ІСТОРІЯ ДОСЛІДЖЕНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ОБ'ЄКТА ПРАВОВІДНОСИН

ЛИСЕНКО Сергій Олексійович – кандидат юридичних наук, доцент, доцент кафедри управління безпекою, правоохоронної та антикорупційної діяльності Міжрегіональної Академії управління персоналом

УДК 340:659.4.327.88(477)

Природно, що питання інформаційної безпеки людини почало формуватися не від владних органів, а в контексті боротьби за реалізацію інформаційних прав людини, зокрема свободи слова, таємниці приватного життя, прав нації на самовизначення, на національно-культурний розвиток тощо. Інформаційна безпека стала перетворюватись на унікальний міжгалузевий напрямок, який охоплює в собі ознаки приватного та публічного права, відрізняючи регулювання відносин між особами та суспільством окремо та відрізняючи відносини особи, суспільства із державою окремо.

Ключові слова: право, інформаційне право, інформаційна безпека

Naturally, information security man began to emerge not from government bodies and in the context of the struggle for the implementation of information rights, including freedom of speech, privacy, rights of nations to self-determination, national-cultural development and so on. Information security was becoming a unique interdisciplinary area that encompasses the features of private and public law. Featuring regulate relations between individuals and society separately, and distinguishing the relations of individuals, society with the state alone.

Постановка проблеми. Сучасні суспільні, економічні та політичні процеси в Україні обумовлюють відокремлення у них, як специфічного напрямку, правовідносин щодо інформаційної безпеки. Безпека інформаційної діяльності у країні постійно заслуговує на увагу, а отже, визнання її як важливого чинника життєдіяльності суб'єктів. Інформаційна діяльність окремих суб'єктів має великий вплив і на функціонування держави в цілому, а отже визначає і її роль у регулюванні, охороні та захисті різноманітних суспільно значимих правовідносин, окремих процесів у них. Це також визначає головні напрями державної політики та зміст діяльності держави, пов'язаної з управлінням окремих сфер у суспільстві. У зв'язку з цим інформаційну безпеку, як правову категорію, пропонується розглядати у контексті складової (елементу) національної безпеки.

Норма ч. 1 ст. 17 Конституції України [1] встановлює, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу». Таким чином, у правовідносинах в Україні інформаційна безпека розглядається на рівні з суверенітетом і територіальною цілісністю, а також з економічною безпекою. При цьому потрібно відмітити, що зазначені поняття у конституційній нормі, що розглядається, не є однорідними за предметом правовідносин. Це зумовило те, що вищезгадані конституційно-правові складові безпеки країни розвиваються у спеціальному законодавстві України за окремими напрямка-

ми регулюванням у різних історичних часових межах існування незалежності сучасної української держави.

Так, у Декларації про державний суверенітет України наголошено, що державний суверенітет України – це «верховенство, самостійність, повнота і неподільність влади Республіки в межах її території та незалежність і рівноправність у зовнішніх зносинах»[2]. З цього випливає думка, що зміст інформаційної безпеки як складової національної безпеки визначається з того, що її джерелом вважається не лише суверенітет держави, а й суверенітет народу та нації як суб'єктів інформаційних відносин.

Слід зазначити, що не так давно, за мірками людської історії, у дослідженнях правників, політологів, управлінців головним суб'єктом інформаційної безпеки вважалася держава. Більшість дослідників, у ретроспективі, притримувалась доктрини, що проблема гарантування, охорони, захисту, підтримки, збереження інформаційної безпеки держави з'явилася багато століть тому. При цьому домінувала концепція, що ключове поняття предмету інформаційної безпеки становить державна таємниця, що по різному простежується з найстаріших часів. Аргументами цього є згадки про перші методики шифрування повідомлень у військовій справі тощо. Вони датуються ще з 4 тисячоліттям до н.е. Наприклад, одним із ранніх підстановочних шифрів був Шифр Цезаря, в якому кожна літера в повідомленні замінювалась літерою через декілька позицій із абетки. Цей шифр отримав ім'я Юлія Цезаря, який його використовував, зі зсувом в 3 позиції, для спілкування з генералами під час військових кампаній [13, с. 35-40].

З точки зору суб'єктного складу правовідносин, важливо зазначити те, що сутність категорії «інформаційна безпека» у державі формувалася відповідно до інтересів керівних прошарків суспільства і ґрунтувалися на пов'язаному з їх волею розвитком норм позитивного права. Однак з плином історії змінювалося ставлення у суспільстві щодо розуміння сутності інформаційної безпеки, як загального, консолідованого об'єкта чи предмета правовідносин, у тому числі їх суб'єктного складу, що визначався змістом спеціальних прав і обов'язків, зобов'язань.

Аналіз останніх публікацій та досліджень. Серед сучасних науковців-правознавців, які займаються даною проблематикою в Україні, пропонується виділити дослідження наступних: Н.В. Банчук, Г.В. Виноградова, О.Д. Довгань, Р.А. Калюжний, І.Ф. Корж, Б.А. Кормич, О.В.Копан, А.І. Марущак, А.І. Мовчан, Е.І. Низенко, В.Г.Пилипчук, В.С. Цимбалюк та інші.

З точки зору безпекознавства спектр змісту категорії «інформаційна безпека» дослідниками визначається із змісту поняття «безпека» починаючи із розуміння її як стану, захищеності і закінчуючи – як суспільні відносини, вид правовідносин.

Але деякі питання історії правових досліджень інформаційної безпеки у суспільстві залишаються ще не розкритими як у складі адміністративного права, так й інформаційного права.

Парадигма сутності інформаційної безпеки пропонується у розумінні трьох її складових, як категорії правознавства: вид інформаційних правовідносин; відповідно – напрямок наукових досліджень у юридичних науках; навчальна дисципліна.

Для цілей дослідження зміст категорії «інформаційна безпека» пропонується розуміти, як умовно виділений вид суспільної діяльності пов'язаної з інформацією певних суб'єктів, що знаходить вираз у множині норм правил поведінки стосовно її гарантуванню, охорони, захисту, збереженню, підтриманню життєво важливих потреб, інтересів людини, громадянина, соціальних спільнот, суспільства, держави, міжнародного співтовариства.

Формулювання цілей статті. На основі системного прикладного аналізу нормативно-правових актів та навчальної і наукової літератури пропонуються на розгляд зацікавленої громадськості окремі результати наукових розвідок стосовно історії досліджень суспільного розуміння інформаційної безпеки в Україні, а також місце її в інформаційному праві, як комплексній галузі правознавства в національній структурі права.

Виклад основного матеріалу дослідження. Сучасне інформаційне право оперує в

суспільних відносинах, що виникають, здійснюються та припиняються у взаємодії через інформацію. За сутністю право в цілому головним своїм компонентом має функцію забезпечення, а саме: дотримання бажаних у суспільстві норм правил поведінки суб'єктів і недопущення відхилень, що визначає зміст правопорядку.

Для подальшого висвітлення окремих результатів теми дослідження зазначеної у назві цієї публікації, за основу розуміння змісту сучасного інформаційного права пропонується взяти думку Г.В. Виноградової, яка вважає, що термін «інформаційне право» слід розглядати як галузь права, що встановлює систему спеціальних правових норм, що реалізуються в інформаційній сфері, тобто у сфері збирання, зберігання, використання і поширення інформації. Вона зазначає також, що інформаційне право є комплексною галуззю права, що ґрунтується на методах публічного і приватного права [3, С.13-14].

Суттєвим історичним, віховим етапом в українському суспільстві на шляху створення єдиного погляду на інформаційні відносини та, відповідно, інформаційну безпеку було прийняття Закону України «Про інформацію» [4]. Однак у цьому Законі формулювання інформаційної безпеки не було подано

Як свідчать наукові розвідки, у дослідників-правників спостерігаються методологічні відмінності до розуміння інформаційної безпеки на різних рівнях суспільних відносин (національному, державному, регіональному, окремих організацій тощо). Так, окремий підхід був застосований до правового відображення організації безпеки Єдиного державного реєстру виконавчих проваджень України. Цей підхід не відрізняється від підходу до організації безпеки локальної мережі в окремому підприємстві.

Це зумовлює необхідність визначення подібних, уніфіковано- нормативних методів, моделей охорони і захисту інформації щодо будь-якого суб'єкта. Другий аспект – потреба законодавчої (на рівні юридичного закону) консолідації норм правил поведінки щодо інформаційної безпеки, що визначається за технологічним аспектом. Наприклад, практично більшість користувачів персональних комп'ютерів (ПК) у світі мають бути ознайомлені з питаннями боротьби з вірусами та іншими шкідливими програмами, мати загальне уявлення про правопорушників, які їх створюють і поширюють – хакерами, спамерами, крекерами, вірусмейкерами (творцями вірусів) і про шахраїв, які обманюють людей у пошуках наживи через отримання корпоративної інформації, що коштує грошей. Адже нерідко зловмисники здійснюють задумане руками своїх жертв. Отже, «технічні» і «фізичні» методи захисту інформації, як складові комплексу інформаційної безпеки, мають бути певним чином унормовані, що полегшує їх передачу через освіту користувачів ПК стосовно так званої комп'ютерної безпеки, як чинника, що формує певний рівень інформаційної культури людини, соціальних спільнот, суспільства, держави, міжнародного співтовариства.

Вважається, що одними з перших проблеми комп'ютерної інформаційної безпеки усвідомили і зробили впевнений крок до їх вирішення державні відомства США в кінці 60-х років XX століття, коли комп'ютери коштували великих грошей, а інтернет зароджувалася з нечисленних, виключно військових і наукових інформаційних мереж [14, с.17].

Щодо парадигми інформаційної безпеки суспільства. Кожна людська спільнота має свою систему цінностей у контексті інформаційної безпеки. Вона обумовлена історією і менталітетом народу, у складі якого існує будь-яка спільнота. Ця система цінностей вироблена досвідом попередніх поколінь окремих соціальних груп, корпорацій тощо. Руйнування цінностей спільноти неминуче веде до негативних суспільних наслідків.

До останнього часу проблема комплексності інформаційної безпеки людини, соціальних спільнот, суспільства, держави в Україні розглядалися фрагментарно. Так, вважалося, що тільки шляхом правового режиму секретності, деклараннями різних юридичних обмежень у сфері збереження, передачі та поширення інформації, можна вирішити проблеми підтримки, гарантування, охорони інформаційної безпеки.

В історичному аспекті слід зазначити, що більшість досліджень стосовно інформаційної безпеки в Україні, як наукова правова школа, здійснювалася переважно під російським вектором впливу, за науковими школами російських дослідників.

На даному історичному етапі розвитку українського суспільства правові заходи щодо комплексності окремих секторів інформаційної безпеки у країні потребують якісно нової, власної, потужної теоретичної бази, з урахуванням не тільки російського досвіду, а й досвіду західних країн Європи, Європейського Союзу та інших міжнародних формувань.

Дослідження світового досвіду в цьому напрямку залишається особливо корисним для вітчизняних науковців. Тому подальше освітлення та вивчення історії права становлення розуміння інформаційної безпеки у світі є важливим кроком до удосконалення українського права щодо. Особливу увагу пропонується звернути на країни, де генеруються світові, передові технології, моделі здійснення комплексної організації інформаційної безпеки.

Під час об'єднання і синхронізації міжвідомчих комп'ютерних мереж органів державної влади, що активно впроваджувалися в усьому світі, гостро постало питання національної інформаційної безпеки як комплексного, багатоаспектного, багатофункціонального явища. Зокрема, вона має розгдядатися у парадигмі організації охорони і захисту інформації, з екстраполяцією із загального у масштабі всієї країни на організовування інформаційної безпеки за секторальним підходом, у тому числі стосовно окремих підприємств, організацій установ, які функціонують у правовому режимі підприємництва, комерції, конкуренції між собою. В умовах розвитку Інформаційного суспільства особливо важливим є те, наскільки легко і швидко можна скопіювати інформацію з обмеженим доступом у конкурента в цифровому вигляді.

Пропонується звернути увагу на зарубіжний досвід комплексності досліджень питань інформаційної безпеки, що виникають під впливом загроз масового розповсюдження нових інформаційних технологій. У 1967 р. під патронажем Національного Комітету Стандартів США була заснована Ініціативна група дослідників з питань комп'ютерної безпеки. До неї увійшли представники університетів, компаній з виробництва комп'ютерів, науково-дослідних центрів та інших організацій. Результатом такого об'єднання зусиль промислових і наукових фахівців США було сформовано так звану умовно «райдужну серію» – ряд національних стандартів і вимог до обладнання, програмного забезпечення та персоналу різних систем автоматичної обробки даних, що належали таким державним структурам США, як: NASA, Міністерство Оборони, Національний комітет стандартів, Міністерство Праці, Офіс з охорони навколишнього середовища, Міністерство з контролю за озброєнням, Національне наукове товариство, Федеральна резервна система і нарешті Центр Об'єднаного Командування Збройних Сил. За такою моделлю у перспективі було створено Національний Центр Комп'ютерної Безпеки, який займався цими питаннями вже системно у прикладному аспекті, цілеспрямовано і комплексно, координуючи дослідників із державних і приватних організаційних структур [14].

У 1981 р. було створено подібний за сутністю спеціальний центр при Міністерстві Оборони США, який розробив і впровадив спеціалізовану «райдужну серію» в 1985 р. Найбільш значущим для оцінки якості комерційних електронно-цифрових виробів, що обробляють і зберігають конфіденційну інформацію, став стандарт «Критерії оцінки довірених комп'ютерних систем», названий Помаранчевою книгою (названий за кольором обкладинки (помаранчевого кольору). Вона нині розглядається як зразковий (модельний) світовий стандарт, у тому числі стосовно специфікації на лазерний аудіодиск і на шейдерну модель OpenGL. Вже за традицією, хоча й удосконалені, стандарти комп'ютерної безпеки в різних країнах також називають «Помаранчевими книгами». Модельною ознакою таких стандартів є максимальна гнучкість і універсальність оцінки інформаційної безпеки різних суб'єктів суспільних відносин в умовах функціонування їх в Інформаційному Суспільстві (на глобальному рівні комп'ютерної телекомунікації) [14].

Як шлях до формування універсальних моделей організації інформаційної безпеки на транскордонному рівні можна розглядати міжнародні нормативно-правові акти. Зокрема, в Меморандумі про взаєморозуміння щодо співробітництва у сфері телекомунікацій і розвитку Всесвітньої інформаційної інфраструктури між урядом України та урядом США сторони наголосили на своєму намірі керуватись принципами створення Всесвітньої інформаційної інфраструктури, для чого впроваджувати приватні інвестиції, конкурентний ринок, гнучку регулюючу систему, доступ без дискримінації та універсальне обслуговування. Такі підходи були зафіксовані у рішеннях Першої Всесвітньої конференції з розвитку телекомунікації Міжнародного союзу електрозв'язку (Буенос-Айрес, 1994 рік) [14].

У Російській Федерації у ході комплексних наукових досліджень свого часу було прийнято закон РФ «Про інформацію, інформатизацію і захист інформації». У цьому законі визначено було складову інформаційної безпеки мету – захист інформаційної сфери (ст. 20): запобігання витоку, розкрадання, втрати, спотворення, підробки інформації; запобігання загрозам безпеки особистості, суспільства, держави; запобігання несанкціонованим діям щодо знищення, модифікації, спотворення, копіювання, блокування інформації; запобігання інших форм незаконного втручання в інформаційні ресурси та інформаційні системи, забезпечення правового режиму документованої інформації як об'єкта власності; захист конституційних прав громадян на збереження особистої таємниці і конфіденційності персональних даних, наявних у інформаційних системах; збереження державної таємниці, конфіденційності документованої інформації у відповідності до законодавства; забезпечення прав суб'єктів в інформаційних процесах і при розробці, виробництві і застосуванні інформаційних систем, технологій та засобів їх забезпечення.

Як свідчать дослідження, питання інформаційної безпеки відіграють сьогодні величезну, модернізовану роль у сфері високих технологій, тому що саме там інформація (особливо цифровій формі) стає одночасно і продуктом, і сировиною. Сучасне масове співтовариство у сфері інформаційних технологій комп'ютерної телекомунікації (IT) побудовано на потоках, так званих електронних даних з різних точок планети. Її виробляють, обробляють, продають і, звичайно, крадуть.

У зв'язку із зазначеним, нині говорячи про інформаційну безпеку, часто мають на увазі так звану безпеку комп'ютерну. Інформація, що знаходиться на електронних носіях відіграє все більшу роль у житті сучасного суспільства. Багато дослідників відзначає, що слабкість захищеності комп'ютерної інформації обумовлена наступними чинниками: величезні обсяги, можлива анонімність доступу, можливість «інформаційних диверсій». Усе це робить завдання організації моделей захищеності інформації, розміщеної у комп'ютерному середовищі, набагато складнішою проблемою, ніж збереження таємниці звичайного паперового поштового листування.

Якщо розглянути захищеність інформації, що зберігається на традиційних носіях (папір, фотовідбитки і т.п.), то вона досягається, як і завжди, дотриманням заходів фізичного захисту. Друга сторона захисту такої інформації пов'язана зі стихійними лихами та техногенними катастрофами. У той же час комп'ютерна інформаційна безпека, у цілому, є більш широким поняттям, порівняно з інформаційною безпекою щодо традиційних носіїв. Це вимагають формування моделей безпеки заснованих на методиках комплексного підходу.

Як свідчать проведені дослідження інформаційна безпека в більшості наукових публікаціях окремих теоретиків розглядається як один з найважливіших аспектів сучасної національної безпеки, що має зумовлювати спрямування і національної інформаційної політики. При цьому компонентна складова її обов'язково конкретизується на рівнях моделей прояву: національному з галузевого; відповідно – галузевого з корпоративного; корпоративного з персонального.

Для ілюстрації наведемо кілька історичних прикладів з окремих історичних джерел:

- за розпорядженням президента США Клінтона (від 15 липня 1996 року, номер 13010) була створена Комісія з питань захисту критично важливої інфраструктури від фізич-

них нападів і від атак, зроблених за допомогою інформаційної зброї. На початку жовтня 1997 року під час підготовки доповіді президенту, глава вищезгаданої комісії Роберт Марш заявив, що в даний час ні уряд, ні приватний сектор не мають засобів захисту від комп'ютерних атак, здатних вивести з ладу комунікаційні мережі та мережі енергопостачання [15];

- американський ракетний крейсер «Йорктаун» був змушений повернутися в порт через численні проблеми з програмним забезпеченням, що функціонувало на платформі Windows NT 4.0 (Government Computer News, липень 1998). Причиною виявився побічний ефект програми ВМФ США стосовно максимально широкого використання комерційного програмного забезпечення, з метою зниження вартості військової техніки [15];

- як повідомив журнал Internet Week від 23 березня 1998 року, втрати найбільших компаній, викликані комп'ютерними вторгненнями, продовжують збільшуватися, незважаючи на зростання витрат на засоби забезпечення безпеки. Згідно з результатами спільного дослідження Інституту інформаційної безпеки і ФБР, у 1997 році збиток від комп'ютерних злочинів досяг 136 мільйонів доларів, що на 36% більше, ніж в 1996 році. Кожен комп'ютерний злочин завдає шкоди приблизно в 200 тисяч доларів [14];

- у середині липня 1997 року корпорація General Motors відкликала 292 860 автомобілів марки Pontiac, Oldsmobile і Buick моделей 1996 і 1997 років, оскільки помилка в програмному забезпеченні двигуна могла призвести до пожежі[14];

- у лютому 2001 року двоє колишніх співробітників компанії Commerce One, скориставшись паролем адміністратора, видалили із сервера файли, що становлять великий (на кілька мільйонів доларів) проект для іноземного замовника. На щастя, була резервна копія проекту, так що реальні втрати обмежилися витратами на слідство і засоби захисту від подібних інцидентів у майбутньому [14];

· одна студентка втратила стипендію в 18 тисяч доларів у Мічиганському університеті через те, що її сусідка по кімнаті скористалася їхнім спільним системним входом і відправила від імені своєї жертви електронного листа з відмовою від стипендії;

- звіт Департаменту по боротьбі із кіберзлочинністю НП України за 2015 рік повідомив, що кіберзлочинність стала одним із п'яти найпоширеніших економічних злочинів в Україні, кожен третій респондент (37%) вважає, що ризик кіберзлочинності підвищився за останні 12 місяців, понад 25% організацій не мають відповідних політик та механізмів реагування на кіберзлочини, 46% опитаних не проходили навчання з кібербезпеки протягом останніх 12 місяців, 58% респондентів з України заявили, що в їхніх організаціях відсутній процес моніторингу відвідування соціальних мереж в Інтернет [5].

У ході цільових наукових досліджень за фінансової підтримки уряду та великих приватних корпорацій у США постійно виявляються нові вразливі місця в системі інформаційної безпеки підприємств. Так, для прикладу, в інформаційному листі Національного центру захисту інфраструктури США (National Infrastructure Protection Center, NIPC) від 21 липня 1999 року повідомлялося, що за період з 3 по 16 липня 1999 року виявлено дев'ять проблем із програмним забезпеченням, ризик використання їх оцінюється як середній або високий. Серед постраждалих операційних платформ – майже всі різновиди ОС Unix, Windows, MacOS [14].

Так що ніхто не може нині почувати себе спокійно у сенсі безпеки людини, соціальних спільнот (корпорацій), суспільства, держави, міжнародного співтовариства, оскільки помилки «технарів» тут же починають активно використовуватися зловмисниками. У ретроспективі в таких умовах завжди формувалися загальні тенденції та моделі організовування інформаційної безпеки будь-яких соціальних організацій. Нові моделі інформаційної безпеки покликані протистояти різноманітним загрозам, небезпекам, викликам як зовнішнім, так і внутрішнім.

Щодо новітніх викликів безпеки в умовах розвитку Глобального Інформаційного Суспільства. Окремими дослідниками звертається увага на те, що іноді в комп'ютерних мережах телекомунікації напад триває долі секунди;

іноді промацування вразливих місць ведеться повільно, розтягується на години, що робить підозрілу активність зловмисників практично непомітною. Основною метою зловмисників завжди буває порушення складових інформаційної безпеки – доступності, цілісності або конфіденційності [16].

На шляху долання проблем інформаційної безпеки приватних організацій та держави протягом доволі короткого терміну існування незалежності сучасної української державності українськими науковцями було ініційовано до розробленя низку нормативних актів. Перша черга їх стосувалася запобігання правовими засобами щодо втручання в особисті права людей, громадян, їх соціальних спільнот, підприємств, організацій, установ усіх форм власності тощо.

Проте, проводячи правовий, порівняльний аналіз змісту окремих міжнародно-правових актів щодо прав людини та відповідні норми Конституції України, зустрічаємо непоодинокі факти, коли допускається протиправні втручання відповідних державних органів у сферу приватної інформації та встановлення відповідних відомчих нормативно-правових обмежень конституційно визначених норм правил поведінки у суспільстві. Зазначене закономірно викликає суспільний спротив, конфлікти інтересів громадян з органами влади.

Цілком сприйнятлива у суспільстві компетенція держави, що і визначено цілим рядом міжнародних та національних законодавчих ~~правових~~ актів, що прийняті у розвиток конституційних положень стосовно складових трьох основних компонентів втручання у суспільне життя країни:

- регулювання інформаційних відносин з метою гарантування національної безпеки, у її складі стосовно територіальної цілісності та громадського порядку, підтримання законності;
- регулювання моделей охорони і захисту державними органами влади правомірних інформаційних відносин з метою забезпечення прав і свобод громадян, здоров'я та суспільної моральності;
- регулювання інформаційних відносин у сфері сумлінного підприємництва, комерційної інформації тощо.

Результатом наукової роботи із створення національної системи інформаційної безпеки було прийняття Доктрини інформаційної безпеки України, затвердженої Указом Президента України від 23 квітня 2008 року. У ст. 3 Доктрини були виділені три основні групи інтересів в інформаційній сфері України: людини, суспільства, держави.

У ході наукових досліджень українських вчених сучасної історичної доби державної незалежності України були визначені вісім сфер, де можливі реальні та потенційні загрози інформаційній безпеці, що знайшли відображення і в нормативно-правових актах законодавчого рівня:

1) у зовнішньополітичній сфері: поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; прояви комп'ютерної злочинності, комп'ютерного тероризму, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем; зовнішні негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет;

2) у сфері державної безпеки: негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності кордонів України; використання засобів масової інформації, а також мережі Інтернет для пропаганди сепаратизму за етнічною, мовною, релігійною та іншими ознаками; несанкціонований доступ до інформаційних ресурсів органів державної влади; розголошення інформації, яка становить державну та іншу передбачену законодавством таємницю, а також конфіденційної інформації, що є власністю держави;

3) у воєнній сфері: порушення встановленого регламенту збирання, обробки, зберігання і передачі інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України; несанкціонований доступ до інформаційних ресурсів, незаконне збирання та використання інформації з питань оборони; реалізація програмно-математичних заходів з метою порушення функціонування

інформаційних систем у сфері оборони України; перехоплення інформації в телекомунікаційних мережах, радіоелектронне глушіння засобів зв'язку та управління; інформаційно-психологічний вплив на населення України, у тому числі на особовий склад військових формувань, з метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби;

4) у внутрішньополітичній сфері: недостатня розвиненість інститутів громадянського суспільства, недосконаліть партійно-політичної системи, непрозорість політичної та громадської діяльності, що створює передумови для обмеження свободи слова, маніпулювання суспільною свідомістю; негативні інформаційні впливи, в тому числі із застосуванням спеціальних засобів, на індивідуальну та суспільну свідомість; поширення суб'єктами інформаційної діяльності викривленої, недостовірної та упередженої інформації;

5) в економічній сфері: відставання вітчизняних наукоємних і високотехнологічних виробництв, особливо у сфері телекомунікаційних засобів і технологій; недостатній рівень інформатизації економічної сфери, зокрема кредитно-фінансової системи, промисловості, сільського господарства, сфери державних закупівель; несанкціонований доступ, порушення встановленого порядку роботи з інформаційними ресурсами в галузях національної економіки, викривлення інформації в таких ресурсах; використання неліцензованого і несертифікованого програмного забезпечення, засобів і комплексів обробки інформації; недостатній рівень розвитку національної інформаційної інфраструктури;

6) у соціальній та гуманітарній сферах: відставання України від розвинутих держав за рівнем інформатизації соціальної та гуманітарної сфер, насамперед освіти, охорони здоров'я, соціального забезпечення, культури; недодержання прав людини, громадянина на одержання інформації, необхідної для захисту їх соціально-економічних прав; поширення в засобах масової інформації невластивих українській культурній традиції цінностей і способу життя, культ насильства, жорстокості, порнографії, зневажливого ставлення до людської і національної гідності; тенденція до витіснення з інформаційного простору та молодіжної культури українських мистецьких творів, народних традицій і форм дозвілля; послаблення суспільно-політичної, міжетнічної та міжконфесійної єдності суспільства; відставання рівня розвитку українського кінематографу, книговидання, книгорозповсюдження та бібліотечної справи від рівня розвинутих держав;

7) у науково-технологічній сфері: зниження наукового потенціалу в галузі інформатизації та зв'язку; низька конкурентоспроможність вітчизняної інформаційної продукції на світовому ринку; відтік за кордон наукових кадрів та суб'єктів права інтелектуальної власності; недостатній захист від несанкціонованого доступу до інформації внаслідок використання іноземних інформаційних технологій та техніки; неконтрольована експансія сучасних інформаційних технологій, що створює передумови технологічної залежності України;

8) в екологічній сфері: приховування, несвоєчасне надання інформації або надання недостовірної інформації населенню про надзвичайні екологічні ситуації чи надзвичайні ситуації техногенного та природного змісту; недостатня надійність інформаційно-телекомунікаційних систем збирання, обробки та передачі інформації в умовах надзвичайних ситуацій; низький рівень інформатизації органів державної влади, що унеможливлює здійснення оперативного контролю та аналізу стану потенційно небезпечних об'єктів і територій, завчасного прогнозування та реагування на надзвичайні ситуації [6, 7].

Серед останніх новацій із-за кордону варто зазначити, що 15 липня 2016 року німецький уряд затвердив план «Біла книга» з питаннь обороної політика та безпеки, в тому числі інформаційної. В ній чітко вказано, що Російська Федерація стала реальною загрозою, що шкодить існуючому міжнародному порядку та європейській безпеці. У першу чергу, це пов'язано з агресією проти України. Німеччина оголосила про зміни в інформаційній політиці щодо РФ на найближчий час. Там вказані пріоритетні інтереси, що слід захищати уряду та силовим структурам країни.

Мова йде про підвищення розміру виділення коштів на оборону. Задекларована необхідність підвищення загальної інформаційної захищеності всього блоку НАТО, для чого виконується низка заходів із перепрограмування засобів інформаційної безпеки та оновлення організації її технічного оснащення. Відмічена особлива важливість створення Європейської ПРО та оновлення механізмів реалізації інформаційної безпеки. Таким чином, Берлін разом із країнами НАТО заявили про свою позицію відносно політики РФ в Україні і Світі, почавши створювати принципово нову систему інформаційної безпеки континенту.

Сучасні українські науковці нарощують свої дослідження в цій галузі. Були окреслені основні напрямки діяльності стосовно організації адекватних моделей інформаційної безпеки людини, громадянина, окремих осіб, суспільства та держави.

Як зазначає український вчений Б.А. Кормич, правова практика будується, насамперед, на принципі свободи інформації та гарантії інформаційних прав і свобод особи, одночасно розглядаючи права держави щодо регулювання інформаційних процесів у контексті її загальних суверенних прав [8, сс.91-92].

Також він визначив ряд основних ознак інформаційної безпеки, що обумовлюються специфікою її як умовно окремого об'єкта правовідносин:

1. Зони інформаційної безпеки перебувають на перехресті функції національної безпеки та інформаційної функції держави.
2. Питання інформаційної безпеки держави носить екстериторіальний зміст.
3. Суспільні відносини, що входять до сфери інформаційної безпеки, є неоднорідними і різноплановими.
4. Компетенція держави у сфері інформаційної безпеки обумовлюється конкуренцією між інформаційними правами особи та функціями держави, і її органів стосовно регулювання інформаційних процесів.
5. У демократичному суспільстві державне регулювання інформаційної сфери можливе лише шляхом встановлення правових норм.
6. Політика інформаційної безпеки має багатовекторний зміст, але її головними складовими (магістральними векторами) завжди є:

- регулювання інформаційних відносин з метою гарантування національної безпеки, у її складі територіальної цілісності та громадського порядку, підтримання законності;
- регулювання інформаційних відносин з метою забезпечення прав і свобод громадян, здоров'я та моральності;
- регулювання інформаційних відносин у сфері комерційної інформації.

Заслуговує на увагу наукової громадськості концепти В.С. Цимбалюка щодо визначення спеціальних об'єктів інформаційної безпеки, наприклад, у залежності від галузі діяльності підприємств [9].

В аналітичній доповіді українських науковців Національною інституту стратегічних досліджень проблема інформаційної безпеки розглядалася трохи під іншим кутом зору. Ними на перший план ставилися питання адекватного розвитку інформаційного простору та інформаційних процесів, і насамперед їхня економічна складова. Підкреслювалося, що «ключовою проблемою інформаційної безпеки є оцінка відповідності існуючого в державі інформаційного простору потребам її громадян, попиту та пропозиції інформаційних послуг у наближених до користувачів місцях та в зручний для них час. Історичний досвід свідчить, що країни, які не спромоглися своєчасно поповнити інформаційний простір більш ефективними технологіями, уповільнювали свій економічний розвиток. І, навпаки, країни, що мали потужний інформаційний потенціал, швидко відновлювали свою роль у світовому розподілі сфер впливу навіть після воєнних поразок (наприклад, Японія після Другої світової війни). Тому наповнення інформаційного простору новітніми технологіями, що здатні істотно підвищувати як адекватність віддзеркалення реальності, так і продуктивність інформаційної діяльності в суспільстві, є нагальною потребою, що, у свою чергу, визначає можливості захисту національних інтересів».

Закон України «Про основи національної безпеки України» [10] не містить окремого тлумачення поняття інформаційної безпеки,

розглядаючи її лише як одну зі складових національної безпеки, що визначається певною специфікою загроз, викликів, небезпек національним інтересам. Зазначене свідчить про недостатність урахування розробниками цього законодавчого акту всіх наукових напрацювань українських дослідників.

Актуально зазначити, що в різноманітності сучасних підходів до проблеми визначення інформаційної безпеки насамперед вона пов'язується з діяльністю уряду України через державні органи щодо скорочення державного фінансування науки та освіти в країні. Відповідні державні органи таким чином нині виступають головним суб'єктом загроз національній безпеці у своєму правовому нігілізмі. Ясна річ, санкціонуватися до реалізації загрози безпеці можуть лише державними компетентними органами в результаті звуженого кругозору розуміння значення вітчизняної науки та освіти, що можна розглядати як прояв комплексу меншовартості, стратегічної обмеженості поглядів окремих урядовців щодо перспектив подальшого становлення самостійності України на геополітичному просторі не як об'єкта, а як суб'єкта міжнародних відносин.

Головне, значною вадою багатьох наукових визначень національної та у її складі інформаційної безпеки є їхня орієнтація лише на захищеність інтересів, а не створення запобіжних умов існування суб'єктів цієї безпеки. Такий підхід звужує зміст суспільного розуміння функціональної її сфери, що підмінює звичайні (традиційні) функції держави і значно обмежує демократичні права та свободи людини.

Потрібно зазначити, що в українському законодавстві, в окремих спеціальних законах, однобоко подаються визначення інформаційної безпеки. Для прикладу, таку ваду має нормативно-правова дефініція інформаційної безпеки, що подана в Національній програмі інформатизації. Зокрема, в п. 3. розділу IV цієї програми зазначається: «Інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки. Об'єктами інформаційної безпеки є інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни» [6, 7].

У той же час поняття інформаційної безпеки людини та суспільства, умови існування яких визначаються насамперед їхніми природними правами і обов'язками, стає актуальним лише в контексті розвитку і впровадження ідей природного права, зокрема прав людини, громадянина. Все інше похідне, в тому числі технологічні предметні прояви інформаційних правовідносин.

Висновки. Розвиток сучасного розуміння багатогранності, багатоаспектності, багатофункціональності інформаційної безпеки, як соціального феномену, у більшій частині світу припадає на кінець 40-х рр. XX ст., коли були прийняті основні міжнародно-правові акти з прав людини, визнані на міжнародному рівні право націй і народів тощо.

У післярадянських країнах, як і в Україні, розвиток напрямків правових досліджень інформаційної безпеки людини і суспільства взагалі бере початок лише в останнє десятиліття XX ст. і пов'язаний зі початком демократичних реформ, пов'язаних з становленням державної незалежності та самостійності.

XX ст. відкрило зовсім нові перспективи, сучасного розуміння інформаційної безпеки, як правової категорії, зробивши завдання захисту інформації, яке превалювало до цього, лише одним з напрямків реалізації прав суб'єктів суспільних відносин на безпеку, поряд з охороною, підтримкою тощо.

Розвиток технічної і гуманітарної сфери науки і виробництва суттєво змінив акценти і підсилив багатоплановість і комплексність поняття «інформаційна безпека», що має знайти відображення і у вітчизняному законодавстві. Воно має стати ефективною базою для формування нормативів, адміністративно-правових засад моделей інформаційної безпеки і підприємств.

Зрозуміло, що в одній публікації неможливо викласти всіх питань, аспектів, проблем та їх рішень, рекомендацій, пропозицій у рамках заданої теми дослідження. Окремі результати дослідження, зокрема, у контексті загальної теми щодо адміністративно-правових засад інформаційної безпеки підприємств були ви-

світлені у попередніх публікаціях автора [17, 18]. Ознайомлення зацікавленого читача тематикою дослідження автора цієї публікації дозволить сформувати загальне наукове бачення проблематики його досліджень.

Література

1. Конституція України. Закон України від 28.06.1996 р. № 254к/96-ВР. Відомості Верховної Ради України. 1996, № 30, с. 141.

2. Декларація про державний суверенітет України від 16.07.1990 р. №55-XII. Відомості Верховної Ради УРСР. 1990, №31, с. 429.

3. Виноградова Г. В. Інформаційне право України. Навчальний посібник. К. МАУП. 2006, с. 144.

4. Про інформацію. Закон України від 02.10.1992 р. № 2657-XII. Відомості Верховної Ради. 1992, № 48, Ст. 650.

5. Офіційний сайт Департаменту кіберполіції Національної поліції України. Режим доступу: https://www.cybercrime.gov.ua

6. Про Національну програму інформатизації. Закон України від 04.02.1998 р. №74/98-ВРУ. Відомості Верховної Ради. 1998, № 27-28, 181 с.

7. Про Концепцію Національної програми інформатизації. Закон України від 04.02.1998 р. №74/98-ВРУ. Відомості Верховної Ради. 1998, № 27-28, 182 с.

8. Корміч Б. А. Інформаційна безпека: організаційно-правові основи. К. Кондор. 2004,- 384 с.

9. Цимбалюк В. С. Проблеми визначення категорії «інформаційна безпека підприємницької діяльності» в праві України за умов формування інформаційного суспільства. Малий і середній бізнес. К. НДІ Приватного права і підприємництва. 2003, №1-2, сс. 43-54.

10. Про основи національної безпеки України. Закон України від 19.06.2003 р. №964-IV. Відомості Верховної Ради. 2003, № 39, 351 с.

11. Довгань О.Д. Національний інформаційний суверенітет – об'єкт інформаційної безпеки. Інформація і право. 2014, №3(12), сс.102-112.

12. Корж І.Ф., Державна безпека. Методологічні підходи до системи складових понять. Правова інформатика. 2012, №4(36), сс. 69-75.

13. Юлій Цезарь. Записки про Гальську війну. М. Азбука-класика. 1999, 284 с.

14. Історія інформаційно-психологічного протиборства. Підручник. Скулиш Є.Д. заг. ред., авт. Скулиш Є.Д., Жарков Я.М., Компанцев Л.Ф., Остроухов В.В., Петрик В.М. К. Наук.-видав. Відділ НА СБУ. 2012, 212 с.

15. Кісінджер Г. Світовий порядок. Вид. М. АСТ. 2015, 511 с.

16. Біленчук П.Д., Гель А.П., Семаков Г.С., Криміналістична тактика і методика розслідування окремих видів злочинів. Навчальний посіб. К. МАУП. 2007, 512 с.

17. Лисенко С.О. Організаційні засади та прийоми моделювання і реконструкції при розслідуанні правопорушенньщодо інформаційної безпеки підприємств, установ та організацій. Стаття. Наукові праці МАУП. К. МАУП. 2015, 24 с.

18. Лисенко С.О. Реконструкція, як метод оцінки та аналізу моделей інформаційної безпеки. Стаття. Fundamental and Applied Reserches in practice of Leading Scientific Schools, 2015-6(12) // http://orcid.org/0000-0003-4037-9652.