інтереси та національні цілі через призму їх носіїв, можна класифікувати об‘єкти системи забезпечення інформаційної безпеки наступним чином: держава *(конституційний лад, суверенітет і територіальна цілісність України,*

політична, економічна та соціальна стабільність, законність і правопорядок, розвиток рівноправного взаємовигідного міжнародного співробітництва тощо); суспільство *(розвиток демократії, збереження культури і духовно-історичної спадщини, збереження і розвиток інформаційних ресурсів, досягнення й розвиток суспільної злагоди, політична стабільність, віротерпимість тощо)*; людина і громадянин *(життя, здоров‘я, культура, традиції тощо)*. Суб’єктами системи забезпечення інформаційної безпеки виступають держава (у т.ч. її інститути, посадові особи), суспільство (соціальні верстви та групи, громадські організації), а також окремі громадяни.

В. Ярочкин фактично ототожнює систему забезпечення інформаційної безпеки та систему інформаційної безпеки, адже пропонує під системою інформаційної безпеки розуміти організовану сукупність спеціальних органів, служб, засобів, методів і заходів, що забезпечують захист життєво важливих інтересів особистості, підприємства й держави від внутрішніх і зовнішніх загроз. Компонентами концептуальної моделі інформаційної безпеки (на прикладі безпеки інформації) за такого підходу визначаються: об’єкти загроз; загрози; джерела загроз; цілі загроз; джерела інформації; способи неправомірного заволодіння конфіденційною інформацією (способи доступу); напрямки захисту інформації; способи захисту інформації; засобу захисту інформації [40, с. 40-52].

О. Довгань пропонує модель системи забезпечення інформаційної безпеки, яка утворюється об’єктами інформаційної безпеки та суб’єктами інформаційної безпеки відповідно. При цьому *до об’єктів інформаційної безпеки* належать: конституційні права і свободи людини і громадянина, фізичне та психологічне здоров’я населення, захищеність людини від деструктивного та маніпулятивного інформаційного впливів; інформаційне забезпечення, гарантії інформаційних прав та права на розвиток населення всіх регіонів України; інформаційний суверенітет, безпека національного сегмента глобального інформаційного простору, інформаційної інфраструктури, захищеність, цілісність, доступність та безпечність інформаційних ресурсів, продукції і послуг. *До суб’єктів* забезпечення інформаційної безпеки у такій системі віднесені: Президент України, Верховна Рада України, Кабінет Міністрів України; Рада національної безпеки і оборони України, Національний банк України; Міністерство інформаційної політики України, Державний комітет телебачення і радіомовлення України, Національна рада України з питань телебачення і радіомовлення; Державна служба спеціального зв’язку і технічного захисту інформації України, Національна комісія України, що здійснює державне регулювання з питань зв’язку та інформатизації; Служба безпеки України, розвідувальні органи України, Державна прикордонна служба України, Збройні Сили України та інші військові формування, утворені відповідно до законів України; центральні органи виконавчої влади, місцеві органи державної влади та органи місцевого самоврядування, судові органи, прокуратура України та інші органи охорони правопорядку, віднесені законодавством до суб’єктів забезпечення національної безпеки України; засоби масової інформації, підприємства, заклади, установи та організації різних форм власності, що здійснюють інформаційну діяльність, наукові установи та вищі навчальні заклади України інформаційного профілю, інститути громадянського суспільства, громадяни України та інші особи (за згодою) [41, с. 13].

На думку В. Пилипчука, до основних суб’єктів системи забезпечення інформаційної безпеки, які мають забезпечувати або брати участь у розробці та реалізації державної інформаційної політики, слід віднести наступні: Міністерство інформаційної політики України; Міністерство юстиції України; Державний комітет телебачення і радіомовлення України; Національну раду України з питань телебачення і

радіомовлення; Державну службу спеціального зв’язку і захисту інформації України; Національну комісію, що здійснює державне регулювання у сфері зв’язку та інформатизації; інші державні й недержавні органи, заклади, установи, підприємства та організації. Найбільш актуальними проблемами інформаційної безпеки дослідник вважає, зокрема: проблему ефективності державної інформаційної політики та політики національної безпеки в інформаційній сфері; проблема забезпечення кібербезпеки; проблему захисту прав, свобод і безпеки людини і громадянина в інформаційній сфері [42, с. 25-26], що дозволяє скласти певне уявлення про систему інформаційної безпеки.

Досліджуючи питання забезпечення інформаційної безпеки, О. Баранов наголошує на необхідності забезпечення інформаційної безпеки у трьох її складових: забезпечення запобігання завдання шкоди через неповноту, невчасність та невірогідність інформації; забезпечення запобігання нанесення шкоди через негативний інформаційний вплив; забезпечення запобігання завданню шкоди через негативні наслідки функціонування інформаційних технологій [43, с. 33]. Система інформаційної безпеки, таким чином, утворюється безпекою інформації, безпекою від негативних інформаційних впливів, безпекою інформаційних технологій. Втім гуманітарна складова інформаційної безпеки містить у собі величезну сукупність проблем, пов’язаних з дотриманням конституційних прав і свобод громадян у сфері духовного розвитку й інформаційної діяльності. То ж безпека інформаційної сфери не може сприйматися суто як захист телекомунікаційних мереж або мереж зв’язку, засобів масової інформації від проникнення небажаної або шкідливої інформації. Про необхідність дослідження загроз інформаційній безпеці людини з точки зору її інформаційних прав та свобод вказує О. Золотар, наголошуючи на тому, що інформаційна безпека людини передбачає в т.ч. реалізацію життєво важливих інтересів людини та гармонійний розвиток в умовах інформаційного суспільства незалежно від наявності інформаційних загроз [44, с. 77].

Таким чином, оскільки метою забезпечення інформаційної безпеки є передусім попередження шкідливих інформаційних впливів та неправомірних дій щодо інформаційних ресурсів та інформаційних систем (біологічних, соціальних та технічних), захист прав та забезпечення реалізації інтересів суб‘єктів інформаційної сфери, а також забезпечення захищеності істотних властивостей інформації, нами вже обґрунтовувалася думка, що система інформаційної безпеки складається з безпеки інформації, безпеки від інформаційних впливів, а також захисту інформаційних прав та належного порядку реалізації інтересів суб’єктів інформаційної сфери [45, с. 155].

При цьому безпека інформації як захищеність її основних властивостей має забезпечуватись не лише щодо інформації з обмеженим доступом, але й іншої інформації, оскільки має бути відвернена не лише загроза порушення конфіденційності інформації, але й загроза порушення її цілісності та достовірності, а також і доступності інформації. Під безпекою від інформаційних впливів слід розуміти безпеку інформаційних систем та зв’язків між ними від інформаційних впливів, що здатні спричинити шкоду, в т.ч. й інформаційно-психологічну безпеку людини й суспільства. Забезпечення інформаційно-психологічної безпеки полягає в мінімізації негативних впливів на свідомість людини та суспільства, пов’язаних передусім із маніпулюванням свідомістю з різною метою, і поширенням суспільно небезпечної інформації, в тому числі деструктивної ідеології (культу насильства та жорстокості, расизму, радикального націоналізму, порнографії тощо) [37, с. 70-71]. Як вважає Брижко В.М., по суті, маніпуляція свідомості – це цензура, яка є засобом інформаційної боротьби, що обмежує свободу слова та порушує складні інформаційні системи, якими є людина, суспільство або держава [14, с. 7, 43-71].

Захист інформаційних прав та забезпечення реалізації інтересів суб’єктів інформаційної сфери як підсистеми інформаційної безпеки пов’язаний з двома іншими її складовими, оскільки мова йде передусім про потребу у безпечному інформаційному середовищі та права на інформацію. Якщо мова йде про інформаційну безпеку як про інформаційний вимір національної безпеки (мається на увазі стан не окремих структур, сторін або відносин нації), а її здатність ефективно функціонувати, незважаючи й всупереч негативним факторам не поступатися своїми інтересами під тиском зовнішніх, внутрішніх або комплексних загроз. Таким чином, категорія “інформаційна безпека” на національному рівні повинна відноситись до країни, до держави, що розуміється як органічна єдність території, населення й влади, і тлумачитися на холістичних засадах, виходячи з якісної своєрідності цілого стосовно до його частин. Ця своєрідність полягає в тому, що інформаційна безпека країни припускає й означає інформаційну безпеку всіх її структур і утворень, але допускає можливе ослаблення її для деяких з них. У той же час, зміцнення інформаційної безпеки окремих об’єктів, сегментів або сфер, узятих окремо, важливо для інформаційної безпеки як складової національної безпеки (її інформаційного виміру), але не створює її.

Отже, інформаційна безпека виступає як стан і умови життєдіяльності соціуму, які забезпечують сприятливі умови для розвитку особистості, суспільства й держави, а так само й інших об’єктів, тоді як інформаційна безпека кожного з цих об’єктів окремо виступає не як її частина, а як її мета та результат. У широкому сенсі інформаційна безпека повинна включати такі проблеми, як протистояння культурній експансії з боку країн з розвиненою аудіовізуальною промисловістю, збереження національної і мовної самобутності, нейтралізацію впливу недоброякісної, недостовірної, хибної інформації (дезінформації) на реалізацію національних інтересів. Слід звернути увагу й на те, що “безпека взагалі” не існує, адже атрибутом існування об’єкта будь-якої природи є наявність загроз, відтак модель системи інформаційної безпеки припускає визначення того, кому, що, чим загрожує, а також можливі механізми й способи протидії загрозливим факторам.

В. Пилипчук та О. Дзьобань відносять до основних видів загроз інформаційній безпеці наступні: витіснення вітчизняних інформаційних агентств, засобів масової інформації із внутрішнього інформаційного ринку та посилення залежності духовної, економічної і політичної сфер громадського життя України від закордонних інформаційних структур; маніпулювання інформацією (дезінформація, приховування чи перекручування інформації); інформаційний вплив іноземних політичних, економічних, військових та інформаційних структур на розробку і реалізацію зовнішньої політики держави; поширення за кордоном дезінформації про зовнішню політику України; порушення прав громадян і юридичних осіб в інформаційній сфері в Україні й за кордоном; спроби несанкціонованого доступу до інформації і впливу на інформаційні ресурси, інформаційну інфраструктуру органів державної влади, що реалізують державну зовнішню політику, українських представництв і організацій за кордоном, представництв України при міжнародних організаціях [46, с. 47-48].

Тому О. Дзьобань та О. Соснін обґрунтовано наголошують на необхідності постійного контролю стану безпеки в інформаційній сфері, ранжування загроз за ступенем впливу на національні інтереси, раціонального перерозподілу сил і засобів для нейтралізації загроз [47, с. 33].

Необхідно також враховувати, що зміст інформаційної безпеки не можна зводити тільки до захищеності – її зміст значно ширший. Забезпечення безпеки передбачає не тільки збереження певного існуючого стану, але й створення можливостей для виходу

на новий, якісно більш високий рівень розвитку. Відповідно, безпека – не стільки незмінний стан об’єкта, скільки його здатність відтворюватися, розбудовуватися, стало й прогресивно розвиватися в умовах конфліктів, невизначеності й ризику. Так само неприйнятним є визначення інформаційної безпеки як “захищеності інтересів”, адже інтереси – це потреби, без задоволення яких нормальне існування соціуму неможливо, то ж їх потрібно не захищати, а реалізовувати. Захисту потребують цінності, необхідні для нормальної життєдіяльності людини, суспільства, держави, і умови, що забезпечують їхній доступ до цих цінностей і можливість користуватися ними. Безпека припускає, насамперед, наявність необхідних цінностей і доступу до них. Відсутність цінностей вимагає пошуку їх нових джерел або їх замінників, а ускладнений доступ до них – усунення перешкод або вжиття заходів для їхнього подолання, що, у свою чергу, визначає зміст категорії “національні цілі”.

Таким чином, інформаційну безпеку України слід визначити як стан, за якого в умовах дії різнопланових загроз забезпечується самозбереження, сталий і прогресивний розвиток інформаційної сфери, в т.ч. захищеність національних цінностей, необхідних для існування суверенної Української держави та виконання нею своїх функцій, а також досягнення відповідних національних цілей та реалізація національних інтересів. Інформаційна сфера при цьому утворюється сукупністю: суб‘єктів інформаційних процесів, інформаційної інфраструктури, інформаційного простору, інформаційних ресурсів, а також суспільних відносин, що складаються у зв‘язку з формуванням, зберіганням, передачею та розповсюдженням інформації. За такого визначення система інформаційної безпеки з точки зору її об’єктів відповідає класичній формулі для об’єктів національної безпеки “територія – народонаселення – система державного управління”, однак замість території для інформаційної безпеки вважаємо за доцільне використовувати поняття “інформаційний простір”, яке в т.ч. охоплюватиме інформаційну модель території та її інформаційне обслуговування.

Відповідно, функціональна система інформаційної безпеки України як складової та інформаційного виміру національної безпеки матиме наступний вигляд, див. далі на Рис.

На нашу думку, розмежування інформаційної безпеки як стану динамічної системи та забезпечення інформаційної безпеки як процесу підтримання цього стану (включаючи самовідтворення, збереження та розвиток) дозволяє певним чином зняти протиріччя між організаційно-структурним і функціонально-діяльнісним підходами до визначення сутності феномену інформаційної безпеки та її системи. То ж система інформаційної безпеки як певне утворення, що характеризується подільністю, відкритістю, адаптивністю та наявністю структури, мети й пріоритетів оптимальної взаємодії елементів [48, с. 86], виступає об’єктом для системи забезпечення інформаційної безпеки, до якої також входять сили й засоби забезпечення інформаційної безпеки.

Зауважимо, що система інформаційної безпеки, особливо на рівні її результуючих компонентів, може бути структурована за різними критеріями. На жаль, на законодавчому рівні питання системи інформаційної безпеки досі системно не вирішено. Навіть нова Доктрина інформаційної безпеки України [49], яка готувалася в умовах, коли наша країна потерпає від гібридної агресії Російської Федерації, а отже – вже потрібно було б усвідомлювати значення інформації, інформаційних впливів та інформаційної сфери в цілому, не орієнтує на вирішення усього комплексу виявлених проблем, не загострює проблеми необхідності їх законодавчого врегулювання.

Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу РФ в умовах розв’язаної нею гібридної війни. Доктрина визначає національні інтереси

України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері. Її правовою основою є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента від 26 травня 2015 року № 287 [22], а також міжнародні договори, згода на обов’язковість яких надана Верховною Радою України.

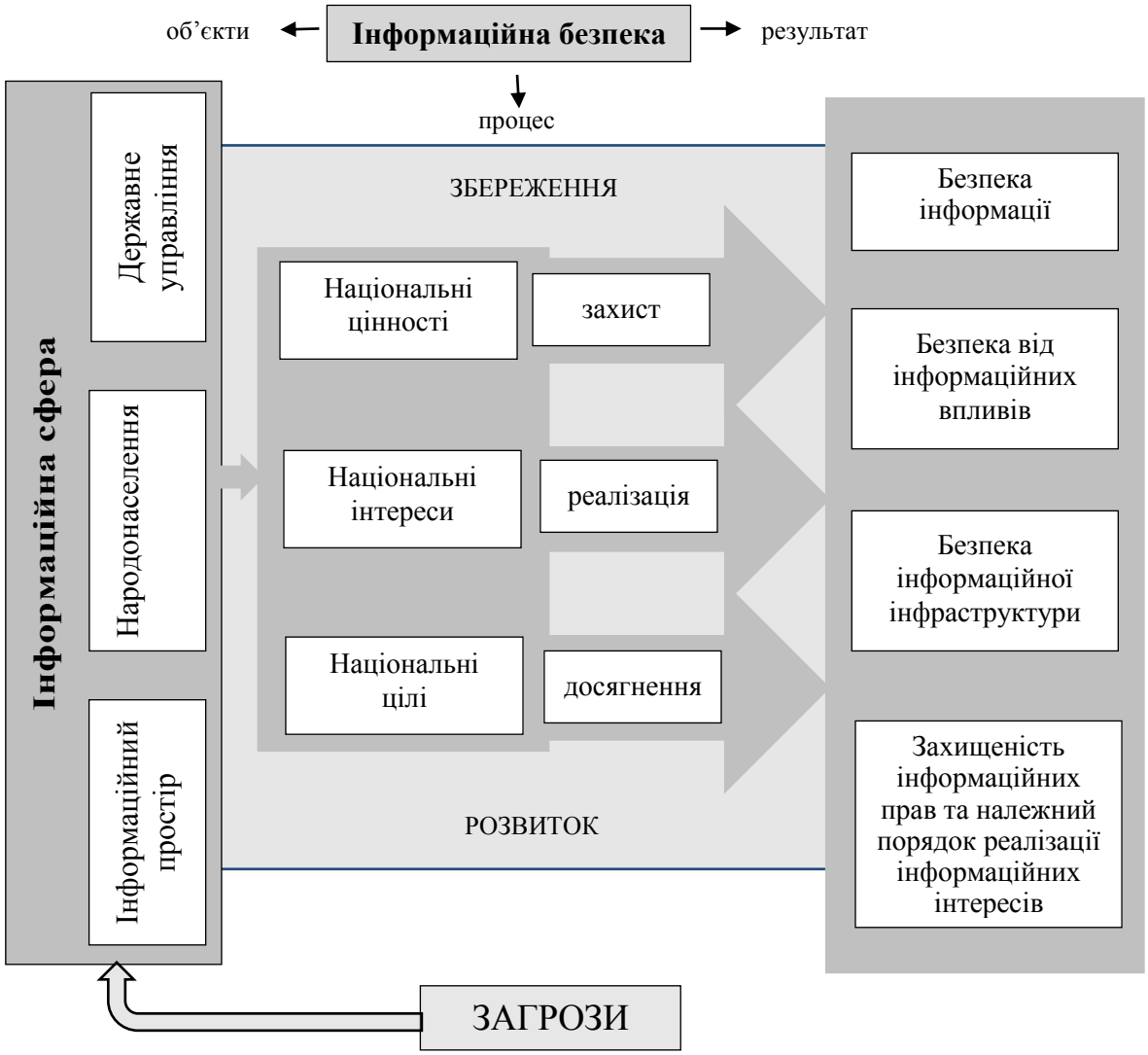

Рис. Система інформаційної безпеки

У тексті Доктрини йдеться про національні інтереси України в інформаційній сфері, актуальні загрози національним інтересам та національній безпеці, пріоритети державної політики в інформаційній сфері і механізм реалізації доктрини. Доктриною передбачається захист українського суспільства від “агресивного інформаційного впливу Російської Федерації”, розвиток публічної дипломатії, в тому числі культурної та цифрової, видалення шкідливої інформації з українського сегменту інтернету та квотування національного аудіовізуального контенту, захист права на вільний доступ до інформації, створення механізмів захисту від пропаганди тощо.

Втім, у експертному середовищі Доктрина отримала переважно негативну оцінку на кшталт “Доктрина інформаційної безпеки України – це лише декларація” або “замість інтеграції Україна встановлює паркан” тощо [50]. Дійсно, у Доктрині держава виклала бачення розвитку й функціонування свого інформаційного простору і визначила, що

Російська Федерація є супротивником, який веде системну інформаційну війну. У документі є пропозиції, як реагувати на агресію та забезпечувати інформацією громадян. Доктрина також визначає поняття “стратегічного наративу” і вказує, що медіа мають самі себе регулювати, але при цьому повинні нести соціальну відповідальність. Втім, Доктрина закладає державну систему постійного моніторингу веб-ресурсів та блокування сайтів, що загрожують безпеці, однак підстави для блокування доволі абстрактні – орган державної влади на свій розсуд зможе тлумачити, що загрожує безпеці, а що – ні. Відповідно, виникає небезпека встановлення цензурованих шлюзів, які відокремлять український інтернет від світу. Крім того, механізм реалізації Доктрини навіть у її позитивних аспектах не містить жодної конкретики, тож у чинній редакції Доктрина не може слугувати базовим документом, на підставі якого мають формуватися і інші правові акти у сфері забезпечення інформаційної безпеки, в тому числі стратегічні та програмні документи.

Ми цілком поділяємо думку О. Довганя, який слушно зазначає, що сьогодні в черговий раз потрібно піднімати питання щодо розробки нормативного акту (закону), яким буде визначено єдиний понятєво-категорійний апарат, державну політику забезпечення інформаційної безпеки, об’єкти інформаційної безпеки та суб’єкти її забезпечення, правові зони відповідальності відомств, залучених до сфери забезпечення інформаційної безпеки, механізми координування їх діяльності щодо реагування на виклики та загрози національній безпеці в інформаційній сфері, порядок правового закріплення взаємовідносин державних безпекових структур із іншими органами та відомствами, віднесеними законодавством до суб’єктів забезпечення національної безпеки України тощо [51, с. 37-38]. Вважаємо, що такий нормативний акт обов’язково має визначати як систему інформаційної безпеки, так і систему забезпечення інформаційної безпеки.

З цього приводу зазначимо, що на засіданні РНБО України 17 січня 2018 року члени РНБО обговорили та підтримали проект Закону України “Про національну безпеку України”, який, за повідомленням офіційного сайту РНБО, “розроблявся у тісній взаємодії з експертами НАТО, США та Європейського Союзу з метою приведення української законодавчої бази у відповідність до стандартів держав-членів НАТО” [52]. На жаль, за результатами аналізу цього проекту слід дійти висновку, що він не відповідає вимогам нормопроектувальної техніки, передусім: базується на підміні понять “суспільна безпека” (“соціальна безпека”) у розумінні “безпека суспільства” та “громадська безпека”; передбачає “точкове” регулювання відносин щодо окремих об’єктів, що входять до систем, перелік складових яких є невичерпним (зокрема, систем на кшталт суспільної безпеки, національної безпеки, системи державних органів, які беруть участь у забезпеченні національної безпеки тощо); містить положення, які не стосуються предмета регулювання, задекларованого в назві проекту та суперечливі норми права, дублює і повторює норми права, які містяться в інших нормативно-правових актах. Проект також не містить визначення основоположних дефініцій у сфері забезпечення національної безпеки, зокрема таких, як “національні цінності”, “національні цілі”, “система забезпечення національної безпеки”, “система національної безпеки”, “вид (сфера) національної безпеки”, “об’єкти національної безпеки”, “основи національної безпеки” тощо, а відтак не може слугувати підґрунтям для визначення відповідних понять у контексті забезпечення інформаційної безпеки.

Натомість, актуалізується нагальна потреба у розробці та прийнятті Закону України “Про інформаційну безпеку України” як базового закону, що регулюватиме

питання інформаційної безпеки. Таким закон, як підґрунтя ефективної стратегії інформаційної безпеки, повинен містити не абстрактні декларації, а чітко визначені основоположні категорії у сфері інформаційної безпеки та підходи до формування системи забезпечення інформаційної безпеки, механізм її функціонування, повноваження і схему взаємодії суб’єктів забезпечення інформаційної безпеки тощо.

Висновки.

Створення належних умов для реалізації державної політики, спрямованої на захист національних цінностей та реалізацію національних інтересів України, гарантування безпеки особи, суспільства і держави від зовнішніх та внутрішніх загроз в інформаційній сфері, потребує формування сучасних ефективних механізмів забезпечення інформаційної безпеки, які відповідатимуть характеру і масштабам викликів сьогодення. Складна воєнно-політична, оперативно-стратегічна та економічна ситуація, яка склалася внаслідок збройної агресії Російської Федерації проти нашої держави, набула загрозливих проявів у інформаційному просторі.

Відповідно, надзвичайно актуальним стає доктринальне та нормативне визначення такої основоположної категорії, як “система інформаційної безпеки”, адже інформаційна безпека є системним, багаторівневим явищем, на стан якого впливають зовнішні і внутрішні чинники, зокрема, політична обстановка у світі; внутрішньополітична обстановка в державі; стан і рівень інформаційно-комунікаційного розвитку країни тощо. Важливим для цього вважаємо розмежування інформаційної безпеки як стану динамічної системи та забезпечення інформаційної безпеки як процесу підтримання цього стану (включаючи самовідтворення, збереження та розвиток) дозволяє зняти протиріччя між організаційно-структурним і функціонально-діяльнісним підходами до визначення сутності феномену інформаційної безпеки та її системи.

У методологічному відношенні важливо не тільки перелічити складові системи інформаційної безпеки, але й доповнити вербалізацію цих явищ операціоналізацією і концептуалізацією понять, що їх позначають. Отже, наразі набуло непересічної актуальності питання розробки та прийняття Закону України “Про інформаційну безпеку України” як базового закону, що регулюватиме питання інформаційної безпеки.

Використана література

1. Конституція України : Закон України від 28.06.96 р. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/254к/96-вр. – Дата звернення 18.02.2018 р.

2. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. – Режим доступу : http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php. – Дата звернення 18.02.2018 р.

3. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник / В. Ліпкан, Ю. Максименко, В. Желіховський. – К. : КНТ, 2006. – 280 с.

4. Данильян О.Г. Національна безпека України : структура та напрямки реалізації : навчальний посібник / О. Данильян, О. Дзьобань, М. Панов. – Х. : Фоліо, 2002 – 285 с.

5. Гурковський В.І. Безпека як об’єкт правовідносин в умовах глобального інформаційного суспільства // Правова інформатика. – 2010. – № 2(26). – С. 72-77.

6. Нижник Н. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : навчальний посібник / Н. Нижник, Г. Ситник, В. Білоус. – Ірпінь : Акад. ДПС України, 2000. – 304 с.

7. Ярочкин В.И. Словарь терминов и определений по безопасности и защите информации / В. Ярочкин, Т. Швецова. – М. : Ось-89, 1996. – 48 с.

8. Питання концепції реформування інформаційного законодавства України / Р. Калюжний та ін. // Правове, нормативне та метрологічне забезпечення системи інформації в Україні : тематичний зб. праць учасників 2-ї науково-технічної конференції. – К., 2000. – С. 17-21.

9. Бєляков К.І. Деякі питання щодо формування реформи інформаційного законодавства України : мат. міжнародної науково-практичної конференції [“Систематизація законодавства в Україні : проблеми теорії і практики”]. – К. : Інститут законодавства Верховної Ради України, 1999. – С. 253-255.

10. Кормич Б.А. Інформаційна безпека : організаційно-правові основи : навчальний посібник / Б.Кормич. – К. : Кондор, 2004. – 382 с.

11. Ліпкан В.А., Харченко Л.С., Логінов О.В. Інформаційна безпека України : глосарій. – К. : Текст, 2004. – 136 с.

12. Шульга В.І. Сучасні підходи до трактування поняття інформаційна безпека / Ефективна економіка. – 2015. – № 4. – Режим доступу : http:// http://www.economy.nayka.com.ua/ ?op=1&z=5514. – Дата звернення 19.02.2018 р.

13. Лукашов А.И. Информационная безопасность как объект уголовно-правовой охраны в законодательстве Республики Беларусь : мат. научной конференции [“Концептуальные проблемы информационной безопасности в союзе России и Беларуси”]. – СПб., 2000. – Режим доступу : http://jurfak.spb.ru/conference/2001.htm. – Дата звернення 19.02.2018 р.

14. Брижко В.М. е-боротьба в інформаційних війнах та інформаційне право : монографія / В.М. Брижко, М.Я. Швець. – К. : НДЦПІ АПрН України, 2007. – 239 с.

15. Фисун Ю.А. Вопросы информационной безопасности личности, общества и государства накануне 21 века : мат. международной конференции [“Информатизация правоохранительных систем”], (м. Москва, 7 – 8 июня 2000 г.). – М., 2000, – С. 86-92.

16. Панарин И. Технология информационной войны : монографія / И. Панарин. – М. : “КСП+”, 2003. – 320 с.

17. Бондар І.Р. Інформаційна безпека як основа національної безпеки / Mechanism of Economic Regulation. – 2014. – № 1. – С. 68-75.

18. Громико І., Саханчук Т. Державна домінантність визначення інформаційної безпеки України в умовах протидії загрозам // Право України. − 2008. − № 8. – С. 130-134.

19. Баранов А.А. Концептуальные вопросы информационной безопасности Украины : сб. материалов [“Нормативно-правовая база защиты информации”]. – К., 1997. – С. 53-58.

20. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України // Політичний менеджмент. – 2008. – № 4. – С. 135-141.

21.Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.07 р. – Режим доступу : zakon5.rada.gov.ua/laws/show/537-16. – Дата звернення 13.02.2018 р.

22. Про телекомунікації : Закон України від 18.11.03 р. – Режим доступу : zakon2.rada.gov.ua/laws/show/1280-15. – Дата звернення 13.02.2018 р.

23. Про рішення Ради національної безпеки і оборони України від 27.01.16 р “Про Стратегію кібербезпеки України” : Указ Президента України від 15.03.16 р. № 96/2016. – Режим доступу: www.president.gov.ua/documents/962016-19836. – Дата звернення 20.08.2018 р.

24. Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri. An Introduction to Information Security. – Online tool. – Available at : https://doi.org/10.6028/NIST.SP.800-12r1. – Accessed 04.10.2017.

25. National Security Telecommunications and Information Systems Security. National Training Standard for Information Systems Security (Infosec) – Online tool. – Available at : //www.cnss.gov/Assets/pdf/nstissi_4011.pdf. – Accessed 04.10.2017.

26. Federal Financial Institutions Examination Council (FFIEC). Information Technology Examination Handbook (IT Handbook) : Information Security (2016). – Online tool. – Available at : https://www/ffiec.gov/press/pdf/ffiec-it-handbook_information_security_booklet.pdf. – Accessed 04.10.2017.

27. Мельник С.В. Понятійно-категоріальний аппарат у системі професійної підготовки майбутніх фахівців з кібербезпеки // Інформаційні технології і засоби навчання. – 2016 – Т. 55. – № 5 – С. 187-197.

28. Баришполец В.А. Информационно-психологическая безопасность : основные положения / РЭНСИТ : Информационные технологии. – 2013 – № 2. – Т 5. – С. 62-104.

29. Николаев А. Государственно-идеологическая компонента информационной безопасности. – Режим доступу : https://cyberleninka.ru/acticle/v/gosudarstvenno-ideologicheskaya-komponenta-informatsionnoy-bezopasnosti. – Дата звернення 15.02.2018 р.

30. Гулай В.В. Загрози інформаційно-психологічній безпеці особи в реаліях інформаційно-психологічної війни як складової “гібридної війни” Російської Федерації проти України. – Режим доступу : //www.asv.ua/content/nauka/editions/25/2016-25/233-244.pdf. – Дата звернення 16.02.2018 р.

31. Уханова Н.С. Інформаційно-психологічна безпека особистості, суспільства та держави. – Режим доступу : //www.ippi.org.ua/ukhanova-ns-informatsiino-psikhologichna-bezpekaosobistosti-suspil stva-ta-derzhavi. – Дата звернення 16.02.2018 р.

32. Жатканбаева А.Е. Функциональные компоненты информационной безопасности // Право и государство. – 2013. – № 4 (61) – С. 73-77.

33. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України : монографія / Б.Кормич. – Одеса : Юридична література, 2003. – 472 с.

34. Довгань О.Д. Сучасні інформаційні структури як компоненти інформаційної безпеки // Інформація і право. – № 2(14)/2015. – С. 111-120.

35. Довгань О.Д. Національний інформаційний суверенітет – об’єкт інформаційної безпеки // Інформація і право. – № 3(12)/2014. – С. 102-112.

36. Довгань О.Д. Нейтралізація міжнародних інформаційних загроз // Правова інформатика. – № 2(42)/2014. – С. 80-89/

37. Тихомиров О.О. Перспективи зміни розуміння інформаційної безпеки // Правова інформатика. – № 4(28)/2010. – С. 68-75.

38. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави : монографія / О. Тихомиров ; заг. ред. Р.А. Калюжний. − К. : Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. – 196 с.

39. Концептуальні засади розвитку системи забезпечення національної безпеки України : аналіт. доп. / [О.О. Резнікова, В.Ю. Цюкало, В.О. Паливода, С.В. Дрьомов, С.В. Сьомін]. – К. : НІСД, 2015. – 58 с.

40. Ярочкин В.И. Информационная безопасность : учебное пособие для студентов непрофильных вузов.. – М. : Междунар. отношения, 2000. – 400 с.

41. Довгань О.Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України // Інформаційна безпека людини, суспільства, держави. – 2015, № 3 (19). – С. 6-17.

42. Пилипчук В.Г. Забезпечення інформаційної безпеки України : сучасні тенденції та проблеми : матеріали наук.-практ. конф. [“Запобігання новим викликам та загрозам інформаційній безпеці України : правові аспекти”], (м. Київ, 6 жовт. 2016 р.) ; упоряд. : В.М. Фурашев. – К : Вид-во “Політехніка”, 2016. – С. 24-28.

43. Баранов О.А. Базовий принцип інформаційного права – забезпечення інформаційної безпеки : матеріали наук.-практ. конф. [“Запобігання новим викликам та загрозам інформаційній безпеці України : правові аспекти”], (м. Київ, 6 жовт. 2016 р.) ; упоряд. : В.М. Фурашев. – К : Вид-во “Політехніка”, 2016. – С. 29-35.

44. Золотар О.О. Загрози інформаційній безпеці людини // Правова інформатика. – № 2(42)/2014. – С. 70-79.

45. Ткачук Т. Складники інформаційної безпеки : аналіз критеріїв / Visegrad journal on human rights. – 2017 (4). – С. 153-158.

46. Пилипчук В., Дзьобань О. Глобальні виклики й загрози національній безпеці в інформаційній сфері // Вісник Національної академії правових наук України. – № 3 (78) 2014. – С. 43-52.

47. Дзьобань О.П., Соснін О.В. Інформаційна безпека: нові виміри загроз, пов’язаних з інформаційно-комунікаційною сферою / Гуманітарний вісник ЗДІА. – 2015. – № 60 – С. 25-34.

48. Могилевский В.Д. Системная безопасность: формализованный подход : мат. конференции [“Проблемы внутренней безопасности России в XXI веке”]. – М. : ЭДАС-ПАК, 2001. – С. 86-89.

49. Про рішення Ради національної безпеки і оборони України від 29.12.16 р. “Про Доктрину інформаційної безпеки України” : Указ Президента України від 25.02.17 р. № 47/2017. – Режим доступу : //www.president.gov.ua/documents/472017-21374. – Дата звернення 20.02.2018 р.

50. Доктрина інформаційної безпеки України – це лише декларація – експерти. – Режим доступу : https://www.radiosvoboda.org/a/28336852.html. – Дата звернення 21.08.2018 р.

51. Довгань О.Д. Інформаційна безпека : стан, проблеми, тенденції : матеріали круглого столу [“Інформаційні ресурси, інтелектуальна власність, комунікації в освітньо-науковій та інноваційній сферах : філософсько-правові та прикладні аспекти”], (м. Вінниця, 12 травня 2017 р.) : упоряд. О.Д. Довгань, М.В. Беланюк, С.А. Лапшин, О.Г. Радзієвська, О.І. Яременко. – К. : Видавничий дім “АртЕк”, 2017. – С. 31-39

52. Про рішення Ради національної безпеки і оборони України від 17.01.18 р. “Про проект Закону України “Про національну безпеку України” : Указ Президента України від 5.02.18 р. № 21/2018. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/21/2018/ paran2#n2. – Дата звернення 22.08.2018 р.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

УДК 340.132+321.011/014+351.86

ДОРОНІН І.М., *кандидат юридичних наук, доцент,*
завідувач наукової лабораторії
НДІ інформатики і права НАПрН України

ТРАНСФОРМАЦІЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНУ ЕПОХУ: ЗАГАЛЬНА ДОКТРИНА ТА ЇЇ ПРАВОВА СКЛАДОВА

Анотація. *У статті досліджено проблему трансформації національної безпеки. “Національна безпека” як доктрина, що виникла після Другої світової війни в США, передбачала правову складову. Досліджено також фактори впливу на розвиток доктрини національної безпеки в інформаційну епоху та викликані цим зміни у законодавстві.*

Ключові слова: *національна безпека, інформаційна епоха, правове регулювання, загрози національній безпеці*

Summary. *This article examines the problem of transformation of national security. National security as doctrine was established after World War II simultaneously with National Security legislation in the United States. In the Information Age there are some factors influencing national security. These factors lead to legislative changes.*

Keywords*: national security, information age, legislation, threats to national security.*

Аннотация. *В статье исследованы проблема трансформации национальной безопасности. “Национальная безопасность” на уровне доктрины возникла в США после Второй мировой войны и изначально предусматривала обязательную правовую составляющую. В статье также исследованы факторы воздействия на развитие доктрины информационной безопасности в информационную эпоху и вызванные ими изменения в законодательстве.*

Ключевые слова*: национальная безопасность, информационная эпоха, правовое регулирование, угрозы национальной безопасности.*

Постановка проблеми. Загальна кількість наукових публікацій, присвячених проблемам національної безпеки, її окремих складових та заходів з її забезпечення, які видані з часу здобуття Україною незалежності, налічує понад тисячу. Більшість з числа таких робіт побудовані на розумінні національної безпеки як певного стану, що стає метою і завданням для діяльності органів державного управління або ідеєю для консолідації суспільства навколо держави як соціального інституту. На початку XXI сторіччя у вітчизняному науковому дискурсі під впливом творів провідних філософів та соціологів (Д. Белл, М. Кастельс, Дж. Райт, Р. Рейч, Е. Тоффлер, А. Турен, С. Хантінгтон, Ф. Фукуяма) розпочалась модифікація ідей, беручи до уваги задекларовану зміну підходів, методів та самої наукової парадигми. Мова йде про усвідомлення основоположного та системоутворюючого характеру таких явищ як глобалізація, формування інформаційного суспільства та інформаційна або “цифрова” епоха, і пов’язані із нею явища цифрової економіки. Існують наукові публікації останнього часу, присвячені дослідженню впливу зазначених явищ на право в цілому та його окремі галузі. Проте щодо права національної безпеки таких праць практично немає, але вплив на нього зазначених явищ є очевидним.

Результати аналізу наукових публікацій. Слід зазначити, що традиційно проблеми забезпечення національної безпеки розглядались на стику права, державного управління і політології, насамперед це мало місце у розробленні теоретичних основ національної безпеки та понятійного апарату в цій сфері. Зокрема саме такий підхід

характеризує праці О. Бєлова, В. Білоуса, В. Горбуліна, О. Данільяна, О. Дзьобаня, Н. Нижник, В. Картавцева, А. Качинського, В. Косевцова, В. Крутова, В. Ліпкана, Г. Новицького, В. Пилипчука, Г. Ситника, Є. Скулиша, М. Стрельбицького, М. Панова, З. Чуйко та науковців, що досліджували окремі складові національної безпеки – економічну, політичну, екологічну, фінансову, інформаційну, соціальну та ін. Що стосується дослідження проблематики забезпечення національної безпеки у контексті інформаційного та адміністративного права то варто відзначити напрацювання Б. Андресюка, В. Бєлєвцевої, К. Бєлякова, О. Довганя, І. Коржа, О. Литвиненка, В. Настюка, Н. Нижник та ін.

Водночас відчувається брак робіт щодо комплексного осмислення проблем права національної безпеки, його особливостей стосовно інформаційної сфери та пов’язаних із цим питань забезпечення інформаційної безпеки, кібербезпеки та захисту інформації з урахуванням глобального характеру соціальних змін в інформаційну (цифрову) епоху.

Мета статті полягає у визначенні проблемних питань трансформації національної безпеки в цифрову епоху, правового регулювання суспільних відносин у цій сфері, з’ясування характеру глобальних змін та їх вплив на право. Також метою статті є визначення основних напрямів наступних досліджень.

Виклад основного матеріалу. Як правило, проблематику національної безпеки та її забезпечення розглядають через призму виникнення та розвитку категорії “безпека”, виводячи розуміння цієї категорії від античних філософів Аристотеля, Платона, Діогена, Епікура, Цицерона та інших [1, с. 122-127; 2, с. 10; 3, с. 29-30; 4, с. 28-30]. Слід зазначити, що універсальне розуміння категорії “безпека” притаманно для різних її видів, а сама термінологія, яка побудована навколо поняття “безпека” використовується у різних суспільних науках.

Стосовно виокремлення з цього блоку понять окремого поняття “національна безпека” в правовій науці слід зазначити наступне. Існують різні точки зору стосовно історичних передумов становлення національної безпеки, але сам термін “національна безпека” безперечно походить із США. У подальшому відбувалась активна рецепція зазначеного терміну та пов’язаної ідеології у політичні погляди та суспільні науки більшості країн світу, не кажучи вже про численні публіцистичні статті і політичні рефлексії. Хоча значення терміну може розглядатись по-різному, а чинне законодавство США уникає прямих дефініцій для понять, що використовуються, можливо розглянути загальне розуміння цього терміну в наступних значеннях. По-перше – це державна політика, яка інтегрує в собі внутрішню, зовнішню та оборонну політику, що спрямована на захист безпеки нації (в значенні – народу США) та просування її інтересів за кордоном. По-друге – це стан національної оборони, що спроможний протидіяти будь-якому супротивнику відкрито чи таємно [5, с. 319]. І нарешті в Директиві *(executive order)* Президента США № 12356 від 2 квітня 1982 року, яка присвячена питанням збереження інформації щодо національної безпеки, зазначене поняття розуміється як національна оборона або зовнішні відносини США (п. “е” ст. 6.1 Директиви) [6]. Але слід зазначити, що таке визначення “національної безпеки” не претендує на універсальний характер і може розумітись лише як визначення сфер державної політики, яких торкатиметься інформація з національної безпеки, що підлягає державному захисту.

На сьогодні дослідники розділились у думках стосовно часу першої згадки терміну. До 1940-х років такий термін вживався в американському політичному дискурсі на рівні промов та дискусій з кінця XVIII сторіччя [7, с. 291].

У подальшому активізація вжиття терміну в суспільному життя та медійному просторі відбулась у рамках діяльності окремих консервативних громадських організацій, насамперед мова йде про Лігу національної безпеки *(National Security League)*, яку було утворено наприкінці 1914 року навколо патріотичної ідеології, спрямованої на підсилення військової могутності країни [7, с. 292]. Ідеологічними засадами цієї організації були американський націоналізм, антикомунізм та антилібералізм. Діяльність Ліги підтримували політики правого спектру поглядів і у період між світовими війнами вона нараховувала понад 50 000 активних членів практично у всіх штатах, тобто була найчисленнішою серед ідеологічно споріднених організацій, активно займалась пропагандистською і видавничою діяльністю і мала вплив на політичні рішення в органах влади. Хоча організація існувала до 1942 року і була розпущена через внутрішні суперечки та фінансові проблеми, її діяльність склала ідеологічне підґрунтя до розробки та прийняття законодавства у сфері національної безпеки США після Другої світової війни.

Розробка спеціального законодавства щодо національної безпеки відбувалась в рамках законодавчого забезпечення “доктрини Трумена” як сукупності політико-правових поглядів, що сформувались на початку холодної війни в умовах протистояння із СРСР та країнами комуністичної ідеології. Саме в актах законодавства було реалізовано концепції та ідеологію “національної безпеки”, що до цього була лише предметом дискусій та публіцистичних виступів. Зазначена концепція з’явилась досить швидко, оскільки ще у період 1943 – 1944 роках у межах стратегічного військового планування опрацьовувалась ідея військової присутності поза межами континентальної частини США і можливе зіткнення інтересів з СРСР [8, с. 349].

Основою нової доктрини був остаточний відхід від політики ізоляціонізму в зовнішній політиці та протидія радянській (комуністичній) ідеологічній експансії по всьому світу. У цей час в США сформувалась досить потужна група експертів та управлінців з числа військових керівників, розвідників, дипломатів та політологів, що спеціалізувались у дослідженні ідеології комунізму та радянської політичної системи. Водночас їх пропозиції стосовно побудови системи державного управління у цій сфері готувались спільно з юридичними радниками адвокатських фірм Нью-Йорку [9, с. 5].

Таким чином, концептуальні погляди щодо побудови системи національної безпеки від початку розглядались у контексті права і законодавства і були втілені у спеціальному законодавчому акті – Акті про національну безпеку 1947 року, який був першим нормативно-правовим актом у системі відповідного законодавства США. Попри свою назву, дефініцій для терміну “національна безпека” законодавчий акт не надає. Мета його прийняття визначена у статті 2 і полягала у забезпеченні комплексної програми майбутньої безпеки США, створенні комплексної політики та відповідних процедур для урядових органів, які пов’язані з національною безпекою, утворення (реорганізації) державних органів з управління військовою організацією, їх координації та цивільного контролю, стратегічного розвитку та єдиного ефективного управління [10]. Таким чином, зазначений законодавчий акт був не загальним документом, що визначає концептуальні засади політики, він мав суто прагматичне значення, а його прийняття зумовило досить істотну реорганізацію державних органів та вищих органів військової адміністрації США у період після закінчення Другої світової війни.

Радянському законодавству термін “національна безпека” був невідомий, а відповідні ідеологічні та світоглядні постулати не відповідали положенням панівної ідеології в СРСР. Лише з початком перебудови та безпосередньо перед розпадом СРСР (1990 – 1991 р.) проект концептуального документа з забезпечення національної безпеки

досить недовго розроблявся спеціально утвореною Президією Верховної Ради СРСР комісією з підготовки військової реформи та реформи системи забезпечення державної безпеки в умовах неприйняття реформ вищим військовим керівництвом держави. Як зазначив в інтерв’ю 2016 року голова цієї комісії Ю.Є. Рижов, відповідний проект не був розроблений, а комісія лише узгодила основні програмні тезиси майбутнього документа [11]. Тому вести мову про концептуальне розуміння національної безпеки в СРСР не видається за можливе. У подальшому законодавство Російської Федерації до 1996 року не вживало термін “національна безпека”.

В Україні термінологія “національної безпеки”, навпаки, відразу увійшла до вітчизняного правового поля. Зокрема, вже в січні 1992 року при Президентові України було створено відповідну комісію з напрацювання пропозицій до створення Ради національної безпеки із завданням розробки концепцій та відповідного законодавства у сфері національної безпеки [12, с. 160-162]. Рада національної безпеки України, як консультативно-дорадчий орган при Президентові України була створена 1 липня 1992 року.

На сьогодні в Україні існує певний масив актів законодавства у сфері національної безпеки і оборони, яке регулює правовідносини у цій сфері, хоча виокремлення права національної безпеки в окрему галузь права було запропоновано вітчизняними вченими порівняно недавно [13, с. 33]. Зазначена точка зору має бути цілком підтримана з огляду на те, що у сфері національної безпеки та оборони існує особлива, окрема, цілісна система відносин, що є об’єктом регуляторного впливу, а сам регуляторний вплив може бути охарактеризований специфічними прийомами регулювання, особливим порядком виникнення і формування прав і обов’язків, їх змісту та реалізації. У сфері, що розглядається, мова йде про коло регулювання, до якого входять суспільні відносини щодо:

- державного стратегічного планування у сфері національної безпеки;
- оборони держави та економічного забезпечення оборонних заходів;
- протидії підривній діяльності іноземних держав та організацій, що використовують невійськові або “гібридні” (поєднання військових, політичних, інформаційних, економічних) методи досягнення цілей;
- здійснення заходів із здобуття особливо важливої інформації за межами держави та впливу на державну політику інших держав щодо України (розвідувальна діяльність);
- проведення тимчасових обмежувальних заходів у ситуаціях, що загрожують безпеці держави;
- заходів з протидії тероризму, сепаратизму та політичному екстремізму;
- політики охорони державного кордону України, а також окремі складові правового режиму воєнної безпеки.

Звичайно, що ґрунтовна розробка проблеми права національної безпеки і оборони на базі вітчизняного законодавства є важливим завданням для правової науки у найближчому майбутньому.

Повертаючись до питання розвитку національної безпеки, як концепції, та її правового забезпечення, варто зазначити, що до початку XXI сторіччя система національної безпеки окремих держав та спільної (колективної) безпеки, яка діяла в рамках міжнародних об’єднань, розвивалась у напрямку вдосконалення механізмів управління, забезпечення економічного, технічного та наукового розвитку оборонного потенціалу держав за умови принципової очевидності супротивника. Такий стан був сталим до виникнення нових загроз глобального характеру. Хоча міжнародний тероризм, організована злочинність транснаціонального характеру, міграція населення були загрозами і раніше, глобалізація сучасного світу і розвиток інформаційних технологій мав особливий вплив на розвиток систем національної безпеки.

Найбільш знаковим фактором є посилення недержавних суб’єктів, здатних впливати на безпеку в глобальному масштабі та на національну безпеку окремих держав. Мова йде про транснаціональні (міжнародні) організації, на які не розповсюджується влада окремої держави і які обмежують суверенітет окремих держав [14, с. 11-12; 15; 16, с. 7-8; 17, с. 94-96; 18, с. 32]. Зазначений аспект проблеми розглядався у науковій літературі в основному в контексті участі таких суб’єктів у військових конфліктах, а також впливу транснаціональних корпорацій на здійснення функцій держави економічного характеру в окремих країнах. Але в останні роки обмеження державного суверенітету набуло особливого характеру з часу розповсюдження криптовалют оскільки відбувається обмеження суверенітету держав на рівні грошового обігу. Попри активне обговорення цього питання у пресі, пряма загроза є віддаленою, але при впровадженні ефективних та швидких механізмів використання криптовалют, як засобу платежів, суверенітет окремих держав, безумовно, буде значно обмежено. Особливість полягає ще й у тому, що розподілений характер криптовалют необмежено розширює кількість недержавних суб’єктів *(“а′кторів”* згідно термінології, що вживається в англомовній соціологічній літературі). Хоча існують координуючі органи, що забезпечують роботу системи криптовалют (наприклад, *Bitcoin Foundation*), але за своєю роллю вони не є органами управління, оскільки прямо не впливають на емісію криптовалюти [19; 20].

Ситуація з криптовалютами яскраво ілюструє вплив нових факторів, характерних насамперед для інформаційної (цифрової) епохи, на національну безпеку. Проте зазначений вплив не є очевидним з огляду на особливості правової системи у різних країнах.

Для України більш важливим є фактор впливу агресії Росії та збройних проявів сепаратизму на сході України на стан законодавства у сфері національної безпеки і оборони. Але навіть у реагуванні на такі фактори спостерігаються прояви трансформації суспільних відносин, характерних для інформаційної (цифрової) епохи.

Не вдаючись в детальний огляд точок зору з означеного питання, висловлених представниками суспільних наук за останні 20 – 30 років, варто зосередитись на наступних ключових моментах. Визначення “інформаційна ера” (інформаційна епоха) не є складовою історичної науки і тому визначити її часові рамки або чітко описати характер в історичному контексті неможливо. Як правило, під “інформаційною епохою” розуміють певний відрізок розвитку людства, що характеризується розповсюдженням персональних засобів обчислювальної техніки, комунікаційної техніки та відповідних технологій обробки і розповсюдження інформації загального користування.

Визначення “цифрової епохи” може розглядатися як синонім поняттю “інформаційної епохи”. Досить часто “цифровий” зміст епохи, особливо у публіцистиці або засобах масової інформації, розглядається синонімічно до “безпаперового”. Але може розумітись і як нове поняття, що визначає період розвитку людства в пост-інформаційну епоху. У такому разі “цифрова епоха” характеризується розповсюдженням соціальних комунікацій, що побудовані на глобальних комп’ютерних мережах (на відміну від традиційних об’єднань людей та подібних соціальних інститутів), скасування паперу та інших подібних технологій зберігання інформації як інформаційної основи, максимальне пришвидшення обміну інформацією, а також пов’язані явища – штучний інтелект, пряма комунікація між технічними пристроями з обмеженим втручанням людини, стрибкоподібний (емерджентний) розвиток технологій у різних сферах, який зумовлюється інформаційними технологіями [21, с. 45].

Слід зазначити, що ситуація, яка складається у світі в період “цифрової епохи”, безперечно впливає на національну безпеку. Як найбільш актуальні загрози варто

згадати масовані кібератаки у межах “гібридної війни” та вплив на формування суспільної думки шляхом застосування технологій маніпуляції в соціальних мережах [22; 23, с. 364; 24, с. 15-16]. Останній вид загроз є дискусійним оскільки на сьогодні немає правових засобів протидії зазначеному явищу, а законодавчі новації в окремих країнах викликають критику щодо можливого порушення інформаційних прав людини – на вільне висловлювання своїх думок, вільне збирання та зберігання інформації тощо [25 – 27; 28, с. 6-9]. Загалом ситуація щодо правового регулювання заходів протидії загрозам зазначеного типу не є простою, а проблеми, що виникають, є серйозним викликом для державного регулювання та права в цілому.

Розглядаючи контекст вітчизняного законодавства у сфері національної безпеки та оборони, слід зазначити, що його формування тривалий час відбувалось традиційним шляхом. Насамперед мова йшла про побудову військової організації держави і законодавче забезпечення нейтралізації та протидії загрозам, характерним для XX століття. Окремо слід зазначити про розпорошення предмету правового регулювання у сфері забезпечення національної безпеки, що було викликано значним розширенням змісту поняття “національна безпека”, якщо порівняти законодавчі дефініції у статті 1 вихідної редакції Закону України “Про основи національної безпеки України” від 19.06.03 р. та у редакції з урахуванням змін, внесених Законом України від 01.07.10 р. Загрози в інформаційній сфері, що відповідали характеру загроз у світовому масштабі з урахуванням трансформацій інформаційної епохи, спочатку розглядались на рівні документів доктринального характеру, починаючи зі Стратегії національної безпеки України, затвердженої Указом Президента України від 12.02.07 р. № 105. Але характер загроз розглядався в основному через призму протидії проявам злочинної діяльності в інформаційній сфері (комп’ютерна злочинність, а у подальшому – комп’ютерний тероризм), а також необхідності забезпечення захисту інформації з обмеженим доступом. Оскільки документи стратегічного планування у сфері національної безпеки фрагментарно визначали певне коло загроз та їх трансформацію, як правило, правове забезпечення так само було фрагментарним.

Після 2014 року масив законодавчих актів у сфері національної безпеки і оборони зазнав серйозних змін, при тому, що такі зміни остаточно ще не завершено. Слід зазначити, що визначення загроз відбувається більш адекватно, виважено, а їх характер визначається вірно. Водночас, до кінця поки що не сформовані напрями державної політики із забезпечення національної безпеки, до того ж існують значні прогалини у чинному законодавстві стосовно застосування військової сили на сході України та щодо відбиття нетрадиційних форм проявів агресії, які характерні для “гібридної війни”.

Висновки.

1. Доктрина “національної безпеки” походить з США, де з самого початку свого втілення (з 1947 року) відбувалось і відповідне її законодавче оформлення в першу чергу шляхом визначення мети законодавчого регулювання у забезпеченні комплексної програми майбутньої безпеки США, створенні державної політики та відповідних процедур для урядових органів, які пов’язані з національною безпекою, утворення (реорганізації) державних органів з управління військовою організацією, їх координації та цивільного контролю, стратегічного розвитку та єдиного ефективного управління. У подальшому зазначена доктрина використовувалась у державній політиці та законодавстві різних країн, але була не характерна для колишнього СРСР суто з ідеологічних причин.

2. У вітчизняному законодавстві термінологія “національної безпеки” вживалась практично з часу здобуття незалежності, з того ж часу відбувалась робота з концептуального визначення системи забезпечення національної безпеки та основ

державної політики у цій сфері, що завершилось прийняттям Закону України “Про основи національної безпеки України” та формуванням масиву відповідного законодавства у цій сфері.

3. Трансформація суспільства та світового порядку в інформаційну та цифрову епоху є фактором впливу в тому числі і на національну безпеку окремих держав. При цьому самі фактори впливу складні, швидкоплинні та непередбачувані. Зміна загроз, актуалізація, модифікація старих і виникнення нових вимагають швидких змін у державній політиці, що відбувається як на доктринальному, так і на законодавчому рівні.

4. Стан та терміни реагування на зміни загроз державними органами та відповідні зміни у законодавстві відбуваються з певним запізненням, що характерно для різних країн. Для України особливо критичною є трансформація тих загроз, що є проявами окремих форм “гібридної війни” проти нашої держави.

5. Ситуація щодо правового регулювання заходів протидії загрозам нового типу (масовані кібератаки, використання соціальних медіа для маніпулювання суспільної свідомістю та комбінація таких дій у кіберпросторі) є складною, а проблеми, що вникають є серйозним викликом для законодавчого регулювання та права в цілому. Зазначена проблематика зумовлює уточнення завдань для дослідження у сфері права національної безпеки на найближче майбутнє.

Використана література

1. Викторов А.Ш. Введение в социологию безопасности / А.Ш. Викторов. – М. : Канон+, 2008. – 567 с.

2. Тимків Я. Теорія і практика сучасної європейської політики безпеки : приклад Польщі / Я. Тимків. – Львів : Вид-во Львівської політехніки, 2011. – 224 с.

3. Шаблистий В.В. Історико-правові аспекти філософської концепції безпеки людини // Право і суспільство. – 2012. – № 5. – С. 109-115.

4. Горбатюк С.Є. Еволюція феномену безпеки : від стародавніх політико-правових учень – до сучасної наукової думки // Вісник НАДУ при Президентові України. – 2016. – № 2. – С. 28-35.

5. O`Leary M. The Dictionary of the Homeland Security and Defense : Words and Terms in Common Usage/Margaret O`Leary. – N.Y. : iUniverse Inc, 2006. – 499 p.

6. US Presidents` Executive Order 12356 “National Security Information”, 02.04.1982. – Режим доступу : https://www.archives.gov/federal-register/codification/executive-order/12356.html. – Назва з екрана. – Дата звернення 01.03.2018 р.

7. Shulman Mark. The Progressive Era Origins of the National Security Act / Mark R. Shulman // Dickinson Law Review. – 2000. – Vol. 104:2. – P. 289-330.

8. Leffler Melvyn. The American Conception of National Security and the Beginnings of the Cold War, 1945-48 // American Historical Review. – 1984. – Vol.89 (No 2). – P. 346-381.

9. Hogan Michael. A Cross of Iron : Harry S. Truman and Origins of the National Security State, 1945-1954. – Cambridge, University Press. 2000. – 540 p.

10. Act of July 26, 1947 (“National Security Act”), Public Law 80-253, 61 STAT 495. – Режим доступу : https://catalog.archives.gov/id/299856. – Назва з екрана. – Дата звернення 01.03.2018р.

11. Веденеева Н. Академик Юрий Рыжов : “Россия стоит на пороге жуткого краха” / “Московский комсомолец”, 26.12.2016. – Режим доступу http://www.mk.ru/science/2016/12/25 /akademik-yuriy-ryzhov-rossiya-stoit-na-poroge-zhutkogo-krakha.html. – Назва з екрана. – Дата звернення 01.03.2018 р.

12. Картавцев В.С. Історико-правові аспекти розбудови системи забезпечення національної безпеки України // Науковий вісник Дипломатичної академії України. – 1998. – Вип. 1. – С. 160-168.

13. Пилипчук В.Г. Пріоритети розвитку правової науки в галузі національної безпеки // Вісник НАН України. – 2009. – № 5 – С. 30-35.

14. Kay Sean. Globalization, Power and Security // Security Dialogue. – 2004. –Vol. 45. – No 1. – P. 9-25.

15. MacKay J. State Failure, Actor-Network Theory and the Theorization of Sovereignty // Brussels Journal of International Studies. – 2006. – Vol.3. – P. 61-98.

16. Глотов Б. Трансформація державного суверенітету в умовах глобалізації: український контекст // Державне управління та місцеве самоврядування. – 2012. – Вип. 4(15). – С. 6-14.

17. Дзьобань О.П. Проблеми захисту національних інтересів України у сфері державної безпеки в умовах геополітичних трансформацій XXI століття / О.П. Дзьобань, В.Я. Настюк, В.В. Бєлєвцева. – Х. : Право, 2013. – 296 с.

18. Сімутін В. Перспективи організації та функціонування механізму сучасної держави // Jurnalul Juridic naţional : teorie şi practică. – 2014. – № 4. – С. 31-35.

19. De Filippi P., Loveluck B. The invisible politics of Bitcoin : governance crisis of a decentralized infrastructure // Internet Policy Review. – 2016. – Vol. 5, Issue 3. – Режим доступу : https://pdfs.semanticscholar.org/5761/af4eff318e876f2990aa53469352826214a0.pdf. – Назва з екрана. – Дата звернення 01.03.2018 р.

20. Oermann M., Töllner Nils. The Evolution of Governance Structure in Cryptocurrencies and the Emergence of Code-Based Arbitration in Bitcoin // Hans-Bredow Institute for Media Research. – Режим доступу : https://publixphere.net/i/noc/page/IG_Case_Study_Bitcoin_and_Autonomous _Systems. – Назва з екрана. – Дата звернення 01.03.2018 р.

21. Доронін І.М. Проблеми трансформації функцій держави в інформаційну епоху : матеріали наук.-практ. конф. [“Теоретико-правові основи формування та розвитку інформаційного суспільства”], (Київ, 29.11.2017 р.) : упоряд. В.М. Фурашев, С.Ю. Петряєв. – К. : Вид-во “Політехніка”, 2017. – С.43-48.

22. Iasiello E. Cyber Attack : A Dull Tool to Shape Foreign Policy/E.Iasiello // 5th International Conference on Cyber Conflict: Tallinn, 2013. – Режим доступу : https://ccdcoe.org/cycon/2013/ proceedings/d3r1s3_Iasiello.pdf. – Назва з екрана. – Дата звернення 08.03.2018 р.

23. Refined Concepts of Massive and Flexible Cyber Attacks with Information Warfare Strategies/ [H.Moga, M.Boscoianu, D.Ungureanu, F.Sandu, R.Boboc] // Journal of Communications. – 2017. – Vol. 2, No 6. – P. 364-370.

24. Social Media as a Tool of Hybrid Warfare. Public Report prepared by the NATO Strategic Communications Centre of Excellence / Ed. Anna Reynolds. – Riga, NATO StratCom COE, 2016. – 47 p.

25. Tambini D. Fake News : Public Policy Responses. Media Policy Brief 20. – London : Media Policy Project, London School of Economics and Political Science. 2017, March. – Режим доступу : http://eprints.lse.ac.uk/73015/1/LSE 20MPP 20Policy 20Brief 2020 20-20Fake 20news_final.pdf. – Назва з екрана. – Дата звернення 08.03.2018 р.

26. Maass D. California Bill To Ban “Fake News” Would Be Disastrous for Political Speech / Electronic Frontier Foundation Issue, March, 28.2017. – Режим доступу : https://www.eff.org/deep links/2017/03/california-bill-ban-fake-news-would-be-disastrous-political-speech. – Назва з екрана. – Дата звернення 08.03.2018 р.

27. Savage P. Russian Social Media Information Operations : How Russia has Used Social Media to Influence US Politics //American Security Project. Fact Sheet, October, 2017. – Режим доступу : https://www.americansecurityproject.org/wp-content/uploads/2017/10/Ref-0206-Russian-Social-Media-Information-Operations.pdf. – Назва з екрана. – Дата звернення 08.03.2018р.

28. Klein D. Fake News : A Legal Perspective/David Klein, Joshua Wueller // Journal of Internet Law. – 2017. – Vol. 20, No 10. – P. 5-13.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

УДК: 342.1+355/359

БОЛДИР С.В., начальник Департаменту охорони державної таємниці та ліцензування Служби безпеки України

РЕФОРМУВАННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ: ПРАВОВІ АСПЕКТИ

Анотація. *У статті аргументується необхідність якнайшвидшого перегляду поглядів та усталених традицій до існуючих у національній практиці напрямів охорони державної таємниці з урахуванням досвіду держав-учасниць НАТО та ЄС, а також наводяться та описуються основні напрями такого перегляду.*

Ключові слова: *реформування законодавства, система охорони державної таємниці, безпека інформації, стандарти НАТО та ЄС.*

Summary. *The article grounds the necessity of prompt reassessment of approaches and established traditions towards existing in national practice directions of protection of classified information taking into consideration the experience of the NATO and EU member states, and also presents and describes the main directions of such reassessment.*

Keywords: *legislation reforming, system of protection of state secrets, information security, NATO and EU standards.*

Аннотация. *В статье аргументируется необходимость скорейшего пересмотра взглядов и упроченных традиций к существующим в национальной практике направлениям охраны государственной тайны с учетом опыта государств-членов НАТО и ЕС, а также определяются и описываются основные направления такого пересмотра.*

Ключевые слова: *реформирование законодательства, система охраны государственной тайны, безопасность информации, стандарты НАТО и ЕС.*

Постановка проблеми. Події, які спостерігаються на світовій арені, супроводжуються процесом перерозподілу зон впливу у світовому просторі, розвитком інформаційних технологій, що породжують нові способи заволодіння інформацією. У зв’язку з цим, питання убезпечення секретної інформації є актуальними та потребують від держав, незалежно від їх розвитку та впливовості, постійного зміцнення власної системи охорони секретної інформації, а також вимагають спроможності не лише відбити загрози безпеці інформації, а й мінімізувати ризики, у разі реального витоку секретних відомостей.

Незмінність курсу нашої держави у євроатлантичний простір, незважаючи на військову агресію Російської Федерації на сході України, окупацію частини нашої суверенної території, а також проведення нею різноманітних спеціальних інформаційних операцій, направлених, зокрема, і на розхитання світового устрою, вимагає від України відійти від традиційних підходів до охорони державної таємниці, які тягнуться з часів СРСР, та виробити зовсім новий погляд на безпеку інформації, спираючись як на власні напрацювання українських вчених, так і на євроатлантичний досвід із зазначеного питання.

Результати аналізу наукових публікацій. На науковому рівні питання, пов’язані з реформуванням системи охорони державної таємниці, досліджували такі науковці як С. Князєв, І. Мейдич, О. Розвадовський, О. Семенюк, Т. Ткачук, В. Шлапаченко та інші. Разом з тим, події XXI сторіччя, пов’язані з витоками секретних відомостей, наштовхують на необхідність ще раз з’ясувати цінність інформації у вільному суспільстві та спробувати оцінити наслідки від її розголошення. Задля мінімізації ризиків витоку такої інформації,

робота з виокремлення та ґрунтовного вивчення напрямів системи охорони державної таємниці, які потребують удосконалення, має вестися на постійній основі як з урахуванням набутого Україною власного досвіду забезпечення безпеки інформації під час протистояння збройній агресії Російської Федерації, так і наявних напрацювань держав-учасниць НАТО та ЄС.

Метою статті є визначення окремих аспектів реформування системи охорони державної таємниці (перегляд функціонування дозвільного порядку провадження діяльності пов’язаної з державною таємницею, допускної системи, а також окремих питань інженерно-технічного захисту інформації) з огляду на євроатлантичні прагнення нашої держави.

Виклад основного матеріалу. Адаптація законодавства до норм Європейського Союзу є однією з найважливіших складових політики європейського вибору України та будь-якої іншої держави, яка йде шляхом європейської інтеграції. За даними міжнародних експертів, для входження України в правове поле Європи необхідно прийняти нові або внести відповідні зміни майже в чотири тисячі законів та інших нормативно-правових актів. Це означає, що все законодавство України повинне бути модифіковане відповідно до міжнародних принципів і стандартів [1, с. 32].

Не є винятком і національне законодавство у сфері охорони державної таємниці та службової інформації. Зазначене обумовлено, передусім, наявністю певних розбіжностей у підходах до захисту інформації з обмеженим доступом у державах євроатлантичної спільноти та в Україні.

Разом з тим, слід зазначити, що реформування законодавства має відбуватися на основі всебічного вивчення досвіду провідних держав світу у сфері безпеки інформації. Однак, потрібно зауважити, що копіювання чужого, нехай і найуспішнішого досвіду, недостатньо продумане перенесення його на наш ґрунт без урахування українських реалій ніколи не приводило до успіху [2, с. 342].

Слід зазначити, що окремі напрями реформування системи охорони державної таємниці та службової інформації (пов’язані із процедурами віднесення інформації до такої, що потребує обмеження у доступі; визначення на законодавчому рівні Національного органу безпеки; питання технічного захисту інформації) було висвітлено у минулому науковому дослідженні [3, с. 79].

Поряд з цим, на увагу заслуговують й інші питання у сфері безпеки інформації, що стосуються дозвільного порядку провадження діяльності, пов’язаної з державною таємницею; процедур перевірки громадян у зв’язку з допуском до державної таємниці, а також окремих питань інженерно-технічного захисту інформації, та потребують подальшого удосконалення в рамках реформування системи охорони державної таємниці та службової інформації. Пропонуємо розглянути кожен із напрямів більш детально.

З огляду на євроінтеграційні прагнення нашої держави, одним з першочергових напрямів, що потребує змін, є дозвільна система провадження діяльності, пов’язаної з державною таємницею.

Відповідно до статті 20 Закону України “Про державну таємницю” державні органи, органи місцевого самоврядування, підприємства, установи, організації мають право провадити діяльність, пов’язану з державною таємницею, після надання їм Службою безпеки України спеціального дозволу на провадження діяльності, пов’язаної з державною таємницею (далі – Спеціальний дозвіл) [4].

Водночас, законодавець повинен визначитись з доцільністю надання такого дозволу державним органам, враховуючи мету їх створення – здійснення функцій держави.

При вирішені вказаного питання слід враховувати, що суб’єктами режимно-секретної діяльності в більшості є державні органи, зупинення чи скасування яким відповідного Спеціального дозволу призведе до припинення їх діяльності. Наведене є неприпустимим з огляду на необхідність забезпечення сталого функціонування певних галузей діяльності держави особливо за умов ведення воєнних (бойових) дій.

Якщо звернутися до міжнародного досвіду із зазначеного питання, зокрема, до законодавства держав-учасниць НАТО та ЄС, можемо пересвідчитися, що державним органам дозвіл на роботу з класифікованою інформацією не оформлюється, оскільки їх діяльність безпосередньо пов’язана з реалізацією та виконанням функцій держави у т.ч. у сфері оборони, державної безпеки та охорони правопорядку тощо.

З огляду на міжнародний досвід, а також з метою мінімізації ризиків уникнення нестабільного виконання органами державної влади своїх функцій, пропонується досконало вивчити питання щодо можливості відмови від оформлення такого дозволу державним органам, які відповідно до покладених завдань виконують секретні роботи, а належний стан режиму секретності на такій категорії суб’єктів режимно-секретної діяльності підтримувати за допомогою заходів офіційного контролю.

Залишається невирішеним і питання щодо процедури надання, переоформлення Спеціального дозволу державним органам, підприємствам, установам, організаціям (далі – Установи), керівником яких є іноземний громадянин.

Сьогодні у процес реформування різноманітних сфер діяльності держави залучаються іноземні громадяни, шляхом призначення їх на керівні посади Установ, у тому числі і на ті, які провадять діяльність, пов’язану з державною таємницею. Водночас, як вже зазначалося вище, такі Установи мають право провадити відповідну діяльність після надання їм Службою безпеки України відповідного Спеціального дозволу. Разом з тим, частиною десятою статті 20 Закону наголошено, що Спеціальний дозвіл не надається, якщо керівник Установи не є громадянином України або не має допуску до державної таємниці [4].

Одним із шляхів вирішення вказаного питання є надання можливості уповноваженому органу СБУ здійснювати заходи з надання, переоформлення Спеціального дозволу Установам, у разі призначення іноземця на керівну посаду, за умови взяття ним письмового зобов’язання щодо збереження державної таємниці та надання йому на підставі відповідного розпорядження Президента України та за дозволом СБУ доступу до державної таємниці.

Стандартами безпеки НАТО та ЄС приділено неабияку увагу й питанням захисту інформації під час виконання підприємствами недержавної форми власності контрактів або робіт, пов’язаних із секретними відомостями.

Так, з метою зниження рівня ймовірності реалізації загроз, пов’язаних із розголошенням інформації з обмеженим доступом, яка використовується промисловими підприємствами під час виконання секретних контрактів, застосовуються заходи і процедури з її охорони. Таким чином, у стандартах безпеки НАТО та ЄС уводиться поняття “промислова безпека”, яке наразі у національному законодавстві відсутнє, в рамках якої і здійснюються відповідні заходи щодо захисту інформації. Разом з тим, для виконання секретних контрактів або роботи над секретним дослідженням з використанням інформації з обмеженим доступом з грифом CONFIDENTIAL (еквівалент грифу секретності “Таємно”) чи вище, підприємству має бути надано відповідний Спеціальний дозвіл [5; 6].

Крім того, вже на стадії попередніх переговорів або проведення тендерів щодо укладення секретних контрактів від підприємств вимагається вжиття відповідних заходів з охорони інформації з обмеженим доступом, а співробітники підприємства до

надання відповідного Спеціального дозволу повинні у встановленому порядку отримати доступ та пройти інструктаж з питань безпеки.

Впровадження зазначеного євроатлантичного досвіду у національне законодавство у частині забезпечення ефективної системи захисту інформації на підприємствах недержавної форми власності, які провадять секретні роботи, а також уведення відповідного поняття, еквівалентного “промисловій безпеці” із відповідним змістовним наповненням надасть змогу, на нашу думку, деякою мірою мінімізувати ті ризики, що виникають під час виконання такими суб’єктами державного замовлення чи передачі секретної інформації від замовника до виконавця тощо.

Поряд із дозвільним порядком провадження діяльності, пов’язаної з державною таємницею, враховуючи умови сьогодення, потребують перегляду і підходи до забезпечення функціонування допускної системи у цій сфері.

Так, у рамках цієї роботи проаналізовано основні положення і вимоги нормативних приписів у зазначеній сфері НАТО, ЄС та окремих держав-учасниць цих міжнародних організацій, формування безпекового законодавства яких відбувалося за схожих з існуючими в Україні умов (Польща, Румунія, Болгарія, Словаччина, Чехія тощо).

За результатами дослідження визначено, що принциповим підходом до можливості надання доступу особам до секретної інформації, закріпленим стандартами НАТО та ЄС, є визначення необхідності доведення до особи секретних відомостей у зв’язку з виконанням нею службових обов’язків (принцип “need-to-know” – “необхідного знання”, як правило, встановлюється керівником суб’єкта режимно-секретної діяльності), наявність свідоцтва про проходження необхідних процедур з питань безпеки, спрямованих на встановлення лояльності та надійності особи (“Personnel Security Clearance” – найближчим еквівалентом в українському законодавстві є “допуск”), а також проведення навчання та інструктажу з питань безпеки, що проводяться відносно особи, якій надається доступ до секретної інформації.

Вбачається, що законодавство України у зазначеній сфері не повною мірою узгоджується зі стандартами безпеки НАТО та ЄС, а також з системою надання доступу до секретної інформації держав-учасниць цих міжнародних організацій.

Відповідно до статті 1 Закону України “Про державну таємницю” – допуск до державної таємниці – оформлення права громадянина на доступ до секретної інформації.

При цьому слід зазначити, що прямий переклад відповідного терміну, що застосовується у стандартах безпеки НАТО та ЄС (“Personnel Security Clearance Certificate”), означає – “сертифікат очистки персоналу з питань безпеки”, “свідоцтво про проходження персоналом процедур безпеки”, тобто мається на увазі, що особі надається сертифікат, який свідчить про позитивний результат перевірки особи щодо її лояльності, міри довіри до неї, що дає можливість надавати їй доступ до секретної інформації [5; 6].

Такі сертифікати, згідно з національним законодавством держав-учасниць НАТО та ЄС (зокрема Польщі, Румунії, Болгарії, Чехії, Словаччини тощо), видаються уповноваженим державним органом, що здійснює (або організовує) відповідну перевірку з питань безпеки, на певний термін залежно від ступеня секретності інформації, з якою особа планує працювати. При цьому, такий сертифікат залишається чинним незалежно від ситуативної потреби особи у роботі з секретними документами.

Необхідно зауважити, що національним законодавством Польщі, Румунії, Болгарії, Чехії, Словаччини тощо передбачено, що глибина перевірки безпосередньо залежить від ступеня секретності інформації, до якої планується надати доступ особі.

Так, відповідно до законів Польщі, Румунії, Болгарії перевірка поділяється на “базову” (для доступу до інформації зі ступенем секретності, еквівалентному “Таємно”),

“розширену” (для доступу до інформації із ступенями секретності, еквівалентними “Цілком таємно”, “Особливої важливості”), а також “контрольну” (здійснюється у разі встановлення підстав для скасування дії такого сертифікату, зокрема таких як нелояльність, ненадійність, неправдивість тощо) [7 – 9].

Разом з тим, залежно від глибини перевірки особи та її оточення застосовуються наступні критерії, які ґрунтуються на визначенні ступеня її надійності, лояльності та рівні довіри до неї. Таким чином, для побудови уявлення про особу враховується інформація щодо:

- можливих протиправних вчинків у сфері шпіонажу, тероризму, саботажу, зради або заколоту;
- алкогольної, наркотичної, лікарської залежності;
- психічних або емоційних розладів;
- здійснення несанкціонованих дій у комунікаційно-інформаційних системах;
- можливої вразливості осіб до тиску з боку родичів та близьких їй осіб, на яких можуть впливати служби іноземних розвідок, терористичні групи чи інші підривні організації або особи [5; 6].

На нашу думку, зазначені критерії перевірки особи та членів її сім’ї чи осіб, які з нею проживають в рамках надання їй доступу до інформації з обмеженим доступом визначеного ступеня секретності вбачаються такими, що охоплюють майже увесь спектр тих рушійних сил, що можуть вплинути на особу та, як наслідок, на безпеку інформації, що їй була довірена.

Крім цього, законодавством Чехії, Словаччини передбачено можливість при перевірці у зв’язку з необхідністю роботи з відомостями зі ступенем секретності, еквівалентним “Особливої важливості”, застосовувати як оперативні, так і оперативно-технічні заходи, спрямовані не лише на об’єкт перевірки, а й на його оточення [10; 11].

У зв’язку з цим, важливим аспектом є строки проведення безпекової перевірки, від яких безпосередньо залежить якість результатів перевірочних заходів (індикативні терміни перевірки, встановлені законодавством окремих держав-учасниць НАТО та ЄС, наведено у таблиці 1).

Таблиця 1

Еквівалентність ступеня секретності інформації, у зв’язку з доступом до якої проводиться безпекова перевірка	**Строки проведення перевірки**			
	Польща	**Чехія**	**Болгарія**	**Румунія**
TOP SECRET – “Особливої важливості”	до 3 місяців	до 6 місяців	30 днів	30 днів
SECRET – “Цілком таємно”			45 днів	60 днів
CONFIDENTIAL – “Таємно”			60 днів	90 днів

Вбачається, що саме диференційований та поглиблений підхід до перевірки осіб у зв’язку з їх доступом до секретної інформації дає уповноваженим органам зазначених держав-учасниць НАТО та ЄС можливість видання вказаних сертифікатів про безпекову перевірку без необхідності їх скасування у зв’язку з відсутністю потреби особи у роботі із секретною інформацією.

Під час збору, обробки та зберігання інформації про особу та її оточення в ході проведення перевірки мають запроваджуватися відповідні заходи щодо її схоронності. Таке збереження зазвичай здійснюється із застосуванням, технічних засобів захисту інформації. Як свідчить вітчизняна практика, в більшості державних органів

використовується програмне забезпечення та інструментальні засоби іноземного виробництва, оскільки на державному рівні недостатньо приділено увагу створенню, удосконаленню та впровадженню власного як технічного, так і програмного забезпечення. Зазначене може спричинити порушення таких властивостей інформації, як цілісність та конфіденційність, що може завдати шкоди інтересами громадян та держави.

Також необхідно зауважити, що законодавством зазначених держав-учасниць НАТО та ЄС не передбачено процедур, аналогічних погодженню “номенклатури посад, перебування на яких потребує оформлення допуску та надання доступу до державної таємниці” на кожному підприємстві, установі, організації, як це визначено в українському законодавстві.

Нормативно-правові акти у сфері охорони інформації з обмеженим доступом окремих країн передбачають складання на підприємствах, установах, організаціях “переліків посад, перебування на яких потребує роботи з відомостями з обмеженим доступом”, що затверджуються керівниками таких суб’єктів режимно-секретної діяльності.

При цьому, Національні органи безпеки мають право контролювати правомірність віднесення посад до такого переліку.

Також, законодавство держав-учасниць НАТО та ЄС не передбачає грошової компенсації особам за роботу в умовах режимних обмежень. Як правило, підвищена грошова винагорода таким особам визначається залежно від тарифікації посад, перебування на яких потребує доступу до секретної інформації.

З огляду на наведене, пропонується основні зусилля у рамках реформування існуючої допускної системи скерувати за такими напрямами:

1. Відмовитись (шляхом внесення змін до законодавчих актів або видання нової редакції відповідного закону) від терміну “допуск до державної таємниці”, який є спадщиною режимних вимог колишнього СРСР та призводить до обмежень застосування органами СБУ усіх можливих підстав для відмови в його наданні або скасуванні, впровадити на його заміну визначення “сертифікат про безпекову перевірку” (або споріднене з ним).

2. Встановити диференційований обсяг (що відповідатиме вимогам стандартів НАТО та ЄС) безпекової перевірки громадян в залежності від ступеня секретності такої інформації.

3. З метою забезпечення якості перевірочних заходів передбачити строк проведення безпекової перевірки до 3 місяців (з урахуванням досвіду Польщі).

4. Розглянути питання щодо можливості встановлення норми, згідно з якою безпекова перевірка здійснюватиметься відносно осіб, які претендують на заняття посади, що передбачає доступ до секретної інформації, тобто ще до їх призначення (зазначені положення існують у законодавстві Польщі, Болгарії тощо).

5. Передбачити, що сертифікат за результатами такої перевірки видається на встановлений строк залежно від ступеня обмеження доступу до інформації та не потребує скасування у разі відсутності потреби у громадянина доступу до секретної інформації (на відміну від норми, встановленої у статті 26 Закону України “Про державну таємницю”).

6. Від грошової компенсації за роботу в умовах режимних обмежень перейти на диференційовану тарифікацію посад, які передбачають роботу із секретною інформацією, оскільки існуюча система провокує необґрунтоване віднесення посад до таких, що передбачають роботу із секретними документами, та призводить до невиправданого розширення кола осіб, що матимуть доступ до секретної інформації.

7. Відмовитися від підготовки підприємствами, установами, організаціями номенклатур посад, перебування на яких потребує оформлення допуску та надання доступу до державної таємниці, та їх погодження органами СБУ. Натомість встановити, що керівники підприємств, установ, організацій здійснюють погодження переліку посад, перебування на яких передбачає доступ до секретної інформації, правильність складання якого перевірятиметься органами СБУ у ході проведення заходів офіційного контролю.

Крім того, надійне функціонування дозвільного та допускного порядку провадження діяльності, пов’язаної з державною таємницею, не може оминати питань застосування заходів та засобів фізичного захисту безпеки інформації та забезпечення контролю доступу до режимних Приміщень (зон, територій).

Так, приписами Закону України “Про державну таємницю” передбачено комплекс заходів, спрямованих на охорону державної таємниці, одним із яких є інженерно-технічний захист відомостей, який досягається відповідними засобами охорони [4].

Зокрема, національним законодавством визначено, що до інженерно-технічних засобів охорони належать інженерні споруди, загорожі, пристрої, обладнані технічними засобами охорони і призначені для запобігання несанкціонованому чи безконтрольному доступу сторонніх осіб в режимні Приміщення (зони, території).

В науковій літературі аспекти інженерно-технічного захисту інформації розглядаються як такі, що загалом спрямовані не безпосередньо на інформацію, а на системи, об’єкти та носії, на яких інформація збирається, обробляється й розповсюджується [12, с. 220].

Разом з тим, варто зазначити, що фінансування питання впровадження надійних заходів та засобів інженерно-технічного захисту суб’єктами режимно-секретної діяльності у більшості випадків здійснюється за залишковим принципом.

Однак, зазначене питання як ніколи набрало своєї значимості, оскільки в умовах військового протистояння відсутність ґрат, залізних дверей чи іншого спеціалізованого обладнання, призначеного для забезпечення режиму секретності на об’єкті, не дозволить, навіть на деякий час, зупинити супротивника та здійснити заходи, передбачені на випадок виникнення надзвичайної ситуації. При цьому, ціна інформації в умовах ведення воєнних дій є вкрай високою, а її неконтрольований витік може спричинити невиправних наслідків для подальшого планування та проведення військових операцій.

Звертаючись до євроатлантичного досвіду із зазначеного питання, слід зазначити, що стандартами безпеки НАТО та ЄС передбачено дещо інший підхід до інженерно-технічного захисту інформації.

Зокрема, уведено поняття “фізична безпека”, зміст якого полягає у застосуванні фізичних захисних заходів щодо місць, будівель та Приміщень, в яких знаходиться інформація, яка потребує захисту від втрати або розголошення [5; 6].

При цьому, зазначені заходи безпеки залежать від загроз, ступенів обмеження доступу і кількості матеріальних носіїв інформації, що захищатимуться.

Тобто для забезпечення фізичної безпеки в усіх Приміщеннях, будинках, офісах, кімнатах (далі – Приміщення) та на територіях, де зберігається та/або обробляється інформація з обмеженим доступом передбачено встановлення зон безпеки інформації відповідного класу (клас I, клас II, адміністративна зона) [5; 6].

Зони безпеки класу I та II призначені для обробки та зберігання інформації зі ступенем NATO CONFIDENTIAL (еквівалент “Таємно”) та вище. Разом з тим, вхід до зони класу I для всіх практичних цілей розглядається як доступ до секретної інформації. При цьому, усі входи та виходи Приміщення обладнуються відповідними системами вхідного контролю, що дозволяють доступ лише тих осіб, яким у встановленому порядку надано допуск та які мають Спеціальний дозвіл до цієї зони.

У зоні безпеки класу ІІ можливо охороняти інформацію з обмеженим доступом визначеного вище ступеня секретності від доступу сторонніх осіб шляхом встановлення внутрішнього контролю. Вхід до цієї зони можливий як особам, яким надано допуск та які мають Спеціальний дозвіл, так і іншим особам, які пропускаються за умовами наявності супроводження або еквівалентного контролю [5; 6].

Навколо або на підходах до зон безпеки класу І та ІІ може встановлюватися адміністративна зона. Така зона вимагає наявності візуально визначеного периметра, усередині якого є можливість здійснювати контроль за персоналом та транспортними засобами. При цьому, в адміністративних зонах може оброблятися та зберігатися тільки інформація із ступенем обмеження доступу не вище NATO RESTRICTED (еквівалент “Для службового користування”) [5; 6].

Тобто встановлення у Приміщеннях або на території відповідної зони безпеки відповідного класу залежить від інформації, яка в них циркулює (ступінь її секретності, кількість і форма обробки, її зберігання), категорії співробітників, які підпадають під дію принципу “необхідного знання” (доступ до інформації обумовлено виконанням службових обов’язків), а також оцінки загроз інформації.

Слід зазначити, що у національній практиці присутній аналог зонування, водночас відмінність полягає у висунутих вимогах до їх обладнання, які більшою мірою залежать тільки від природи виникнення носія інформації, заходи із захисту якої планується здійснювати.

Таким чином, в рамках комплексного підходу до зміцнення системи охорони державної таємниці, вбачається доцільним розглянути питання щодо впровадження диференційованих підходів до застосування фізичних та технічних заходів захисту інформації залежно від наданого грифу обмеження доступу до інформації. Вказане дозволить запобігти, своєчасно виявити, перешкодити протиправній діяльності іноземних спеціальних служб, спрямованій на здобування секретних відомостей, посяганням на інформацію з боку окремих організацій, нелояльних співробітників чи їх груп, полегшити процес розмежування доступу до секретної інформації, з урахуванням принципу “необхідного знання”, що звузить коло обізнаних осіб, а також надасть можливість удосконалити діяльність з виявлення порушень встановлених правил безпеки.

Крім того, слід наголосити, що з огляду на необхідність підвищення рівня захисту державної таємниці, а також приведення законодавства України у вказаній сфері діяльності у відповідність до стандартів безпеки НАТО та ЄС, з метою сприяння подальшій інтеграції України в європейське співтовариство, питання реформування системи охорони державної таємниці та службової інформації є доволі важливим та потребують залучення до їх вирішення різних інституцій держави та громадськості.

Висновки.

Підсумовуючи зазначене, можна дійти висновку, що наразі державна таємниця розглядається як один із найважливіших видів інформації з обмеженим доступом, а розголошення її може призвести до породження нових загроз державній безпеці. Таким чином, охорона державної таємниці є однією із складових частин загальної системи забезпечення національної безпеки України. А подальший розвиток та постійне вдосконалення системи охорони державної таємниці та службової інформації забезпечуватиме адекватне і гнучке реагування на можливі загрози її безпеці.

Саме тому метою зазначеної статті було визначення окремих напрямів реформування системи охорони державної таємниці, а також надання відповідних пропозицій, зокрема:

- Спеціальний дозвіл на провадження діяльності, пов’язаної з державною таємницею державним органам, які відповідно до покладених завдань виконують секретні роботи не

оформлювати, а належний стан режиму секретності на такій категорії суб’єктів режимно-секретної діяльності підтримувати за допомогою заходів офіційного контролю;

- на заміну терміну “допуск до державної таємниці” впровадити визначення “сертифікат про безпекову перевірку” (або споріднене з ним);

- відмовитися від підготовки підприємствами, установами, організаціями номенклатур посад, перебування на яких потребує оформлення допуску та надання доступу до державної таємниці, та їх погодження органами СБУ;

- встановити диференційований обсяг (що відповідатиме вимогам стандартів НАТО та ЄС) безпекової перевірки громадян в залежності від ступеня секретності такої інформації;

- впровадити диференційовані підходи до застосування фізичних та технічних заходів захисту інформації залежно від наданого грифу обмеження доступу до інформації.

На нашу думку, реалізація висвітлених напрямів реформування системи охорони державної таємниці докорінно змінять підходи до забезпечення безпеки інформації та нададуть змогу убезпечити власну таємницю.

Використана література

1. Нормативно-правове забезпечення стратегічного курсу України на європейську та євроатлантичну інтеграцію : навчальний посібник-хрестоматія : у 2-х ч. ; уклад. і коментар І.В. Артьомов, Д.В. Вітер, Л.І. Загайнова, О.М. Казакевич, О.М. Руденко. – Ужгород : Ліра, 2007. – Ч. 1. – С. 32.

2. Семенюк О.Г. Проблеми охорони державної таємниці : кримінально-правові та кримінологічні аспекти : монографія. – К. : ТОВ “Видавничий дім “АртЕк”, 2017. – С. 342.

3. Болдир С.В. Перспективи реформування системи охорони державної таємниці та службової інформації // Інформація і право. – № 4(23)/2017. – С. 79-85.

4. Про державну таємницю : Закон України від 21.01.94 р. № 3855-XII // Відомості Верховної Ради України (ВВР). – 1994. – № 16.

5. Security within the North Atlantic Treaty Organisation (C-M(2002)49). – Available as : http://arhives.nato.int/amendments-to-nato-document-security-within-nato-c-m-55-15-final

6. Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU). – Available as : http://publications.europa.eu/en/publication-detail/-/publication/d43001e3-356d-11e3-806a-01aa75ed71a1/language-en

7. The Act of 5 August 2010 on the Protection of Classified Information (Poland). – Available as : http://www.infor.pl/akt-prawny/194475,metryca,ustawa-o-ochronie-informacji-niejaw nych.html

8. National standarts on the protection of classified information in Romania, Government decision no 585/2002 [Online tool]. – Available as: http://www.orniss.ro/en/legislatie/pdf/GD585.pdf.

9. Classified Information Protection Act (Bulgaria) [Online tool]. – Available as : http://www.dksi.bg/NR/rdonlyres/070CA55F-EAD3-435D-BE41A01-AC62A005D/-/0/-CLASSIFIEDINFORMATIONPROTECTIONACT.doc

10. Czech Republic: Act No. 412 of 21 September 2005 on the Protection of Classified Information [Online tool]. – Available as : http://www.right2info.org/laws/Chech_Protection_classified_info.pdf/at_download/file

11. Slovakia : Act No. 215/2004 Coll. On the Protection of Classified Information and on Amendments to Certain Acts (as amended up to July 1, 2013) [Online tool]. – Available as : http://www.wipo.int/wipolex/en/details.jsp?id=15574

12. Кормич Б.А. Інформаційне право : підручник / Б.А. Кормич. – Харків : “Бурун і К”, 2011. – С. 220.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 343.98.065

ПАРФИЛО О.А., *кандидат юридичних наук, старший науковий співробітник,*
професор кафедри інформаційно-правової культури
та комунікативної політики Укртелерадіопресінституту
ЛЕОНОВ Б.Д., *доктор юридичних наук, старший науковий співробітник,*
провідний науковий співробітник
Національної академії Служби безпеки України

ЗАСТОСУВАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ І МЕТОДІВ ВИЯВЛЕННЯ ТА РОЗПІЗНАВАННЯ ОСІБ, ЯКІ МАЮТЬ НАМІР ВЧИНИТИ ТЕРАКТ

Анотація. *У статті розглядаються актуальні питання застосування сучасних технологій і методів виявлення та розпізнавання осіб, які мають намір вчинити теракт. Аналізується позитивний зарубіжний досвід експлуатації систем виявлення та розпізнавання осіб. Виділяються найбільш оптимальні способи розпізнавання облич.*

Ключові слова*: розпізнавання облич, особи, які мають намір вчинити теракт, сучасні технології.*

Summary. *The article deals with urgent questions of the use of state-of-art technologies and methods of person’s identification and face recognition (persons who intend to commit a terrorist attack). The positive foreign experience of using the system of person’s identification and face recognition is analyzed. Attention is drawn to the best ways of face recognition.*

Keywords: *face recognition, persons who intend to commit a terrorist attack, state-of-art technologies.*

Аннотация*. В статье рассматриваются актуальные вопросы применения современных технологий и методов выявления и распознавания лиц, имеющих намерение совершить теракт. Анализируется позитивный зарубежный опыт эксплуатации систем выявления и распознавания лиц. Выделяются наиболее оптимальные способы распознавания лиц.*

Ключевые слова*: распознавание лиц, лица, имеющие намерение совершить теракт, современные технологии.*

Постановка проблеми. Результати аналізу щоденних повідомлень міжнародних інформагентств підтверджують високий рівень терористичної загрози у світі. Драматичні події, які відбулися 22 травня 2017 року у Манчестері та 17 серпня 2017 року у Барселоні, засвідчили, що проблеми тероризму набули глобального характеру та потребують нових ідей та рішень у боротьбі з цим явищем. Незважаючи на зусилля світового співтовариства у протидії тероризму, непоодинокі терористичні акти практично у всіх країнах світу свідчать про недостатню ефективність створюваних систем протидії терористичній загрозі.

Оскільки тероризм постійно змінює форми та набуває глобального масштабу, його способи і методи стають все більш витонченими та руйнівними. Вступ людства в інформаційну епоху, розвиток науково-технічного прогресу потребує розробки та впровадження новітніх технологій та технічних рішень з метою протидії проявам тероризму. Саме тому в останні роки відбувається все більш широке впровадження технологій біометричної ідентифікації осіб. Зростання інтересу до цих технологій пояснюється швидкозростаючою їх ефективністю та можливостями використання саме за напрямом протидії терористичним загрозам. Підвищення ефективності технологій

біометричної ідентифікації забезпечується зростанням потужності обчислювальної техніки, що робить можливим швидкий пошук у великих базах даних біометричних ознак і дозволяє в реальному часі реалізовувати дедалі складніші та ефективніші алгоритми і набори біометричних ознак.

Біометричні технології можуть бути використані для вирішення різноманітних завдань, серед яких головною є криміналістична ідентифікація людини. Її сутність полягає у пошуку у максимально наповненій базі даних зразків, найбільш схожих з тією, яку ідентифікують. У криміналістиці для цього широко використовують методи габітоскопічної ідентифікації, особливо ідентифікації людини за зображенням обличчя. До переваг системи ідентифікації особистості за зображенням обличчя можна віднести наступні: відсутність фізичного контакту із пристроєм введення даних (особі непотрібно обов’язково дивитися у відеокамеру), прихованість, доступність даних та простота їх отримання.

Водночас, успіх системи ідентифікації особи за фотопортретом багато в чому залежить від точності виявлення, локалізації та розпізнання особи на зображенні.

Результати аналізу наукових публікацій. Окремі аспекти криміналістичного дослідження зовнішності з метою ідентифікації особи висвітлено у працях, авторами яких є: Н. Ахтирська, В. Бахін, Р. Бєлкін, П. Біленчук, І. Борисенко, І. Винниченко, В. Гарбар, М. Герасимов, В. Гончаренко, Ю. Дубягін, О. Дубягіна, В. Житніков, В. Захаров, О. Зінін, В. Колдін, В. Колмаков, І. Крилов, П. Кузнєцов, В. Кузьмічов, В. Лукашевич, Г. Мамедов, І. Мартиненко, Є. Моісеєв, В. Образцов, М. Салтевський, З. Самошина, М. Сегай, В. Снєтков, О. Сокиринська, М. Терзієв, А. Топорков, А. Ухаль, П. Цвєтков, М. Чернець, В. Шепітько, М. Яблоков та інших учених.

Декілька наукових робіт, зокрема А. Мовчан [1], О. Свістільніков [2], було присвячено застосуванню сучасних технологій для вирішення завдань оперативного розпізнання терористичних загроз.

Разом з тим питання виявлення та розпізнавання осіб, які мають намір вчинити теракт, із застосуванням сучасних інноваційних технологій та методів залишається не до кінця розкритим, що й зумовлює актуальність даного дослідження.

Метою статті є виявлення на основі аналізу позитивного зарубіжного досвіду у сфері боротьби з тероризмом найбільш оптимальних способів розпізнавання осіб, які мають намір вчинити теракт.

Виклад основного матеріалу. Технології та методи розпізнавання осіб в історії криміналістики почали застосовуватися, коли з’явилися перші фотокартки (з XIX-го століття), ще до активного впровадження пошуку людей за відбитками пальців.

Спосіб розпізнавання обличчя людини заснований на тому, що є певні точки і відстані між ними – міжбровна відстань, відстань між зіницями та інші, які не змінюються, як не змінюють зовнішність. Вони відносяться до будови черепа, а не до м'яких тканин. Тобто, борода, вуса і навіть пластичні операції не можуть змінити обличчя настільки, щоб не можна було впізнати особу.

Раніше за допомогою лінійки вимірювали розташування таких точок на обличчі і звіряли з записами на папері. Тепер, в епоху цифрових технологій, камери з високою роздільною здатністю передають дані програмам, які міряють відстань між “вузловими точками” обличчя: довжину і ширину носа, відстань між очима тощо. Потім на інших знімках, навіть в різних ракурсах, можна порівняти відстань між заданими точками і з великою ймовірністю ідентифікувати людей.

Базовим принципом інтелектуальних систем відеоспостереження є відеоаналітика – технологія, що базується на методах та алгоритмах розпізнавання образів і обробки

зображення, автоматизованого збору даних в результаті аналізу відеопотоку. Створені алгоритми без участі людини здатні виявити і відстежити в реальному часі задані цілі (автомобіль, групу людей), потенційно небезпечні ситуації (задимлення, загорання, несанкціоноване втручання в роботу відеокамер) та вчасно видати тривожний сигнал.

Сьогодні одним з основних методів детектування (знаходження) осіб в кадрі є метод, який використовує каскади Хаара. Найчастіше висока точність виявлення досягається для осіб, зображення яких потрапили в кадр анфас, при цьому в загальному випадку класифікатор методу можна навчити розпізнавати зображення облич і в інших положеннях.

Що стосується сучасного етапу розвитку технології розпізнавання облич, новим рішенням стало використання тривимірного моделювання за допомогою стереокамер. 3D-модель обличчя допомагає досягти значно вищих показників точності. В алгоритм роботи системи додається ще один етап – це побудова 3D-моделі обличчя в режимі реального часу з подальшим аналізом особливостей обличчя вже просторової моделі.

Найбільш популярні системні рішення для розпізнавання осіб “Face-Інтелект” (розробник – компанія AxxonSoft), “Kipod” (компанія Синезис) і “VOCORD FaceControl” (компанія VOCORD) демонструють: високу ймовірність ідентифікації об’єкта (до 99 %); підтримку широкого діапазону кутів повороту відеокамер; можливість виявлення осіб навіть в щільному натовпі; варіативність складання аналітичних звітів. Зокрема, “Face-Інтелект” може використовувати сторонні бази даних осіб, наприклад, урядових установ або правоохоронних органів. Підтримка універсального протоколу обміну даними забезпечує ще більшу ефективність використання таких систем на об’єктах транспортної, спортивної та розважальної інфраструктур [3].

З кожним роком збільшується роздільна здатність відеокамер та удосконалюються самі алгоритми розпізнавання осіб. Сьогодні ці системи працюють досить ефективно в багатьох країнах світу. Наприклад, китайська компанія Cloud Walk тестує систему, що не тільки розпізнає обличчя, але й аналізує ходу людини, місця її перебування і які товари вона купує. Якщо людина, скажімо, відвідує магазини зброї, вона стає підозрілою. За словам представника Cloud Walk, немає нічого кримінального, якщо людина, наприклад, купила кухонний ніж. Але якщо разом з ножем вона ще купила мішок і молоток, а також часто з’являється в місцях масового скупчення, – така особа для системи вважається потенційно небезпечною [4]. Перевага такої системи полягає в тому, що вона працює автономно – сама збирає й обробляє масив даних з відеокамер, і сама повідомляє про підозрілих осіб в правоохоронні органи.

Згідно з даними дослідницької компанії IHS Markit, в Китаї налічується більше 176 мільйонів камер спостереження, очікується, що далі їх число буде лише зростати. На сьогоднішній день владою Китаю вже встановлені системи розпізнавання осіб в навчальних закладах, на вулицях і в місцях масового скупчення людей для запобігання порушенню правил громадської поведінки, дорожнього руху і виявлення випадків девіантної поведінки. За словами заступника Міністра науки й технологій КНР Лі Мена, використання розумних систем і технологій штучного інтелекту дозволить визначати заздалегідь, хто може скоїти щось протизаконне та хто може бути потенційним терористом [5].

Після терактів у Парижі керівництво громадським транспортом у Франції почало впровадження низки заходів із забезпечення безпеки пасажирів. Завдяки припиненому нападу на пасажирів потягу Thalys влітку 2016 року, на всіх вокзалах, що відправляють потяги міжнародних ліній, були встановлені програмно-апаратні комплекси з камерами, датчиками і рамками з металодетекторами. Програмне забезпечення цих

комплексів здатне реєструвати аномальні зміни голосу, температури тіла, ходи, а потім на основі аналізу цих даних попереджати про підозрілу поведінку того або іншого пасажира. Фахівці, знайомі з технікою аналізу поведінки пасажирів, зазначають, що можливо заздалегідь визначити потенційну небезпеку людини, яка має намір здійснити теракт [6].

У Німеччині також запроваджено систему розпізнавання облич. Зокрема, на берлінській залізничній станції Зюдкройц розпочали тестувати систему розпізнавання облич, яка покликана підвищити безпеку людей у громадських місцях. Відеокамери цієї системи розташовані на контрольному пункті і система фіксує всіх пасажирів, що перетинають контрольний рубіж. При виявленні ознак схожості пасажира з розшукуваним злочинцем (що знаходиться в розшуку не лише за злочини терористичного характеру, а й за інші протиправні діяння) система сигналізує про це співробітникам поліції [7].

Існує вулична мережа камер зі схожими алгоритмами розпізнавання і в лондонському Сіті. Поліція Уельсу почала тестування аналогічної технології під час проведення фіналу Ліги чемпіонів в м. Кардіфф. Якщо цей досвід буде визнаний успішним, правоохоронні органи Великої Британії сподіваються розширити використання нових методів для запобігання злочинам. Вони можуть застосовуватися для забезпечення громадської і національної безпеки, наприклад, для контролю ситуації в аеропортах [8].

Слід зазначити, що до цього часу спеціалістами провідних країн світу продовжується розробка програмних продуктів та технічних рішень на працездатність яких не повинні впливати інтенсивність освітлення, раса і вік особи, зміна зачіски, макіяж, окуляри, а також інші фактори.

Завдяки нейромережам системи комп’ютерного зору досягли рекордної точності в розпізнанні облич. Особа людини майже безпомилково розпізнається на звичайних фотографіях, навіть на тих де обличчя видно лише частково. Створені алгоритми, що враховують навіть одяг, ходу та вік людини. Наприклад, OpenFace у 80 % випадках змогла ідентифікувати осіб на змінених “старінням” фото людей.

Розглянемо на прикладі системи розпізнавання на основі відеосканування “FaceVACS” можливості та функціональність таких систем, зокрема:

- відслідковує та ідентифікує одне або багато облич за допомогою відеокамер прямої трансляції або матеріалів відео-зйомки;
- здійснює порівняння у реальному часі з базами даних зображень і списками особливого контролю;
- паралельно обробляє численні потоки зображень з камер і відеоданих;
- здійснює спостереження за громадськими місцями (наприклад, за стадіонами, залізничними вокзалами, аеропортами або конференц-центрами для виявлення та ідентифікації конкретних осіб);
- здійснює спостереження за режимними об’єктами, доступ до яких дозволено лише службовим особам (наприклад, за АЕС, військовими базами, хімічними заводами тощо) для виявлення та ідентифікації зловмисників і сторонніх осіб;
- порівнює зображення обличчя людини з цільовими даними (розшукуваними людьми або підозрюваними у вчиненні терористичних злочинів особами);
- порівнює збіги з наявними оперативними даними або з архівом відеоданих;
- порівняння відбувається з даними, що зберігаються в системі, або з наявними правовими базами даних (національною базою даних, базами ФБР, Інтерполу, власними базами даних тощо), з якими система з’єднана;

- систему можна під’єднати до графічної надструктури систем безпеки, що робить можливим поточний он-лайн-контроль місця, де перебуває особа, за якою ведеться спостереження.

Висновки.

Підсумовуючи вищенаведене, зазначимо, що з огляду на позитивний зарубіжний досвід експлуатації систем виявлення та розпізнавання осіб ці технології ефективно можуть бути використані і в антитерористичній діяльності. Водночас слід відзначити окремі аспекти застосування сучасних технологій виявлення та розпізнавання осіб, які мають намір вчинити теракт, а саме:

1. Більшість провідних країн світу запроваджують системи розпізнавання облич, використовуючи різні технології. Найбільш оптимальним способом розпізнавання облич є 3D-розпізнавання – алгоритм якого має суттєві переваги перед більш ранніми системами, реалізованими за допомогою двовимірного відеозображення. Метод вимагає установки декількох спеціальних стереокамер, синхронізованих між собою.

2. Сьогодні існує декілька легальних способів захисту від оперативного розшуку за допомогою систем розпізнавання облич. Наприклад, як справжні футбольні вболівальники, так і особа, яка має намір проникнути на стадіон інкогніто зі злочинною метою, можуть за допомогою спеціального макіяжу, який візуально змінює геометрію і пропорції обличчя людини, розфарбуватися в кольори футбольного клубу (чи збірної), і тим самим порушити визначення лицьових опорних точок. Оскільки сучасними об’ємними тривимірними камерами обладнано не дуже багато таких систем, розпізнавання розмальованого у такий спосіб обличчя людини з двомірного “плоского” знімку є досить проблематичним.

3. Політика більшості провідних країн світу виходить із необхідності створення комплексної системи протидії тероризму з боку світової спільноти, що включає: посилення взаємодії правоохоронних та розвідувальних органів, надання допомоги та сприяння в боротьбі з тероризмом, у т.ч. шляхом обміну інформацією щодо терористичних організацій та бойовиків-терористів, включаючи їх біометричні ідентифікаційні дані.

4. Впровадження програмно-апаратних комплексів біометричної ідентифікації людини в правоохоронну діяльність створить технічні можливості для виявлення осіб, причетних до терористичної та іншої протиправної діяльності. Реалізація цієї пропозиції вимагає розробки та впровадження на міжнародному рівні уніфікованого програмного забезпечення, що за критерієм вибірковості охоплюватиме всі ідентифікаційні дані осіб, які підозрюються у терористичній діяльності, відомості про яких містяться у відповідних інформаційних базах правоохоронних органів та спеціальних служб.

Використана література

1. Мовчан А.В. Застосування сучасних технологій для вирішення завдань оперативного розпізнання терористичних загроз // Боротьба з організованою злочинністю і корупцією (теорія і практика) : наук.-практ. журнал. – 2013. – № 1(29). – С. 53-61.

2. Свистильников А.Б. Использование автоматизированных информационно-поисковых систем в идентификации личности террориста и предупреждении террористических актов на объектах транспорта. – Режим доступу : https://cyberleninka.ru/article/n/ispolzovanie-avtomatizirovannyh-informatsionno-poiskovyh-sistem-v-identifikatsii-lichnosti-terrorista-i-preduprezhdenii

3. Розпізнавання і пошук схожих осіб. – Режим доступу : http://www.axxonsoft.com/ua/products/intellect/faceintellect

4. Система распознавания лиц. – Режим доступу : http://carnegie.ru/commentary/73279

5. Как в Китае готовятся арестовывать за будущие преступления. – Режим доступу : https://news.tj/ru/news/world/20171005/kak-v-kitae-gotovyatsya-arestovivat-za-budutshie-prestup leniya

6. Железные дороги Франции тестируют программу распознавания террористов. – Режим доступу : http://www.penki.lt/Informacionnye-tekhnologii/ZHeleznye-dorogi-Francii-testiruyut-programmu-raspoznavaniya-terroristov.im?id=354192&f=c

7. У Берліні тестують систему розпізнавання облич у громадських місцях. – Режим доступу : http://www.eurointegration.com.ua/news/2017/08/23/7070084

8. Атака на Лондон : 15 главных мер в борьбе с террором. – Режим доступу : http://www.bbc.com/russian/uk/2015/07/150707_london_bombing_changes

9. FaceVACS – система розпізнавання на основі відеосканування. – Режим доступу : http://vabb.com.ua/service/innovation/faces

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

УДК 342.52

МАРУЩАК А.І., *доктор юридичних наук, професор*,
директор Навчально-наукового інституту перепідготовки
та підвищення кваліфікації кадрів СБУ
Національної академії Служби безпеки України

ІНФОРМАЦІЙНО-ПРАВОВІ АСПЕКТИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Анотація. *У статті досліджуються питання інформаційно-правових аспектів протидії кіберзлочинності в Україні. Сформульовано пропозиції щодо удосконалення інформаційного та кримінального процесуального законодавства з метою підвищення ефективності розслідування кіберзлочинів правоохоронними органами України.*

Ключові слова: *кіберзлочин, правоохоронні органи, інформаційне право, протидія кіберзлочинності.*

Summary. *The article deals with the issues of information law aspects of counteraction to cybercrime in Ukraine. The proposals on improvement of information and criminal procedural legislation are formulated in order to increase the effectiveness of the investigation of cybercrime by law enforcement agencies of Ukraine.*

Keywords: *cybercrime, law enforcement agencies, information law, counteraction to cybercrime.*

Аннотация. *В статье исследуются вопросы информационно-правовых аспектов противодействия киберпреступности в Украине. Сформулированы предложения по усовершенствованию информационного и уголовного процессуального законодательства с целью повышения эффективности расследования киберпреступлений правоохранительными органами Украины.*

Ключевые слова: *киберпреступление, правоохранительные органы, информационное право, противодействие киберпреступности.*

Постановка проблеми. Комп’ютерна або кіберзлочинність набула міжнародних масштабів, кількість злочинів у сфері інформаційних технологій постійно зростає. Серйозне занепокоєння викликає використання та розповсюдження програм-вірусів, “троянів”, фішингових програм, поширення фактів несанкціонованого доступу до державних інформаційних ресурсів, викрадення інформації з баз даних, знищення та модифікація даних у інформаційних системах, перехоплення інформації тощо.

Україна останніми роками дедалі більше відчуває на собі масштаби кібернетичних загроз і їх негативні наслідки. Так, у 2017 році підрозділами Національної поліції України розслідувалось понад 21,7 тис. кримінальних правопорушень у сфері інформаційних технологій. У 2017 році виявлено майже 14 тис. таких кримінальних правопорушень. Розслідувались наступні категорії злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж, відповідальність за які встановлена статтями 16 розділу особливої частини Кримінального кодексу України: за ст. 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку) КК України – 2606; ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програм чи технічних засобів, а також їх розповсюдження або збут) КК України – 56; ст. 361-2 (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) КК України – 83; ст. 362 (Несанкціоновані дії з інформацією, яка оброблюється 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) КК України – 863, ст. 363 (Порушення правил експлуатації електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку або порядку чи правил захисту інформації, яка в них оброблюється) КК України – 34 та ст. 363-1 (Перешкоджання роботі електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку шляхом масового розповсюдження повідомлень електрозв’язку) КК України – 4.

Крім цього, виявлено кваліфіковані види кримінальних правопорушень й інших категорій, пов’язані з використанням інформаційних технологій, відповідальність за вчинення яких, передбачено ст. 176 (Порушення авторського права і суміжних прав) КК України – 107, ст. 185 (Крадіжка) КК України – 173^1, ч. 3, 4 ст. 190 (Шахрайство) КК України – 419^2, ст. 200 (Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення) КК України – 456, ст. 229 (Незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару) КК України - 32, ст. 231 (Незаконне збирання інформації, що становить банківську таємницю) КК України – 61 та ч. 3, 4, 5 ст. 301 (Ввезення, виготовлення, збут і розповсюдження порнографічних предметів) КК України – 647.

У 10236 або 47 % кримінальних правопорушень про кіберзлочини, досудове розслідування у яких здійснювали слідчі Національної поліції, оголошено про підозру, з них у 9552 або 68 %, що вчинені у поточному році [1].

27 червня 2017 р. відбулася масована кібератака на інформаційно-телекомунікаційні системи державних органів. З метою з’ясування методів реалізації акції кібертероризму, встановлення джерел її походження, виконавців, організаторів і замовників, СБ України організовано взаємодію з партнерськими правоохоронними органами, спеціальними службами іноземних країн та міжнародними організаціями у сфері кібербезпеки. До проведення детального дослідження отриманого тіла вірусу, з’ясування обставин вірусного ураження комп’ютерних мереж об’єктів критичної інфраструктури, можливих негативних наслідків залучено можливості інопартнерів (ФБР США, Національної агенції по боротьбі зі злочинністю (NCA) Великобританії, МІТ Туреччини).

Останні кібератаки на державні органи, установи і підприємства України зумовили посилення заходів кібербезпеки на загальнодержавному рівні. Так, прийнятий Верховною Радою України Закон “Про основні засади забезпечення кібербезпеки України” визначив правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [2].

Результати аналізу наукових публікацій свідчать про те, що питання інформаційно-правових аспектів протидії кіберзлочинності частково були предметом досліджень. У вітчизняній юридичній літературі науковим розвідкам окремих питань цієї проблематики в різні часи приділяли увагу такі фахівці, як В. Брижко, В. Бутузов, В. Пилипчук, К. Тітуніна, М. Швець, О. Юрченко та інші. Автор розглядав дотичні питання у контексті розвитку інформаційного права України як науки [3].

Метою статті є розкриття інформаційно-правових аспектів протидії кіберзлочинності в Україні. Робимо акцент на проблемних питаннях виявлення, припинення і розслідування кіберзлочинів, виникнення яких (проблем) пов’язане, по-перше, із сутністю інформації, а, по-друге, із недостатнім правовим регулюванням інформаційної та правоохоронної діяльності.

Виклад основного матеріалу. Насамперед відзначимо, що протидія кіберзлочинності ускладнена недостатнім врахуванням сучасних інформаційних технологій у відповідному інформаційному і кримінальному процесуальному законодавстві. Тому на сьогодні, **“**збирання доказів в електронній формі є достатньо нелегким процесом, що зумовлено складністю об’єктів… не кожний слідчий володіє спеціальними знаннями у сфері комп’ютерних технологій у достатній мірі, щоб успішно організувати розслідування… Тому вилучення та дослідження об’єктів в електронній формі за можливості має проводити фахівець**”** [4].

Складність виявлення, припинення і розслідування кіберзлочинів значною мірою пов’язана із електронною формою інформації. Наприклад, сьогодні користувачі широко використовують хмарні технології зберігання інформації, порядок доступу до якої визначається власником інформації і власником ресурсу для збереження інформації, який може знаходитися (і часто знаходяться) у різних державах під різними юрисдикціями. Відповідно для українських правоохоронців важливо знати і правильно використовувати законодавство тієї держави, де фізично зберігається інформація про факт або сліди кіберзлочину. Знання вимог інформаційного права такої держави дозволяє правильно сформулювати запит щодо надання офіційної правової допомоги, про що йдеться нижче.

З метою виявлення, припинення і розслідування кіберзлочинів існує необхідність суттєвого удосконалення існуючої системи обміну інформацією в режимі реального часу між основними суб'єктами забезпечення кібербезпеки. Активні процеси щодо удосконалення взаємодії правоохоронних органів (насамперед, Кіберполіції та СБ України) з Держспецзв’язком України дещо покращить оперативність розслідування кіберзлочинів, однак не вирішить питань взаємодії двох правоохоронних органів.

Крім того, виявлення, припинення і розслідування кіберзлочинів потребує належної взаємодії не тільки правоохоронних органів між собою, а й з приватними суб’єктами. Наприклад, сьогодні в Україні відсутня загальнодержавна база IP-адрес, існування якої сприяло б забезпеченню негайного розкриття вчинених кіберзлочинів. Адже встановлення унікальної IP-адреси і її зв’язок зі злочинцем (потерпілим) є одним із найважливіших етапів розслідування кіберзлочинів. Проблемним також є той факт, що унаслідок обмеженої кількості IP-адрес провайдери використовують динамічні IP-адреси (Dynamic IP Address) завдяки протоколу динамічного налаштування вузла (Dynamic Host Configuration Protocol – DHCP) [4].

Таку базу IP-адрес, як видається, доцільно створити у межах державно-приватного партнерства Держспецзв’язку з операторами, провайдерами послуг Інтернет-доступу.

Припинення кіберзлочину та ліквідація його наслідків вимагає оперативності. У процесуальному законодавстві багатьох країн-учасниць Конвенції про кіберзлочинність є норми, які передбачають особливий порядок перехоплення і розкриття інформації про рух даних у комп’ютерних системах задля розслідування кіберзлочинів [5].

Однак, відповідно до чинного Кримінального процесуального кодексу України (КПК України) [6] для отримання інформації від операторів і провайдерів, необхідної для припинення злочину або встановлення винних у його вчиненні, ліквідації негативних

наслідків від кримінального правопорушення, зокрема блокування (обмеження) ресурсу з протиправним контентом, правоохоронні органи витрачають значний час для отримання відповідного рішення суду в межах кримінального провадження. Таким чином, і**снує потреба у** наданні додаткових повноважень правоохоронним органам, які здійснюють розслідування кіберзлочинів, пов’язаних із доступом до інформації, яка має значення при розслідуванні кіберзлочинів. Більшість таких повноважень передбачені Конвенцією про кіберзлочинність. Крім того, Указ Президента України від 13.02.17 р. № 32 **“**Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 **“**Про загрози кібербезпеки держави та невідкладні заходи щодо їх нейтралізації**”** передбачає розробку законодавчих пропозицій щодо підвищення ефективності протидії злочинам у кіберпросторі [7].

У цьому контексті, зважаючи на особливості інформаційних відносин у кіберпросторі, насамперед, необхідно:

– закріпити визначення поняття цифрових (електронних) доказів;

– передбачити ефективний і оперативний механізм обмеження (блокування) певного інформаційного ресурсу (інформаційного сервісу);

– впровадити специфічні умови проведення обшуку і арешту цифрових (електронних) доказів, насамперед, передбачити процесуально значиму можливість копіювання даних.

Підвищить ефективність розслідування кіберзлочинів імплементація у вітчизняне законодавство статей 16-18 Конвенції про кіберзлочинність, а саме невідкладне фіксування і подальше зберігання даних операторами, провайдерами телекомунікацій, постачальниками послуг хостингу, власниками ресурсу (веб-сайту, веб-сторінки, тощо) із забезпеченням їх цілісності. Потребують впровадження у вітчизняне законодавство норми статті 19 (Обшук і арешт комп’ютерних даних, які зберігаються) Конвенції про кіберзлочинність шляхом закріплення можливості копіювати електронні дані, здійснювати їх пошук, а також їх блокувати/арештовувати. Відповідні процесуальні дії доцільно здійснювати на підставі ухвали слідчого судді, суду, а фактичні дані, отримані подібними способами вважати допустимими доказами у кримінальному провадженні.

Доволі чутливим для громадянського суспільства, але виправданим з огляду на характер загроз безпеці людини, суспільства і держави в кіберпросторі, є запровадження обмеження (блокування) доступу до інформаційних ресурсів (сервісів), що здійснюватиметься операторами, провайдерами телекомунікацій, постачальниками послуг хостингу, власниками ресурсу (веб-сторінки, веб-сайту тощо) стосовно інформації, що містить ознаки діяння, передбаченого законом України про кримінальну відповідальність на підставі ухвали слідчого судді, суду. Подібний процесуальний захід доцільно застосовувати у вичерпних випадках, а саме щодо ресурсів, через які розповсюджуються або з використанням яких вчиняються: пропаганда війни; публічні заклики, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади; публічні заклики, спрямовані на зміну меж території або державного кордону України на порушення порядку, встановленого Конституцією України; дитяча порнографія; шахрайства, яке вчиняється з використанням інформаційно-телекомунікаційних систем; незаконне розповсюдження зброї, бойових припасів або вибухових речовин; незаконне розповсюдження наркотичних засобів, психотропних речовин, їх аналогів чи прекурсорів або фальсифікованих лікарських засобів.

Безумовно існує потреба у законодавчій регламентації механізмів сприяння правоохоронним органам України у формі надання необхідної інформації з метою

підвищення ефективності розслідування кіберзлочинів. Частково відповідні відносини врегульовано статтею 11 Закону України “Про основні засади забезпечення кібербезпеки України”, яка містить декларативну норму про обов’язок державних і приватних суб’єктів сприяти суб’єктам забезпечення кібербезпеки, повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об’єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків [2, ст. 11]. Разом з тим, законодавство України (у статті 39 Закону України **“**Про телекомунікації**”** [8]) має передбачати конкретні форми такого сприяння. Наприклад, з метою забезпечення можливості ідентифікації особи користувача пропонується закріпити обов’язок операторів, провайдерів телекомунікаційних послуг мати список своїх користувачів і надавати його правоохоронним органам на письмову вимогу останніх.

Доцільно також передбачити обов’язок операторів, провайдерів зберігати електронні дані із забезпеченням їх цілісності та неспростовності, у тому числі дані про рух трафіка, а також обов’язок обмежувати доступ своїх абонентів до інформаційного ресурсу (інформаційного сервісу), адреси мережі Інтернет, веб-сайту, веб-сторінки, через які розповсюджується злочинний контент.

Розслідування кіберзлочинів вимагає швидкого аналізу та збереження електронних даних. Відповідно до принципів міжнародного права тільки правоохоронні органи держави можуть проводити слідчі дії на її території. Оскільки, нерідко місце вчинення, знаряддя злочину, потерпілі і злочинець можуть знаходитися під різною територіальною юрисдикцією, виникає необхідність багатьох формальних погоджень, що значно уповільнює розслідування транснаціональних кіберзлочинів. Тому існує потреба у більш інтенсивному міжнародному співробітництві у порівнянні з боротьбою з будь-якими іншими проявами транснаціональної злочинності.

Новітнє законодавство України у сфері кібербезпеки передбачає можливість надання правоохоронними органами інформації з питань, пов’язаних із боротьбою з міжнародною кіберзлочинністю, іноземній державі на підставі запиту, навіть без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи і може сприяти компетентним органам іноземної держави у припиненні кібератаки, своєчасному виявленні і припиненні кримінального правопорушення з використанням кіберпростору [2, ст. 14]. Залишається сподіватися, що на принципах взаємності інші держави світу передбачатимуть подібну можливість оперативного надання інформації з метою розслідування кіберзлочинів.

На сьогодні ж, відповідно до ст. 541 КПК України, таке співробітництво здійснюється за принципами міжнародної правової допомоги – тобто проведення компетентними органами однієї держави процесуальних дій, виконання яких необхідне для досудового розслідування, судового розгляду або для виконання вироку, ухваленого судом іншої держави або міжнародною судовою установою [6, ст. 541]. Угода між Україною та Європолом про оперативне та стратегічне співробітництво надає змогу правоохоронним органам України через Департамент міжнародного співробітництва Нацполіції (яка визначена головним органом взаємодії з Європолом) здійснювати інформаційний обмін з Європолом, зокрема направляти запити на інформацію, необхідну для розслідування злочинів.

Однак, потребує удосконалення протокол офіційної правової допомоги з урахуванням норм національного законодавства для ефективного розслідування

кіберзлочинів щодо вилученої та збереженої інформації у електронному (цифровому) вигляді з метою оперативного отримання такої інформації.

Висновки.

Розуміння інформаційно-правових проблем протидії кіберзлочинності, а також можливостей їх вирішення підвищить ефективність розслідування кіберзлочинів правоохоронними органами України. Для цього існує необхідність:

деталізації законодавства, яке б відображало положення Конвенції про кіберзлочинність, щодо отримання електронних доказів, обмеження (блокування) певного інформаційного ресурсу (інформаційного сервісу), специфічних умов проведення обшуку і арешту цифрових (електронних) доказів;

закріплення механізмів сприяння правоохоронним органам України операторів, провайдерів щодо забезпечення цілісності та неспростовності електронних даних, обмеження доступу абонентів до інформаційного ресурсу (інформаційного сервісу), адреси мережі Інтернет, веб-сайту, веб-сторінки, через які розповсюджуються злочинний контент тощо;

створення у межах державно-приватного партнерства загальнодержавної бази IP-адрес для забезпечення негайного розкриття вчинених кіберзлочинів;

удосконалення протоколу офіційної правової допомоги з урахуванням норм національного законодавства для ефективного розслідування кіберзлочинів щодо вилученої та збереженої інформації у електронному (цифровому) вигляді;

використання правоохоронними органами України механізмів, передбачених Угодою між Україною та Європолом про оперативне та стратегічне співробітництво у напрямку оперативного (через глобальну захищену міжнародну мережу електронного зв'язку) отримання інформації про кіберзлочини і кіберзлочинців.

Перспективним напрямком у зв’язку з означеними проблемами є регулярне підвищення кваліфікації слідчих та інших задіяних співробітників правоохоронних органів з метою вивчення актуальних питань тактики проведення слідчих дій для отримання електронних доказів при розслідуванні кіберзлочинів.

Використана література

1. Офіційні відомості Національної поліції України. – Режим доступу : //www.npu.gov.ua

2. Про основні засади забезпечення кібербезпеки України : Закон України. – Режим доступу : http://zakon3.rada.gov.ua

3. Марущак А.І. Пріоритети розвитку інформаційного права України // Інформація і право. – № 1(1)/2011. – С. 20-24.

4. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / [М.В. Гребенюк, Г.В. Попов, В.Д. Гавловський, М.В. Гуцалюк, В. Г. Хахановський та ін.] ; за заг. ред. М.В. Гребенюка. – К. : МНДЦ при РНБО України, 2017. – 76 с.

5. Конвенція про кіберзлочинність від 23.11.01 р. // Офіційний вісник України. – 2007. – № 65. – Ст. 253.

6. Кримінальний процесуальний кодекс України від 13.04.12 р. // Офіційний вісник України. – 2012. – № 37. – Ст. 1370.

7. Про рішення Ради національної безпеки і оборони України від 29.12.16 р. **“**Про загрози кібербезпеки держави та невідкладні заходи щодо їх нейтралізації**” :** Указ Президента України від 13.02.17 р. № 32. – Режим доступу : http://zakon3.rada.gov.ua

8. Про телекомунікації : Закону України від 18.11.03 р. // Відомості Верховної Ради України (ВВР). – 2004. – № 12. – Ст. 155.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 35.078.3+004.056

ТКАЧУК Н.А., старший науковий співробітник НДІІП НАПрН України

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ФОРМУВАННЯ ПЕРЕЛІКУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Анотація. *У статті автор досліджує організаційно-правові засади, стан та проблемні питання формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави як важливого елемента системи заходів із забезпечення кіберзахисту та кібербезпеки України.*

Ключові слова*: інформаційно-телекомунікаційні системи, критична інформаційна інфраструктура, кібербезпека, кіберзагрози, кіберзахист.*

Summary. *The article examines the organizational and legal bases, the status and problems of formation of the national critical information and communication systems list as an important component of comprehensive measures to ensure cyber security and cyber protection of Ukraine.*

Keywords: *information and telecommunication systems, critical information infrastructure, cyber security, cyber threats, cyber protection.*

Аннотация. *В статье автор исследует организационно-правовые основы, состояние и проблемные вопросы формирования перечня информационно-телекоммуникационных систем объектов критической инфраструктуры государства как важного элемента системы мероприятий по обеспечению киберзащиты и кибербезопасности Украины.*

Ключевые слова: *информационно-телекоммуникационные системы, критическая информационная инфраструктура, кибербезопасность,киберугрозы, киберзащита.*

Постановка проблеми. Забезпечення надійного кіберзахисту об’єктів критичної інфраструктури є однією з ключових умов безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Наслідки масованих кібератак на комп’ютерні мережі банківського, енергетичного, транспортного секторів, галузі зв’язку, а також органів державної влади України, які відбулися у червні 2017 року, викликали значний резонанс у суспільстві та засвідчили невідповідність існуючого стану захисту критичної інформаційної інфраструктури держави актуальним та потенційним кіберзагрозам сьогодення.

Підвищення ефективності та удосконалення організаційно-правових засад забезпечення кіберзахисту об’єктів критичної інфраструктури, в тому числі тих, які перебувають у приватній власності, а також встановлення відповідних вимог у цій сфері до їх власників та операторів не можливі без визначення на загальнодержавному рівні безпосереднього переліку їх інформаційно-телекомунікаційних систем (далі – ІТС), що потребують пріоритетного захисту від кібератак та повинні належати до критичної інформаційної інфраструктури держави.

Водночас, незважаючи на ініціативи вищих органів влади щодо формування такого переліку, наразі, це питання в Україні залишається не вирішеним, що негативно впливає на подальший розвиток спроможностей держави з протидії кіберзагрозам.

Результати аналізу наукових публікацій. Теоретичні та нормативно-правові аспекти кіберзахисту об’єктів критичної інфраструктури держави розглядалися такими науковцями як Д. Бірюков, В. Бурячок, С. Гнатюк, О. Довгань, Ю. Дрейс, Д. Дубов, О. Корченко,

В. Панченко та ін. Проте, у науковій літературі відсутні публікації, присвячені вивченню проблематики формування переліку інформаційно-телекомунікаційних систем таких об’єктів, що є необхідним для подальшого розвитку організаційно-правових засад кіберзахисту та обумовлює актуальність теми статті.

Метою статті є визначення організаційно-правових засад, стану та проблемних питань формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури України як пріоритетної складової системи заходів із забезпечення кіберзахисту та кібербезпеки держави.

Виклад основного матеріалу. Інформаційна складова є важливим елементом критичної інфраструктури будь-якої країни. В умовах актуалізації кіберзагроз та перетворення кібератак на інструмент міждержавного протистояння, а також засіб реалізації гібридної агресії з боку Російської Федерації, перед нашою державою виникла нагальна потреба – забезпечити у контексті розбудови національної системи кібербезпеки належний захист інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури.

Вочевидь, одним із перших кроків у цьому напрямку визначається розроблення переліку об’єктів, що належать до критичної інформаційної інфраструктури держави, організація та проведення оцінки стану їх захищеності. Саме такі завдання, виконання яких повинно було завершитись до кінця 2016 року, були поставлені Урядом перед Державною службою спеціального зв’язку та захисту інформації України відповідно до п. 4 Плану заходів щодо захисту державних інформаційних ресурсів, затвердженому розпорядженням Кабінету Міністрів України від 5.11.14 р. № 1135-р [1].

Однак, протягом 2014 – 2016 років ці завдання повною мірою реалізовані не були. Натомість, на виконання вказаного розпорядження, Держспецзв’язку спільно із зацікавленими державними органами було розроблено Порядок формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави (далі – Порядок), який визначав механізм, за яким відбуватиметься формування переліку таких систем, та повинен був стати “вагомим кроком у напряму підвищення рівня захисту інформації, що обробляється в інформаційно-телекомунікаційних системах об'єктів критичної інфраструктури держави” [2].

У серпні 2016 року Порядок було затверджено Постановою Кабінету Міністрів України “Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави” № 563 (далі – Постанова) [3], яка зобов’язувала органи державної влади у тримісячний строк подати Адміністрації Державної служби спеціального зв’язку та захисту інформації пропозиції до переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави, попередньо погоджені з СБ України, на підставі яких Держспецзв’язку доручалося сформувати у шестимісячний строк перелік таких систем та подати його в установленому порядку Кабінету Міністрів України.

Однак, станом на лютий 2018 року, перелік ІТС об’єктів критичної інфраструктури в Україні (далі – Перелік) досі не сформовано. Основними чинниками негативного впливу на цей процес можна визначити наступні.

По-перше, формальне ставлення керівництва державних органів, у власності чи розпорядженні яких перебувають об’єкти критичної інфраструктури держави або до сфери управління яких вони належать, до задачі щодо своєчасного подання інформації стосовно ІТС таких об’єктів Держспецзв’язку для подальшого врахування у Переліку. Переважна більшість міністерств та відомств або взагалі не подало інформацію у встановлені терміни, або подана інформація була неповною.

За результатами розгляду цієї проблеми на засіданні Ради національної безпеки і оборони України рішенням РНБО України “Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації” від 29.12.16 р. [4] було доручено Кабінету Міністрів України забезпечити у місячний строк виконання міністерствами, іншим центральним органам виконавчої влади завдання, передбаченого Постановою Кабінету Міністрів України “Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави” від 23.08.16 р. № 563, та вжити в установленому порядку заходів щодо притягнення до відповідальності осіб, які не забезпечили його виконання у визначений постановою строк.

Також, подання Адміністрацією Держспецзв’язку Кабінету Міністрів України переліку ІТС об’єктів критичної інфраструктури держави до кінця першого кварталу 2017 року з метою його затвердження було передбачене п. 5 Плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України, затвердженому Розпорядженням КМУ від 10.03.17 р. № 155-р. [5]

Хоча, фактично, формування та затвердження актом Уряду такого Переліку, на той час, не мало під собою достатніх юридичних підстав. Адже до прийняття у жовтні 2017 року Закону України “Про основні засади забезпечення кібербезпеки України” [6] Кабінет Міністрів жодним законодавчим актом не було уповноважено затверджувати критерії, порядок віднесення об’єктів до об’єктів критичної інфраструктури та їх перелік, в тому числі перелік їх інформаційно-телекомунікаційних систем.

Ще одним чинником, який унеможливлює подання уповноваженими державними органами повної інформації до Переліку є відсутність належної взаємодії з приватним сектором, до якого належить значна кількість об’єктів критичної інфраструктури держави, та які не зобов’язані подавати інформацію про їх інформаційно-телекомунікаційні системи в рамках виконання Постанови.

Більше того, у зв’язку з тим, що надання статусу критичної інформаційної інфраструктури передбачає збільшення зобов’язань та вимог із кіберзахисту власних систем (що в т. ч. потребуватиме збільшення фінансових витрат), а також запровадження відповідальності за їх порушення, значна кількість представників приватного сектору, наприклад, сфери телекомунікацій, фактично саботують діяльність із формування Переліку, аргументуючи, що це призведе до “надмірного та необґрунтованого навантаження” на бізнес [7].

Наступним проблемним питанням формування Переліку критичної інформаційної інфраструктури держави є відсутність нормативно закріплених критеріїв визначення оцінки негативних наслідків, до яких може призвести кібератака на інформаційно-телекомунікаційну систему, з урахуванням яких і повинні формуватися пропозиції до Переліку. Зокрема, Постанова КМУ “Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави” зазначених критеріїв не містить.

Аналіз міжнародного досвіду свідчить, що до таких критеріїв, як правило, належать: сума фінансових збитків державі, кількість жертв, площа території ураження, можливість виведення з ладу інших секторів критичної інфраструктури тощо [8].

Також, у разі циркуляції в ІТС об’єктів критичної інфраструктури інформації з обмеженим доступом, при формуванні критеріїв необхідно враховувати можливі негативні наслідки для національних інтересів держави у разі витоку такої інформації та/або розголошення державної таємниці.

Виникає цілком закономірне питання – чи можливо взагалі визначити перелік ІТС об’єктів критичної інфраструктури за умови відсутності в державі безпосередньо переліку таких об’єктів?

Відповідно до чинного законодавства, об’єктами критичної інфраструктури є підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов’язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров’я людей [6].

На сьогодні єдиний перелік зазначених об’єктів в Україні відсутній, а захист об’єктів, які згідно із світовою практикою відносять до категорії “критичної інфраструктури” регламентується численними нормативно-правовими актами, що носять переважно відомчий характер [9].

Загрози критичній інфраструктурі, зазвичай, розподіляють на три групи, що включають аварії й технічні збої, природні лиха та небезпечні природні явища, зловмисні дії (груп або окремих осіб, таких як терористи, злочинці й диверсанти, промислове шпигунство, а також бойові дії) [10]. протидія кіберзагрозам та заходи з кіберзахисту ІТС об’єктів критичної інфраструктури повинні реалізовуватись, перш за все, у рамках комплексної системи захисту критичної інфраструктури держави як один із її елементів.

Наразі в країні відбувається активний процес розбудови такої системи. Згідно із Законом України “Про основні засади забезпечення кібербезпеки України” [6], а також Концепцією створення державної системи захисту критичної інфраструктури, затвердженій розпорядженням Кабінету Міністрів України від 6.12.17 р. № 1009-р [11], передбачено розроблення переліку об’єктів критичної інфраструктури, методології та визначення критеріїв віднесення таких об’єктів до критичної інфраструктури, порядку їх паспортизації та категоризації.

Таким чином, формування переліку об’єктів критичної інфраструктури держави є першочерговим кроком, необхідним для визначення інформаційно-телекомунікаційних систем таких об’єктів, які потребуватимуть пріоритетного захисту від кібератак.

Також, як свідчить досвід провідних країн, центральним компонентом у визначенні критичної інфраструктури є інформаційна складова [8; 12]. Тож поняття “критична інформаційна інфраструктура” не повинно включати лише ІТС об’єктів критичної інфраструктури, як це передбачено Законом України “Про основні засади забезпечення кібербезпеки України”, відповідно до якого, “об’єкт критичної інформаційної інфраструктури – комунікаційна або технологічна система об’єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об’єкта критичної інфраструктури” [6].

Це поняття повинно охоплювати також інші інформаційні системи, зокрема, національні електронні інформаційні ресурси, кібератака на які може призвести до значних негативних наслідків та суттєвої шкоди життєво важливим інтересам держави. Наприклад, Єдині та державні реєстри (Єдиний реєстр нотаріусів України, Державний реєстр речових прав на нерухоме майно, Державний реєстр актів цивільного стану громадян тощо), які за формальними ознаками не є інформаційно-телекомунікаційними системами об’єктів критичної інфраструктури, водночас, з урахуванням потенційних негативних наслідків для держави, до яких може призвести протиправний кібервплив на такі ресурси, повинні належати до критичної інформаційної інфраструктури та забезпечуватись підвищеним рівнем кіберзахисту.

Висновки.

1. Існуючі організаційно-правові засади формування переліку інформаційно-телекомунікаційних об’єктів критичної інфраструктури держави, на сьогодні, не можуть забезпечити дійсне формування і затвердження такого переліку та потребують удосконалення.

2. Основними проблемними питаннями формування переліку ІТС об’єктів критичної інфраструктури є:

– відсутність у державі переліку об’єктів критичної інфраструктури, який повинен бути основою при подальшому формуванні переліку інформаційно-телекомунікаційних систем таких об’єктів;

– відсутність чітких, нормативно-закріплених критеріїв щодо оцінки негативних наслідків, до яких може призвести кібератака на інформаційно-телекомунікаційну систему, що визначатиме належність ІТС до критичної інформаційної інфраструктури держави та обумовлюватиме необхідність включення до Переліку;

– низький рівень співпраці з приватним сектором та небажання власників і операторів об’єктів критичної інфраструктури брати на себе додаткові зобов’язання у сфері кіберзахисту;

– формальний підхід відповідальних посадових осіб центральних органів виконавчої влади до формування Переліку.

3. З метою удосконалення організаційно-правових засад формування Переліку запропоновано:

- реалізовувати завдання із формування переліку ІТС об’єктів критичної інфраструктури та їх кіберзахист в рамках системи комплексного захисту критичної інформаційної інфраструктури держави та на підставі попередньо сформованого переліку таких об’єктів, а також визначеної методики щодо оцінки потенційних негативних наслідків кібератак на їх інформаційно-телекомунікаційні системи;

- уточнити на законодавчому рівні поняття “критична інформаційна інфраструктура”, яке повинно включати не лише інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури, але й національні електронні інформаційні ресурси (державні реєстри, бази даних тощо) кібератака на які може призвести до завдання суттєвої шкоди національним інтересам;

- налагодити ефективний механізм державно-приватного партнерства та взаємодії із власниками та операторами об’єктів критичної інфраструктури у напряму забезпечення включення до Переліку інформації щодо об’єктів критичної інфраструктури, які перебувають у приватній власності, та організації належного рівня її кіберзахисту;

- підвищити контроль з боку компетентних держаних органів, зокрема Національного координаційного центру кібербезпеки при РНБО України, за станом виконання відповідальними посадовими особами органів державної влади завдань, передбачених чинними нормативно-правовими актами, щодо реалізації заходів з розбудови ефективної системи кіберзахисту ІТС об’єктів критичної інфраструктури держави, у тому числі щодо формування Переліку, та вжити в установленому порядку заходів щодо притягнення до відповідальності осіб, які не забезпечили своєчасне виконання зазначених завдань.

Використана література

1. Про затвердження плану заходів щодо захисту державних інформаційних ресурсів : Розпорядження Кабінету Міністрів України від 5.11.14 р. № 1135-р. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/1135-2014-%D1%80

2. Кабмін затвердив Порядок формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави, який був розроблений за сприяння Адміністрації Держспецзв’язку. – Режим доступу : http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article%3Bjsessionid=2A9C287BFE0D1CA5AB75C3EFEC060867.app1?art_id=261878&cat_id=240232

3. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави : Постанова Кабінету Міністрів України від 23.08.16 р. № 563. – Режим доступу : https://www.kmu.gov.ua/ua/npas/249267402

4. Про рішення Ради національної безпеки і оборони України від 29.12.16 р. “Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації” : Указ Президента України від 13.02.17 р. № 32/2017. – Режим доступу : http://www.president.gov.ua/ documents/322017-21282

5. Про затвердження Плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України : Розпорядженням Кабінету Міністрів України від 10.03.17 р. № 155-р. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/155-2017-%D1%80

6. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.17 р. № 2163-19. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2163-19

7. Відкритий лист Інтернет Асоціації України від 28.02.17 р. № 32 Президенту України щодо Рішення РНБО від 29.12.16 р. “Про загрози кібербезпеці держави та невідкладні заходи їх нейтралізації”. – Режим доступу : http://inau.ua/document/lyst-no32-vid-28022017-prezydentu-ukrayiny-shchodo-rishennya-rnbo-vid-29122016-pro-zagrozy

8. Гнатюк С.О. Визначення критичної інформаційної інфраструктури та її захисту : аналіз підходів / Зв’язок. – № 4 (2014). – С. 3-7.

9. Щодо створення державної системи захисту критичної інфраструктури : аналітична записка Національного інституту стратегічних досліджень. – Режим доступу : http://www.niss.gov.ua/articles/ 2490

10. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки : аналітична записка. – (Національний інститут стратегічних досліджень). – Режим доступу : http://www.niss.gov.ua/articles/2532

11. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : Розпорядження Кабінету Міністрів України від 6.12.17 р. № 1009-р. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/1009-2017-%D1%80

12. Дрейс Ю.О. Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури держави // Захист інформації. – Т. 19. – № 3 (2017). – С. 214-222.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 930:342.7

ЗОЛОТАР О.О., *кандидат юридичних наук,* завідувач науковим сектором
НДІ інформатики і права НАПрН України

ҐЕНЕЗА СУСПІЛЬНИХ ВІДНОСИН ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ

Анотація. *Досліджуються історичні передумови становлення інституту інформаційної безпеки людини.*

Ключові слова*: інформаційна безпека, права людини, захист інформації, інформаційний вплив.*

Summary*. The historical preconditions for formation of the Institute of human information security are researched.*

Keywords*: information security, human rights, protection of information, information influence.*

Аннотация*. Исследуются исторические предпосылки становления института информационной безопасности человека.*

Ключевые слова*: информационная безопасность, права человека, защита информации, информационное воздействие.*

Постановка проблеми. В умовах стрімкого технологічного розвитку забезпечення інформаційної безпеки виступає однією з найважливіших гарантій прав людини. В основі таких гарантій лежить дотримання принципів конфіденційності, цілісності та доступності інформації та інформаційних систем. Для забезпечення інформаційної безпеки людини здійснюється вироблення спеціальних правових принципів захисту права на недоторканність приватного життя, а також додаткових механізмів його захисту, пов’язаних з встановленням специфічних вимог у сфері збору та обробки особистої інформації. Проте це не єдина складова інформаційної безпеки людини.

Результати аналізу наукових публікацій. Як вже зазначено, інформаційна безпека людини до цього часу досліджується переважно у складі більш широкої проблематики – інформаційної безпеки, або у зв’язку з питаннями інформаційної безпеки держави і суспільства. Тому окремі питання ґенези суспільних відносин щодо інформаційної безпеки розглядались в роботах Петрика В.М., Кузьменка А.М., Остроухова В. В. та ін. – під кутом історії інформаційного протиборства та з огляду на інформаційну безпеку держави, Стоїцького А.Б., Тимошенка О.І., Гуз А.М. – історія захисту інформації, Артамонової Я.С., Лопатіна В.М. – з огляду на трансформацію ідеї інформаційної безпеки під впливом розвитку засобів комунікації, Брижка В.М., Баранова О.А., Пилипчука В.Г., Мельника К.С.– щодо захисту персональних даних та становлення інституту приватності, Грицяк Н.В., Політанського В.С., Тихомирова О.О. – щодо виокремлення та правового закріплення окремих інформаційних прав людини, Арістової І.В., Грачева Г.В., Кормича Б.А., Сулацького Д.В. – щодо формування методологічних підходів до розуміння інформаційної безпеки людини.

Метою статті є виявлення тенденцій, що сформувались історично і мають бути враховані з метою гарантування інформаційної безпеки людини в сучасних умовах.

Виклад основного матеріалу. Перш ніж аналізувати історію, слід визначитись, що саме ми розуміємо під інформаційною безпекою людини. Проаналізовані доктринальні

праці щодо розуміння інформаційної безпеки людини дозволили окреслити два основні підходи[1], базуючись на яких сформульовано авторську дефініцію – *інформаційна безпека – це захищеність людини від шкоди або інших небажаних результатів для її гідності та вільного розвитку, що полягає у гарантованій можливості задоволення своїх інформаційних потреб, свободі інформації та приязному інформаційному середовищі*. Інформаційна безпека людини, водночас, є і станом, і процесом, оскільки виступає невід’ємною частиною життя, в якому людина постійно перебуває під дією конкретних інформаційних впливів. З огляду на вищезазначене, в цій статті взято до уваги історичні передумови захисту інформації, використання інформаційних впливів на людину в інтересах держави та інших суб’єктів, а також зародження інформаційних прав людини, зокрема, права на захист персональних даних та доступ до публічної інформації. Очевидно, цим переліком не вичерпується проблема, проте обмежений обсяг статті і цілі нашого дослідження обумовили саме такий вибір.

Історія захисту інформації.

Початок історії захисту інформації вчені пов’язують з появою можливості фіксації інформаційних повідомлень на твердих носіях, тобто з винаходом писемності, а першим видом інформації, що підлягала захисту, вважають державну таємницю. Практично одночасно з народженням писемності виникли перші методи захисту інформації, як шифрування і приховування. Один з найстаріших шифрованих текстів з Месопотамії (2000 років до н. е.) Являє собою глиняну табличку, що містить рецепт виготовлення глазурі в гончарному виробництві, в якому ігнорувалися деякі голосні і приголосні і вживалися числа замість імен.

Історія охорони і захисту інформації на території сучасної України також сягає ще додержавних часів. Першим видом інформації, яку потрібно було охороняти, була військова інформація. Спочатку охорону такої інформації забезпечував князь, потім особа, яку він призначав особисто. Війна була на той час головним і загальновизнаним способом ведення зовнішньої політики будь-якої держави, тому захист військової інформації був головним у політиці князів Олега, Ігоря, Святослава, Ярослава та княгині Ольги. Князі, йдучи в похід, намагалися приховати інформацію про кількість війська і напрям головного удару. Ворог не міг адекватно реагувати на небезпеку, а заздалегідь розпущені чутки, перебільшення і неправдива інформація ще більше призводили до паніки [1, с. 11]. Зазначимо, що в 988 році Володимир розпочав релігійну реформу, і тому ще один вид інформації про віросповідання теж підлягав спочатку охороні. Перші князі тримали своє віросповідання в секреті, зокрема Ольга, а сам Володимир не відразу наважився прийняти християнське віровчення попри неодноразові пропозиції Візантії. За Володимира та Ярослава особливого розмаху набуває зовнішньополітична, дипломатична діяльність держави, саме інформація про дипломатичні відносини підлягала охороні. Деякі науковці висловлюють припущення, що вже в період Київської Русі з'явилися державні службовці, які здійснювали захист окремих видів інформації. Можливо, це були представники молодшої дружини, а саме: отроки, боярські діти та пасинки.

В Литовсько-Польській державі, до складу якої увійшли українські землі, найважливішою так само визначалась військова інформація, інформація про особу князя (потім короля), і в Литовському статуті Великого князівства литовського (1588 р.) з’являється новий вид інформації, що охоронялася, – державна таємниця. В Речі

[1] Більш детально це питання нами викладено в статті “Информационная безопасность человека: доктринальные подходы к определению категории” [2].

Посполитій пошуком і знешкодженням шпигунів з метою захисту інформації займалися призначені королем відповідальні особи з його найближчого оточення.

В Російській імперії було встановлено кримінальну відповідальність за розголошення такого виду інформації як державна таємниця. Зокрема, у “Соборному Уложении” (1649 р.) була стаття, що визначала смертну кару за такі дії [1, с. 27]. Водночас, централізованої системи охорони державної таємниці не існувало. Найбільш розвиненою була система захисту військової інформації. Її основними напрямами були створення і вдосконалення системи контррозвідувальних органів; організація комплексної системи захисту інформації, що містить військову таємницю; вдосконалення системи фельд’єгерського зв’язку; організація військової цензури.

Наступний період (приблизно з середини XIX ст.) пов’язують з появою технічних засобів обробки інформації та передачі повідомлень за допомогою електричних сигналів і електромагнітних полів (наприклад, телефон, телеграф, радіо). У зв’язку з цим виникли проблеми захисту від технічних каналів витоку. На початку XIX століття криптографія збагатилася чудовим винаходом – системою шифрування “дисковим шифром”, автором якого бувсекс-президент США Томас Джефферсон.

Суттєво вдосконалено систему охорони інформації та її нормативно-правове забезпечення було у XX сторіччі, чому суттєво посприяли дві світові війни.

Для забезпечення захисту інформації в процесі передачі по телефонними і телеграфними каналами зв’язку з’явилися способи та технічні засоби, що дозволяють шифрувати повідомлення в реальному часі. Також в цей період активно розвиваються технічні засоби розвідки, багаторазово збільшуючи можливості промислового та державного шпигунства. Величезні, дедалі зростаючиі збитки підприємств і фірм сприяли науково-технічному прогресу в створенні нових та удосконаленні старих засобів і методів захисту інформації.

В той же час, правова регламентація охорони інформації недержавного і невійськового змісту має місце лише з другої половини XX сторіччя. Сучасний період свідчить про найбільш інтенсивний розвиток засобів захисту інформації починається у зв’язку з масовою інформатизацією суспільства.

Наприкінці 20 сторіччя математично було доведено, що забезпечити повну безпеку інформації в системах її обробки неможливо [3].

Історія використання інформаційних впливів на людину.

В різні періоди історичного розвитку людської цивілізації інтенсивність застосування інформаційного впливу, як і досконалість його організації, дуже різнилися. Тому з метою дослідження цієї діяльності з точки зору її історичного розвитку, виявлення основних чинників, які так чи інакше впливали на цей розвиток, науковці умовно поділяють історію інформаційного протиборства на три основні періоди.

Перший період інформаційного протиборства охоплює античні часи, епоху Середньовіччя та частину Нового часу до XVIII ст. включно. Перші письмові згадки про інформаційний вплив на суспільство у Стародавньому Китаї. Одним з найдавніших історичних джерел, де йдеться про застосування прийомів інформаційного протиборства, можна вважати Трактат про мистецтво війни китайського полководця Сунь-Цзи (VI ст. до н. е.) [4]. У ньому наводиться опис і яскраві приклади застосування прийомів і методів психологічного впливу, які давали змогу досягати перемоги без битв або з мінімальними втратами. Важливе місце, зокрема, відводиться дезінформуванню противника, психологічній обробці власного населення і війська з метою досягнення єдності в суспільстві напередодні і під час війни, здійснення інформаційних диверсій для розладнання військових союзів ворожої держави з іншими державами тощо.

Подальший розвиток воєнного мистецтва незмінно супроводжувався удосконалюванням форм інформаційно-психологічного впливу. Так, тривалий час у війнах Стародавнього Китаю застосовувався такий самостійний прийом інформаційно-психологічного впливу, як проголошення справедливою війни зі свого боку і несправедливою – з боку супротивника. Як бачимо, цей спосіб не втратив актуальності й досі активно використовується в сучасних умовах.

На період греко-перських воєн припадають згадки про спроби використання театру, поезії, образотворчого мистецтва з метою політичної пропаганди, а також протидії цьому з боку політичних опонентів. Новий етап розвитку практики пропаганди мав місце в античному Римі [5, с. 54] Зокрема, з’являються такі жанри, як написання тенденційних біографій з метою уславлення певних аристократичних родів, мемуарний та епістолярний жанри, стають популярними різноманітні легендарні версії з історії Риму та походження римського народу. В часи імперії характерним моментом римської пропаганди, піднятої до рангу державної політики, стало освячення і обожнення особи імператора. Спеціального розгляду в аспекті порушеної проблеми заслуговує психологічне та ідейно-пропагандистське забезпечення церквою різних воєнних акцій, таких, як, наприклад, збройна відсіч поганським навалам гунів, аварів, вандалів, відвоювання християнських святинь під час хрестових походів, міжконфесійна боротьба та боротьба з єресями. Не менш активно використовували релігійний аспект мусульманські завойовники.

До XIII ст. належить один з перших історичних прикладів масштабного застосування дезінформації у воєнних цілях. Пов’язаний цей приклад із вторгненням монголів до Угорщини у 1241 р. Розбивши угорців та їхніх союзників на річці Шайо, монголи серед захоплених трофеїв знайшли королівську печатку. За наказом Батия грамотні полонені від імені короля Бели написали угорською мовою указ про припинення опору, копії якого, скріплені королівською печаткою, було розіслано в різні кінці ще не завойованої країни [там само, с. 56]

Винайдення Й. Гутенбергом друкарського верстату кардинально змінило можливості поширення інформації, прискоривши швидкість тиражування та здешевивши виготовлення книг. У XVI ст. в окремих країнах Європи з’являється інформаційне публічне видання – газета, яка спочатку була рукописною, а з часом – друкованою. З цим фактом пов’язують необмежені можливості, причому не лише у військовій, а практично в усіх сферах суспільної діяльності (політичній, економічній, культурній тощо). Перший випадок використання друкованих, а не рукописних листівок, відноситься до більш раннього періоду – війни Нідерландів за незалежність від Іспанії в XVI ст. На території Фрісландії було надруковано кілька тисяч примірників звернення до населення, яке стало важливим елементом консолідуючої пропаганди в 1567 р. у війні проти військ герцога Альби та звільнення фламандців від іспанського панування [там само, с. 60]

У Запорізькій Січі та державі Богдана Хмельницького вироблені були своєрідні форми захисту військово-політичної інформації. Хмельницький широко використовував дезінформацію. В спогадах польських урядовців та військових часто зустрічається рядки на кшталт “одне думає, про інше пише”, “наміри його жодним чином не можна зрозуміти”. Хмельницький зазначав у жовтні 1648 р.: “А військова справа така: коли мисль буде йти на війну, щоб тої мислі ніхто не відав і недруг би не остерігався” [1, с. 14].

Другий період інформаційного протиборства починається з середини XVIII ст. і закінчується Другою світовою війною включно. Найбільш яскравою є діяльність пропагандистського апарату Наполеона Бонапарта і нацистського Третього Рейху.

Ставши імператором, Наполеон активно використовує можливості поліцейського відомства у справі ідеологічно-психологічного впливу на населення і контролю за ним для збереження власної диктатури. Він був також одним із перших можновладців Європи, хто по-справжньому оцінив роль преси у формуванні громадської думки. Широковідомим є його висловлювання: “Чотири газети зможуть заподіяти ворогові більше шкоди, ніж стотисячна армія”. Усвідомлюючи повною мірою силу впливу преси на формування громадської думки, Наполеон диференційовано підходив до діяльності органів друку усередині країни та за кордоном. У Франції він вилучив зі сфери обговорення газет усю внутрішню та зовнішню політику і скоротив кількість газет з 73 до 13. А у кожній окупованій країні він засновував офіційний друкований орган: “Газетт де Мадрид”, “Газетт де Берлін”, “Журналь дю Капітоль” тощо. При поданні матеріалів на сторінках наполеонівської преси набули широкого поширення методи замовчування і дезінформації [5, с. 62].

На зламі XIX-XX ст. виникає суто науковий інтерес до феноменів впливу на людську свідомість, зокрема на свідомість мас. У 1879 р. у Лейпцигу за ініціативою відомого вченого В. Вундта відкривається перша психологічна лабораторія. П’ятнадцять років по тому у Франції виходить знаменита “Psyhologie des foules” (Психологія натовпу) Г. Лебона, який одним із перших заявив про прихід “ери натовпу”.

Характерною рисою інформаційно-пропагандистської діяльності в європейських країнах періоду Першої і Другої світових воєн стало те, що вона набула централізованого характеру, для чого були створені спеціальні органи і установи, які утримувалися коштом урядових бюджетів. Війна велася не лише зброєю, здатною фізично уражати супротивників та їх матеріальну базу, а й такою, що ранила душі, руйнувала боєздатність ворожих військ ще до вступу в бій.

Так, в часи Другої світової війни, в Англії існувало Міністерство інформації та Департамент пропаганди на супротивника, у Франції – служба військової пропаганди зосереджувалася при 11-му відділі Генерального штабу, а також “Будинок преси” та неофіційна організація “Альянс Франсе”. Хоча США приєдналися до бойових дій на завершальному етапі війни, проте пропагандистську роботу на її потреби здійснювали з широким розмахом. При штабі американської експедиційної армії в Європі функціонувала “Психологічна підсекція”, яка, поряд з проведенням широкомасштабних операцій з розповсюдження листівок, займалась і розробленням соціально-психологічної методики вивчення моралі противника, а в США діяв спеціальний орган пропаганди – Комітет громадської інформації, який мав поділ на секції: новин, іншомовних газет, громадської освіти, кінофільмів, відносин з промисловцями, реклами і карикатур.

Пропагандистські машини СРСР і нацистського Третього Рейху не лише масово творили нові методи пропаганди, але й використовували населення своїх країн як своєрідні полігони, на яких проходили випробування нові зразки інформаційної зброї.

Ефективність радянської пропаганди було продемонстровано ще в ході громадянської війни. Вже у грудні 1917 р. при Народному Комісаріаті іноземних справ було створено відділ міжнародної революційної пропаганди, а при видавництві ВЦВК – військовий відділ друку літератури іноземними мовами. Комуністична партія пропаганду за значенням ставила на один рівень з організацією бойових дій.

Найбільшого успіху у справах організації політичної пропаганди, безумовно, досягли комісари-пропагандисти Червоної Армії. Маніпулюючи емоціями та свідомістю населення, вони вирішували питання комплектування збройних сил, управління економікою, формування нової структури адміністрації. Ідеологія класових інтересів отримала значну підтримку завдяки ефективному впливу її постулатів на широкі прошарки населення. “Шляхом пропаганди й агітації ми відібрали у Антанти її війська” – цю фразу приписують Леніну [5, с. 64].

Після того як було придушено контрреволюцію, апарат радянської пропаганди та агітації ефективно використовується для впливу на радянське населення, щоби перетворити останнього в покірну безлику масу безликих. Для цього терміново створюється нова міфологія з новими “героями”, “титанами”, “гігантами” і епічними картинами боротьби як на традиційному, так і на трудовому фронті. Схожі методи використовували міфотворці і вожді мас Третього Рейху. Незначна різниця полягала, напевне, лише в їх більшій відвертості та відкритому визнанні шляхів, якими вони діяли. Наприклад, з’їзд націонал-соціалістичної партії в Нюрнбергзі в 1936 р. прикрашав плакат “Пропаганда допомогла нам прийти до влади. Пропаганда допоможе нам завоювати увесь світ”. Процес централізації контролю над пропагандою призвів спочатку до створення міністерства пропаганди, а пізніше міністерства громадської освіти і пропаганди. Характерною рисою фашистської пропагандистської діяльності було ґрунтовне використання наукових розробок у цій сфері. Настільними книгами рейхсміністра пропаганди Геббельса були “Психологія натовпу” та роботи Е. Бернейса. Активно використовувалися напрацювання з психології підсвідомого. Відповідаючи на питання, чому Гітлер не робить значного враження на іноземців, К. Юнг зазначав: “... для будь-якого німця Гітлер є дзеркалом його підсвідомого, у якому не для німця, звичайно, нічого не відображається. Він рупор, настільки посилюючий неясний шепіт німецької душі, що його може почути вухо його підсвідомого”. Розроблені німецькими пропагандистами прийоми впливу на маси, до сьогодні використовуються в політтехнологіях. Це передусім театралізовані партійні з’їзди, масові зустрічі на стадіонах, радіотрансляції виступів вождів на масові аудиторії тощо. Але основною характеристикою фашистської інформаційної політики, безумовно, є інформаційний монополізм.

На сучасному етапі наука має в розпорядженні такі теоретичні надбання, на базі яких здійснюється технологізація інформаційної боротьби, тобто відповідні державні і недержавні структури, що причетні до такої діяльності, здійснюють розробку і апробацію нових інформаційних технологій, прийомів, методів здійснення психологічного впливу, технічних засобів необхідних для такої діяльності. Подібні зрушення не могли не відбитися на зростанні ефективності застосування інформаційних технологій, яке може призводити до кардинальних змін в суспільній, економічній, політичній та іншій сферах окремої країни, або ж у світовому масштабі.

З кінця 1940 до середини 1980-х рр., в епоху так званої холодної війни, протистояння двох супердержав СРСР і США, спричинило подальше вдосконалення форм і методів пропаганди та психологічної війни.

У 1970-х рр. остання інформаційна революція, пов’язана з винаходом комп’ютера, висунула на перший план нову галузь – інформаційну індустрію, яка пов’язана зі створенням технічних засобів, методів, технологій для нових знань. Найважливішими складовими інформаційної індустрії стають усі види інформаційних технологій, особливо телекомунікації. Стрімке зростання обсягів інформації й об’єктивна зміна умов психологічної діяльності людини в сучасному світі призвели до перерозподілу

питомої ваги даних про оточуючий світ, що надходять до індивіда за допомогою генетичних каналів і в результаті безпосереднього сприйняття дійсності, на користь даних, що отримуються ним із засобів масової інформації.

Сучасні можливості електронних ЗМІ, космічних систем передачі інформації, поліграфії, розмножувальної й іншої техніки в поєднанні з науковою та публіцистичною літературою і періодикою дозволяють ефективно впливати на розум, свідомість і психіку мільйонів людей. Інформація і пропаганда стали сьогодні настільки могутніми, що здатні впливати на появу, перебіг і кінцевий результат політичних подій, торкаючись глобальних проблем миру і війни.

Становлення інформаційних прав людини.

На теренах континентальної Європи намагання виділити об’єкт правової охорони, який би відображав суспільну потребу в захисті “автономії” особи, призвів до формулювання теорії “прав особистості”, тобто невідчужуваних природних прав, пов’язаних із людиною як біосоціальною істотою. [6, с. 125]. Водночас, прекурсором сучасного права на захист персональних даних стало поняття “privacy”, сформульоване в 1890 р. американськими юристами С. Уорреном і Л. Брандейсом, які визначили його як “the right to be alone”. Першим прецедентом, створеним на основі наукових розробок “права бути залишеним у спокої”, стало рішення Верховного Суду штату Джорджія *у* справі “Павєсіч vs. Нью Ігленд Лайф Іншуранс Ко.” (1905 р.). Задовольняючи позов чоловіка, зображеного без його згоди в рекламному оголошенні, суд визначив об’єкт і мету правового захисту таким чином: “Той, хто бажає жити життям відносного усамітнення, має право обрати час, місце та способи, у які він буде піддавати себе громадському спостереженню” [7, с. 65]. А у справі “Griswold vs. Connecticut” суддя Верховного суду США Дуглас вивів “право на приватність” з перших п’яти поправок до Конституції США, визнавши, що ці поправки “охороняють різні аспекти недоторканності приватного життя”, зазначивши: “правом на недоторканність приватного життя старше ніж Білль про права” [8].

Усвідомлення зміни ролі інформації у суспільстві відбувалось поступово і нерівномірно в географічній перспективі. У 1946 році Генеральна Асамблея ООН ухвалила одну зі своїх найперших резолюцій, де зазначено: *“Свобода інформації є фундаментальним правом людини і ...критерієм для всіх свобод, яким присвячено Організацію Об’єднаних Націй”* [9, с. 8]. Проте, вперше на міжнародному рівні право на інформацію було задекларовано в ст. 19 Загальної декларації прав людини. Так, Загальна Декларація прав людини визначила свободу шукати, одержувати і поширювати інформацію та ідеї складовою права кожної людини на свободу переконань і на вільне їх виявлення. Аналогічне закріплення право на інформацію одержало також в інших міжнародно-правових документах, Європейській Конвенції про захист прав людини і основоположних свобод (п. 1 ст. 10), Міжнародному Пакті про громадянські і політичні права 1966 року (п. 2 ст. 19) та ін. На основі цього можна зробити висновок, що права на свободу інформації, свободу думки і слова належать до так званих прав “першого покоління” – громадянських і політичних прав, які від початку вважалися і вважаються невід’ємною частиною людської особистості [10, с. 94]. Оскільки, процесу розвитку ідеї прав людини властиві як кількісні, так і якісні зміни, то, безперечно, варто погодитись з думкою, що розширює колективні права людини (третє покоління) піднесення та поглиблення права на інформаційний простір світу, на надання різноманітних послуг, що ґрунтуються на інтелектуальних інформаційних технологіях (зокрема на новітніх технологіях досліджень) і технологіях зв’язку (глобальна мережа Інтернет), забезпечення інформаційних відносин усередині країни і за кордоном. До розвитку

сучасних кібернетичних систем під простором поширення інформації розуміли атмосферу, стратосферу, космос, водні акваторії океанів і морів. Зараз розуміння інформаційного простору включає додатково кібернетичні та віртуальні системи [11].

Умови становлення інформаційного суспільства перетворили інформацію на національне багатство і одночасно кинули новий і небезпечний виклик людині, суспільству і державі. Причини спеціального відокремлення поняття “персональні дані” із загальної маси різноманітних даних пов’язані з тим, що вони є одним з найбільш важливих, делікатних та вразливих атрибутів недоторканості приватного життя людини, що потребує захисту за допомогою юридичних та організаційних заходів [12, с. 100].

Починаючи з кінця 60-х років XX століття на теренах Європи у багатьох країнах почали розроблятись національні закони стосовно регулювання питання автоматизованої обробки та захисту персональних даних.

В Україні формування правових основ та системи захисту персональних даних на підставі приписів міжнародно-правових стандартів почалося у 1996 році [13] та продовжується до нашого часу [14].

В. Брижко виокремлює три основні причини для руху в напрямі удосконалення нормативно-правового упорядкування відносин у сфері захисту персональних даних, із яких виходять європейські та інші країни: усунення передумов та порушень прав людини на її персональні дані; розвиток е-комерції (е-бізнесу, е-торгівлі); гармонізація національних законодавств відповідно до приписів континентального права та норм європейських правових стандартів [15, с. 31-32].

Поруч із захистом персональних даних на базі свободи інформації, принципу гласності, свободи слова та друку в другій половині XX ст. як окреме суб’єктивне право виокремлюється *право на доступ до інформації*. Історія цього права корінням сягає ще 1766 року, коли в Швеції було закріплено “права знати” у Декларації прав людини і громадянина 1789 року [16]. Закон був суттєво послаблений після перевороту Густава III у 1772 році, тим не менше, закладені ним принципи стали основою для принципів, закладених у XX столітті. А рівень Швеції за ВВП і соціальними стандартами, а також культура підзвітності й прозорості є найкращим доказом важливості забезпечення права на доступ до інформації й, зокрема, доступу до публічної інформації. Проте, ідея конституційного закріплення права на доступ до інформації була відроджена лише в другій половині XX ст. Проголошення “права знати” у країнах Європи та Сполучених Штатах Америки – це наслідок становлення громадянського суспільства та демократичних перетворень, що відбувались у цих країнах протягом останніх трьох століть, а в країнах, які розвиваються, – це умова утвердження громадянського суспільства.

На межі XX і XXI століть інформаційні ресурси стали визначальним фактором розвитку і більшість країн констатували початок нової епохи – інформаційного суспільства. У 2000 році прийнята Окінавська хартія глобального інформаційного суспільства, у якій було закріплено, що “всі люди повсюдно, без винятку повинні мати можливість користуватися перевагами глобального інформаційного суспільства. Стійкість глобального інформаційного суспільства ґрунтується на стимулюючих розвиток людини демократичних цінностях, таких як, вільний обмін інформацією та знаннями, повага до особливостей інших людей” [17]. У той же час в інформаційному суспільстві руйнується традиційна ієрархічна система цінностей. Кардинально змінюється і трактування понять “людина” і її “особистість”. Організаційним принципом культурного життя людини стає принцип трансформації. Свобода особистості стає гарантом її безпеки [18].

Таким чином, проблема прав людини вийшла далеко за межі окремої держави, а обсяг прав і свобод людини в сучасному суспільстві визначається не лише особливостями певного співтовариства людей – національної держави, а й розвитком людської цивілізації в цілому. В науковій думці відсутній однозначний підхід до визначення інформаційних прав людини. П.М. Сухорольський у дослідженні підкреслює, що, наприклад, в англомовних джерелах виділяються так звані цифрові права людини (digital rights), під якими розуміють сукупність загальновизнаних та інших прав людини у контексті поширення нових цифрових технологій, зокрема Інтернету [19, с. 21].

Розробка “Декларації прав людини і правових норм в інформаційному суспільстві” [20] стала першою спробою визначення міжнародно-правових рамок в цій сфері. Декларація була розроблена Комітетом експертів Ради Європи з інформаційного суспільства. Значну увагу на форумі було присвячено розробці норм відповідальної поведінки в інформаційному суспільстві. Учасники Міжнародного форуму “Права людини в інформаційному суспільстві: відповідальна поведінка головних дійових осіб”, ініційованого Радою Європи, закликали уряди захищати всі права людини, які стосуються інформаційного суспільства, від свободи слова до приватності і копірайту, не забуваючи про завдання подолання інформаційної нерівності і про належне управління. На їхню думку, “цілковита повага свободи слова та інформації державними та недержавними інститутами є необхідною передумовою побудови вільного інформаційного суспільства для всіх, а інформаційно-комунікаційні технології не повинні використовуватися для обмеження цієї фундаментальної свободи” [21].

Висновки.

Інститут інформаційної безпеки людини в Україні і світі є наймолодшим, порівняно з інформаційною безпекою держави чи суспільства. Протягом багатьох тисячоліть інформаційна безпека розглядалась, насамперед, з перспективи інтересів держави. Згодом інтенсифікація процесів інформатизації в усіх сферах, а особливо, зростання значення технічного захисту інформації зумовило становлення правового забезпечення захисту інформації як невід’ємної складової безпеки підприємств, установ та організацій, а також окремих галузей господарства. На межі тисячоліть гостро постало питання про міжнародну інформаційну безпеку, а також кібербезпеку у складі інформаційної безпеки. Тим не менш, на кожному з цих етапів інформаційна безпека людини залишалась вторинною.

Використана література

1. Організаційно-правові основи захисту інформації з обмеженим доступом : навч. посіб. / [Тоцький А.Б., Тимошенко О.І., Гуз А.М. та ін.]. – К : Європ. ун-т, 2006. – 232 с.

2. Золотар О. Информационная безопасность человека : доктринальные подходы к определению категории. SCI-ARTICLE.RU : науч. период. электрон. журн. – 2017. – № 52. URL : http://sci-article.ru/stat.php?i=1513689444

3. Хронологія розвитку засобів і методів захисту інформації. URL : http://kspu.kr.ua/index.php

4. Сунь-цзи. Мистецтво війни. – К. : Арій, 2014. – 128 с.

5. Соціально-правові основи інформаційної безпеки / [Петрик В.М., Кузьменко А.М., Остроухов В.В. та ін.] : навч. посіб. : за ред. В.В.Остроухова. – К. : Росава, 2007. – 496 с.

6. Покровский И.А. Основные проблемы гражданского права : монография. – М.: Статут, 2001. – 353 с.

7. Рішення Верховного Суду штату Джорджія у справі “Павєсіч vs. Нью Ігленд Лайф Іншуранс Ко.” від 1905 р. (цит. за Information privacy law: Textbook / D.J. Solove, M. Rotenberg. New York: Aspen Publishers, 2003. – 795 p.).

8. U.S. Supreme Court GRISWOLD vs. CONNECTICUT, 381 U.S. 479 (1965). URL: http://supreme.justia.com/cases/federal/us/381/479/case.html

9. Свобода інформації : навч. посіб. – К. : Тютюкін, 2010. – 128 с.

10. Кормич Б.А. Інформаційне право : підр. – Х. : БУРУН і К., 2011. – 334 с.

11. Шапиро В.С. Права и свободы человека в отрасли информационного права : мат. международной научно-практической конференции [“Права человека : история, теория, практика”], (г. Курск, 9-10 декабря 2010 года). – Курск : ЮЗГУ, 2010.

12. Мельник К.С. Іноземний та вітчизняний досвід становлення інституту захисту персональних даних // Інформаційна безпека людини, суспільства, держави. – 2013. – № 2 (12). – С. 97-103.

13. Защита персональных данных / А. Баранов, В. Брыжко, Ю. Базанов. – К. : Національне агентство по інформатизації при Президентові України, ВАТ КП ОТІ, 1998. – 128 с.;

Права человека и защита персональных данных / А. Баранов, В. Брыжко, Ю. Базанов. – Харьков : Фолио, 2000. – 280 с.

14. Становлення і розвиток правових основ та системи захисту персональних даних в Україні : монографія / [В.Г. Пилипчук, В.М. Брижко, О.А. Баранов, К.С. Мельник] ; за ред. В.М. Брижка, В.Г. Пилипчука. – К. : ТОВ “Видавничий дім “АртЕк”, 2017. – 226 с.

15. Брижко В.М. Захист персональних даних : реалії та практика сучасності // Інформація і право. – № 3 (9)/2013. – С. 31-49.

16. Історія становлення інституту доступу до інформації у світі та міжнародні стандарти / Доступ до публічної інформації: від А до Я. URL : https://courses.prometheus.org.ua

17. Окинавская хартия глобального информационного общества : рекомендации стран “восьмерки“ о принципах и направлениях развития информационного общества. Окинава, 22 июля 2000 г. / Дипломатический вестник. – 2000. – № 8. – С. 51-56.

18. Мищериков А.А. Безопасность и свобода личности в информационном обществе : анализ проблемы. Теория и практика общественного развития. – 2011. – № 1. URL : http://cyberleninka. ru/article/n/bezopasnost-i-svoboda-lichnosti-vinformatsionnom-obschestve-analiz-problemy

19. Сухорольський П. Проблеми забезпечення та розвитку прав людини в умовах інформаційного суспільства / Український часопис міжнародного права. – 2013. – №1. – С. 21.

20. Declaration on Human Rights and the Rule of Law in the Information Society. 2005, May 13. URL: https://coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805da1a0

21. Адылханов А.А., Казезов А.Н. Права человека в киберпространстве. Актуальные вопросы юридических наук : мат. II междунар. науч. конф., (г. Челябинск, февраль 2015 г.). – Челябинск : Два комсомольца, 2015. URL: moluch.ru/authors/10704

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

Інформація в інших галузях права

УДК 343.214+340.134:340.132.6

РАДУТНИЙ О.Е., *доктор філософії (Ph.D.) з юридичних наук, доцент*,
доцент кафедри кримінального права № 1
Національного юридичного університету ім. Ярослава Мудрого

ШТУЧНИЙ ІНТЕЛЕКТ, ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАКОНОТВОРЧИЙ ПРОЦЕС (КРИМІНАЛЬНО-ПРАВОВИЙ АСПЕКТ)

Анотація. *В статті розглянуто недоліки сучасного стану законотворчої діяльності, що межують з проявами інформаційної агресії, та досліджено можливості використання штучного інтелекту під час підготовки законопроектів та експертизи чинних нормативних актів.*

Ключові слова*: законотворча діяльність, кримінально-правова охорона, інформаційна безпека, інформаційна агресія, штучний інтелект, національна безпека, петиція Президенту України, наукове ворожіння.*

Summary. *The article considers the disadvantages of the current state of lawmaking activity, bordering on the manifestations of information aggression, as well as the possibilities of using artificial intelligence in drafting bills and examining the existing regulatory acts*

Keywords*: law-making activity, criminal and legal protection, information security, information aggression, artificial intelligence, national security, petition to the President of ~~the~~ Ukraine, scientific divination.*

Аннотация. *В статье рассмотрены недостатки современного состояния законотворческой деятельности, граничащие с проявлениями информационной агрессии, а также исследованы возможности использования искусственного интеллекта при подготовке законопроектов и экспертизы действующих нормативных актов*

Ключевые слова*: законотворческая деятельность, уголовно-правовая охрана, информационная безопасность, информационная агрессия, искусственный интеллект, национальная безопасность, петиция Президенту Украины, научное гадание.*

Постановка проблеми. Інформаційна безпека людини, суспільства та держави є невід’ємно пов’язаною з якістю нормотворення, в тому числі в сфері кримінально-правового регулювання та реалізації кримінальним законодавством функції охорони суспільних відносин в галузі обміну, поширення, створення та збереження певної інформації.

На жаль, в кримінально-правовій сфері чинне законодавство поступово втрачає ознаку правової визначеності, що викликає обґрунтовану занепокоєність багатьох вчених і практиків. Так, на думку В.Я. Тація, правотворчій діяльності останніх років властивий безсистемний та хаотичний характер [24, с. 29-35]. В.Д. Швець вказує на копіювання нормативних розробок інших держав без відповідної адаптації [29, с. 35-40]. М.І. Панов зазначає, що окремі новели у кримінальному законодавстві не передбачають єдиного методологічного підходу, суперечать основним принципам та науковим засадам кримінального права [20, с. 17]. В.А. Тимошенко та С.В. Дрьомов звертають увагу на таку сумну обставину, що нехтування приписами Регламенту Верховної Ради України для вітчизняного парламенту стало вже буденною справою [25, с. 27], а стенограма обговорення окремого законопроекту (реєстр. № 1840 від 26.01.15 р.) та голосування за

ним мали б стати предметом дослідження Генеральної прокуратури України щодо наявності складу злочину в діях окремих народних депутатів, які свідомо, ігноруючи приписи Регламенту Верховної Ради України, спотворили текст законопроекту, внесеного Кабінетом Міністрів України, та направили до Комітету Верховної Ради України з питань законодавчого забезпечення правоохоронної діяльності фактично новий законопроект.

Багаточисельність законопроектів та схвалених на їх підставі нормативних актів має своїм негативним наслідком логічно обумовлене зниження загальної якості як самих новацій, так і КК України у цілому через інфікування останнього окремими різновидами “законодавчого вірусу” [18, с. 142-151].

Так, за спостереженням В.І. Тютюгіна, впродовж п’яти місяців роботи 6-ої сесії Верховної Ради України (з 7 лютого по 14 липня 2017 р.) було подано 1284 законопроекти, прийнято 294 (23 %), з них законів – 105 (8 %) і постанов – 189 (15 %), тобто кожного місяця приймалося по 21 закону, що з урахуванням фактичної тривалості сесійних засідань становить 9 – 10 законів на кожні чотири сесійні дні, а на кожний сесійний день припадає по 2 – 3 закони [27, с. 50-51], але останнім бракувало ретельної підготовки, глибокого вивчення розглядуваних питань та їх обговорення, врахування думки наукової спільноти та практичних працівників, прогнозування наслідків того чи іншого нормативного акту.

З цього самого приводу В.О. Туляков слушно зазначає, що у сучасних кримінально-правових дослідженнях багато уваги приділяється аналізу питань криміналізації, застосуванню новітніх (альтернативних) покарань і заходів впливу, але мало уваги приділяється аналізу ефективності відповідних покарань та прогнозу ефективності самої норми [26, с. 86], таким чином у погоні за широким охопленням кримінально-правовою забороною втрачається справжній зміст і спрямованість законотворчого процесу.

Таким чином, забезпечення якості законодавчого процесу є не тільки підґрунтям існування демократичного суспільства, але й одним з визначальних чинників інформаційної безпеки у протистоянні різноманітним проявам інформаційної агресії. В цьому процесі доволі значною стає роль штучного інтелекту, який може дорівнювати або перевищувати інтелект людини.

Результати аналізу наукових публікацій. Проблемі ефективності нормотворення на рівні загальної теорії держави і права приділено увагу в роботах таких вчених, як О.В. Петришин, Ю.М. Тодика, М.В. Цвік та багатьох інших, а в сфері кримінально-правового забезпечення зазначене питання було предметом наукових розвідок Д.С. Азарова, П.П. Андрушко, М.І. Бажанова, Ю.В. Бауліна, О.І. Бойко, В.І. Борисова, Л.П. Брич, І.М. Даньшина, О.О. Дудорова, З.А. Загиней (Тростюк), І.І. Карпєц, М.В. Карчевського, В.А. Козака, М.Й. Коржанського, Н.Ф. Кузнєцової, В.А. Мисливого, А.А. Музики, В.О. Навроцького, М.І. Панова, К.К. Панько, Ю.А. Пономаренко, Н.А. Савінової, В.В. Сташиса, В.Я. Тація, П.Л. Фріса, В.І. Шакуна, М.І. Хавронюка, В.Б. Харченко, Н.М. Ярмиш та інших, але продовжує залишатися актуальним.

Вагомі внески у дослідженні правових питань щодо штучного інтелекту внесені О.А. Барановим, В.М. Брижко, К.С. Мельником, В.Г. Пилипчуком та іншими. Питанням ролі і місця штучного інтелекту в сфері кримінально-правових відносин приділено увагу в роботах В.А. Мисливого, М.В. Карчевського та Н.А. Савінової. Втім, за кожним стриманим кроком наукового пошуку відкриваються ще більші горизонти безмежного пізнання дійсності.

Метою статті є визначення взаємозв’язку між інформаційною безпекою та процесом законотворення, негативного впливу на останній засобами інформаційної агресії, місця і ролі штучного інтелекту у зазначених процесах під кутом зору кримінально-правового аспекту охорони та регулювання суспільних відносин в інформаційній галузі.

Виклад основного матеріалу. Спрощення доступу до інформаційних ресурсів, прискорення інформаційного обміну та розвитку технологій обумовлюють залучення до творчої діяльності в законодавчій сфері більш широкі верстви населення, ніж це було раніше. Типовим різновидом реагування суспільства на злободенні проблеми є динамічне набирання обертів інститутом електронних петицій на адресу Президента України, в тому числі у вигляді пропозицій майже тотальної криміналізації тих чи інших проявів суспільно небажаної, небезпечної або шкідливої поведінки.

Прикладами вказаних ініціатив виступають такі звернення, як петиція № 22/037714-еп “Кримінальна відповідальність за виробництво неякісного дорожнього покриття” (дата оприлюднення 12 червня 2017 р., 415 голосів, не підтримана), № 22/037526-еп “Ввести кримінальну відповідальність за вживання сотні разів слів “чорт”, “дідько” в україномовних фільмах. Це явна, спланована антиреклама української мови” (дата оприлюднення 07 червня 2017 р., 21 голос, не підтримана), № 22/035439-еп “Притягнути до кримінальної відповідальності всіх причетних осіб до підвищення комунальних тарифів, а також позбавити їх власності і фінансових коштів, також визначивши їх в камери смертників для задоволення громадян України” (дата оприлюднення 31 березня 2017 р., 299 голосів, не підтримана), № 22/032215-еп “Запровадити кримінальну відповідальність за пропаганду безбожництва та сексуальних збочень” (дата оприлюднення 30 грудня 2016 р., 38 голосів, не підтримана), № 22/024017-еп “Ввести адміністративну або кримінальну відповідальність за рекламу відпочинку на окупованих територіях” (дата оприлюднення 19 травня 2016 р., 79 голосів, не підтримана), № 22/022261-еп “Встановити адміністративну відповідальність у вигляді штрафу в розмірі 5100 грн. за вживання матірщини (російського мату) в громадських місцях, встановити кримінальну відповідальність за повторне таке правопорушення” (дата оприлюднення 16 березня 2016 р., 78 голосів, не підтримана), № 22/018528-еп “Заборона транслювання в салонах громадського транспорту музикальних композицій, що романтизують кримінальний спосіб життя” (дата оприлюднення 14 грудня 2015 р., 109 голосів, не підтримана) тощо [14].

Зазначений сплеск соціальної активності громадян личить справжньому демократичному суспільству, тому, насправді, дає привід пишатися цим на противагу високим показникам ураження країни корупцією так званого “візантійського” типу (зміст якої полягає у тому, щоб за допомогою адміністративного ресурсу, зв’язків, надання неправомірної вигоди тощо, отримати те, що є і без того гарантованим законами)[2]. Навіть ті пропозиції, які на перший або поверховий погляд виглядають курйозними, насправді порушують серйозні питання, як то в петиції № 22/027163-еп “Запровадити кримінальну відповідальність для орендаторів, на полях яких спалено стерню” (дата оприлюднення 27 липня 2016 р., 37 голосів, не підтримана) [14] – проблема нелюдяного знищення дрібних птахів та тварин на полях після збирання урожаю.

[2] Корупція іншого, так званого “римського” типу (сплатити хабар, якщо позначити це явище за старою термінологією, за те, щоб отримати надмірне або заборонене), існує навіть у благополучних країнах Європи та Америки, але їх презирство та обурення на адресу України викликані саме перебуванням останньої у зазначеному питанні на рівні Камеруну, Ірану, Непалу, Нікарагуа, Парагваю, Гондурасу тощо.

Вказана творчість населення та громадських організацій з питання ініціювання законопроектів, якими б примітивними або недосконалими вони б не були з точки зору досвідчених фахівців, не може розглядатися як непотрібна, адже вона становить первинний рівень законодавчого процесу (демократія з глибин, коли кожний може розраховувати на те, щоб його голос був почутий) і фокусує зацікавленість у вирішенні тієї чи іншої актуальної проблеми, на яку законодавцеві необхідно реагувати відповідним чином.

Зовсім по-іншому слід розглядати ситуацію з замовним характером законопроектів, автори яких діють цілеспрямовано на руйнацію правової системи. Таку діяльність в сфері законотворчості слід визнавати проявами інформаційної агресії на законодавчому рівні, загрозою національній безпеці України в інформаційній сфері, поряд з тими, що передбачені ст.7 Закону України “Про основи національної безпеки України” № 964-IV від 19.06.03 р. [21, с. 158-162]. Зазначена діяльність може мати внутрішніх або зовнішніх замовників, або викликана корисливим спонуканням отримання та опрацювання грантів, які, здебільшого, теж мають іноземне походження і фінансування.

В тому випадку, коли автори законопроектів діють несвідомо і причиною їх руйнівної діяльності є відсутність освіти, фаху та досвіду, що не дозволяє їм здійснити глибоке вивчення змісту своїх пропозицій та спрогнозувати можливі наслідки прийняття того чи іншого нормативного акту, доречно знов повернутися до питання про професіоналізм в сфері законотворчості.

На жаль, в Європі вже відкрито називають наших законодавців творцями законодавчого сміття: місія Європарламенту під керівництвом його екс-голови Пета Кокса проаналізувала діяльність Верховної Ради України і підготувала звіт з 52 рекомендаціями, в якому, серед іншого, зазначається, що Верховна Рада України є “слабкою ланкою”, перенавантажена великою кількістю законопроектів, які мають доволі низьку якість та являють собою “законодавче сміття” (“законодавчий спам”, “законодавче цунамі”) [30].

Фактично таку саму оцінку діяльності законотворців, представників виконавчої гілки влади та представників політичних сил надає у зворотному зв’язку електорат, висловлюючи своє обурення через згаданий інститут петицій: № 22/037844-еп “Ініціювати притягнення до кримінальної відповідальності народних депутатів, що здійснюють голосування за інших депутатів” (246 голосів; не підтримана), № 22/036085-еп “Ввести закон про кримінальну відповідальність за “кнопкодавство” та використання чужих індивідуальних карток іншими депутатами ВР України” (дата оприлюднення 25 квітня 2017 р., 327 голосів, не підтримана), № 22/030753-еп “Введення кримінальної відповідальності для депутатів ВР та Президента України” (дата оприлюднення 18 листопада 2016 р., 76 голосів, не підтримана), № 22/028533-еп “За популізм у політиці притягати до кримінальної відповідальності” (дата оприлюднення 5 вересня 2016 р., 25 голосів, не підтримана), № 22/025863-еп “Впровадити кримінальну відповідальність за невиконання політичних обіцянок” (дата оприлюднення 30 червня 2016 р., 96 голосів, не підтримана), № 22/024269-еп “Пропоную, щоб кожен обраний “народний слуга” ніс кримінальну та матеріальну відповідальність за невиконання своєї виборчої програми. Обманювати Український народ це великий злочин!” (дата оприлюднення 26 травня 2016 р., 272 голоси, не підтримана), № 22/021859-еп “Про кримінальну та адміністративну відповідальність Прем’єр міністра, міністрів усіх міністерств України, депутатів Верховної ради України, міських та сільських голів та депутатів місцевих самоврядувань України за брехню” (дата оприлюднення 4 березня 2016 р., 388 голосів, не підтримана), № 22/019916-еп “Видати закон, який передбачає кримінальну відповідальність для всіх

депутатів, які не виконали своїх обіцянок перед своїми виборцями” (дата оприлюднення 14 січня 2016 р., 251 голос, не підтримана), № 22/017238-еп “Кримінальна відповідальність за невиконання політичних обіцянок” (дата оприлюднення 02 листопада 2015 р., 62 голоси, не підтримана), № 22/017179-еп “Ввести кримінальну відповідальність за обман громадян України в передвиборній агітації” (дата оприлюднення 2 листопада 2015 р., 32 голоси, не підтримана) [14] тощо.

Свідомо або підсвідомо таке ставлення має своїм підґрунтям поінформованість про те, що група у кількості 450 не повною мірою компетентних осіб (відсутність відповідної освіти, фаху, досвіду тощо) опікується досить важливою державною діяльністю (процесом законотворчості), пояснення чому, напевно, слід шукати в містичній або езотеричній практиці (можливо, у цьому є певний незбагненний промисел: зібрати докупи випадкових для конкретної справи людей, дати їм завдання, а в тому, що з’явиться в результаті їх діяльності, шукати проявлений дух та потім надавати цьому тлумачення у системному зв’язку з вже існуючими нормами права і намагатися наявними науково-практичними силами усунути виявлені протиріччя методом “наукового ворожіння” [22, с. 58-68]), або в іншій площині (напр., через наявність групового ефекту (ефекту групи) – оптимізацію процесів усередині певної групи через складну систему сигналізації, обміну інформацією та взаємних відносин, що веде до підвищення життєздатності та ефективності існування для задоволення життєвих потреб усіх її членів).

Якщо впродовж всіх років державотворчості один з найважливіших органів формується з непрофесіоналів, то у вищенаведеній духовній або езотеричній практиці не повинно бути нічого соромітного або образливого, адже, як зазначає І.А. Ісаєв, філософія права як відкрита наука має можливість просунутися уперед тільки завдяки поверненню до своїх ідейних, духовних та, можливо, релігійних витоків, адже влада та закон, як явища метафізичного порядку, постійно зберігають у собі певну недомовленість, таємницю, яку так і не вдається з’ясувати сучасному раціоналізованому мисленню [17, с. 8-9].

Втім, існує інший підхід до процесу законотворчості. Якщо не доручити розробляти нормативні акти фахівцям (юристам-науковцям та правникам-практикам), розв’язання проблеми може полягати у використанні можливостей штучного інтелекту.

Сьогодні штучний інтелект задіяно в алгоритмах, які підказують водіям вірний напрямок руху за навігаційними картами [2], або самі керують транспортними засобами [23], здійснюють пропозиції споживачам на підставі аналізу їх попередніх замовлень, пропонують новини та аналітичні огляди певної спрямованості на підставі аналізу Big Data, підтримують процес прийняття рішень щодо лікування онкологічних захворювань молочної залози, підбирають варіанти лікування та розшифровують електрокардіограми тощо.

Системи розпізнавання обличчя людини, мовних, текстових та відео матеріалів, що побудовані на базі штучного інтелекту, вже є доволі розвинутими і використовуються у багатьох країнах світу поліцією та іншими департаментами.

Штучний інтелект перевершив людину у здібності до читання та розуміння тексту (результати людини в відповідному тесті складають 82.304, штучного інтелекту компанії Alibaba – 82.440, а Microsoft – 82.650) [7]. Юридична фірма Baker & Hostetler звільнила п’ятдесят юристів і прийняла на роботу штучний інтелект ROSS для ведення справ про банкрутство; вчені з Університетського коледжу Лондона і Університету Шеффілда створили “комп’ютерного суддю”, який передбачає рішення ЄСПЛ з точністю до 79 % [10]; у змаганнях між юристами лондонських фірм зі штучним інтелектом Case Cruncher Alpha у розв’язанні справ про виплату страхових відшкодувань

переміг останній [13]; робот-юрист на ім’я DoNotPay допомагає оскаржувати штрафи за паркування [8]; видання The Economist було надрукувано першу статтю, яка була підготовлена штучним інтелектом [9]. За прогнозами консалтингової фірми Cognizant через 10 – 15 років роботи відберуть 12 % робочих місць у жителів США, але з’являться такі нові професії, як детектив з роботи з даними (Data Detective), медичний технік з роботи зі штучним інтелектом (AI-Assisted Healthcare Technician), командний менеджер з роботи людини та машини (Man-Machine Teaming Manager), фахівець з довіри (Chief Trust Officer), аналітик квантового машинного навчання (Quantum Machine Learning Analyst), фахівець з етичних джерел (Ethical Sourcing Officer) [4] тощо.

На штучний інтелект покладають надії щодо зміни судової практики на краще: виявляти типові правові ситуації, розробляти алгоритми дій, зіставляти зі зразком, абстрагуватися від обставин, фактів, документів, речей та інших доказів, які не мають відношення до предмету розгляду, не охоплюються предметом спору або не відбивають обраний позивачем спосіб захисту, або не передбачені відповідною нормою матеріального права, виявляти нетипову поведінку суду за звичайних умов, обробляти значний обсяг інформації, готувати проект судового рішення тощо.

На думку фахівця в галузі теоретичної фізики та активного популяризатора науки у будь-якому прояві Мітіо Каку (Michio Kaku) цифрові технології дозволять позбавитися докучливої присутності посередників між виробником та споживачем, у всіх галузях з рутинними діями (складання довідок, листів, заяв тощо) штучний інтелект замістить людей, визволяючи їх час та енергію для більш креативних занять [19].

Штучний інтелект голосно заявляє про себе в сфері музики [12]. Розробники з SONY, Google та технічного підрозділу студії Abbey Road працюють над емоційною складовою штучного інтелекту – навчити роботів не тільки розпізнавати та імітувати почуття, але по-справжньому їх відчувати.

В Харківській державній академії залізничного транспорту у ногу з часом відкрита нова спеціальність “Інформаційні системи і технології в освітній програмі “Технології штучного інтелекту” [28]: базова підготовка розширена за рахунок проектування та програмування на Python, C, C ++, C #, Java, JavaScript, SQL, R, PHP, HTML5, CSS3, UML, розробки додатків для Windows, Linux, Android, iOS, створення програм класу “розумних” машин, “Інтернету речей”, інтелектуальних сенсорних систем з використання хмарних сервісів Microsoft, IBM, Amazon, Google та інструментів розробки для Arduino, Raspberry Pi, ESP8266 тощо. Не виключається поява спеціальності з умовною назвою “правові аспекти штучного інтелекту” в alma mater Національному юридичному університеті ім. Ярослава Мудрого (м. Харків).

Середньозважені прогнози щодо появи суперінтелекту (англ. – Artificial Superintelligence, ASI) виглядають наступним чином: звичайно за 5 – 10 років повністю вдосконалюються ті технології, які вже існують, за 15 – 20 років реалізуються ті, які сьогодні перебувають на рівні лабораторних досліджень. При цьому, скоріш за все, необхідно зробити поправку на постійне (у порівнянні з минулими сторіччями та десятиріччями) прискорення процесів обміну інформацією та розвитку економічних відносин, що може означати більш стрімкий наступ цифрового майбутнього.

Проблему ознайомлення з усіма публікаціями за певною тематикою та напрацювання на підставі цього конкретних рекомендацій успішно долає пошукова система Semantic Scholar, яка розроблена зусиллями Allen Institute for Artificial Intelligence (http://allenai.org – дослідницькою установою, що вивчає штучний інтелект) та забезпечує пошук за межами ключових слів у міждисциплінарних дослідженнях. На сьогодні жодна людина не має змоги відстежити всі системні зв’язки так, як це може

зробити штучний інтелект. В процесі правотворчості така здатність допоможе уникнути системних помилок всередині галузі та за міжгалузевими перехрещеннями.

Для того, щоб доручити штучному інтелекту розробку нових нормативних актів та(або) перевірку чинних й підготовку змін до них, останній повинен мати здатність до комплексної обробки значних обсягів інформації, здобутих з різних джерел, з’ясовувати системні співвідношення не тільки у межах однієї галузі, але й встановлювати міждисциплінарні зв’язки, мати здатність до самонавчання, в тому числі, накопичувати досвід, узагальнювати, відшукувати неочевидні логічні ланцюжки, робити конкретні умовиводи, вміти планувати тощо.

Наскільки це є можливим для нього, свідчать більш-менш виважені прогнози: до 2022 року штучний інтелект буде мислити повністю як людина (а не лише за окремими напрямками – медицина, гра в шахи тощо) на 10 %, до 2040 року – на 50 %, до 2075 року його процеси мислення неможливо буде відрізнити від людських так само, як невдовзі складно буде відрізнити між собою штучні та біологічні об’єкти, віртуальні світи стануть більш захоплюючими, ніж реальне оточення.

Штучний інтелект вже зараз наділений або невдовзі буде мати такі властивості, які у сукупності перевищують розумові здібності будь-якої людини: здатність до абстрактного мислення; сприйняття та розпізнання всіх сигналів зовнішнього світу (на противагу цьому людина, наприклад, не сприймає ультразвук та інфразвук, взагалі, те, що вона сприймає своїм органом зору, складає лише приблизно 2 % від повного електромагнітного діапазону тощо [16]); потужна теоретична база, знання всіх норм чинного законодавства та обізнаність у рішеннях за будь-якими судовими справами незалежно від галузевої належності; здатність до поширення і самозбереження; вирішення завдання способом мозкового штурму з залученням багатьох копій самого себе; стратегічне мислення, здатність заздалегідь прорабляти та прогнозувати різні варіанти; здатність до дедукції та індукції, аналізу та синтезу; здатність до моделювання; здатність ефективно працювати в умовах невизначеності та вірогідності; використання доступної інформації у найбільш доцільний та оптимальний спосіб; обізнаність у принципах своєї роботи і завдяки цьому здатність до самовдосконалення (перша версія утворює вдосконалену версію самої себе і так переписує програму до нескінченності) тощо.

Такий різновид штучного інтелекту матиме правовий статус “електронної особи (особистості)”, наукова та законодавча поява якого запропонована у Резолюції Європейського Парламенту від 16 лютого 2017 р. (European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL) [6].

Наділення штучного інтелекту статусом “електронної особи (особистості)”, скоріш за все, не повинне зустріти заперечень та неприйняття у сфері кримінально-правових та інших відносин. Адже звичним є закріплення за юридичною особою (яка, фактично, теж є віртуальним утворенням) правового статусу суб’єкта численних правовідносин, а, крім того, можливість застосування до неї заходів кримінально-правового характеру.

Наділення особи (“електронної особи (особистості)”), яка здійснює підготовку законопроекту, вищезазначеними когнітивними здібностями і властивостями з одночасним програмування функції покладення вето на неприйнятні пропозиції, дозволить переформатувати чинне законодавство, в тому числі узгодити його з іншими правовими системами, уникнути помилок у майбутньому.

З метою використання у законотворчій діяльності штучний інтелект необхідно буде навчити обґрунтовувати соціальну обумовленість певної норми, врахувати певні правила (тотожності, несуперечності, виключення третього, достатньої підстави тощо) і методи

(історичний, порівняльний, догматичний, системний, логічний та інші), за допомогою засобів, прийомів і правил нормотворчої техніки об’єктивувати правову норму у вигляді тексту, зміст якого повинен бути узгоджений на рівні системних зв’язків структурних частин норми права, в межах певного інституту, закону про кримінальну відповідальність та щодо всієї галузі кримінального права у нерозривній єдності з основоположними конституційними принципами та міжнародними зобов’язаннями України.

За наслідками роботи штучного інтелекту депутатському корпусу буде надано законопроект найкращої форми та змісту, який вже буде узгоджений на правозастосовному (залежно від суб’єкта майбутнього застосування певної норми) та науковому (відповідність фундаментальним теоретичним знанням) рівнях [15, с. 30-31]. На розгляд законодавцям залишиться лише буденний аспект законопроекту, що існує на рівні правосвідомості звичайного громадянина та представника народу і відповідає політичній ситуації у суспільстві.

Оскільки штучний інтелект є певним алгоритмом, зберігається небезпека протиправного втручання в його роботу, відповідальність за що сьогодні передбачена ст. 376-1 (“Незаконне втручання в роботу автоматизованої системи документообігу суду”) КК України або ст.ст. 361 – 363-1 Розділу “Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку” КК України, але надалі може бути закріплена в іншій відповідній нормі.

Ще одна небезпека полягає у тому, що людина може втратити контроль над штучним інтелектом повністю або частково. На таку можливість вказують умовиводи професора Оксфордського університету Ніка Бострома (Niklas Boström) [5], засновника компаній Tesla і SpaceX Ілона Маска (Elon Musk) [11], професора University of Washington School of Law та директора UW Tech Policy Lab Райана Кало (Ryan Calo) [3], професора Umeå Universitet (Швеція) Пітера Асаро (Peter M. Asaro) [1]. Їх стриманий оптимізм і застереження полягають у наступному: 1) внаслідок можливості до саморозвитку штучний інтелект перетвориться на суперінтелект; 2) у суперінтелекта з’являться свої власні потреби і цілі (він може бути менш людяним, ніж розумний прибулець); 3) суперінтелект може спробувати використати людей проти їх волі (наприклад, з метою отримання доступу до ресурсів); 4) суперінтелект може забажати залишитися єдиним інтелектом навкруги; 5) людина, як система зручно згрупованих атомів, може зацікавити суперінтелект в якості ресурсу; 6) людство не є готовим до зустрічі з суперінтелектом і ще не буде готове багато років; 7) людство повинно навчитися тримати штучний інтелект під достатнім контролем.

Висновки та пропозиції.

З метою підвищення рівня інформаційно-фахового забезпечення законодавчої діяльності, в тому числі в кримінально-правовій сфері та запобігання проявам інформаційної агресії на законодавчому рівні вбачається можливим використання штучного інтелекту під час підготовки законопроектів та експертизи чинних нормативних актів. При цьому вимоги до навичок штучного інтелекту можуть бути наступними: здатність обґрунтовувати соціальну обумовленість певної норми, врахувати певні правила (тотожності, несуперечності, виключення третього, достатньої підстави тощо) і методи (історичний, порівняльний, догматичний, системний, логічний та інші), за допомогою засобів, прийомів і правил нормотворчої техніки об’єктивувати правову норму у вигляді тексту, зміст якого повинен бути узгоджений на рівні системних зв’язків структурних частин норми права, в межах певного інституту, закону про кримінальну відповідальність та щодо всієї галузі кримінального права у нерозривній єдності з основоположними конституційними принципами та міжнародними

зобов’язаннями України. Такий підхід здатен підвищити рівень інформаційної безпеки, запобігти негативним впливам, але спроможний породити нові виклики, на які вже сьогодні необхідно вчитися реагувати належним чином.

Перспективи подальших досліджень. Порушені питання та надана їм авторська оцінка є дискусійними та відкритими для широкого обговорення з огляду на їх актуальність та важливість для забезпечення сталого розвитку суспільства, забезпечення інформаційної безпеки, прав та свобод громадян.

Використана література

1. Asaro P. Robots and Responsibility from a Legal Perspective. – Mode of access : http://www.peterasaro.org/writing/ASARO_Legal_Perspective.pdf. – Title from the screen.

2. Airbus начнет выпускать летающее такси в 2020 году**.** – Режим доступу : https://inforesist.org/airbus-nachnet-vyipuskat-letayushhee-taksi-v-2020-godu. – Заголовок з екрану.

3. Calo R. Robots in American Law / Legal Studies Research Paper No. 2016-04 / University of Washington School of Law. – Mode of access : http://www.datascienceassn.org/sites/default/files/ Robots_in_American_Law.pdf. – Title from the screen.

4. Caroline Cakebread. Robots aren't just taking our jobs, they're creating them – here are 21 weird jobs humans will have in the future. – Mode of access : http://www.businessinsider.com/21-weird-jobs-humans-will-have-when-robots-take-over-2017-11/#data-detective-1. – Title from the screen.

5. Etzioni Oren. No, the Experts Don’t Think Superintelligent AI is a Threat to Humanity. – Mode of access : https://www.technologyreview.com/s/602410/no-the-experts-dont-think-superintel ligent -ai-is-a-threat-to-humanity. – Title from the screen.

6. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL). – Режим доступу : http://www.europ arl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//EN. – Заголовок з екрану.

7. Fenner Robert. Alibaba's AI Outguns Humans in Reading Test / Bloomberg Technology, 15 Jan 2018. – Mode of access : https://www.bloomberg.com/technology. – Title from the screen

8. – Режим доступу : https://donotpay-search-master.herokuapp.com

9. How soon will computers replace The Economist’s writers? Robots. – Mode of access : https://www.economist.com/news/science-and-technology/21732805-weve-got-few-years-left-least-how-soon-will-computers-replace-economists. – Title from the screen.

10. Knapton Sarah. Artificially intelligent ‘judge’ developed which can predict court verdicts with 79 per cent accuracy. – Mode of access : http://www.telegraph.co.uk/science/2016/10/23/artifica lly -intelligent-judge-developed-which-can-predict-court. – Title from the screen.

11. Kumparak G. Elon Musk Compares Building Artificial Intelligence To “Summoning The Demon”. – Mode of access : https://techcrunch.com/2014/10/26/elon-musk-compares-building-artifi cial-intelligence-to-summoning-the-demon. – Title from the screen.

12. Moth Anastasia. Убьёт ли искусственный интеллект музыку? – Режим доступу : https://storia.me/ru/@anastasia.moth/nauka-i-tekhnologii-3hnlal/ubet-li-iskusstvennyi-intellekt-muzy ku -3j99vd. – Заголовок з екрану.

13. Rory Cellan-Jones. The robot lawyers are here – and they’re winning. – Mode of access : http://www.bbc.com/news/technology-41829534. – Title from the screen.

14. Електронні петиції. Офіційне Інтернет-представництво Президента України. – Режим доступу : https://petition.president.gov.ua. – Заголовок з екрану.

15. Загиней З. Кримінально-правова герменевтика : монографія / З. Загиней. – К. : Видавничій дім “АртЕк”, 2015. – 380 с. – С. 30-31

16. Иллюзия восприятия: ограниченность зрения, слуха и других органов чувств человека. – Режим доступу : http://bp21.livejournal.com/103392.html. – Заголовок з екрану.

17. Исаев И.А. Топос и номос : пространства правопорядков / И.А. Исаев. – М. : Норма, 2013. – 416 с. – С. 9.

18. Киричко В.М. Законодавчий вірус у системі КК України : визначення і актуалізація проблеми на прикладі ст. 368-2 КК “Незаконне збагачення” : зб. наук. праць “Проблеми законності” ; відп. ред. В.Я. Тацій. – Харків : Нац. юрид. ун-т імені Ярослава Мудрого, 2016. – Вип. 133. – 282 с. – С. 142-151.

19. Носырев И. Митио Каку : “Бесполезные посреднические профессии отомрут”. – Режим доступу : http://fastsalttimes.com/sections/solution/1586.html. – Заголовок з екрану.

20. Панов М.І. Принципи кримінального права і їх реалізація у кримінальному правотворенні : матеріали міжнар. наук.-практ. конф [“Проблеми науки кримінального права та їх вирішення у законотворчій та правозастосовній діяльності”], (м. Харків, 8 – 9 жовт. 2015 р.) ; редкол. В.Я. Тацій (голов. ред.), В.І. Борисов (заст. голов. ред.) та ін. – Х. : Право, 2015. – 528 с. – С. 11-18.

21. Радутний О.Е. Інформаційна агресія в законодавчій сфері : матеріали міжнар. наук.-практ. конф [“Проблеми науки кримінального права та їх вирішення у законотворчій та правозастосовній діяльності”], (м. Харків, 8 – 9 жовт. 2015 р.) ; редкол. В.Я. Тацій (голов. ред.), В.І. Борисов (заст. голов. ред.) та ін. – Х. : Право, 2015. – 528 с. – С. 158-162.

22. Радутний О.Е. Нарис стану інформаційно-законодавчої діяльності на прикладі КК України // Інформація і право. – № 3 (18)/2016. – С. 58-68.

23. Стартап сооснователя Google показал “летающий автомобиль”. – Режим доступу : https://inforesist.org/startap-soosnovatelya-google-pokazal-letayushhiy-avtomobil. – Заголовок з екрану.

24. Тацій В.Я. Десять років чинності Кримінального кодексу України : здобутки та шляхи вдосконалення : матеріали міжнар. наук.-практ. конф. [“10 років чинності Кримінального кодексу України : проблеми застосування, удосконалення та подальшої гармонізації із законодавством європейських країн”], (м. Харків, 13 – 14 жовт. 2011 р.) ; редкол. : В.Я. Тацій (голов.ред.), В.І. Борисов (заст.голов.ред.) та ін. – Х. : Право, 2011. – 456 с. – С. 29-35.

25. Тимошенко В.А., Дрьомов С.В. Проблеми законодавчого забезпечення протидії створенню терористичної організації в Україні : матеріали міжнар. наук.-практ. конф [“Проблеми науки кримінального права та їх вирішення у законотворчій та правозастосовній діяльності”], (м. Харків, 8 – 9 жовт. 2015 р.) ; редкол. В.Я. Тацій (голов. ред.), В.І. Борисов (заст. голов. ред.) та ін. – Х. : Право, 2015. – 528 с. – С. 23-27)

26. Туляков В.О. Право на злочин та право бути покараним у контексті розвитку прав людини : матеріали міжнар. наук.-практ. конф. [“Кримінально-правове забезпечення сталого розвитку України в умовах глобалізації”], (м. Харків, 12 – 13 жовт. 2017 р.) ; редкол. : В.Я. Тацій (голов. ред.), В.І. Борисов, (заст. голов. ред.) та ін. – Х. : Право, 2017. – 560 с. – С. 85-88.

27. Тютюгин В.И. К вопросу о качестве законотворчества в уголовном законодательстве : матеріали міжнар. наук.-практ. конф. [“Кримінально-правове забезпечення сталого розвитку України в умовах глобалізації”], (м. Харків, 12 – 13 жовт. 2017 р.) ; редкол. В.Я. Тацій (голов. ред.), В.І. Борисов, (заст. голов. ред.) та ін. – Х. : Право, 2017. – 560 с. – С. 50-56.

28. Харьковский вуз открыл фантастическую специальность. – Режим доступу : http://www.sq.com.ua/rus/news/novosti/05.07.2017/harkovskiy_vuz_otkryl_fantasticheskuyu_spetsialnost. – Заголовок з екрану.

29. Швець В.Д. Практика внесення змін і доповнень до КК України : здобутки та прорахунки [“10 років чинності Кримінального кодексу України : проблеми застосування, удосконалення та подальшої гармонізації із законодавством європейських країн”], (м. Харків, 13 – 14 жовт. 2011 р.) ; редкол. В.Я. Тацій (голов.ред.), В.І. Борисов (заст.голов.ред.) та ін. – Х. : Право, 2011. – 456. – С. 35-40.

30. Шпайхер Т. В Европе назвали украинских депутатов “творцами законодательного мусора” / Экономические известия, 13.03.2016 года. – Режим доступу : http://news.eizvestia.com/news_politics/full/655-v-evrope-nazvali-ukrainskih-deputatov-tvorcami-zakodatelnogo-musora

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 343.97

БЕСПАЛЬ О.Л., асистент кафедри кримінального права і процесу
Навчально-наукового Юридичного інституту
Національного авіаційного університету

СОЦІАЛЬНО-ДЕМОГРАФІЧНІ ОЗНАКИ ОСІБ, ЯКІ ВЧИНИЛИ СІМЕЙНЕ НАСИЛЬСТВО ЩОДО ДІТЕЙ

***Анотація**. Розглянуто соціально-демографічні ознаки (стать, вік, місце проживання, сімейний стан, освітній рівень) структури особистості злочинця, яка вчинила насильство в сім’ї проти життя та здоров’я щодо дітей.*

***Ключові слова**: насильство в сім’ї, соціально-демографічні ознаки, діти, кримінологічний портрет.*

***Summary.** The socio-demographic traits (sex, age, place of residence, marital status, educational level) of the personality structure of the perpetrator who committed domestic violence against life and health against children are considered.*

***Keywords**: domestic violence, socio-demographic traits, children, criminological portrait.*

***Аннотация**. Рассмотрены социально-демографические признаки (пол, возраст, место жительства, семейное положение, образовательный уровень) структуры личности преступника, совершившего насилие в семье против жизни и здоровья в отношении детей.*

***Ключевые слова**: насилие в семье, социально-демографические признаки, дети, криминологический портрет.*

Постановка проблеми. Однією з вагомих складових дослідження проблеми сімейного насильства є вчення про особистість злочинця, яке має велике як наукове, так і практичне значення, що дозволить вирішити ряд кримінологічних питань, зокрема, детермінанти сімейного насильства щодо дітей, а також розроблення заходів запобігання злочинам, які вчиняються на ґрунті сімейних відносин щодо дітей.

Кримінологічна характеристика особистості злочинця розкривається через її структуру. Структурна будова особистості злочинця охоплює певним чином сконструйовану органічно цілісну систему взаємозв’язків між її елементами [1, с. 35].

Результати аналізу наукових публікацій. В науці кримінального права та кримінології проблемі сімейного насильства та насильства щодо дітей, зокрема, були присвячені наукові роботи таких вітчизняних вчених, як, зокрема: О.І. Белової, А.Б. Благої, В.М. Бондаровської, В.В. Вітвіцької, Б.М. Головкіна, Т.В. Журавель, С.Г. Киренка, О.О. Кочемировської, Л.В. Крижної, Ю.М. Крупки, Л.В. Левицької, М.П. Мишляєва, Ю.Л. Приколотіної, Л.В. Самарай, М.Ю. Самченко, Н.С. Юзікової.

Однак, незважаючи на наявні наукові напрацювання щодо кримінологічної характеристики особистості злочинця та її структури, необхідно констатувати, що в кримінології немає комплексного дослідження особистості злочинця насильства в сім’ї саме проти життя та здоров’я щодо дітей.

Метою статті є визначення соціально-демографічних ознак осіб, які вчиняють насильство в сім’ї проти життя та здоров’я дітей.

Виклад основного матеріалу. Соціально-демографічні ознаки властиві будь-якій особі й самі по собі не мають кримінологічного значення. Проте у статистичній звітності стосовно осіб, які вчинили злочини, соціально-демографічні ознаки дають

відомості, без яких неможлива повна кримінологічна характеристика особи злочинців [2, с. 87]. До основних соціально-демографічних ознак належать, як вважаємо, стать, вік, місце проживання, сімейний стан, освітній рівень.

За даними офіційної статистики з 2013 р. по 2016 р. (див. Таблицю) середній показник осіб, які перебували на обліку за вчинення насильства в сім’ї, становить 91,7 % для чоловіків, а середній показник для осіб жіночої статі за вказані роки – 8,3 %. Виходячи з цього, можна зазначити, що насильство в сім’ї проти життя та здоров’я щодо дітей вчиняється здебільшого особами чоловічої статі.

Таблиця.

Кількість осіб, що перебували на обліку,
які схильні до вчинення насильства в сім’ї за 2010 – 2016 роки [3]

Роки	**2013 р.**	**2014 р.**	**2015 р.**	**2016 р.**
Перебувало на профілактичному обліку, всього	92 772	77 634	65 462	63 605
% до попереднього року	-	*16,3 %*	*15,7 %*	*2,9 %*
З них чоловіків	90,9 %	91,6 %	91 %	90,9 %
З них жінок	9,1 %	8,4 %	9 %	9,1 %

За результатами проведеного анкетування співробітників служб у справах дітей 72,1 % чоловіків та 27,9 % жінок вчинили сімейне насильство безпосередньо щодо дітей.

Багато вчених акцентують увагу на тому, що злочинна активність чоловіків загалом у шість разів перевищує злочинну активність жінок. Це вони пояснюють так: жінка обмежена у своїй діяльності колом сімейного життя, зайнята домашнім господарством, а тому вона набагато рідше, ніж чоловік, піддається враженням, що збуджують пристрасті; у чоловіка, у порівнянні з жінкою, набагато більше найрізноманітніших і сильних відчуттів, під впливом яких виникає план злочину; чоловіки більше схильні до вживання алкоголю і наркотиків, зловживання якими призводить до злочину [4, с. 192].

Так, дійсно, значна частина чоловіків, вчиняючи насильство щодо дітей, характеризуються нестриманістю, імпульсивністю дій, використовують фізичну перевагу стосовно дітей-жертв насильства, намагаючись покарати, провчити або вплинути на поведінку останніх (наприклад, припинити нестримний плач дитини).

Г.Ю. Мустафаєв та І.І. Довгаль зазначають про існування “чоловічої культури насильства”. Ця субкультура конкретно не належить до визначеної соціальної групи або класу, релігії, професії чи нації. Чоловіки всіх суспільних груп, перебуваючи під впливом чоловічого середовища, засвоюють норми, етичні цінності і переконання, які стосуються чоловічого домінування [5, с. 20]. Такі чоловіки, намагаючись зберегти “владу”, закріпити патріархальні відносини та тримати членів сім’ї у визначених рамках, вчиняють різні види сімейного насильства (фізичне, психічне, економічне), що посягають на життя та здоров’я дітей.

Стосовно жінок, які вчиняють насильство щодо дітей, то вважаємо, що воно є ганебним і таким явищем, що суперечить самій природі жінки-матері, яка дає нове життя та повинна піклуватись й оберігати дітей. Варто погодитись з думкою Р.В. Перелигіної, що жінка за своєю природою асоціюється з такими цінностями, як турбота, ніжність, збереження домашнього затишку. Виступаючи проти суспільства, вчиняючи злочин, жінка не просто підриває основи загального добробуту, але і деформує власну природу, порушує в собі гармонію біологічного і соціального начал [6, с. 86].

Крім того, побутові негаразди, безробіття, незатребуваність, невлаштованість особистого життя і т.д. – все це негативно впливає на психічний стан жінки, що в результаті може призвести до вчинення насильства щодо дітей. У наш час прогресує жіночий аморалізм, що проявляється у сексуальній розпусті, пияцтві, побутовій неохайності. Певна частина жінок стає грубими, жорстокими й агресивними [1, с. 40].

Вважаємо, що однією з проблем сьогодення є соціальна та особиста невлаштованість жінок, в результаті чого збільшується психічна напруга, невдоволеність життям, як наслідок – такі жінки “зриваються” на дітях. За даними офіційної статистики в 2016 році 20,1 % жінок народили дітей поза шлюбом, з них найбільша кількість припадає на вік 25-29 років – 26,1 % від зальної кількості жінок, які народили дітей в незареєстрованому шлюбі, на другому місці вікова категорія 20-24 роки – 23,3 % таких жінок. Окрему увагу варто приділити віковій категорії “до 20 років” – на них припадає 12,1 % жінок, які народили дітей поза шлюбом [7, с. 19]. Здебільшого такі жінки (крім загальноосвітньої) не мають освіти, яка б дозволила їм працевлаштуватись на кваліфіковану та вище оплачувану роботу. Їхній інтелектуальний рівень, відсутність певних знань та навичок теж впливають на поведінку, ставлення до дітей та методи їх виховання, в результаті чого такі жінки особисті, побутові проблеми та негаразди “виливають” на дітей, вчиняючи насильство над ними.

Разом з тим, 90 % жінок, які займаються бізнесом, визнають, що з кар’єрним ростом частіше стали бити своїх дітей [8, с. 17]. Тобто, жінки, які мають високий інтелектуальний рівень, мають значні успіхи в професійній діяльності, часто застосовують фізичне насильство до своїх дітей. Це свідчить про те, враховуючи постійну зайнятість таких жінок, дітям не приділяється належна увага, матері не цікавляться проблемами дітей, інтересами, вподобаннями, а в разі виникнення непорозуміння або інших проблем – застосовують фізичне насильство, як метод виховання.

Найчастіше вчиняють насильство в сім’ї проти життя та здоров’я щодо дітей особи вікової групи 30-49 років – 81,3 %, на другому місці вікова група 25-29 років – 9,2 %, на третьому 50 і старше – 4,7 %, найменше вчиняють особи вікової категорії 14-17 років та 18-24 роки – 2,5 % та 2,3 % відповідно.

Особи віком 30-49 років становлять найбільшу кількість від загальної чисельності населення України – майже 30 % [9, с. 4-5]. На вікову групу від 30 до 49 років доводиться значна кількість осіб, які зловживають спиртними напоями, що є однією з умов скоєння злочинів проти дітей. Стан сп’яніння призводить до зниження самоконтролю за поведінкою, до перекручення, неадекватної оцінки різних ситуацій, стимулюючи у такий спосіб прояви агресії [10, с. 36].

Результати нашого дослідження свідчать, що найбільше осіб, які вчинили сімейне насильство щодо дітей, мешкають у селах та селищах – 57,4 %, у містах – 39,9 %, найменше вчиняли особи без визначеного місця проживання (2,7 %). Такі дані свідчать про те, що саме в селах та селищах більш розповсюджене сімейне насильство проти життя та здоров’я щодо дітей, а також це пояснюється тим, що в містах сімейне життя більш закрите, ніж у сільській або селищній місцевості, де жителі знають один одного і їхні приватні та сімейні проблеми, які мають місце, важко приховати від оточення.

Рівень освіти має важливе значення при дослідженні особистості злочинця. Безумовно прямої залежності між рівнем освіти і формою поведінки особи не існує, проте освітній рівень впливає на правосвідомість, на здатність вибору суспільно одобрюваного варіанту поведінки [1, с. 44]. Переважна більшість осіб, які вчинили сімейне насильство щодо дітей, мали повну загальну середню освіту (44,7 %), середню

спеціальну мали 29,5 %, неповну середню – 19 %, вищу освіту мали 5 %, початкову загальну та взагалі без освіти були 1,8 % осіб.

Тож, враховуючи вищенаведені дані, можна стверджувати, що найбільше вчиняли сімейне насильство щодо дітей особи, які не мали середньої спеціальної або вищої освіти – 65,5 %. Досліджуючи злочини у сфері сімейно-побутових відносин, Л.В. Крижна слушно зауважила, що ці злочини найчастіше вчинюють особи з невисоким освітнім рівнем. Для них властиві такі негативні риси, як: нестриманість емоцій, брутальність, егоїзм, безтактність, уїдливість, черствість тощо, через що вони менше володіють собою в конфліктних ситуаціях і часто задовольняють свої бажання, застосовуючи грубу фізичну силу [11, с. 20].

Дослідження сімейного стану осіб, які вчинили насильницькі посягання на життя та здоров’я дітей показало, що більшість винних перебували у: фактичному (незареєстрованому) шлюбі – 40,7 %, зареєстрованому шлюбі – 38,8 %, розірваному шлюбі – 10,6 %. Найменша кількість винних осіб взагалі були не одруженими (холостяками) – 8,1 %, вчинення вдовою (вдівцем) – 1,8 %.

Переважна більшість винних осіб, які вчинили насильство стосовно дітей, що перебувають поза шлюбом пояснюється тим, що в Україні останнім часом є поширеними фактичні шлюбні відносини (без реєстрації шлюбу). Як свідчить статистика станом на 2016 рік із загальної кількості зареєстрованих шлюбів (299 453 одиниць) 43,4 % (129 997 одиниць) становлять розлучення [7, с. 55]. Особи, в яких не склались попередні шлюбні відносини, намагаються в подальшому влаштувати своє особисте життя. На жаль, в такій ситуації діти залишаються без належної уваги або стають об’єктом “зігнання” всіх особистих негараздів і невдач в житті батьків.

За даними нашого дослідження винні особи за сімейними ролями розподілились наступним чином: батько – 37,1 %, мати – 22,8 %, вітчим – 18,3 %, співмешканці – 17,8 %, найменше вчиняли мачуха, опікуни та піклувальники – 3 %, 0,7 %, 0,3 % відповідно. Тобто найчастіше вчиняли сімейне насильство проти життя та здоров’я щодо дітей рідні батьки (54,5 % загалом).

Особи, які вчинили зазначені злочини, найчастіше мешкали в родині: з дружиною (чоловіком) і рідними дітьми – 35 %, з співмешканцем (співмешканкою) і рідними дітьми – 16,2 %, з дружиною (чоловіком) та їх дітьми – 12 %, з співмешканцем (співмешканкою) і нерідними дітьми – 10,8 %, з співмешканцем (співмешканкою) та їх дітьми – 9,6 %, сам (сама) з рідними дітьми – 8,7 %, з дружиною (чоловіком) і нерідними дітьми – 7,2 %, сам (сама) з нерідними дітьми – 0,5 %.

Важливе значення для встановлення портрету особистості злочинця мають відомості про соціальне положення та рід занять. Отримані нами результати досліджень свідчать про те, що переважна більшість винних осіб у вчинені сімейного насильства проти життя та здоров’я щодо дітей не займалися суспільно-корисною працею, тобто 52 % осіб не працювали і не вчилися без поважних причин, 36,7 % – робітники, 7 % – не працювали і не вчилися з поважних причин (до числа яких входили особи, які перебували у відпустці по догляду за дитиною), 1,8 % – вчилися у вищих навчальних закладах. Необхідно зауважити, що серед винних осіб небагато було пенсіонерів та службових осіб – 1,7 % та 0,8 % відповідно.

Серед тих осіб, які були працевлаштованими, були зайняті у сфері: сільського господарства – 12,3 %, надання послуг – 11,6 %, торгівлі – 5,9 %, 16,2 % – зайняті іншими видами діяльності, які не були встановлені.

Згідно із дослідженням, значна більшість осіб, які не працювали і не вчилися без поважних причин (50,4 %) перебивались тимчасовими заробітками, 29,8 % – жили за

рахунок доходів дружини (чоловіка) або родичів, 10,9 % – мали нетрудові джерела існування (збереження, спадщина тощо), 4,5 % – заробляли на життя антисуспільним способом, 4,4 % – мали пенсію.

Висновки.

На основі вищенаведених даних можна зробити висновки, що в основному вчиняють сімейне насильство проти життя та здоров’я щодо дітей особи чоловічої статі – 72,1 % (з них 54,5 % – рідний батько), вікової групи 30-49 років (81,3 %), які мешкають у сільській місцевості (57,4 %), мають повну загальну середню освіту (44,7 %), перебувають у незареєстрованому (фактичному) шлюбі (40,7 %). Особи, які вчинили таке насильство, найчастіше мешкали в родині з дружиною (чоловіком) і рідними дітьми – 35 %, переважна більшість осіб не займалася суспільно-корисною працею, тобто 52 % осіб не працювали і не вчилися без поважних причин, з них 50,4 % перебивались тимчасовими заробітками. Серед тих осіб, які були працевлаштованими, були зайняті найбільше у сфері сільського господарства – 12,3 %.

Отже, на підставі соціально-демографічних ознак, як однієї зі складових кримінологічного портрету осіб, які вчинили насильство в сім’ї проти життя та здоров’я щодо дітей, маємо можливість дослідити детермінанти такого насильства, що в сукупності дозволить розробити та запропонувати заходи запобігання насильству в сім’ї проти життя та здоров’я щодо дітей.

Використана література

1. Головкін Б.М. Кримінологічні проблеми умисних вбивств і тяжких тілесних ушкоджень, що вчиняються у сімейно-побутовій сфері / Б.М. Головкін. – Х. : Нове слово, 2004. – 252 с.

2. Іванов Ю.Ф. Кримінологія : навч. посіб. / Ю.Ф. Іванов та ін. – К. : Вид. ПАЛИВОДА А.В., 2006. – 264 с.

3. Лист Департаменту інформаційної підтримки та координації поліції “102” Національної поліції України від 13.03.17 р. № 27/02/2-Б-88.

4. Самарай Л.В. Кримінологічна характеристика особи кривдника, який учинив сімейне насильство під впливом агресії // Науковий вісник. – К. : НАВС, 2013. – Вип.1(86). – С.190-197.

5. Методичний посібник для фахівців, які впроваджують корекційні програми для осіб, які вчинили насильство в сім’ї ; укладачі Мустафаєв Г.Ю., Довгаль І.І. – К., 2011. – 192 с.

6. Перелигіна Р.В. Кримінологія насильства осіб жіночої статі : дис. на здобуття наук. ступеня канд. юрид. наук (12.00.08) / Р.В. Перелигіна. – К. : Київський університет права НАН України. 2015. – 234 с.

7. Природний рух населення за 2016 рік : статистичний бюлетень. – К. : Державна служба статистики, 2017. – 57 с. – Режим доступу : http://www.ukrstat.gov.ua/druk/publicat/kat_u/2017/bl/06/bl_prn2016pdf.zip

8. Дементьева И. Жестокое обращение с ребенком в семье : последствия для личностного развития // Практична психологія та соціальна робота. – 2011. – № 6 (147). – С.17-20.

9. Розподіл постійного населення за статтю та віком на 1 січня 2017 року. / Державна служба статистики України. – (Експрес-випуск від 21.06.17 р. № 151/0/10.2вн-17. – Режим доступу : http://www.ukrstat.gov.ua/druk/publicat/kat_u/publnasel_u.htm

10. Вітвіцька В.В. Запобігання насильству стосовно дитини : наук.-практ. рекомендації / В.В. Вітвіцька. – Донецьк : Донецький юрид. ін-т. Луганського ДУВС, 2010 р. – 79 с.

11. Крижна Л.В. Злочини у сфері сімейно-побутових відносин (кримінологічний аспект) : монографія / Л.В. Крижна. – К. : КІВС, 2003. – 105 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 347.9 + 316.3:027

СОЛОНЧУК І.В., старший викладач кафедри інформаційного права
і права інтелектуальної власності Факультету соціології і права
Національного технічного університету України
“Київський політехнічний інститут імені Ігоря Сікорського”

ІНФОРМАЦІЙНІ ПРАВОВІДНОСИНИ В КОНТЕКСТІ ЦИВІЛЬНОГО СУДОЧИНСТВА

Анотація. *Стаття присвячується дослідженню проблемних питань щодо інтеграції інформаційних правовідносин в сферу цивільного судочинства через призму новел сучасної судової реформи. Представлений аналіз основних положень цивільного процесуального законодавства України щодо перспективи успішного використання інформаційно-комунікаційних технологій з метою полегшити доступ до правосуддя, покращити здійснення судового провадження в справах, та загалом підвищити рівень цивільного судочинства. На ґрунті вимог міжнародних стандартів правосуддя та основних положень інформаційного права запропонована спроба дослідження сутності та доцільності використання таких категорій як “електронний позов”, “електронний документообіг”, “електронний суд”. Здійснено порівняльний аналіз положень законодавства України та положень цивільного процесуального законодавства іноземної держави, які регулюють подібні правовідносини, для формування висновків щодо можливості запозичення позитивного досвіду та удосконалення національного законодавства у сфері використання сучасних інформаційних технологій в цивільному судочинстві.*

Ключові слова: *інформаційне суспільство, інформаційні правовідносиниі, цивільне судочинство, судова реформа, інформаційно-комунікаційні технології, електронний позов, електронний документообіг, електронний суд.*

Summary. *The article is devoted to the research of the processes of integration of information legal relations in the sphere of civil proceedings in accordance with the requirements of modern judicial reform. The research provides analysis of the main provisions of the civil procedural legislation of Ukraine regarding the prospects for the successful use of information and communication technologies to facilitate access to justice, improve the implementation of judicial proceedings, and generally improve the level of civil litigation. Considering international standards of justice and basic provisions of information law, an attempt was made to investigate the nature and appropriateness of using such popular categories as “electronic lawsuit”, “electronic document management”, “electronic court”. A comparative analysis of the provisions of Ukrainian legislation and provisions of the civil procedural legislation of other states regulating such legal relations was made with the aim of drawing conclusions about the possibility of borrowing positive experience and improving national legislation in the field and using modern information technologies in the implementation of civil proceedings.*

Keywords: *information society, information legal relations, civil proceedings, judicial reform, information and communication technologies, electronic lawsuit, electronic document management, electronic court.*

Аннотация. *Статья посвящается исследованию процессов интеграции информационных правоотношений в сферу гражданского судопроизводства в соответствии с требованиями современной судебной реформы. Представлен анализ основных положений гражданского процессуального законодательства Украины касательно перспектив успешного использования информационно-коммуникационных технологий с целью облегчить доступ к правосудию, улучшить осуществление судебного производства, и в целом повысить уровень гражданского судопроизводства. Учитывая международные стандарты правосудия и основные положения информационного права, выполнено исследование сущности и целесообразности использования*

таких популярных категорий как “электронный иск”, “электронный документооборот”, “электронный суд”. Осуществлен сравнительный анализ положений законодательства Украины и положений гражданского процессуального законодательства других государств, регулирующих подобные правоотношения, с целью формирования выводов о возможности заимствования положительного опыта и совершенствование национального законодательства в сфере использования современных информационных технологий при осуществлении гражданского судопроизводства.

Ключевые слова: *информационное общество, информационные правоотношения, гражданское судопроизводство, судебная реформа, информационно-коммуникационные технологии, электронный иск, электронный документооборот, электронный суд.*

Постановка проблеми. Кожна сфера суспільного життя об’єктивно зазнає вплив інформаційного прогресу. Суспільство сучасності – це, в першу чергу, інформаційне суспільство, для якого є характерною інтеграція інформаційних відносин в усі сфери діяльності. Зважаючи на вимоги часу, сфера правосуддя, зокрема сфера судочинства, не може, та і не повинна залишатися осторонь цієї проблеми. Зазначені інтеграційні процеси пов’язані з розвитком інформаційних технологій, які потребують уточнення наукової визначеності фундаментальних правових категорій.

Питання реформування судової системи України та вдосконалення процесу відправлення правосуддя в контексті успішного використання інформаційних технологій наразі є своєчасним та нагальним, на чому невпинно акцентують увагу міжнародні інституції. Так, Консультативною радою європейських суддів ще 9 листопада 2011 року був прийнятий Висновок № 14 “Судочинство та інформаційні технології”, який включає низку рекомендаційних положень для держав-членів Ради Європи з метою використання інформаційних технологій як засобу покращення здійснення судочинства, що може полегшити доступ до правосуддя, покращити процес розгляду та руху справ, та загалом підвищити рівень судочинства [5].

Проаналізувавши положення Цивільного процесуального кодексу України в редакції Закону від 3 жовтня 2017, можемо зазначити, що наразі законодавство України містить прогресивні новели щодо використання інформаційних технологій в цивільному судочинстві [7]. Безумовно, такі зміни на законодавчому рівні є необхідними, але не менш важливе значення мають дієві механізми практичного впровадження вказаних нововведень, пов’язані із загальними принципами інформаційної політики держави..

Результати аналізу наукових публікацій. Проблема розвитку інформаційних відносин, інформаціного права та інформаційного суспільства останніми роками активно досліджувалась в працях таких провідних науковців як Баранов О.А., Брижко В.М., Фурашев В.М. та ін., див у [1 – 2]. Система електронного судочинства є предметом дослідження Кушакової-Костицької Н.В. [3]. Водночас, враховуючи зміни у законодавстві України, потребує підвищення рівень ґрунтовних досліджень щодо можливостей та впливу сучасних інформаційних технологій на процес організації та здійснення судочинства.

Метою статті є порівняльний аналіз правових положень законодавства України та міжнародних нормативних документів в контексті запровадження інформаційних технологій з метою покращення організації та здійснення цивільного судочинства. Також представлена спроба обґрунтувати можливості застосування та недоліки таких термінологічних словосполучень, як “електронний суд”, “електронний документообіг”, “електронний позов” та ін.

Виклад основного матеріалу. На нашу думку, інформаційне право як галузь права, в порівнянні з іншими галузями права, має найбільш стрімкий розвиток, що

визначається об’єктивними факторами, пов’язаними з розвитком технічного процесу. Крім того, спостерігається невпинна та стрімка інтеграція інформаційних відносин в інші сфери життєдіяльності суспільства. Наукові категорії, розроблені в межах інформаційного права, дедалі частіше використовуються іншими галузями знань, що свідчить про універсальність інформаційного права та про його вплив у всіх сферах наукових досліджень. Без перебільшень можна констатувати, що, наприклад, такі терміни як “електронний уряд”, “електронна демократія”, “електронна торгівля” та подібні увійшли в сферу повсякденного вжитку. В цьому аспекті виникає нагальна потреба у чіткому визначенні основоположних понять, якими оперують дослідники. Зокрема, на думку Баранова О.А., на сьогодні все ще існує певна неоднозначність щодо визначення дефініції “інформаційне суспільство”, яка спровокувала поширення низки недостатньо обґрунтованих термінів, в тому числі терміну “електронний суд” [1, с. 32]. В контексті даної роботи дослідження базується на його твердженні про те, що інформаційне суспільство – це суспільство, в якому вся сукупність суспільних відносин з метою підвищення ефективності людської діяльності в різних сферах (політиці, економіці, публічному управлінні, військовій справі, освіті, культурі, розвагах, особистому житті тощо) реалізується на основі максимального використання інформаційних комп’ютерних технологій [1, с. 33].

Сфера правосуддя як невід’ємна складова апарату державного управління на сучасному етапі перебуває в стані реформування, метою якого є покращення судочинства та підвищення ефективності організації і діяльності судів. Надбання, які є результатом розвитку технічного прогресу, дозволяють демократичній державі максимально використовувати сучасні інформаційні технології в процесі відправлення правосуддя. Ефективне застосування сучасних інформаційних технологій, безумовно, полегшує функціональні повноваження, зокрема, на нашу думку, може слугувати засобом вирішення нагальної проблеми перевантаження судів. Окремої уваги в цьому аспекті заслуговує судочинство, оскільки на сьогодні величезна кількість справ, які розглядаються та вирішуються в судах, є саме цивільними. Так, за даними аналітичних таблиць щодо надходження справ і матеріалів до місцевих загальних судів за перше півріччя 2017 року, до місцевих загальних судів як до судів першої інстанції надійшло 342 658 цивільних справ (для порівняння: за аналогічний період кримінальних справ надійшло 66 694) [4].

Консультативною радою європейських суддів (далі – КРЄС) був розроблений та прийнятий 9 листопада 2011 року висновок “Судочинство та інформаційні технології” (далі – Висновок) на основі ряду важливих документів Ради Європи: Конвенції про захист приватних осіб у відношенні до автоматизованої обробки даних особистого характеру (1981 р.), Доповіді “Європейські судові системи” (2010 р.) Європейської комісії з ефективності правосуддя; а також міжнародних юридичних документів: Європейської Стратегії Правосуддя Європейського Союзу [5], Директиви 95/46/ЄС Європейського Парламенту і Ради про захист осіб у зв’язку з обробкою персональних даних і вільного обігу таких даних*.

---

* ***Від. ред.*** На початку 2016 р. Європейський Парламент і Рада прийняли рішення про скасування Директиви 95/46/ЄС Європейського Парламенту і Ради від 24.10.95 р. та введення в дію нових правил і порядку захисту персональних даних (“Пакет захисту даних”). Його безпосереднє застосування передбачено з 25 травня 2018 року для держав-членів ЄС, а також для країн, які мають зв’язки з ЄС. До вказаного терміну національні законодавства повинні бути приведені в повну відповідність до положень нових правил (див. // Інформація і право. – № 3(18)/2016. – С. 45-57]).

КРЄС однозначно визначає сучасні інформаційно-комунікаційні технології як засіб покращення здійснення судочинства, наділений наступними якостями:

- здатні полегшити доступ до правосуддя;
- можуть покращити процес розгляду та руху справ;
- підвищити рівень судочинства [5].

Водночас підкреслюється, що інформаційно-комунікаційні технології розглядаються як інструмент покращення адміністрування судочинства і не можуть повністю витіснити людський фактор. Судочинство не є суто технічним процесом, адже конкретні види процесуальної діяльності, поряд з іншим, ґрунтуються на правосвідомості судді, що чітко визначено законодавцем. Так, принцип верховенства права, яким суд керується при розгляді цивільної справи згідно статті 10 Цивільного процесуального кодексу (далі – ЦПК) України, надає суду право дійти висновку про те, що закон або ж інший правовий акт суперечить Конституції України. В цьому випадку одночасно виникає обов’язок суду як учасника цивільних процесуальних правовідносин не застосовувати такий закон чи інший правовий акт, а застосовувати норми Конституції України як норми прямої дії. На підставі ч. 6 ст. 10 ЦПК України суд після ухвалення рішення у такій справі зобов’язаний звернутися до Верховного Суду для вирішення питання стосовно внесення до Конституційного Суду України подання щодо конституційності закону чи іншого правового акта, вирішення питання про конституційність якого належить до юрисдикції Конституційного Суду України. Також згідно ч. 1 ст. 89 ЦПК України суд оцінює докази у справі за своїм внутрішнім переконанням, яке ґрунтується на всебічному, повному, об’єктивному та безпосередньому дослідженні наявних у справі доказів [6]. Важливе значення людський фактор має в оцінці поведінки сторін та їх свідків в судовому засіданні, що і становить складову роботи судді.

На підтвердження даної позиції в п. 6 Висновку КРЄС надано рекомендація, що судочинство обов’язково має включати людський фактор, оскільки стосується реальних людей та вирішення їхніх спорів [5]. Тому, на даному етапі правового регулювання цивільних процесуальних правовідносин, про перетворення суду в традиційному розумінні як особливого державного органу, створеного у визначеному законом порядку для здійснення правосуддя на засадах верховенства права, на новий “електронний суд” говорити не доводиться. Законодавство України в сфері регулювання організації судоустрою та судочинства термін “електронний суд” жодним чином не регулює. На нашу думку, це не досить виправдано, оскільки такий термін наразі присутній, але охоплює дещо інше розуміння. Зокрема, на офіційній сторінці Державної судової адміністрації України “Судова влада України” в розділі “Реєстри та системи” є сторінка під назвою “Електронний суд”, що передбачає: сплату судового збору он-лайн, інформацію щодо стадій розгляду судових справ, єдиний державний реєстр судових рішень, оприлюднення відомостей у справах про банкрутство, надсилання процесуальних документів електронною поштою учасникам судового процесу, надсилання судової повістки у вигляді SMS-повідомлень [11]. Тобто, мова йде про обмін інформацією в електронній формі між судовими установами, учасниками судового процесу, а також іншими державними структурами. Це, звичайно, є позитивним моментом в організації судоустрою, але виникає логічне запитання, чи можна все це називати даним терміном. На основі викладеного дослідження можемо зробити висновок, що термін “електронний суд” на сьогодні є невизначеним, а тому використовується довільно без насичення відповідним сутнісним змістом.

У Висновку КРЄС є пропозиція щодо запровадження терміну “електронний документообіг”, який означає застосовування сучасних інформаційно-комунікаційних

технологій для розширення можливостей учасників судочинства. Згідно пункту 23 Висновку учасники справи, зокрема, мають змогу ініціювати процес в електронному вигляді, мають можливість прослідкувати за стадіями розгляду справи шляхом отримання доступу електронної версії історії руху справи [5].

Для порівняння цікавим є міжнародний досвід імплементації даної рекомендації. Так, стаття 334 Цивільного процесуального кодексу Естонії встановлює правило, що різноманітні заяви, клопотання, заперечення і скарги надаються до суду в розбірливій формі машинопису або надрукованими на комп’ютері у форматі А-4. А також ще додатково, але із застереженням “по можливості”, учасники процесу надають до суду письмові процесуальні документи ще і в електронний спосіб [8]. Тобто, вся відповідальність за зміст документів в електронній формі покладається на самих учасників процесу. Окремо стаття 336 Цивільного процесуального кодексу Естонії детально визначає порядок подання до суду документів в електронний спосіб. Зокрема зазначається, що таке подання документів виконується за умови, що у суду є можливість дані документи роздрукувати та зняти з них копії. Такий документ повинен мати електронно-цифровий підпис відправника або ж передаватися ним аналогічним безпечним способом, який дає можливість встановити відправника. Однозначним підтвердженням відправника визнається посвідчення автентичності, утворене за допомогою персонального ключа відправника.

Щодо національного законодавства, то ч. 2 ст. 175 ЦПК України передбачає виключно письмову форму позовної заяви, яка має бути підписана позивачем чи його представником, або ж іншою особою, якій законом надано право звертатися до суду в інтересах іншої особи (органи державної влади, органи місцевого самоврядування, фізичні та юридичні особи, Уповноважений Верховної Ради України з прав людини, прокурор). Відзив на позовну заяву, який подає відповідач у строк, встановлений судом в ухвалі про відкриття провадження у справі, також подається у письмовій формі за підписом відповідача або ж його представника. На основі аналізу положень ЦПК України можемо констатувати, що на даному етапі всі заяви з процесуальних питань в судочинстві подаються виключно в письмовій формі, але в традиційний спосіб. Подання процесуальних документів в цивільному судочинстві України в електронний спосіб наразі є неможливим, оскільки ще існує певний перехідний період, пов'язаний із запровадженням прогресивних нововведень. В першу чергу маємо на увазі ту обставину, що на даному етапі ще не функціонує Єдина судова інформаційно-телекомунікаційна система, одним із завдань якої є забезпечення судам та учасникам процесу можливості надсилання та отримання документів в електронній формі.

В Естонії згідно ст. 56 Цивільного процесуального кодексу в кожній цивільній справі суд веде досьє, в якому в хронологічному порядку збираються процесуальні документи по всіх стадіях процесу та інші, пов'язані зі справою, процесуальні документи, а також предмети, пов’язані з провадженням у справі. Зазначене досьє представляє собою сукупність письмових документів. Водночас ст. 57 допускає ведення досьє повністю або частково в цифровій формі, в якому документи на папері скануються та заносяться у відповідне провадження в інформаційній системі судів. Інформаційна система судів автоматично записує час запису документа в системі і відомості про особу, яка зробила запис. Документи, записані в інформаційній системі судів, замінюють документи, представлені на паперовому носії. Ст. 60^1 передбачена інформаційна система розгляду електронного досьє (або система електронного досьє) – це база даних, яка належить до державної інформаційної системи та ведеться з метою оброблення процесуальних та особистих відомостей в цивільному провадженні.

Інформаційна система розгляду електронного досьє забезпечує моніторинг цивільних справ, які перебувають у провадженні, відображає відомості щодо вчинених процесуальних дій, забезпечує збір необхідної судової статистики, надає можливість передавати відомості та документи в електронний спосіб [8].

В судах України наразі запроваджується вже згадувана Єдина судова інформаційно-телекомунікаційна система (далі – ЄСІТС), на яку покладається ряд функцій, в тому числі реєстрація в день надходження позовних та інших заяв, скарг та інших передбачених законом процесуальних документів, що подаються до суду і можуть бути предметом судового розгляду, а також забезпечення обміну документами (надсилання та отримання документів) в електронній формі між судами, між судом та учасниками судового процесу, між учасниками судового процесу [6]. На нашу думку, з початком функціонування ЄСІТС відбудеться вдосконалення судочинства, оскільки суд матиме змогу направляти судові рішення, судові повістки про виклик до суду, судові повістки-повідомлення, інші процесуальні документи учасникам судового процесу на їхні офіційні електронні адреси, а також вчиняти інші процесуальні дії в електронній формі із застосуванням ЄСІТС. Позитивним моментом є та обставина, що закон зобов’язує адвокатів, нотаріусів, приватних виконавців, арбітражних керуючих, судових експертів, державні органи, органи місцевого самоврядування та суб’єктів господарювання державного та комунального секторів економіки реєструвати офіційні електронні адреси в ЄСІТС в обов’язковому порядку. Але для всіх інших осіб реєстрація офіційних електронних адрес в ЄСІТС здійснюється в добровільному порядку.

Всім особам, які виконали зазначену реєстрацію, суд матиме змогу та, одночасно, зобов’язання надсилати будь-які документи у справах, в яких такі особи беруть участь, виключно в електронній формі шляхом їх направлення на офіційні електронні адреси таких осіб, що не позбавляє їх права отримати копію судового рішення у паперовій формі за окремою заявою.

Але на даному етапі виникають певні ускладнення, пов’язані з категорією “офіційна електронна адреса”. У Верховній раді України 26 грудня 2017 року зареєстровано проект Закону № 7443 про внесення змін до Закону України “Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань” щодо присвоєння офіційної електронної адреси під час державної реєстрації [14]. Пропонується визначення офіційної електронної адреси як адреси електронної пошти юридичної особи та фізичної особи-підприємця, що використовується для офіційного листування в електронному вигляді. Властивістю офіційної електронної адреси є те, що вона залишається незмінною до внесення запису про державну реєстрацію припинення юридичної особи, припинення підприємницької діяльності фізичної особи. Всі листи, повідомлення, які надсилаються на офіційну електронну адресу, вважаються такими, що надіслані офіційно, та не потребують додаткового документального підтвердження. На основі запропонованого розуміння можемо зробити висновок, що офіційну електронну адресу пропонується присвоювати “автоматично” під час державної реєстрації створення юридичної особи або ж реєстрації статусу фізичної особи-підприємця. Що ж до фізичних осіб та порядку реєстрації їх офіційних електронних адрес, то ця проблема потребує негайного вирішення на законодавчому рівні. Проаналізувавши зазначений проект Закону та норми ЦПК України можемо лише припустити, що все це буде відбуватися в добровільному порядку. Враховуючи тенденції розвитку інформаційного суспільства, сміливо можемо стверджувати, що для людей молодого віку такий порядок реєстрації та можливостей використання офіційної електронної адреси є цілком прийнятним. Для основної частини

людей більш старшого віку, можливо, виникатимуть додаткові ускладнення, пов’язані з необхідністю офіційно зареєструвати свою електронну адресу.

Цікавим нововведення є положення частини ч. 9 ст. 14 ЦПК України про те, що суд проводить розгляд справи за матеріалами судової справи в електронній формі. Всі докази та документи по справі протягом трьох днів від дня надходження до суду мають бути переведені з паперової в електронну форму та долучені до матеріалів електронної судової справи. І тут виникають деякі питання. По-перше, чи не буде таке переведення матеріалів справи в електронну форму додатковим засобом затягування розгляду справи, адже пояснення “не можна виконати через технічні проблеми” для кожного знайоме. В умовах сучасного судочинства, де кожний день зволікань закономірно призводить до вже згадуваного перевантаження суду поточними справами, ситуація, коли не працює “база” або ж “система”, чи взагалі не має доступу до мережі Інтернет, є неприпустимою. По-друге, які працівники апарату суду безпосередньо будуть виконувати таке переведення документів та доказів з паперової в електронну форму? Слідуючи популярному вислову про те, що кожний має займатися своєю справою, вважаємо за необхідне наголосити, що, для уникнення зазначених ускладнень, це мають бути саме фахівці в сфері інформаційних технологій. Всі ці важливі нюанси слід врахувати в Положенні про Єдину судову інформаційно-телекомунікаційну систему, яке згідно ч. 13 ст. 14 ЦПК України має бути затверджене Вищою радою правосуддя за поданням Державної судової адміністрації України та після консультацій з Радою суддів України. На нашу думку є недоліком та обставина, що законодавцем не визначено дату, коли це має бути здійснено. Єдине що, згідно п. 15 Перехідних Положень ЦПК України, Єдина судова інформаційно-телекомунікаційна система починає функціонувати через 90 днів з дня опублікування Державною судовою адміністрацію України у газеті “Голос України” та на веб-порталі судової влади оголошення про створення та забезпечення функціонування Єдиної судової інформаційно-телекомунікаційної системи [6]. До цього моменту розгляд справи здійснюється за матеріалами справи у паперовій формі.

Дедалі більшого поширення набуває інший термін – “електронний позов”. Для вичерпності розуміння хочемо наголосити, що положеннями ЦПК України на даному етапі сутність такого терміну не визначається. Для початку вважаємо за необхідне звернути увагу, що наука Цивільного процесуального права розрізняє категорії “позов” та “позовна заява”. Позов є процесуальним засобом захисту прав, свобод та інтересів особи у цивільному судочинстві. Науковцями позов визначається як звернена через суд матеріально-правова вимога позивача до відповідача щодо захисту порушеного, оспорюваного чи невизнаного права або охоронюваного законом інтересу, яка розглядається у визначеному законом процесуальному порядку [9, с. 108]. Тобто, позов – це певна вимога щодо права. А тому позов не може розглядатися як електронний чи будь-який інший. На сучасному етапі можемо спостерігати, що категорія “електронний позов” вживається саме для позначення позовної заяви, поданої до суду в електронній формі, що не відповідає сутнісному змісту даного поняття.

Поняття позову та позовної заяви слід розмежовувати, оскільки ч. 1 ст. 184 ЦПК України визначає, що позов пред’являється шляхом подання позовної заяви до суду першої інстанції. Частина 1 статті 175 ЦП України визначає, що позовна заява до суду подається в письмовій формі. Причому на даний час сам термін “письмова форма” законодавцем не конкретизується, на підставі чого можемо зробити висновок, що позовна заява може бути як надрукованою, так і написаною власноруч. Подати до суду позовну заяву в електронній формі в Україні на сьогодні неможливо, оскільки, як вже зазначалося, ще не працює ЄСІТС. Із запровадженням ЄСІТС подати позовну заяву та інші

процесуальні документи матимуть можливість виключно особи, які зареєстрували власні офіційні електронні адреси в ЄСІТС та мають власний електронний цифровий підпис, який прирівнюється до власноручного підпису відповідно до Закону України “Про електронний цифровий підпис” [15].

Для порівняння: в Естонії учасники процесу подають ще додатково до друкованої позовної заяви також і її текст в електронній формі, якщо тільки у них є така можливість. Згідно ст. 336 Цивільного процесуального кодексу Естонії позовна заява в електронній формі повинна мати електронно-цифровий підпис відправника або передаватися іншим аналогічним безпечним способом, що дозволяє встановити відправника. Беззаперечним підтвердженням відправника є посвідчення автентичності, утворене за допомогою персонального ключа відправника, яке додається до такої позовної заяви [8].

Враховуючи зазначене, можемо констатувати, що наразі питання форми позовної заяви в судочинстві нашої держави є визначеним недостатньо, омкільки повністю не відображені можливості сучасних інформаційних технологій. В свою чергу, на нашу думку, така недостатня визначеність даного процесуального поняття спровокувала появу терміну “електронний позов”, який, на нашу думку, застосовується, не відображаючи суті явища. Не претендуючи на вичерпність розуміння, вважаємо доцільніше оперувати терміном “електронна позовна заява”.

Таким чином, можемо зазначити, що використання сучасних інформаційних технологій забезпечить посилення ролі судової системи в дотриманні верховенства права. Водночас характеризуватиме рівень економічного розвитку держави, адже ситуація, коли “зависла” система, щодо сфери правосуддя є неприпустимою. Проаналізувавши міжнародні стандарти в сфері правосуддя щодо впровадження інформаційних технологій в судах, Консультативна рада європейських суддів у Висновку рекомендує в процесі реформування сфери правосуддя зважати на потреби тих осіб, які не мають змоги використовувати засоби сучасних інформаційних технологій [5]. Зважаючи на стрімкий розвиток технічного процесу, можемо сміливо припустити, що кількість таких осіб з кожним днем зменшується. Тому визначена тема потребує додаткового детального наукового обговорення, аналізу та розвитку.

Висновки.

Підсумовуючи викладене, можемо визначити наступне:

1. Особливою рисою розвитку інформаційного права та інформаційних правовідносин зокрема є дуже швидкий розвиток та повна інтеграція у всі сфери життєдіяльності суспільства. Сфера цивільного судочинства не може залишатися “поза інформаційною”, а тому нововведення судової реформи, які є, безумовно, позитивними, мають своєчасно втілюватися в практичну діяльність, без додаткових зволікань, викликаних тим, що питання є не достатньо врегульованим на законодавчому рівні.

2. Інформаційне право наділене такою особливою рисою, як універсальність. Наукові категорії, розроблені в межах інформаційного права, дедалі частіше використовуються іншими галузями знань, що свідчить про його позиціонування у всіх сферах наукових досліджень. В цьому аспекті виникає нагальна потреба у чіткому визначенні основоположних понять, якими оперують дослідники. Щодо цивільного судочинства, то взаємодія галузей інформаційного права та цивільного процесуального права спровокувала виникнення таких категорій, як “електронний суд”, “електронний позов”, “електронні докази”, “електронний документообіг”, “розгляд справи за матеріалами судової справи в електронній формі”, “реєстрація офіційної електронної адреси”, “електронна форма копії технічного запису судового засідання”.

3. Цивільне судочинство не слід розглядати як суто технічний процес, адже визначені законом певні види процесуальної діяльності, поряд з іншим, ґрунтуються на правосвідомості судді, що чітко визначено законодавцем. Зокрема право суду дійти висновку про те, що закон або ж інший правовий акт, який застосовується при вирішенні справи, суперечить Конституції України. В цьому випадку одночасно виникає обов’язок суду як учасника цивільних процесуальних правовідносин не застосовувати такий закон чи інший правовий акт, а застосовувати норми Конституції України як норми прямої дії. Також при розгляді справи суд оцінює докази за своїм внутрішнім переконанням, яке ґрунтується на всебічному, повному, об’єктивному та безпосередньому дослідженні наявних у справі доказів. Вагоме значення людський фактор має в оцінці поведінки сторін та їх свідків в судовому засіданні, що і становить складову роботи судді.

4. Однією із засад судочинства є відкритість інформації для кожного щодо своєї справи. Повна інформація щодо суду, який розглядає дану справу, учасників справи, предмета позову, дати надходження позовної заяви, іншої заяви, скарги, клопотання у справі, вжитих заходів з забезпечення позову, забезпечення доказів, стадії розгляду справи, місця, дати і часу судового засідання, руху справи з одного суду до іншого є відкритою та оприлюднюється на офіційному веб-порталі судової влади України у порядку, визначеному законом. Тому питання наукового обґрунтування категорій, які застосовуються з цією метою, є наразі актуальним.

5. Законодавство України в сфері регулювання організації судоустрою та судочинства термін “електронний суд” жодним чином не регулює, що призвело до насичення даного терміну довільним змістом. Найчастіше терміном “електронний суд” називають обмін інформацією в електронній формі між судовими установами, учасниками судового процесу, а також іншими державними структурами. На нашу думку, в такому розумінні доцільно застосовувати термін “електронний документообіг”, що і зроблено у свій час у Висновку КРЄС. Зважаючи на ті положення, які відображає проект “Електронний суд” на офіційному сайті “Судова влада України”, запропонований термін “електронний документообіг”, на нашу думку, більш точно відображає процеси, що відбуваються.

6. Термін “електронний позов” також виходить за межі правового регулювання. Цивільне процесуальне законодавство, чітко розмежовуючи поняття позову та позовної заяви, визначає, що позов пред’являється шляхом подання позовної заяви до суду першої інстанції. Не претендуючи на вичерпність розуміння, вважаємо більш доцільним оперувати терміном “електронна позовна заява”.

7. Цивільне процесуальне законодавство України зазнало прогресивних змін щодо впровадження в організацію судоустрою інформаційно-комунікаційних технологій. Але фактичне виконання таких змін виходить за межі цивільних процесуальних правовідносин і залежить також від загальної інформатизації держави. Адже чи буде працювати Єдина судова інформаційно-телекомунікаційна система, якщо державні органи будуть “заощаджувати” на її впровадженні? Чи зможе фізична особа сповна використати всі переваги ЄСІТС, якщо вона не зареєструє свою офіційну електронну адресу та не оформить електронний цифровий підпис? Питання, швидше, риторичні. Тому можемо зробити однозначний висновок, що цивільне законодавство України на даному етапі розвитку інформаційних відносин потребує вдосконалення з врахуванням потреб сьогодення.

Використана література

1. Баранов О.А. Правові проблеми “електронної демократії” // Інформація і право. – № 1(20)/2017. – С. 28-38.

2. Брижко В.М., Фурашев В.М. Конвергенція новітніх технологій : стан і перспективи змін у інформаційних відносинах // Інформація і право. – № 1(20)/2017. – С. 51-67.

3. Кушакова-Костицька Н.В. Електронне правосуддя : українські реалії та зарубіжний досвід // Юридичний часопис Національної академії внутрішніх справ. – 2013. – № 1. – С. 103-109.

4. Аналітичні таблиці щодо стану здійснення правосуддя за І півріччя 2017 року : Надходження справ і матеріалів до місцевих загальних судів. – (Судова влада України)]. – Режим доступу : http://court.gov.ua/inshe/sudova_statystyka/I_pivricha_2017

5. Висновок № 14 (2011) Консультативної ради європейських суддів “Судочинство та інформаційні технології” : міжнародний стандарт судочинства, прийнятий КРЄС на 12-ому пленарному засіданні (Страсбург, 7 – 9 листопада 2011 року). – (Судова влада України). – Режим доступу : http://court.gov.ua/inshe/mss

6. Цивільний процесуальний кодекс України : Закон України від 18.03.04 р. № 1618-IV // Відомості Верховної Ради України (ВВР). – 2004. – № 40 – 41, 42. – С. 492.

7. Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України : Закон України від 03.10.17 р. № 2147-VIII // Відомості Верховної Ради України (ВВР). – 2017. – № 48. – Ст. 436.

8. Гражданский процессуальный кодекс Эстонии. – Режим доступу : http://infosila.ee/main/1398-zakonodatelstvo-estonii-na-russkom-yazyke.html

9. Логінов О.А. Цивільний процес України : навч. посібник / О.А. Логінов, О.О. Штефан. – К. : Юрінком Інтер. – 2012. – С. 368.

10. Про реалізацію проекту щодо надсилання судами SMS-повідомлень учасникам судового процесу (кримінального провадження) у місцевих та апеляційних загальних судах : Наказ Державної судової адміністрації України від 20.11.13 р. № 119. – Режим доступу : http://court.gov. ua/smsec

11. Судова влада України. – Режим доступу : http://court.gov.ua/reyestri-ta-sistemi/ecourt

12. Правове регулювання суспільних відносин в умовах демократизації Української держави : матеріали VII міжнародної науково-практичної конференції, (м. Київ, 18 – 19 травня 2017 р.,) ; уклад. О.О. Кравчук, Т.О. Чепульченко, В.Ю. Пряміцин. – К. : ТОВ НВП “Інтерсервіс”, 2017. – 296 с.

13. Теоретико-правові основи формування та розвитку інформаційного суспільства : матеріали науково-практичної конференції, (м. Київ, 29 листопада 2017 р. ; упоряд. В.М. Фурашев, С.Ю. Петряєв. – К. : Вид-во “Політехніка”, 2017. – 266 с.

14. Про внесення змін до Закону України “Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань” щодо присвоєння офіційної електронної адреси під час державної реєстрації : проект Закону від 26.12.17 р. № 7443. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=63226

15. Про електронний цифровий підпис : Закон України від 22.05.03 р. № 852-IV // Відомості Верховної Ради України (ВВР). – 2003. – № 36. – Ст. 276.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

До відома читачів

НОВЕ НАУКОВЕ ВИДАННЯ

Становлення і розвиток правових основ та системи захисту персональних даних в Україні : монографія / [В.Г. Пилипчук, В.М. Брижко, О.А. Баранов, К.С. Мельник] ; за ред. В.М. Брижка, В.Г. Пилипчука. – К. : ТОВ “Видавничий дім “АртЕк”, 2017. – 226 с.

У науковому виданні на основі історичного та системного аналізу розглядаються актуальні проблеми формування і розвитку правових основ та системи захисту персональних даних в контексті євроінтеграції України. Висвітлюється стан наукової розробки, історико-правові аспекти формування інституту захисту персональних даних, відповідний досвід країн-членів Ради Європи та Європейського Союзу, організаційно-правові проблеми захисту персональних даних та розвитку системи захисту персональних даних в Україні. У додатках наводяться тексти проектів та чинних правових актів у цій сфері.

Видання розраховане на фахівців, експертів і вчених, представників державних і недержавних організацій та усіх, хто цікавиться проблемами захисту персональних даних.

Якщо Вас, шановні читачі, зацікавило видання, звертайтеся за адресою:

01032, м. Київ, вул. Саксаганського, 110-В. Науково-дослідний інститут інформатики і права Національної академії правових наук України. Тел.: 234-94-56

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

ПЕРЕЛІК СТАТЕЙ,

опублікованих у журналі “Інформація і право” у 2017 р.

№ з/п	Назва статті	Автор(и)	№ жур., стор.
Інформаційне право			
1	Інформаційна сфера як соціально-правове явище: проблеми наукової ідентифікації та регулювання	Яременко О.І.	1(20)/2017, с. 5-13
2	Комунікація влади і суспільства в умовах децентралізації	Корж І.Ф.	1(20)/2017, с. 14-27
3	Правові проблеми “електронної демократії”	Баранов О.А.	1(20)/2017, с. 28-38
4	Обробка та захист персональних даних в процесі верифікації соціальних виплат громадян	Мельник К.С.	1(20)/2017, с. 45-53
5	Від менеджменту документальних потоків до менеджменту державних комунікацій: роль документознавця в сучасних органах державної влади	Дубова С.В.	1(20)/2017, с. 45-50
6	Герменевтичний метод у сучасних цивілістичних дослідженнях: до питання про доцільність застосування	Дзьобань О.П., Яроцький В.Л.	2(21)/2017, с. 5-12
7	Вдосконалення законодавства України щодо комерційної таємниці суб’єктів господарювання	Кравченко О.М.	2(21)/2017, с. 5-12
8	Система основних термінів, як основа вдосконалення законодавства у сфері правового регулювання інформаційної взаємодії у місцевому самоврядуванні	Дубняк М.В.	2(21)/2017, с. 20-33
9	Теоретичні засади правового регулювання державної статистики в Україні	Николаєнко Г.В.	2(21)/2017, с. 34-40
10	Реформування і розвиток системи захисту персональних даних в Україні	Пилипчук В.Г., Брижко В.М.	3(22)/2017, с. 5-21
11	Об’єкт і предмет наукового дослідження в інформаційній сфері	Корж І.Ф.	3(22)/2017, с. 22-29
12	Сучасне праворозуміння відносин в інформаційній сфері та методологія їх систематизації	Яременко О.І.	3(22)/2017, с. 30-41
13	Отримання публічної інформації в Україні: теорія і практика	Беланюк М.В.	3(22)/2017, с. 42-50
14	Визначення поняття персональних даних як правової категорії: сучасні проблеми та шляхи вирішення	Дяковський О.С.	3(22)/2017, с. 51-56
15	Захист персональних даних: вітчизняний та зарубіжний досвід	Крилова Ю.І.	3(22)/2017, с. 57-63
16	Інформаційний продукт як об’єкт права власності	Брижко В.М.	4(23)/2017, с. 5-15
17	Електронна демократія і цифрова диктатура	Золотар О.О.	4(23)/2017, с. 16-25
Правова інформатика			
18	Конвергенція новітніх технологій: стан і перспективи змін у інформаційних відносинах	Брижко В.М., Фурашев В.М.	1(20)/2017, с. 51-67
19	Напрями розвитку системи “електронного парламенту” в Україні	Дорогих С.О.	1(20)/2017, с. 68-74
20	Інтернет речей (IoT): правові моделі використання обмеженного радіочастотного ресурсу (Частина І)	Баранов О.А.	2(21)/2017, с. 41-50

21	Використання сучасних технологій розподіленої обробки даних: право та функції держави	Доронін І.М.	2(21)/2017, с. 51-58
22	Відкриті дані та інші дані у публічному доступі: правові аспекти	Тарасюк А.В.	2(21)/2017, с. 59-65
23	Термінологічна мережева модель як відображення процесів денцентралізації влади в Україні	Ланде Д.В., Фурашев В.Н.	2(21)/2017, с. 66-71
24	Модель Національної системи правової інформації в Україні	Дорогих С.О.	2(21)/2017, с. 72-76
25	Міжнародно-правовий режим сучасних електронних комунікації: загальні засади	Забара І.М.	3(22)/2017, с. 64-72
26	Інтернет речей (IoT): правові моделі використання обмеженого радіочастотного ресурсу (Частина ІІ)	Баранов О.А.	3(22)/2017, с. 73-84
27	Криптовалюти: соціально-економічні фактори, право та функції держави	Доронін І.М.	3(22)/2017, с. 85-93
28	Інтернет речей (IoT): правові проблеми застосування розумних контактів	Баранов О.А.	4(23)/2017, с. 26-40
29	Розвиток емерджентних (новітніх) технологій та регулювання у цій сфері як реалізація функцій держави	Доронін І.М.	4(23)/2017, с. 41-48
30	Інтернет-технології:оцінка пріоритетності маніпулювання свідомістю за допомогою методів ранжування	Качинська К.А., Варичева Д.І., Свириденко С.В.	4(23)/2017, с. 49-62
Інформаційна і національна безпека			
31	Інформаційна безпека в контексті інформаційної культури	Дзьобань О.П., Мануйлов Є.М.	1(20)/2017, с. 74-81
32	Давньоіндійський трактат “Артхашастра” в контексті забезпечення інформаційної безпеки та протидії негативним інформаційно-психологічним впливам	Вронська Т.В., Беланюк М.В.	1(20)/2017, с. 82-91
339	Інформаційна грамотність та цифрова нерівність: убезпечення дитини в сучасному інформаційному просторі	Радзієвська О.Г.	1(20)/2017, с. 92-103
34	Правове регулювання забезпечення кібербезпеки у реалізації окремих функцій держави	Доронін І.М.	1(20)/2017, с. 104-111
35	Забезпечення охорони державної таємниці у сфері оперативно-розшукової діяльності за законодавством окремих держав: порівняний аналіз	Ковальов К.Є., Леонов Б.Д.	1(20)/2017, с. 112-122
36	Еволюція наукових поглядів на забезпечення діяльності з охорони державної таємниці	Семенюк О.Г.	1(20)/2017, с. 123-131
37	Взаємозв’язок корупції та екстремізму: проблеми протидії	Скулиш Є.Д., Ірха Ю.Б.	2(21)/2017, с. 77-87
38	Правові засади та пріоритети розвитку протидії негативним інформаційним впливам на дітей	Радзієвська О.Г.	2(21)/2017, с. 88-98
39	Вдосконалення чинного законодавства з питань протидії кіберзлочинності та забезпечення кібербезпеки	Гуцалюк М.В.	2(21)/2017, с. 99-107
40	Окремі проблеми криміналістичного забезпечення розслідування злочинів, пов’язаних з неправомірним дистанційним доступом до комп’ютерної інформації	Серьогін В.С., Леонов Б.Д.	2(21)/2017, с. 108-115
41	Комплексний підхід як методологічна основа дослідження проблем забезпечення охорони державної таємниці	Семенюк О.Г.	2(21)/2017, с. 116-123
42	Допуск до державної таємниці як різновид діяльності держави з надання адміністративних послуг	Семенюк О.Г.	3(22)/2017, с. 94-100

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

До відома авторів

“**ІНФОРМАЦІЯ І ПРАВО**” – спеціалізований науковий фаховий журнал по результатах фундаментальних і прикладних наукових досліджень, а також дисертаційних робіт на здобуття наукових ступенів доктора і кандидата юридичних наук з проблем права та інформаційного законодавства, правової інформатики, інформаційних технологій, інформатизації, інформаційної і національної безпеки та інформаційних ресурсів в інших галузях права в умовах становлення інформаційного суспільства.

Зміст матеріалів статей має описувати та пояснювати наукове вирішення визначених автором завдань згідно з такими основними напрямами досліджень, як:

інформаційне право; правова інформатика, інформаційна і національна безпека.

Вимоги до оформлення

1) **Статтю слід подавати українською мовою, виготовлену у друкарський спосіб, та її електронну версію** (структура та зміст якої повністю відповідають друкованому варіанту) у вигляді файлу:
   – *у редакторі Word, шрифт – Times New Roman, з розширенням .doc, кегль – 13;*
   – *параметри сторінки – формат А-4, розташування тексту (таблиці, діаграми тощо) книжне, береги поля (верхній, нижній, лівий і правий краї) – 20 мм;*
   – *відстань між рядками – 1 інтервал;*
   – *кількість матеріалу однієї статті – не більше 15 стор.*

   Стаття має передбачати такі обов’язкові структурні елементи:
   - УДК.
   - Ім’я та прізвище, науковий ступінь, вчене звання автора, місце роботи.
   - Назва статті.
   - Анотація та ключові слова – укр., англ., рос. мовами.
   - **Розв’язання проблеми,** шляхом наукового вирішення завдання:
     - **постановка проблеми** *(загальна характеристика)* та **результати аналізу наукових публікацій** *(досліджень),* в яких започатковано розв’язання проблеми, виділення не вирішених її частин, котрим присвячується стаття;
     - **формування мети** *(постановка завдання)* статті;
     - **виклад основного матеріалу** – опис вирішення завдання та обґрунтування наукової цінності та практичного значення визначених у статті результатів.
   - **Висновки** за результатами розв’язання проблеми та вирішення завдання, які визначають наукову новизну роботи. Можуть супроводжуватися пропозиціями, оцінками, гіпотезами, описаними у статті, а також визначенням перспектив подальших досліджень.
   - **Використана література** *(згідно з наказом ВАК України від 26.01.08 р. № 63).*
   - Підпис, адреса (е-адреса), телефон автора.

2) **Подавати письмовий Відгук на статтю, підписаний особою, яка має науковий ступінь.**
   Відгук має бути чітко структурований та обґрунтований згідно з такими частинами:
   - ***Актуальність теми.***
   - ***Новизна та обґрунтованість одержаних наукових результатів.***
   - ***Наукова (практична) цінність результатів.***
   - ***Заключення про можливість відкритої публікації.***

3) Рукопис статті та Відгук мають бути ретельно вичитаними, виправленими і підписаними відповідними особами.

4) Окремим файлом автори подають електронну версію **розширеної анотації статті** (до 1 сторінки формату А-4) **англійською мовою,** яка буде розміщена на веб-сторінці журналу, відповідно до наказу Монмолодьспорту України “Про затвердження порядку формування переліку наукових фахових видань України” від 17.10.12 р. № 1111.

5) За надання послуг щодо розгляду, форматування, корегування, тиражування та ін. робіт, пов’язаних з публікацією статей та виданням журналу, **пропонується здійснити оплату в розмірі 280 грн. на рахунок Інституту**.

Реквізити для оплати робіт:

Науково-дослідний інститут інформатики і права Національної академії правових наук України. Р/р 31251259111870 в Державній казначейській службі України МФО: 820172, ЄДРПОУ: 25959933 (з приміткою – за науковий журнал).

Адреса редакції: 01032, м. Київ, вул. Саксаганського, 110-В.

Копію квитанції прохання направити на е-адресу: bvm777@ukr.net

Д о у в а г и

- Редакційна колегія не завжди поділяє погляди авторів публікацій.
  Статті видаються в авторській редакції.
  Автори несуть відповідальність за достовірність інформації, що міститься у статтях і повідомленнях до журналу, а також за додержання авторських прав відповідно до законодавства.
- Редакційна колегія залишає за собою право на:
  – відхилення матеріалів статей, які не відповідають тематиці журналу, або таких, які виконані з порушенням зазначених вимог до оформлення статей та Відгуків;
  – внесення до статті змін редакційного змісту у зв’язку зі скороченням обсягу матеріалу.

* * * * * * * * * * *

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 1(24)

2018

Засновники журналу:	- Науково-дослідний інститут інформатики і права Національної академії правових наук України; - Національна бібліотека України ім. В.І. Вернадського Національної академії наук України; - Відкритий міжнародний університет розвитку людини “Україна”.
Видавець:	© Науково-дослідний інститут інформатики і права Національної академії правових наук України.
Адреса редакції:	01032, м. Київ, вул. Саксаганського, 110-В. НДІ інформатики і права НАПрН України. Тел.: 234-94-56, e-mail: bvm777@ ukr.net
Веб-сторінки журналу у мережі Інтернет:	//www.ippi.org.ua – НДІ інформатики і права НАПрН України; //www.nbuv.gov.ua – Нац. бібліотека України ім. В.І. Вернадського.