МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ЮРИДИЧНИЙ ФАКУЛЬТЕТ
ДЕННА ФОРМА НАВЧАННЯ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ С.Я. Лихова
«____»_____ 2020 р.

КВАЛІФІКАЦІЙНА РОБОТА
ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»
ЗА ОСВІТНЬО-ПРОФЕСІЙНОЮ ПРОГРАМОЮ
«Правоохоронна діяльність»

Тема: «Правове забезпечення інформаційної безпеки в умовах гібридної війни»

Виконавець: студентка 2 курсу, групи ПР-202 Вовканич Діана Михайлівна

Керівник: доктор юридичних наук, професор Кунєв Юрій Дем’янович

Київ – 2020

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Юридичний факультет
Кафедра кримінального права і процесу
Освітньо-професійної програми «Правоохоронна діяльність»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ С.Я. Лихова

«____»_____ 2020 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи
Вовканич Діани Михайлівни

1. Тема роботи «Правове забезпечення інформаційної безпеки в умовах гібридної війни», затверджена наказом ректора від 24 вересня 2020 р. № 1771/ст.

2. Термін виконання та захисту роботи: з 05 жовтня 2020 р. по 13 грудня 2020 р.; з 21 грудня по 27 грудня 2020 року.

3. Вихідні дані роботи: стан теорії і практики правового забезпечення інформаційної безпеки в Україні.

4. Зміст пояснювальної записки: Аналітичний огляд літературних джерел з тематики диплому. Оцінка стану розвитку інформаційної безпеки в Україні з аналітичних джерел. Надання рекомендацій щодо законодавчого забезпечення інформаційної безпеки в Україні

5. Календарний план-графік

№ пор	Завдання	Термін виконання	Відмітка про виконання
1	Вибрати тему кваліфікаційної роботи	до 01.10.2020	виконано
2	Затвердити тему і план роботи у наукового керівника	до 05.10.2020	виконано
3	Визначити статистичну,інформаційну базу дослідження скласти бібліографію	до 26.10.2020	виконано
4	Оформити і обговорити з науковим керівником перший розділ роботи	до 30.10.2020	виконано
5	Оформити і обговорити з науковим керівником другий розділ роботи	до 11.11.2020	виконано
6	Оформити і обговорити з науковим керівником третій розділ роботи	до 20.11.2020	виконано
7	Доопрацювати роботу, оформити її кінцевий варіант	до 29.11.2020	виконано
8	Отримати відгук керівника та рецензії	до 05.12.2020	виконано
9	Підготувати доповідь на захист	до 10.12.2020	виконано

6. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Консультанти з окремих розділів не залучались			

7. Дата видачі завдання: 05.10.2020 р.

Керівник кваліфікаційної роботи доктор юридичних наук,професор
_____ Кунєв Юрій Дем’янович
(підпис)

Завдання прийняв до виконання _____ Вовканич Діана Михайлівна
(підпис)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Правове забезпечення інформаційної безпеки в умовах гібридної війни»: 105 с, 66 літературних джерел.

ГІБРИДНА ВІЙНА, ІНФОРМАЦІЙНА ДІЯЛЬНІСТЬ, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНЕ ЗАКОНОДАВСТВО, ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО, ІНФОРМАЦІЙНА ВІЙНА, ПОРУШЕННЯ ІНФОРМАЦІЙНОГО ЗАКОНОДАВСТВА.

Об’єкт дослідження - суспільні відносини, що виникають із питань правової організації інформаційної безпеки.

Мета роботи - аналіз теоретичних основ та законодавства України у сфері інформаційної безпеки, а також визначення проблем, пріоритетів та напрямів розвитку нормативно-правового регулювання в цій сфері.

Методи дослідження - методологічною основою дослідження стала сукупність методів, підходів та прийомів наукового пізнання – як загальнонаукових, так і спеціальних: діалектичний, історико-правовий, логічний, системного аналізу, статистичний, системно-структурний, порівняльно-правовий, логіко-семантичний, формально-юридичний та ін.

Значущість отриманих результатів дослідження полягає у вдосконаленні теорії вітчизняного інформаційного права, вдосконаленні законодавства та приведенні його у відповідність до міжнародно-правових стандартів.

Рекомендації щодо використання результатів: результати роботи можуть бути корисними для теорії і практики правоохоронної діяльності,

зокрема для подальших теоретичних розробок та впровадження рекомендацій в правотворчий процес.

Результати дипломної роботи були оприлюднені в матеріалах VI Всеукраїнській науковій конференції молодих вчених «Актуальні питання адміністративного права та процесу» 27 листопада 2020 р. м. Кривий Ріг.

ЗМІСТ

ВСТУП

Актуальність теми зумовлюється тим, що розгляд питань інформаційної безпеки стає стратегічним питанням розвитку національної безпеки, особливо під час ведення гібридної війни, важливою складовою якої є інформаційна війна.

Сфера правового забезпечення інформаційної безпеки є важливою складовою інформаційного права України в цілому, так і зокрема, зав'язків правозастосовної практики з теоретичними розробками науки інформаційного права. Важливою складовою інформаційної безпеки є норми пов'язані з поняттям інформаційної війни, оскільки питання інформаційної війни є важливим предметом для протидії її наслідків правовими методами і засобами.

Під час активної фази війни проти України з боку Росії кількість науково-практичних досліджень питань правового забезпечення інформаційної безпеки збільшується і наше дослідження є одним з таких досліджень, яке набуде певного прикладного значення у протидії інформаційній агресії .

Усе вищевикладене обґрунтовує необхідність комплексного дослідження даної проблематики та вироблення власних підходів до її вирішення.

Значний внесок у розробку правових основ інформаційного права і інформаційної зробили вчені, як: Арістова І.В., Бачило І.Л., Брижко В.М., Бєлєвцева В.В., Гуцалюк М.В., Калюжний Р.А., Кормич Б.А., Копан О.В., Копилов В.А., Кунєв Ю.Д., Логінов О.В. Новицький А.М, Олійник О.В., Рассолов М.М., Тихомиров Ю.А., Цимбалюк В.С. Бєляков К.І., Баранов О.А, Довгань О.Д., Дзьобань О.П., Дубов Д.В., Жиляєв І.Б. , Ланде Д.В., Ліпкан В.А., Марущак А.І.,Ожеван М.А., Остроухов В.В, Панарін І.Н., Петрик В.М., Почепцов Г.Г., Пилипчук В.Г., Скулиш Є.Д., Сопілко І.М., Стрельбицький М.П., Фурашев В.М., Швець М.Я, Ярочкін В.І. та інші.

Незважаючи на достатню розробленість теми, деякі питання, зокрема щодо змісту правової організації діяльнісної складової інформаційної

безпеки, залишилися поза увагою вчених, що зумовлює актуальність обраної теми.

Мета і завдання виконаної дипломної роботи. *Метою даної роботи* є аналіз теоретичних основ та законодавства України у сфері інформаційної безпеки, а також визначення проблем, пріоритетів та напрямів розвитку нормативно-правового регулювання в цій сфері.

Досягненню поставленої мети сприяє розв'язання наступних *завдань*:

– на підставі аналізу джерел сформулювати власне поняття інформаційної безпеки та навести напрямки його реалізації;

– з'ясувати сутність правового забезпечення інформаційної безпеки як предмету дослідження

– визначити особливості інформаційної безпека в умовах гібридної війни

– розкрити основні положення правового забезпечення інформаційної безпеки

– порівняти міжнародні стандарти інформаційної безпеки з українським законодавством

– дати характеристику змісту відповідальності за правопорушення пов'язані із забезпеченням інформаційної безпеки

– визначити напрями розвитку правового забезпечення інформаційної безпеки в умовах гібридної війни

Об'єктом дослідження є суспільні відносини, що виникають із питань правової організації інформаційної безпеки.

Предметом дослідження є правове забезпечення інформаційної безпеки в умовах гібридної війни.

Методи дослідження. Методологічною основою дослідження стала сукупність методів, підходів та прийомів наукового пізнання – як загальнонаукових, так і спеціальних: діалектичний, історико-правовий, логічний, системного аналізу, статистичний, системно-структурний, порівняльно-правовий, логіко-семантичний, формально-юридичний та ін.

Нормативно-правову основу дослідження складає інформаційне законодавство України і зарубіжних країн (країн ЄС, США) та міжнародно-правові акти.

Науково-теоретичною основою дослідження є теоретичні розробки вітчизняних та зарубіжних фахівців з теорії держави і права та галузевих наук. Емпіричною основою дослідження стали матеріали результатів діяльності органів державної влади, довідкові видання, статистичні матеріали, судова практика українських та зарубіжних судів, а також Європейського Суду з прав людини.

Наукова новизна отриманих результатів.

Удосконалено систему понять з питань інформаційної безпеки за напрямами інформаційної діяльності.

Розроблено пропозиції в інформаційне законодавство щодо розвитку змісту норм з питань інформаційної безпеки в умовах гібридної війни.

Практичне значення отриманих результатів полягає у вдосконаленні теорії вітчизняного інформаційного права, вдосконаленні законодавства та приведенні його у відповідність до міжнародно-правових стандартів. Робота може бути корисною для подальшого розвитку положень інформаційного права України.

Особистий внесок здобувача. Робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Апробація отриманих результатів. Деякі результати дослідження, висновки й рекомендації оприлюднені на VI Всеукраїнській науковій конференції молодих вчених «Актуальні питання адміністративного права та процесу» 27 листопада 2020 р. м. Кривий ріг.

Публікації. Результати дослідження, висновки й рекомендації висвітлені у тезах доповіді VI Всеукраїнській науковій конференції молодих вчених «Актуальні питання адміністративного права та процесу» 27 листопада 2020 р. м. Кривий ріг. – Режим доступу: http://www.dli.donetsk.ua/.

РОЗДІЛ 1.
ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Поняття і зміст інформаційної безпеки і її забезпечення

Розгляд основних проблем безпеки соціальних систем дає підстави зробити висновок про те, що їх теоретичний аналіз і розробка розпочалися нещодавно. Донині у спеціальній літературі триває несистемний розгляд базових законів та закономірностей функціонування й розвитку соціальних систем, формулюються та уточнюються основні категорії, поняття й терміни.

Термін «безпека» зазвичай означає відсутність небезпеки (неприпустимого ризику), пов’язаної з можливістю завдання будь-якої шкоди для системи.

Безпека — це такі умови, в яких перебуває складна система, коли дія зовнішніх факторів і внутрішніх чинників не призводить до процесів, що вважаються негативними по відношенню до даної складної системи у відповідності до наявних, на даному етапі, потреб, знань та уявлень [1].

Важливим питанням є й визначення «безпеки», що це: стан, умови, властивості певної системи.

Головна мета державно-правової організації соціальних процесів і систем – баланс інтересів трьох учасників процесу забезпечення безпеки: держави, певної організації, людини.

Будь-яка наука провадить дослідження, ідучи або від простого до складного, або, навпаки, від складного до простого. Дослідження безпеки традиційно провадяться від простого до складного. Установлюються природні зв’язки між безпекою особи та організації, організації та регіону, регіону і держави. Для кожної зі складових забезпечення безпеки певною мірою відрізняється. Так, безпека особи залежить від певних умов, зокрема заробітної плати або пенсії, рівень якої має забезпечити продовольчу, медичну,

кримінальну, побутову, цінову та деякі інші різновиди безпеки кожному мешканцю країни. Крім того, кожна організація створює і забезпечує додаткові різновиди або вищий рівень безпеки своєї та своїх працівників, наприклад: соціальну, правову, організаційну, медичну, психологічну тощо [2, с. 175].

Усі рівні забезпечуються відповідними заходами, які повинна використовувати державна влада та власними зусиллями організації та регіону. Виходячи із засад науки про надійність, безпека оцінюється станом безпеки найменш захищеного ланцюжка (наприклад, на рівні особи – станом пенсіонерів з мінімальним рівнем пенсії).

Безпека організацій складається з безпеки окремих членів організації (тобто з безпеки особи – працівника організації) та із забезпечення безпеки самої організації (таких напрямків, як психологічна та психічна безпека, що пов'язано з необхідністю плідного співіснування, колективної безпеки тощо).

Кожен вищий рівень безпеки має забезпечувати нижчому рівню відповідну безпеку. Організація мусить забезпечувати безпеку кожному з її членів, а держава має забезпечувати безпеку як організації, так і особи.

Усі засоби та заходи безпеки оцінюються за результатами, які, у свою чергу, визначаються їх відповідністю значенням критичних обмежень. Тобто безпека особи, організацій, регіонів та держави має єдину за методологією систему оцінки їх досягнення та єдині параметри: поріг чутливості, поріг вразливості, поріг розпаду і стан спокою. На різних рівнях безпека відрізняється лише за масштабами вимірів та деякою специфікою [2, с. 178].

Різниця в масштабах відбивається в тому, що кожен об'єкт безпеки має відповідний рівень у системі критичних обмежень. Рівень критичних обмежень безпеки держави має забезпечувати відповідний рівень безпеки всім її складовим частинам. Треба врахувати, що кожна з цих систем (людина – біоенергетична, держава – суспільна організація середнього рівня складності управління; світове співтовариство – суспільна організація вищого рівня складності управління) має свої параметри, свої особливості (переваги та недоліки), має дещо спільне та відмінне від інших систем.

Сьогодні головними чинниками прийняття найважливіших рішень залишаються національні держави, якими б особливостями та відмінностями щодо внутрішнього устрою вони не відрізнялися. Діючи на світовій арені, вони повинні дбати перш за все про власні інтереси, а потім уже – про інтереси інших. Такий підхід цілком природний, оскільки цього очікують від держави її громадяни, якщо вони користуються демократичними свободами.

Безпека соціальної системи – це найбільш комплексне питання державно-правової організації соціальних процесів і систем, тут інтегруються різни види діяльності за відповідними напрямками. Розглядаючи питання безпеки соціальної системи, складно розділити діяльність щодо забезпечення безпеки, діяльність з виконання основних та забезпечувальних функцій і діяльність з організації ефективного управління в системі. Тому будемо вважати діяльність із забезпечення безпеки соціальної системи складовою або напрямом забезпечення ефективної організації функціонування системи.

Інформаційна безпека набуває все більшого значення як важливий елемент національної безпеки України. У статті 3 Закону України «Про Національну безпеку України», зазначено, що: «Державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо» [3].

Поняття інформаційної безпеки в теорії

Поняття інформаційної безпеки в теорії існує достатня кількість, розглянемо основні.

Коваленко Ю.О. вважає, що «Інформаційна безпека — це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін,

ознайомлення, перевірки запису чи знищення (у цьому значенні частіше використовують термін «захист інформації»)» [4, с. 74].

В. Гурковський вважає, що «інформаційна безпека України – 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 державо утворювальної 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, с. 74].

Р. Калюжний вважає, що: «інформаційна безпека – це вид суспільних інформаційних правовідносин стосовно створення, підтримки, охорони та захисту бажаних для людини, суспільства й держави безпечних умов життєдіяльності, спеціальних правовідносин, які пов'язані зі створенням, зберіганням, поширенням і використанням інформації» [6, с. 18-19].

Л. О. Кочубей вважає, що: «інформаційна безпека – це такий стан захищеності життєво важливих інтересів, а, отже, й інформаційної озброєності держави, суспільства, особистості, за якого жодні інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів» [7, с. 221-222].

Б.А. Кормич, котрий вважає, що: «інформаційна безпека - це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування й розвитку людини, всього суспільства та держави» [43, с.10].

О.А. Ніщименко вважає, що «інформаційна безпека – це стан захищеності національних інтересів України в інформаційній сфері, що складаються з сукупності збалансованих інтересів особи, суспільства та держави від внутрішніх і зовнішніх загроз, що відповідає принципу забезпечення національної безпеки в інформаційній сфері».

І.Ф. Корж вважає, що: «*інформаційна безпека держави* являє собою збалансований стан функціонування інститутів держави і суспільства, за якого забезпечується мінімальний вплив негативних факторів на національні інтереси держави та її громадян в інформаційному просторі і тим самим забезпечується формування та розвиток цього простору в інтересах особистості, суспільства і держави» [9, с. 38].

Більшість науковців юристів під інформаційною безпекою розуміють інформаційну безпеку держави, навіть не вказуючи на систему, безпеку якої вони розглядають.

А.А. Князєв вважає, що: Інформаційна безпека держави – ступінь захищеності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості і т. д.) стосовно небезпечних (дестабілізаційних, деструктивних, суперечних інтересам країни тощо), інформаційним впливам, причому як до впровадження, так і до вилучення інформації [10].

Дещо удосконалено визначення інформаційної безпеки, спираючись на наведені вище визначення і способи поводження з інформацією наступним чином:

Інформаційна безпека – це стан систем, пов'язаних з обігом (створенням, поширенням, перетворенням і використанням) інформації, формуванням і використанням інформаційних ресурсів, функціонування інформаційних систем, при якому забезпечено якості таких систем, необхідні для реалізації інтересів і задоволення потреб фізичних та юридичних осіб в інформаційній сфері.

Поняття «інформаційної безпеки» в Україні визначено законодавством. Тук у законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [11]: п.13. «Інформаційна безпека в інформаційному суспільстві. За умов швидкого розвитку глобального інформаційного суспільства, широкого використання ІКТ у всіх сферах життя особливого значення набувають проблеми інформаційної безпеки.

«Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації».

Поряд з поняттям «інформаційна безпека» використовуються також поняття, пов’язані з безпекою та інформацією: «безпека інформації», «кібербезпека», «ІТ-безпека», «безпека інформаційних технологій», «комп’ютерна безпека».

Поняття «безпека інформації» визначено у ISO/IEC 27000 п. 3.28 (information security) «Безпека інформації» - збереження конфіденційності (3.10), цілісності (3.36) та доступності (3.7) інформації. Відповідно до Примітки 1 для кваліфікації безпеки в сфері інформації мають враховуватися і інші властивості, такі як справжність (3.6), звітність, неприйняття (3.48) та надійність (3.55). В національному вимірі поняття безпека інформації передбачає захищеність інформації від несанкціонованих дій (випадкових чи навмисних), що призводять до модифікації, розкриття чи знищенням даних [12].

Стандарт ICO/IEC 27032 надає визначення «кібербезпеки» через категорію безпеки кіберпростору – збереження конфіденційності, цілісності та доступності інформації у кіберпросторі. При цьому, кіберпростором є середовище, що виникає внаслідок функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-комунікаційних систем.

Відповідно до ДСТ України ISO/IEC 27032:2016 п. 4.21 Кіберпростір – це складне середовище, що виникає в процесі взаємодії людей, програмного забезпечення та послуг у мережі Інтернет, за допомогою технологічних пристроїв або об'єднаних мереж, яка не існує в будь-якій фізичній формі.

«В англійській мові поняття безпеки IT має два значення. Поняття функціональної безпеки (англ. safety) означає, що система коректно і у повному обсязі реалізує ті і лише ті цілі, що відповідають намірам її власника, тобто функціонує відповідно до існуючих вимог. Поняття власне інформаційної безпеки (англ. security) стосується безпечності процесу технічної обробки інформації і є властивістю функціонально безпечної системи. Така система повинна унеможливлювати несанкціонований доступ до даних та запобігати їхній втраті у разі виникнення збоїв» [12].

Поняття: «безпека інформації», «IT-безпека», «безпека інформаційних технологій», «комп'ютерна безпека», «кібербезпека» охоплюються поняттям «інформаційна безпека», або є її складовими.

Таким чином, ще на початку розгляду теми дослідження можна помітити превалювання переважно функціонального підходу до сприйняття інформаційної безпеки, як протидія, в першу чергу, шкоді у сферах технічній, технологічній, економічній та незначна увага приділяється шкоді пов'язаної із аспектами здійснення цілеспрямованого шкідливого негативного впливу на моральний і психологічний стан груп людей, яка завдається шляхом:

– не повноти, невчасності та невірогідності інформації, що використовується;

– перекручування інформації;

– подання неправдивої інформації;

– маніпулювання свідомістю за допомогою інформації.

У поверхневому сприйнятті розуміння інформаційної безпеки превалює «фізична» шкода інтересам громадянина і суспільства (цілісність інформації та її захищеність), а не психічна (цілісність психіки людини та її захищеність від шкідливих інформаційних впливів.

Інформаційна безпека (information security) — збереження конфіденційності, цілісності та доступності інформації; крім того, повинні враховуватися інші властивості, такі, як автентичність, відстежуваність, неспростовність та надійність.

Підхід до інформаційної безпеки потрібен дещо ширший ніж безпека інформації та її властивостей, а безпека у сфері інформаційної діяльності, як категорії загальної та універсальної».

Наступною важливою складовою дослідження питань підрозділу є поняття *забезпечення інформаційної безпеки*.

Забезпечення безпеки – вжиття заходів щодо зменшення загального рівня небезпеки за рахунок передбачення умов, коли може бути завдана шкода, розробка та вжиття заходів і засобів, які зменшать або ліквідують ризик завдання шкоди.

Забезпеченість безпеки соціальної системи визначається станом найбільш вразливого її напрямку (закон мінімуму за О. О. Богдановим). Таким вважають напрямок, показники якого найближчі до значення критичних обмежень.

Треба враховувати, що знання про інформаційну безпеку мають прикладний характер, тому всі дослідження та результати мають бути реалізовані на практиці.

Для створення нового визначення «забезпечення інформаційної безпеки» поєднаємо два визначення «забезпечення безпеки» і «інформаційна безпека». Вийшло наступне.

Забезпечення інформаційної безпеки – вжиття заходів щодо зменшення загального рівня небезпеки систем, пов'язаних з обігом інформації за рахунок передбачення умов, коли може бути завдана шкода, розробка та вжиття заходів і засобів, які зменшать або ліквідують ризик завдання шкоди.

Коли починають говорити про забезпечення безпеки, то автоматично треба визначити *ризики небезпеки, рівні забезпечення безпеки з подальшою реалізацією заходів з її забезпечення, хоча б на мінімально можливому рівні*.

Наступним визначенням є «інформаційна безпека держави». Під час розгляду цього питання будемо спиратися на вище наведені визначення науковців.

Інформаційна безпека держави – це стан інститутів держави і суспільства в структуру яких входять підсистеми, пов'язані з обігом

(створенням, поширенням, перетворенням і використанням) інформації, формуванням і використанням інформаційних ресурсів, функціонування інформаційних систем, необхідні для реалізації інтересів і задоволення потреб фізичних та юридичних осіб в інформаційній сфері.

Ознаки інформаційної сфери (інформаційний простір), в якій ми досліджуємо питання інформаційної безпеки.

Селезньова О.М., вважає, що «інформаційний простір – це частина інформаційної сфери, обмеженої матеріальною і нематеріальною територією поширення, центром якої є сукупність суб'єктів, що здійснюють інформаційну діяльність, а її складовими – інформація та інформаційні відносини, інформаційна наука та інформаційна культура, інформаційна діяльність та інформаційна інфраструктура, інформаційне право та інформаційне законодавство» [13].

Таким основними ознаками інформаційної системи держави є інформаційна діяльність та інформаційне законодавство.

Інформаційна діяльність

Поведінка суб'єктів у сфері обігу інформації виявляється у вигляді інформаційної діяльності, яка, згідно зі ст. 12 Закону України «Про інформацію» [14], є сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави.

Законодавство, використовує також дефініцію «напрями інформаційної діяльності»: політичний, економічний, соціальний, духовний, екологічний, науково-технічний, міжнародний та ін. Держава гарантує свободу інформаційної діяльності в цих напрямках усім громадянам та юридичним особам у межах їх прав і свобод, функцій і повноважень.

Окремо визначено такий напрям, як міжнародна інформаційна діяльність, що реалізується у двох аспектах:

– забезпечення громадян, державних органів, підприємств, установ і організацій офіційною документованою або публічно оголошуваною

інформацією про зовнішньополітичну діяльність України, про події та явища в інших країнах;

– цілеспрямоване поширення за межами України державними органами і об'єднаннями громадян, засобами масової інформації та громадянами всебічної інформації про Україну.

Виокремлено чотири основних види інформаційної діяльності (ст. 14 Закону України «Про інформацію»):

– *одержання інформації* – набуття, придбання, накопичення відповідно до чинного законодавства України документованої або публічно оголошуваної інформації громадянами, юридичними особами або державою;

– *використання інформації* – задоволення інформаційних потреб громадян, юридичних осіб і держави;

– *поширення інформації* – розповсюдження, оприлюднення, реалізація в установленому законом порядку документованої або публічно оголошуваної інформації;

– *зберігання інформації* – забезпечення належного стану інформації та її матеріальних носіїв [14].

Інформаційне законодавство – сукупність нормативно-правових актів, окремих норм (іноді їх називають інформаційно-правовими нормами), положень міжнародних договорів, які регулюють відносини, пов'язані з реалізацією конституційного права кожного на інформацію, зі здійсненням інформаційної діяльності та її публічно-правовим регулюванням.

Під час розгляду питань *інформаційної безпеки держави* в Україні існує *сукупність проблем*, серед яких такі:

1) недостатня теоретична розробленість категорій безпеки, методології її дослідження та забезпечення у сфері державно-правової організації соціальних систем;

2) визначення інформаційної безпеки держави пов'язане з визначенням пріоритетності завдань держави (реальних, а не фіктивних, що тільки

декларуються), на які будуть спиратися при визначенні ефективності забезпечення національної безпеки;

3) безпека – категорія конкретна, треба визначати підстави й умови результативного функціонування тієї чи іншої інформаційної системи за всіма напрямками діяльності, а у сфері правової організації публічної діяльності не дуже прагнуть розраховувати комплексні показники на сучасному етапі розвитку держави;

4) інформаційна система держави – система стосовно якої традиційно не прийнято розглядати ефективність її роботи багатоаспектно, тобто ефективність виконання системою усіх суспільних функцій інформаційної політики України і правової забезпеченості її виконання на необхідному для держави рівні, що мається на увазі при визначенні інформаційної безпеки держави як складової національної безпеки;

5) практична реалізація заходів безпеки передбачає побудову зрозумілої та обґрунтованої структури забезпечення безпеки (правової, кадрової, інформаційної, матеріально-технічної) за всіма напрямками діяльності, що є достатньо складним завданням не тільки для окремого державного органу, але і для держави в цілому.

Усі різновиди інформаційної безпеки тісно пов’язані між собою, від рівня безпеки окремого напрямку інформаційної діяльності залежить рівень забезпечення інформаційної безпеки суспільства та держави і навпаки, безпека держави і суспільства створює умови безпеки інформаційної діяльності органів публічної влади до рівня особистої безпеки.

Стан інформаційної безпеки держави не може бути вищим за рівень розвитку інформаційного суспільства, підготовлений Турукало Андрієм, який скористався 4 основними індексами які відображають стан розвитку інформаційного суспільства, а саме: NRI - Індекс мережевої готовності (Networked Readiness Index, NRI) EGDI - Індекс розвитку електронного уряду (E-Government Development Index, EGDI) EPI - Індекс електронного участі (E-Participation index, EPI) IDI - Індекс розвитку ІКТ (ICT Development Index, IDI)

У рейтингу країн світу за індексом мережевої готовності в 2016 р вона відстала від лідера на 2,0, тому зайняла 71 позицію. У рейтингу по глобальному інноваційному індексі - на 28,5 (63 позиція). У рейтингу з розвитку електронного уряду - на 0,443 (87 позиція). У рейтингу з розвитку ІКТ- на 3,71 (79 позиція) [15].

За цими показниками можна оцінити рівень розвитку забезпечення інформаційної безпеки держави, яку можна оцінити за рівнем розвитку найслабшої ланки розвитку інформаційного суспільства держави – 87 позиція.

У межах теорії та практики державно-правової організації можна визначити межі зони стійкості, порушення яких призводить до деструкції системи, і визначити основні напрямки не тільки забезпечення безпеки, але й підвищення ефективності функціонування держави України.

Спираючись на розробки В. Д. Могилевського та інших вчених, визначимо ряд принципових положень, котрі найбільше впливають на безпеку соціальної системи, зокрема держави.

1. Найуразливішою для втрати стійкості є структура системи, тобто відносини між елементами, їх взаємозв’язки, а не закони функціонування цих одиниць, які також визначають динаміку системи, але меншою мірою її існування.

2. У сфері державно-правової організації соціальних систем істотне значення має нормативно-правова база їх функціонування. Остання може розглядатися як один з найважливіших елементів будь-якої системи (а правове регулювання діяльності і відносин є визначальним для діяльності державних органів), отже, істотний чином впливати на рівень оптимальності функціонування системи.

3. Структура неоднаково чутлива до руйнування. Найбільшої шкоди завдають порушення у верхніх рівнях ієрархії, а саме в центрах обробки узагальненої інформації, вироблення і прийняття адміністративних рішень.

4. Руйнуванню структури еквівалентні розрив інформаційних каналів або їх перевантаження, оскільки це призводить до ускладнення комунікації між елементами системи та зовнішнім середовищем.

5. На якість роботи системи сильно впливає достовірність інформації, що надходить. Цілеспрямоване перекручення останньої, дезінформація може привести систему до стійкої дезорганізації. Важливу роль відіграє й рівень розвитку інформаційного права в державі.

Фактично за кожним з цих положень, які впливають на систему найбільше, в інформаційній системі держави існує цілий ряд проблем, які потребують негайного розв'язання. Це стосується проблем організаційної структури управління, правового забезпечення основної діяльності й управління в системі, інформаційного забезпечення (надійності й захищеності інформаційних каналів), слабкого розвитку прогнозування тощо. Розв'язання цих проблем має відбуватися комплексно, тому що забезпеченість інформаційної безпеки визначається станом найбільш слабкого її напрямку.

Є.Б. Кубко пише, що «будь-яка криза організаційного розвитку системи може послужити поштовхом для підвищення рівня оптимальності, а отже і загальної ефективності функціонування соціальних систем».

Підсумовуючи, можна зазначити, що інформаційна безпека, по-перше, є важливим елементом у забезпеченні національної безпеки, по-друге, система органів публічної влади повинна дбати про власну безпеку для ефективного забезпечення інформаційної безпеки України.

1.2. Правове забезпечення інформаційної безпеки як предмет правового дослідження

З терміном «забезпечення інформаційної безпеки» ми визначилися в попередньому розділі. Зараз завдання з'ясувати сутність і зміст поняття «правове забезпечення інформаційної безпеки».

Забезпечення інформаційної безпеки – вжиття заходів щодо зменшення загального рівня небезпеки систем, пов'язаних з обігом інформації за рахунок передбачення умов, коли може бути завдана шкода, розробка та вжиття заходів і засобів, які зменшать або ліквідують ризик завдання шкоди.

Саме поняття «забезпечення інформаційної безпеки» – це діяльність, яка повинна забезпечуватися в межах реалізації певної політики держави (інформаційної).

Найбільш простий підхід це «забезпечення інформаційної безпеки» за використання правових методів і засобів.

Найважливішим питанням є визначення того, що є правовою діяльністю в інформаційній сфері правового регулювання.

У системі діяльності право одночасно може бути подано як матеріал, засіб, норма, продукт діяльності, й ці комбінації у кооперації різних актів діяльності, де елементом є право, створюватимуть різні види правової діяльності: правотворчої, правозастосовної та їх різновидів [16].

Звернувшись до опублікованих наукових праць, що стосуються об'єкта інформаційного права можна виділити декілька різних позицій щодо конкретного складу явищ і процесів.

Щодо визначення об'єкта інформаційного права більшість науковців збігаються на думці, що об'єктом інформаційного права є «суспільні відносини»: «декілька комплексів суспільних відносин» [17]; «суспільні інформаційні відносини» [18]; «певний вид суспільних відносин» [19].

Цікавою є думка Селезньової О.М., що «галузь законодавства» характеризується сукупністю нормативно-правових актів, які регулюють відповідну сферу життєдіяльності у її працях поряд із «інформаційними відносинами» з'являється як об'єкт «інформаційна діяльність» [13].

Основним різновидом суспільної діяльності у інформаційній сфері є інформаційна діяльність, яка потребує правового регулювання і фактично є об'єктом правового регулювання.

Більшість науковців збігаються у думці, що: «Інформаційна діяльність – це сукупність певних дій із застосуванням відповідних способів і методів, пов'язаних зі створенням, одержанням, збиранням, зберіганням, використанням та поширенням, а також охороною та захистом інформації».

Різновиди інформаційної діяльності відповідно до закону «Про інформацію»: «Основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації», ми навели в попередньому розділі.

Автори підручника «Інформаційне право» також виділяють різновиди діяльності, які потребують правового регулювання у інформаційній сфері таким чином: «а) всі види діяльності, пов'язані з інформаційним ресурсом як об'єктом діяльності (продукту інтелектуальної, виробничої, будь-якої іншої соціальної діяльності); б) управління в галузі відносин, пов'язаних з певним інформаційним ресурсом та окремими видами роботи з інформацією; в) використання нових технологій роботи з інформацією – формування і забезпечення сумісності інформаційних систем і систем комунікацій в інформаційних системах та мережах; г) забезпечення безпеки у сфері інформації та інформатизації; д) реалізація юридичної відповідальності в галузі інформації, інформатизації, телекомунікацій» [20, с. 97].

Переважна більшість вчених схиляється до визнання предметом інформаційного права – діяльності в інформаційній сфері [21].

Було визначено, що «категорія «правова організація діяльності» означає упорядкування, узгодження взаємопов'язаних систем норм діяльності й норм права, необхідних для набуття якостей та закріплення закономірностей, які забезпечують результативність і розвиток певної діяльності й відповідної соціальної системи і полягає в організації систем діяльності з реалізації норм права та організації системи норм, що визначають діяльність.

Правова організація діяльності – це та основа, яка дозволяє по-новому підійти до процесів модернізації соціальних процесів і систем, в якій поєднуються основні підходи до «діяльнісного універсуму», «управління

розвитком» та нормування діяльності різного роду в нормах адміністративного права».

Тоді предметом інформаційного права будемо вважати правові організованості інформаційної діяльності [21].

У плані тлумачення терміна «інформаційна діяльність» необхідно взяти до уваги два варіанти подальшого його асоціювання:

– *з «обігом інформації»* («під час аналізу інформації як об'єкта правовідносин не можна говорити про неї взагалі, не конкретно. Об'єктом розгляду повинна бути насамперед інформація, що знаходиться в обороті».

– з «*створенням, функціонуванням та розпорядженням певними інформаційними об'єктами*» («об'єкти, у зв'язку з якими суб'єкти вступають в інформаційні правовідносини (об'єкти правовідносин). Об'єкти інформаційних правовідносин (інформаційних об'єктів) – документована інформація, інформаційні продукти й послуги; виключні права; елементи інформаційної безпеки (інформаційні права і свободи особи, стан захищеності особистості, захищеність інформації, інформаційних ресурсів, інформаційних продуктів тощо); інформаційні технології й засоби їх забезпечення (у тому числі програми для комп'ютерів), інші об'єкти в інформаційній сфері») [21].

За допомогою цих основних варіантів асоціювань прикметника «інформаційний» формуються й такі поняття та зв'язки понять: «інформаційна діяльність», «державна інформаційна діяльність», «інформаційне законодавство».

Тоді *державна інформаційна діяльність – це діяльність держави із застосування, забезпечення виконання й дотримання інформаційного законодавства та запобігання його порушенню*.

Інформаційне законодавство – комплекс законів та інших нормативно-правових актів держави, пов'язані з обігом інформації, створенням, функціонуванням та розпорядженням певними інформаційними об'єктами [21].

Важливим у цьому контексті є визначення поняття «інформаційна політика».

Виходячи з вищенаведеного матеріалу, де проаналізовано структурні складові, можна визначити основні процесні складові загальної діяльності, залучені у сферу формування й реалізації інформаційної політики, що дозволить побудувати складну, багатовимірну модель інформаційної політики.

За аналогією визначення Кунєвим Ю.Д. і Баязітовим Л.Р. поняття «митна політика» можна визначити поняття та зміст поняття «інформаційна політика».

Якщо інформаційну політику України розглядати як соціально-діяльнісну систему, то система передбачає розгляд підсистем за рівнями (етапами) її формування й реалізації, які в сукупності становлять замкнений цикл інформаційної політики:

1) діяльність з формування моделі майбутніх змін інформаційних відносин, зокрема у частині фізичного обігу інформації;

2) діяльність міжнародних інститутів з формування моделі майбутніх змін міжнародних інформаційних відносин та міжнародного інформаційного законодавства;

3) діяльність правотворча з реалізації державними інститутами моделі майбутніх змін інформаційних відносин, пов’язаних з фізичним обігом інформації в нормативно-правових актах інформаційного законодавства;

4) публічна діяльність державних інститутів, що пов’язана з виконанням інформаційного законодавства (інформаційна діяльність держави);

5) приватна діяльність, що безпосередньо пов’язана з дотриманням правових норм інформаційного законодавства;

6) обіг інформації та внутрішнє виробництво інформаційних ресурсів у частинах, що безпосередньо не пов’язані з дотриманням правових норм інформаційного законодавства, але залежать від моделі відносин щодо обігу інформації та існуванням інформаційних об’єктів [21].

З наведених вище діяльностей виділено перші три як діяльності, які безпосередньо можна зарахувати складовими діяльності з формування

*інформаційн*ої політики – власне становлять основу політичної діяльності, що стосується правового регулювання *інформаційн*ої сфери. Три інших можна зарахувати складовими діяльності з реалізації *інформаційн*ої політики».

Від того, чи включаємо ми у зміст поняття «інформаційна політика» питання реалізації інформаційного законодавства, залежить, яку державу ми будуємо. Інформаційна політика формалізується в нормах інформаційного законодавства та *реалізується* в правозастосовчій діяльності органів публічної влади та інших суб'єктів у сфері, пов'язаній з фізичним обігом інформації. Тому важлива думка про те, що в умовах демократичної, правової держави інформаційне законодавство має бути єдиним продуктом інформаційної політики.

Провівши синтез властивостей діяльностей, які утворюють інформаційну політику, можна сформулювати таке: *інформаційну політику можна розуміти як діяльність держави з трансформації владних повноважень і певних інтересів суспільства (громадян), держави, торгівлі, промисловості в норми законів та правил, що стосуються обігу інформації, створенням, функціонуванням та розпорядженням певними інформаційними об'єктами*.

Завдання інформаційної політики полягає у формуванні законодавчо визначеної системи перешкод (бар'єрів) вільному обігу інформації або законному розпорядженню певними інформаційними об'єктами (програмами, ресурсами або системами) [21].

Визначено різновиди інформаційно-правової діяльності, які фактично й є предметами інформаційного права:

1. Публічна діяльність державних інститутів, що пов'язана з виконанням інформаційного законодавства:

а) діяльність органів публічної влади з реалізації позитивних прав і обов'язків суб'єктів приватного права, що полягає в застосуванні норм інформаційного законодавства – складається переважно із процесуальних норм і процедур;

б) діяльність органів публічної влади спрямована на організаційно-правове забезпечення дотримання норм інформаційного законодавства, пов’язана із запобіганням його порушенню;

в) діяльність органів публічної влади з організаційно-правового забезпечення попередніх діяльностей реалізується під час виконання державою адміністративних та операційних функцій.

2. Приватна діяльність з реалізації власних позитивних прав і обов’язків, що безпосередньо пов’язана з дотриманням та виконанням правових норм інформаційного законодавства [21].

Інформаційно-правова діяльність – це організована за стандартами інформаційного законодавства кооперована діяльність суб’єктів правової взаємодії державних органів та осіб, яких це стосується, що виконують власні зобов’язання, спрямовані на розгляд і реалізацію державних та приватних інтересів, пов’язаних із обігом інформації та існуванням інформаційних об’єктів. [21].

Визначальною складовою інформаційної безпеки є її правовий компонент, який полягає в наявності системи правових норм та гарантій їх дієвості за напрямами реалізації функцій держави у сфері інформаційної діяльності: регулятивної та охоронної.

Таким чином, предмет правового забезпечення інформаційної безпеки утворюється сукупністю суспільних відносин, пов’язаних з інформацією, інформаційною діяльністю, інформаційною інфраструктурою і правовим статусом суб’єктів інформаційної сфери, що належать до об’єктів національних інтересів, а також із проявом загроз безпеці цих об’єктів.

Правове забезпечення інформаційної безпеки держави є складовою предмету інформаційного права, зокрема, як складової адміністративного права.

За Шмідтом-Асманом [22, с. 175] адміністративне право обіймає індивідуально-правові й інституціональні шари правового регулювання діяльності. За запропонованими різновидами адміністративної діяльності

перший різновид діяльності можна віднести до індивідуально правового шару, а другий – до інституційного шару.

За Шмідтом-Асманом Інформаційно-адміністративне право обіймає індивідуально-правові й інституціональні шари.

Індивідуально-правовий шар

Основні положення індивідуально-правового шару інформаційно-адміністративного права в тому, що *інформаційна правова позиція* громадянина, забезпечується концепціями нормативного обмеження дій адміністрації і системного захисту даних.

Індивідуально-правовий шар складають обмеження загроз для індивідуальних прав і свобод, шляхом застосування класичних захисних механізмів *втраченого адміністративного права у* публічно-адміністративній діяльності за напрямками:

– дисциплінування публічно-адміністративної діяльності, пов'язаної з отриманням інформації та її обробкою;

– *захист індивідуальних даних;*

– цілеспрямоване інформування населення органами публічної адміністрації;

– інформування громадськості, у разі ухвалення адміністративних рішень, які мають територіальне значення;

– *забезпечення відповідальності за порушення права системою санкцій;*

– отримання довідок та ознайомлення з документами;

– інформаційні пропозиції звітів, книжок і реєстрів публічної влади;

– забезпечення доступу до інформації;

– доступ до екологічної інформації органів публічної адміністрації;

– доступ до документації установ публічної влади;

– обов'язок органів публічної адміністрації вести облік інформації;

– узгодження права доступу з захистом реалізації права з боку держави та з захистом процесу ухвалення адміністративних рішень;

– *поводження виконавчої влади з наявною в неї інформацією;*

– існування інтересу у збереженні публічної та приватної таємниці.

Інституційні шари

Інституційні шари полягають у об'єктивно-правовому забезпеченні зростання інформаційних потреб і зростання важливості інформаційної діяльності під час комунікаційних стосунків між громадянином та публічною адміністрацією, а також між самими адміністративними одиницями та визначається за напрямками:

– публічне адміністрування знань за допомогою адекватних процедур;

– юридичне впорядкування базових моделей, у яких комунікація набуває публічного характеру;

– відповідальності держави за інформацію;

– забезпечення обов'язку органів публічної адміністрації дотримуватися нейтральності;

– добір доступної інформації та захист від маніпуляцій;

– поводження з неповною інформацією;

– забезпечення якості даних.

Забезпечення доступу до інформаційної інфраструктури, допомога держави у сфері інформації, захист від неконтрольованого регулювання за допомогою інформації, розбудова механізмів саморегуляції та захист шляхом створення системи – є найважливішими орієнтирами та рамковими умовами інформаційно- адміністративного права.

Напрямки інформаційно-адміністративної діяльності узагальнили наступним чином:

– напрямки приватної інформаційної діяльності, які підлягають адміністративно-правовому регулюванню;

– напрямки інформаційної діяльності публічної адміністрації з реалізації основних функцій держави;

– юрисдикційна діяльність органів публічної адміністрації з питань правопорушень у сфері обігу інформації.

Інформаційно-адміністративне право – сукупність правових норм, що регулюють інформаційно-адміністративну діяльність, пов’язану з правовим регулюванням приватної інформаційної діяльності, інформаційну діяльність публічної адміністрації з реалізації основних функцій держави, особливості юрисдикційної діяльності органів публічної адміністрації з питань правопорушень у сфері обігу інформації, формування і використання публічних інформаційних ресурсів, функціонування публічних інформаційних систем з метою забезпечення інтересів і задоволення потреб фізичних та юридичних осіб.

Вище, описуючи напрями інформаційної діяльності виокремлені курсивом.

Фактично діяльність із забезпечення інформаційної безпеки є складовою інформаційної діяльності за усіма рівнями і сферами та норми з правового забезпечення інформаційної діяльності є складовими адміністративного права, як інформаційно-адміністративного, яке регулює правовими нормами діяльності пов’язані із забезпеченням інформаційної безпеки.

Тенденції суспільного розвитку та сучасні соціальні процеси обумовлюють необхідність інтенсивної розробки теоретичних проблем правового впливу на суспільну діяльність, форм та засобів реалізації права, механізму правового регулювання, застосування норм права і багатьох інших питань.

Незважаючи на важливість поняття «правове забезпечення», «правова організація» досі не вироблено їх сталого визначення та немає єдиного підходу до виділення його складових елементів. Про це свідчить аналіз праць фахівців з права, державного та соціального управління, методології, соціології тощо.

Найважливішою та найсуттєвішою складовою, яка поєднує різні підсистеми й напрямки діяльності соціальної системи, особливо якщо це стосується діяльності органів влади, є правове забезпечення їх діяльності.

Правове забезпечення діяльності із забезпечення інформаційної безпеки можна подати як упорядкування, узгодження взаємопов’язаних систем норм

діяльності й норм права, необхідних для набуття якостей та закріплення закономірностей, які забезпечують результативність і розвиток певної діяльності й відповідної соціальної системи.

Таким чином, *правове забезпечення діяльності із забезпечення інформаційної безпеки надає цілісності та ефективності систем норм права і діяльності й полягає в організації систем діяльності з реалізації норм права та організації системи норм, що визначають діяльність. До цієї системи залучається різне коло суб'єктів, яке визначається досліджуваними видами діяльності.*

Можна стверджувати, що за допомогою права регулюється весь процес державно-правової організації соціальних систем. Право опосередковує процеси організації, і зокрема управлінську діяльність, та покликане сформувати для неї оптимальний правовий режим, тому важливе значення має правова організація управління. Без цього знижується ефективність діяльності державних органів, послаблюється вплив на державні, господарські й соціальні справи.

За допомогою права організовується виконання глобального завдання – забезпечення інформаційної безпеки. Переважну частину виконання цього завдання покладено на різні органи публічної влади України. У сфері діяльності із забезпечення інформаційної безпеки за допомогою права організовуються, а щодо діяльності забезпечуються такі об'єкти:

1) діяльність органів державної виконавчої влади на які покладено завдання із забезпечення інформаційної безпеки щодо організації суспільної діяльності об'єктів сфери зовнішньої взаємодії (вплив: переконання і примус; послуги, координація, надання дозволів, захист, охорона тощо), або зовнішня адміністративна діяльність. Цю діяльність розкривають через основні функції, які можна розподілити на типологічні групи, властиві для органів виконавчої влади;

2) діяльність органів державної виконавчої влади щодо організації діяльності внутрішньосистемних об’єктів, або внутрішня адміністративна діяльність;

3) діяльність з розвитку – проектна або інноваційна щодо перших двох діяльностей та формування нових знань (теорії) про неї;

4) система і структура органів державної виконавчої влади, її органів та підрозділів;

5) діяльність інших суб’єктів, які взаємодіють з органами державної виконавчої влади з питань забезпечення інформаційної безпеки, або підпадають під регулювання їх діяльності адміністративно-правовими нормами;

6) адміністративні відносини, від яких залишаються реальними суб’єктні права і обов’язки. Сюди також можна зарахувати повноваження відповідних суб’єктів державного управління, систему заходів юридичного примусу.

Усі названі елементи організовування взаємозалежні й повинні бути чітко погоджені та унормовані.

Принципове значення має комплексна правова організація всієї системи адміністративно-правової діяльності як системи і процесу. Право активно впливає на підвищення рівня організованості й ефективності діяльності, на подальший розвиток економіки, науково-технічного прогресу, культури, на охорону й раціональне використання ресурсів, на підвищення рівня життя народу. У свою чергу, це сприяє посиленню і використанню організуючого потенціалу права.

Правове забезпечення адміністративної діяльності – це набуття певної якості процесів і систем за допомогою та у сфері дії публічної влади. Основний об’єкт правової організації – *діяльність* органів публічної влади.

Предметом розгляду правового забезпечення інформаційної безпеки є не тільки сама діяльність але й елементи, включені до системного подання цієї діяльності, тобто повна схема кооперації діяльностей учасників взаємодії при здійсненні такої діяльності – це, зокрема:

– *правозастосовча діяльність* органів державної виконавчої влади на які покладено завдання із забезпечення інформаційної безпеки, які виконують її основні функції;

– діяльність суб'єктів діяльності із забезпечення інформаційної безпеки, яка залучається до системи діяльності органів державної виконавчої влади на які покладено завдання із забезпечення інформаційної безпеки;

– *правотворча діяльність з питань формування та реалізації інформаційної політики* щодо забезпечення інформаційної безпеки;

– діяльність фахівців, які виконують забезпечувальні (ресурсні) функції із забезпечення інформаційної безпеки;

– діяльність адміністрації органів державної виконавчої влади на які покладено завдання із забезпечення інформаційної безпеки з організування, керівництва та управління діяльністю їх органів та підрозділів на різних рівнях системи.

Річ у тім, що діяльність передбачає не тільки дію, але й визначення цілей, завдань, добір норм, методів і засобів, що забезпечують виконання завдань, і лише після цього – використання цих засобів і методів до об'єкта, тобто безпосередня дія.

Кожен з напрямків діяльності за функціональною спрямованістю розглядається за різними аспектами. Кожен з аспектів дослідження (організаційний та правовий) має в основі власну функціональну модель, що відображає певний бік функціонування системи та побудований за ієрархічним принципом, від планетарного масштабу до масштабу окремої людини.

1.3. Гібридна війна. Інформаційна війна

Гібридна війна – війна з поєднанням в застосуванні конвенційної зброї, партизанської війни, тероризму та злочинної поведінки з метою досягнення певних політичних цілей, основним інструментом якої є створення державою-

агресором в державі, обраній для агресії, внутрішніх протиріч та конфліктів з подальшим їх використанням для досягнення політичних цілей агресії, які досягаються звичайною війною.

Експерти називають гібридну війну типом конфлікту, який все частіше буде застосовуватися у 21 столітті [23].

Розвиток світової політичної системи початку XXI століття надає серйозний виклик державному суверенітету. Відбувається розмивання меж між «внутрішніми» і «зовнішніми» політичними, економічними, інформаційними та іншими процесами. Держави змушені рахуватися, з одного боку, з міжнародними урядовими організаціями та інститутами, з іншого – зі своїми ж внутрішньодержавними регіонами, а також з численними неурядовими організаціями. Якщо раніше внутрішньодержавні регіони прагнули впливати лише на внутрішньополітичні процеси, а міжнародні організації – на ті питання, які обмежувались зовнішньо-політичною сферою, то тепер ситуація змінилася. Міжнародні організації та інститути все активніше втручаються у внутрішньополітичні питання, такі як врегулювання конфліктів, дотримання прав людини, визначення фінансової політики держав тощо, а внутрішньодержавні регіони прагнуть до зовнішньополітичної діяльності, іноді нарівні з центральною владою, тим підтверджуючи обґрунтованість тези про зростаюче взаємопроникнення внутрішньої і зовнішньої безпеки. Втручаючись «зверху» у внутрішні конфлікти, наднаціональні організації та інститути все частіше підривають прерогативи державного суверенітету [24].

«Влада і її органи стають більш вразливими для проникнення в них зловмисних елементів і сил, шкідливі можливості яких також суттєво зростають, а саме, впливу на державну політику з боку внутрішніх та зовнішніх політичних акторів, підтримки націоналістичних і сепаратистських рухів, постачання їх зброєю, фінансування бойових дій будь-яких воєнізованих формувань в зонах збройних конфліктів та воєн. Застосування в державному управлінні, зокрема, силовими структурами, комп’ютерних та інформаційних систем відкриває можливості для електронного проникнення злочинності у

владу, деструктивних дій внутрішніх і зовнішніх екстремістських сил, яке може обернутися політичними рішеннями і діями, здатними завдавати соціуму і громадянину нечувані біди, спотворювати волевиявлення народу на виборах і референдумах, породжувати транспортні, інформаційні та інші катастрофи тощо, і, нарешті, викликати глобальний хаос» [24].

«Особливо актуальним для нашої держави є, на жаль, агресивна політика з боку східного сусіда, що виявляється у воєнному, політичному, економічному, соціальному, гуманітарному, інформаційному вимірах. Нинішня російсько-українська війна названа гібридною, підтвердженням чого є те, що протистояння російській агресії та впливу в різних сферах відбувається не тільки на лінії фронту, а й на всій території України. Елементами гібридної війни давно є пропаганда, в основі якої лежить відкрита брехня, маніпуляції та підміна понять, заперечення самого факту війни та участі РФ у ній; звинувачення України у власних злочинах, викривлення фактів української історії; торговельно-економічний тиск та енергетична блокада; терор і залякування громадян України; кібератаки та спроби дестабілізувати критичну інфраструктуру. Можна погодитися з фактом, що в Україні вжито ряд заходів, спрямованих на протидію агресії російської пропаганди, зокрема, накладено заборони на окремі російські соціальні мережі, певним чином посилено кібербезпеку (за міжнародного сприяння). Однак, РФ продовжує проводити спеціальні інформаційні операції по всій території України, використовуючи найрізноманітніші канали, зокрема незаборонені медіа-ресурси та соціальні мережі, тим самим підриваючи процеси реформування країни [25].

Гібридна агресія (гібресія) Росії проти України переросла в активну фазу на початку 2014 року, хоча підривну діяльність проти України вона стала вести одразу після проголошення Україною незалежності у 1991 році. Такої думки дотримується більшість (51,4%) з 37 українських експертів, які взяли участь в опитуванні, що здійснювалось у період з 18 по 28 серпня 2017 року Центром глобалістики «Стратегія XXI» за підтримки ЄС і Міжнародного фонду «Відродження». Оцінки українських експертів також свідчать про те, що Росія

завжди працювала над ослабленням України, і ця діяльність особливо активізувалась з приходом В.Путіна до влади [26].

Технологічне бачення реалізації концепції гібридної війни належить головному політичному консультанту Кремля Владиславу Суркову, який апелює до базового 4-тактного алгоритму нелінійних процесів, детально описаного в аналітичній публікації «Війни XXI: Полігібресія Росії» Центру глобалістики «Стратегія XXI», що використовуються для гібридних технологій ведення війни: 1) хибно цільове програмування партнера-противника через «кооперацийну модель» під прикриттям якої реалізується програма його крипто-деструкції; 2) трансформація визначеностей і станів у сукупність невизначеностей, хаотизація причинно наслідкових ланцюжків; 3) управління хаосом через швидкі рішення, ініціативні дії та превентивні заходи щодо інших áкторів; 4) впорядкування хаосу, реінжиніринг простору, отримання нової реальності через синергетику. Наслідки нелінійних процесів часто виявляються непередбачуваними, довільними, самоорганізованими [26].

За розвитку та проникнення в усі сфери життя суспільства інформаційних технологій і висунення на перший план інформаційної діяльності їхній вплив на життя держави можуть зруйнувати її стабільність і в цілому державу.

На сучасному етапі розвитку інформаційного суспільства «з'явилися нові аспекти міждержавної безпеки:

– інформаційна агресія;

– інформаційна війна;

– гібридна війна;

– фінансова інтервенція і багато інших, визнані і невизнані на міжнародному рівні загрози, які можуть фундаментально порушити внутрішній устрій держави, аж до позбавлення суверенітету» [24].

Гібридна війна поєднує принципово різні типи і способи ведення війни, які скоординовано застосовуються задля досягнення основних цілей [28].

Типовими компонентами гібридної війни є використання методів, що сприяють виникненню та поглибленню в державі, обраній для агресії, внутрішніх конфліктів:

– створення внутрішніх суспільних протиріч через пропаганду з її переходом у інформаційну війну;

– створення економічних проблем через економічне протистояння з переходом в економічну війну та протидію зв'язкам країни-жертви з сусідніми країнами;

– підтримка сепаратизму та тероризму аж до актів державного тероризму; побудова псевдо державних утворень як гібридного ідеал-проекту державотворення;

– сприяння створенню нерегулярних збройних формувань (повстанців, партизан та ін.) та їх оснащення.

При цьому сторона-агресор намагається та може залишатися публічно непричетною до розв'язання конфлікту.

Гібридну війну можна поділяти за різними складовими, зокрема, за способами ведення, за засобами які використовуються, за стадіями тощо.

Інформаційна війна

На заміну залізній зброї приходить зброя інформаційна. По своїй суті інформаційна війна є поєднанням дій, спрямованих на конфліктну ситуацію, коли інформація одночасно є зброєю, ресурсом та ціллю [29].

Інформаційна війна – форма ведення інформаційного протистояння між різними суб’єктами (державами, неурядовими, економічними та іншими структурами), яка передбачає проведення комплексу з нанесення шкоди інформаційній сфері конкуруючої сторони і захисту власної інформаційної сфери, конкуруючої сторони і захисту власної інформаційної безпеки [30].

Завдання інформаційної війни:

– створення атмосфери бездуховності, негативного ставлення до культури та історичної спадщини у суспільстві конкурента чи ворога;

– маніпулювання громадською думкою і політичною орієнтацією населення держави з метою створення політичного напруження та стану, близького до хаосу;

– дестабілізація політичних відносин між партіями, об'єднаннями та рухами з метою розпалювання конфліктів, стимулювання недовіри, підозри, загострення ворожнечі, боротьба за владу;

– провокування соціальних, політичних, національно-етнічних і релігійних зіткнень;

– провокування, застосування репресивних дій з боку влади щодо опозиції;

– зниження рівня інформаційного забезпечення органів влади та управління, інспірація помилкових управлінських рішень;

– введення населення в оману щодо роботи державних органів влади, підрив їх авторитету, дискредитація їх дій;

– ініціювання страйків, масових заворушень, інших акцій протесту та непокори;

– підрив міжнародного авторитету держави, її співпраці з іншими державами;

– створення чи посилення опозиційних угруповань чи рухів;

– дискредитація фактів історичної, національної самобутності народу; зміна системи цінностей, які визначають спосіб життя і світогляд людей;

– применшення та нівелювання визнаних світових досягнень у науці, техніці та інших галузях, перебільшення значення помилок, недоліків, наслідків хибних дій та некваліфікованих урядових рішень;

– формування передумов до економічної, духовної чи військової поразки, втрати волі до боротьби та перемоги;

– представлення свого способу життя як поведінки та світогляду майбутнього, які мають наслідувати інші народи;

– підрив морального духу населення і, як наслідок, зниження обороноздатності та бойового потенціалу;

– здійснення іншого деструктивного ідеологічного впливу;

– нанесення шкоди безпеці інформаційно-технічної інфраструктури (машинно-технічним засобам, програмному забезпеченню, засобами та режиму захисту від несанкціонованого витоку інформації);

– захист від іншого деструктивного і інформаційно-психологічного та інформаційно-технічного впливу [30].

Професор Лібіцкі запропонував одну з перших класифікацій інформаційних воєн. Він виокремлює сім різних аспектів цього феномена:

1) війна у сфері контролю та управління;

2) розвідувальна війна;

3) електронна війна;

4) психологічна війна;

5) хакерська війна;

6) економічна інформаційна війна;

7) кібервійна [31].

Наведена професором Лібіцкі класифікація, це скоріше не класифікація інформаційних воєн, а генеза засобів і способів ведення інформаційних війн.

В. Петрик виокремлює наступні різновиди інформаційних війн:

– психологічна війна;

– кібервійна;

– мережева війна;

– ідеологічна війна;

– радіоелектронна боротьба, яка може проявитися такими способами;

– телебачення і радіомовлення можуть бути подавлені;

– ресурси телебачення і радіомовлення можуть бути захоплені/підкорені для здійснення дезінформації;

– мережі комунікацій можуть бути заблоковані або недоступні;

– операції фондової біржі можуть саботуватися електронним втручанням, даючи витік чутливої інформації або поширюючи дезінформацію.

Інформаційній війні притаманна інформаційна зброя – це різновид зброї, головними елементами якої є інформація, інформаційні технології (зокрема технології інформаційного впливу), інформаційні процеси та технічні засоби, що застосовуються в інформаційному протиборстві [30].

Головне завдання інформаційних війн полягає у маніпулюванні масами. Мета такої маніпуляції найчастіше полягає у:

– внесенні у суспільну та індивідуальну свідомість ворожих, шкідливих ідей та поглядів;

– дезорієнтації та дезінформації мас;

– послабленні певних переконань, устоїв;

– залякуванні свого народу образом ворога;

– залякуванні супротивника своєю могутністю.

За умов трансформації інформаційної війни будуть змінюватися також її форми. Так, для інформаційної боротьби першого покоління це:

– вогневе придушення (у воєнний час) елементів інфраструктури державного та військового управління;

– ведення радіоелектронної боротьби;

– отримання розвідувальної інформації шляхом перехоплення й розшифровки інформаційних потоків;

– здійснення несанкціонованого доступу до інформаційних ресурсів з наступною їх фальсифікацією чи викраденням;

– масове подання в інформаційних каналах супротивника чи глобальних мережах дезінформації для впливу на особи, які приймають рішення;

– одержання інформації від перехоплення відкритих джерел інформації.

Інформаційна боротьба другого покоління передбачає:

– створення атмосфери бездуховності й аморальності, негативного відношення до культурної спадщини противника;

– маніпулювання суспільною свідомістю соціальних груп населення країни з метою створення політичної напруженості та хаосу;

– дестабілізація політичних відносин між партіями, об'єднаннями й рухами з метою провокації конфліктів, розпалення недовіри, підозрілості, загострення політичної боротьби, провокування репресій проти опозиції і навіть громадянської війни;

– зниження рівня інформаційного забезпечення органів влади й управління, інспірація помилкових управлінських рішень;

– дезінформація населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління;

– підрив міжнародного авторитету держави, його співробітництва з іншими країнами;

– нанесення збитку життєво важливим інтересам держави в політичній, економічній, оборонній та інших сферах [32].

Фактично це не форми ведення інформаційної війни, а напрямки ведення воєнної діяльності в інформаційній сфері.

«Російська агресивна політика має системний і скоординований характер та задля реалізації стратегічних і тактичних завдань використовує широкий арсенал засобів гібридної агресії, серед яких можна виокремити наступні: 1. Використання інформаційної зброї, повномасштабна пропаганда російського телевізійного контенту, створення та розповсюдження фейкової продукції, як наслідок – створення певної віртуальної реальності. Так, експерти спеціальної робочої групи при Європейській службі зовнішніх дій (East StratComTask Force) лише протягом жовтня 2015р. - липня 2016р. зареєстрували 1 649 випадків дезінформації, фейкових повідомлень з боку прокремлівських ЗМІ, що розповсюджувалися в Європі і світі 18 мовами 16. У 2018 р. аналітики ЄС (проект «EU vs Disinformation» 17 зафіксували 1 000 випадків дезінформації в російських ЗМІ (461 з них припадає на Україну). Шляхом телевізійних програм, новин, соціальних мереж відбувається руйнація української національної ідентичності, нав’язування російського варіанту української історії та української державності» [33].

У доповіді «Маніпулювання інформацією” (вересень 2018р.), підготовленій Центром аналізу, прогнозування і стратегії (CAPS) та Інститутом стратегічних досліджень Воєнної школи (IRSEM), йдеться про російське втручання у референдуми (Нідерланди, Brexit, Каталонія) та виборчі процеси (США, Франція, Німеччина). Широкого розголосу в західному істеблішменті набула нещодавня спроба РФ вплинути на референдум у Македонії (30 вересня 2018 р.) з перейменування країни, що відкривало вступ до ЄС і НАТО. Як стверджує С.Тісдалл в The Guardian: «…методи Росії в Македонії виглядають дуже знайомими. Кампанії з дезінформації, фейкові новини, війна в кіберпросторі, атаки хакерів, фальшиві аккаунти у Facebook та Twitter, секретні грошові виплати – все це, як стверджується, було використано» [34].

Основними *об’єктами* деструктивного *інформаційного впливу* під час ведення інформаційної війни є:

– ідеологічно-психологічне середовище суспільства, пов’язане з використанням інформації, інформаційних ресурсів та інформаційної інфраструктури для здійснення впливу на психіку і поведінку людей;

– ресурси, які розкривають духовні, культурні, історичні, національні цінності, традиції, надбання держави, нації в різних сферах життя суспільства;

– інформаційна інфраструктура, тобто абсолютно всі проміжні ланки між інформацією та людиною;

– система формування суспільної свідомості (світогляд, політичні погляди, загальноприйняті правила поведінки тощо);

– система формування громадської думки;

– система розроблення та прийняття політичних рішень;

– свідомість та поведінка людини [30].

Визначення в законодавстві шкідливих впливів дозволяє припиняти впливи визнані шкідливими хоча б на рівні правопорушень та використання адміністративних засобів припинення.

Автори аналітичного документа «Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства» до основних небезпек в інформаційній сфері відносять такі:

– прогалини законодавчого поля в сфері інформаційної безпеки, відсутність належних механізмів для перешкоджання діяльності українських ЗМІ та інших носіїв інформації, які ретранслюють проросійські наративи чи інші види інформації антиукраїнського характеру;

– низький рівень координації дій ЦОВВ в інформаційні сфері, що дозволяє агресору використати інформаційні продукти української влади в цілях власної пропаганди;

– несформована політика інформаційного супроводу закріплення національної ідентичності в Україні, в частині роботи з населенням України, перш за все на окупованих територіях;

– недостатнє фінансово-технічне забезпечення державних органів України для оперативного та своєчасного реагування на відповідні акти інформаційної агресії на фоні фінансової та інструментальної переваги Росії в інформаційній складовій гібридної війни проти України [26].

гібридні загрози:

– постійне використання Росією в офіційній (МЗС РФ) та політичній площині спеціальних наративів та інформаційних ярликів з метою делігитимації української влади («партія війни», «київська хунта», «бандерівці», «фашисти», «нацисти»);

– формування Росією каналів інформаційно-пропагандистської роботи із дискредитації української влади за цільовими групами: 1) громадяни Росії та громадяни України на окупованих територіях; 2) громадяни України; 3) країни Заходу, партнери України з протидії агресії; 4) суспільства країн, що перебувають в орбіті впливу Росії;

– відкрите і приховане використання демократичних норм та процедур країн ЄС, а також США й інших країн-партнерів для інформаційної

дискредитації України та її спроб формувати міжнародну підтримку протидії російській агресії;

- політичні та лобістські заходи на Заході, які використовуються Росією для формування сумніву у правильності позиції країн ЄС щодо продовження санкційного впливу на Кремль, а також для легітимації анексії Криму;

– розширене використання Кремлем інформаційних каналів РПЦ – УПЦ МП зі створенням нових пропагандистських та дезінформаційних потоків на Україну з метою деморалізації та дезорієнтації населення, зниження його резистентного потенціалу агресору;

– використання українських телевізійних каналів та інших медіа для трансляції проросійських наративів у дозованому вигляді чи під опозиційними гаслами;

– переважне використання громадянами України російських соціальних мереж (навіть попри заборону в Україні) для спілкування та отримання/поширення інформації;

– поширення інформаційних продуктів з використанням регіональної, етнонаціональної, мовної та іншої партикулярної ідентичності серед громадян України для формування ліній розколу в суспільстві, нав'язування відчуття дискримінації та незахищеності, підготовки соціальної бази для протестів та провокацій;

– формування ізольованої соціально-культурної та інформаційної реальності на окупованих територіях України, блокування доступу жителів цих територій до українського інформаційного контенту;

– використання українських експертів та лідерів думок для формування негативного інформаційного образу українського експертного середовища, делігитимізації основних доказів російської агресії;

у кібер-сфері небезпеки:

– низькі культура та рівень знань серед державних службовців щодо забезпечення безпеки своєї робочої та приватної переписки та комунікації через електронні засоби;

– встановлення програмного забезпечення, розробленого іноземними, в тому числі російськими, компаніями, та неліцензійного програмного забезпечення;

гібридні загрози:

– масові кібератаки проти ЦОВВ, об’єктів стратегічної та критичної інфраструктури України;

– технічні можливості приховування справжніх виконавців злочинів у кіберпросторі;

– використання програмних продуктів для прихованого збору інформації про фізичних осіб та організації на території України;

– несанкціонований доступ до приватних та робочих електронних скриньок українських політиків та державних службовців [26].

Те, що стосується інформаційної війни, то засоби її ведення стають відомими швидко, але реагування політичної системи на її виклики є дуже повільним на рівні правотворчості та правозастосовної діяльності.

В історичному плані змінюються акценти щодо превалювання шкідливих факторів і засобів їх доведення до адресата. Актуальним стає питання акцентування уваги на протидії шкоді та найбільш ефективному засобу – правового регулювання.

За визнання важливості публічного характеру шкоди постає питання правової протидії шляхом визнання шкоди та протидії визнаній шкоді.

І тут важливе правове регулювання питань протидії шкодам публічного характеру на різних рівнях. В першу чергу це ЗМІ, та суспільні мережі кіберпростору, які використовуються ворогом для масового впливу на свідомість населення території України та окупованих територій.

«Інформаційно-психологічна війна є найгострішою формою протиборства в інформаційно-психологічній сфері, здійснюваного шляхом впливу на цю сферу противника з метою вирішення стратегічних завдань. Серед іншого це передбачає цілеспрямоване і планомірне використання інформаційно-психологічних інструментів та інших засобів (дипломатичних,

військових, економічних та ін.) для впливу на думки, настрої і в кінцевому підсумку на поведінку противника з метою змусити його діяти в бажаному напрямі. Таким чином, інформаційно-психологічний вплив (ІПВ) – це застосування інформаційно-психологічних засобів для впливу на психіку людини з метою коригування в потрібному для суб'єкта впливу на прямі і внесення змін до поведінки та/або світогляду. Головним критерієм успішності ІПВ виступає результат цього процесу, що може виражатися у вигляді зміни настанов, поведінки, намірів та оцінок конкретного індивіда або групи осіб» [35, с. 59–60].

«Крім цього, якщо проаналізувати досвід України щодо правил роботи ЗМІ в умовах інформаційної війни, то цей досвід явно недостатній – особливо на відміну від Росії, де кожна інформаційна атака ретельно планується і виконується з особливою обережністю. Наприклад, у 2016 році Кремль затвердив збільшення витрат на російську пропаганду в Європі. Україна ж поки що перебуває у процесі навчання боротьбі з інформаційною агресією. Згідно з дослідженням у нашій статті «Особливості поведінки в умовах інформаційної війни», український медіапростір має такі слабкі сторони в інформаційній агресії з боку Росії: 1) не контролюється виникнення нових електронних ресурсів. Спостерігається тенденція появи інтернет-медіа, спрямування яких досить часто має антиукраїнський, пропагандистський характер; 2) вільне і активне проникнення в телемедіа, які можна приймати за допомогою супутників, соціальні мережі відвертих пропагандистських матеріалів; 3) Україна не може гідно протистояти вірусам та шкідливому програмному забезпеченню, які не лише розповсюджують російську пропаганду, але є її частиною; 4) у Росії з'являється чимало різноманітних розробок, спрямованих на пропаганду та маніпулювання свідомістю» [35, с. 70].

З досвіду України реакції правової системи на зовнішні загрози в інформаційній сфері дуже повільні й можуть тривати роками.

«Досліджуючи російську агресію як виклик українському безпековому простору, варто констатувати факт, що за період незалежності України, влада

не спромоглася забезпечити дієві заходи захисту економічного, інформаційного та гуманітарного простору, не створила умови для розвитку безпекових структур, і це стосується не тільки Збройних Сил України, а і створення дієвих інститутів по розробці механізмів захисту національної та політичної безпеки України. Фактично з початку незалежності Україні не вдалося побудувати ефективної економічної та політичної платформи, яка б стала надійною основою для подальшого захисту від агресивних впливів. Проаналізувавши основні аспекти російсько-української гібридної війни, автор зазначає, що державні та політичні структури не були готові до російської агресії. Російська агресія проти України розпочала новий період у формуванні політичної безпеки країни, коли державні інститути, громадянське суспільство консолідуються і роблять подальшу стратегію розвитку Української державності та її захисту від потенційних загроз, бо в і іншому випадку – виникає ризик колапсу політичної системи України, та процес розпаду держави, що викличе подальше неконтрольоване примноження загроз» [33, с. 139].

Інформаційна війна путінської Росії проти України призвела до того, що більше половини опитаних росіян готові воювати з українцями. Вірусом ненависті насамперед заражені молоді люди, які ніколи не були в Україні і не мають контактів із її громадянами. Старших людей лякають «бандерівцями-головорізами, які прийшли до влади». Це результат планомірної тотальної брехні, яка розробляється ідеологами Кремля, транслюється телебаченням [36].

Щороку Росія витрачає проти України на інформаційну війну до 4 млрд дол. [37]. В. Філіпчук на “круглому столі” на тему “Як виграти інформаційну війну” зазначив, що Росія веде структуровану інформаційну війну, яка є складовою частиною гібридної війни [38].

З напрямками інформаційної діяльності, за якими потрібно забезпечувати інформаційну безпеку визначилися у підрозділі 1.1. Але проблема забезпечення інформаційної та кібербезпеки загострюється під час зовнішніх загроз. Тобто звичайні засоби і способи інформаційної діяльності використовуються стандартні, але важливість їх передбачення у правовому регулюванні і

загостренням і урахуванням зовнішніх загроз значно зростає за всіма напрямами інформаційної діяльності.

У XXI ст. інформаційна війна стала розглядатися як невід'ємний елемент військової доктрини будь-якої держави. На сьогоднішній день активно розвивають цей напрям США, Канада, Китай, Індія, Японія, Країни ЄС: Франція, Німеччина, Великобританія, Російська федерація.

Головне завданням правового забезпечення інформаційної безпеки є перетворення змісту інформаційної політики з питань забезпечення інформаційної безпеки в якості інформаційного законодавства.

Висновок до розділу 1

Розгляд основних проблем безпеки соціальних систем дає підстави зробити висновок про те, що їх теоретичний аналіз і розробка розпочалися нещодавно. Донині у спеціальній літературі триває несистемний розгляд базових законів та закономірностей функціонування й розвитку соціальних систем, формулюються та уточнюються основні категорії, поняття й терміни.

Удосконалено основні поняття сфери інформаційної безпеки, серед яких.

Інформаційна безпека – це стан систем, пов'язаних з обігом (створенням, поширенням, перетворенням і використанням) інформації, формуванням і використанням інформаційних ресурсів, функціонування інформаційних систем, при якому забезпечено якості таких систем, необхідні для реалізації інтересів і задоволення потреб фізичних та юридичних осіб в інформаційній сфері.

Забезпечення інформаційної безпеки – вжиття заходів щодо зменшення загального рівня небезпеки систем, пов'язаних з обігом інформації за рахунок передбачення умов, коли може бути завдана шкода, розробка та вжиття заходів і засобів, які зменшать або ліквідують ризик завдання шкоди.

Інформаційна безпека держави – це стан інститутів держави і суспільства в структуру яких входять підсистеми, пов’язані з обігом (створенням, поширенням, перетворенням і використанням) інформації, формуванням і використанням інформаційних ресурсів, функціонування інформаційних систем, необхідні для реалізації інтересів і задоволення потреб фізичних та юридичних осіб в інформаційній сфері.

Інформаційне законодавство – сукупність нормативно-правових актів, окремих норм (іноді їх називають інформаційно-правовими нормами), положень міжнародних договорів, які регулюють відносини, пов’язані з реалізацією конституційного права кожного на інформацію, зі здійсненням інформаційної діяльності та її публічно-правовим регулюванням.

Під час розгляду питань інформаційної безпеки держави в Україні існує сукупність проблем, серед яких такі:

1) недостатня теоретична розробленість категорій безпеки, методології її дослідження та забезпечення у сфері державно-правової організації соціальних систем;

2) визначення інформаційної безпеки держави пов’язане з визначенням пріоритетності завдань держави (реальних, а не фіктивних, що тільки декларуються), на які будуть спиратися при визначенні ефективності забезпечення національної безпеки;

3) безпека – категорія конкретна, треба визначати підстави й умови результативного функціонування тієї чи іншої інформаційної системи за всіма напрямками діяльності, а у сфері правової організації публічної діяльності не дуже прагнуть розраховувати комплексні показники на сучасному етапі розвитку держави;

4) інформаційна система держави – система стосовно якої традиційно не прийнято розглядати ефективність її роботи багатоаспектно, тобто ефективність виконання системою усіх суспільних функцій інформаційної політики України і правової забезпеченості її виконання на необхідному для

держави рівні, що мається на увазі при визначенні інформаційної безпеки держави як складової національної безпеки;

5) практична реалізація заходів безпеки передбачає побудову зрозумілої та обґрунтованої структури забезпечення безпеки (правової, кадрової, інформаційної, матеріально-технічної) за всіма напрямками діяльності, що є достатньо складним завданням не тільки для окремого державного органу, але і для держави в цілому.

За цими показниками можна оцінити рівень розвитку забезпечення інформаційної безпеки держави, яку можна оцінити за рівнем розвитку найслабшої ланки розвитку інформаційного суспільства держави – 87 позиція.

Підсумовуючи, можна зазначити, що інформаційна безпека, по-перше, є важливим елементом у забезпеченні національної безпеки, по-друге, система органів публічної влади повинна дбати про власну безпеку для ефективного забезпечення інформаційної безпеки України.

Визначальною складовою інформаційної безпеки є її правовий компонент, який полягає в наявності системи правових норм та гарантій їх дієвості за напрямами реалізації функцій держави у сфері інформаційної діяльності: регулятивної та охоронної.

Таким чином, предмет правового забезпечення інформаційної безпеки утворюється сукупністю суспільних відносин, пов’язаних з інформацією, інформаційною діяльністю, інформаційною інфраструктурою і правовим статусом суб’єктів інформаційної сфери, що належать до об’єктів національних інтересів, а також із проявом загроз безпеці цих об’єктів.

Правове забезпечення інформаційної безпеки держави є складовою предмету інформаційного права, зокрема, як складової адміністративного права.

Фактично діяльність із забезпечення інформаційної безпеки є складовою інформаційної діяльності за усіма рівнями і сферами та норми з правового забезпечення інформаційної діяльності є складовими адміністративного права,

як інформаційно-адміністративного, яке регулює правовими нормами діяльності пов’язані із забезпеченням інформаційної безпеки.

Проблема забезпечення інформаційної та кібербезпеки загострюється під час зовнішніх загроз, зокрема, інформаційної війни. Тобто звичайні засоби і способи інформаційної діяльності використовуються стандартні, але важливість їх передбачення у правовому регулюванні і загостренням і урахуванням зовнішніх загроз значно зростає за всіма напрямами інформаційної діяльності.

Головне завданням правового забезпечення інформаційної безпеки є перетворення змісту інформаційної політики з питань забезпечення інформаційної безпеки в якості інформаційного законодавства.

Предметом розгляду правового забезпечення інформаційної безпеки є не тільки сама діяльність але й елементи, включені до системного подання цієї діяльності, тобто повна схема кооперації діяльностей учасників взаємодії при здійсненні такої діяльності – це, зокрема:

– *правотворча діяльність з питань формування та реалізації інформаційної політики* щодо забезпечення інформаційної безпеки;

– *правозастосовча діяльність* органів державної виконавчої влади на які покладено завдання із забезпечення інформаційної безпеки, які виконують її основні функції;

– діяльність суб’єктів діяльності із забезпечення інформаційної безпеки, яка залучається до системи діяльності органів державної виконавчої влади на які покладено завдання із забезпечення інформаційної безпеки;

– діяльність фахівців, які виконують забезпечувальні (ресурсні) функції із забезпечення інформаційної безпеки;

– діяльність адміністрації органів державної виконавчої влади на які покладено завдання із забезпечення інформаційної безпеки з організування, керівництва та управління діяльністю їх органів та підрозділів на різних рівнях системи.

У XXI ст. інформаційна війна стала розглядатися як невід’ємний елемент військової доктрини будь-якої держави. На сьогоднішній день активно

розвивають цей напрям США, Канада, Китай, Індія, Японія, Країни ЄС: Франція, Німеччина, Великобританія, Російська федерація.

Головне завданням правового забезпечення інформаційної безпеки є перетворення змісту інформаційної політики з питань забезпечення інформаційної безпеки в якості інформаційного законодавства.

РОЗДІЛ 2.
ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Основні положення нормативно-правових актів, щодо забезпечення інформаційної безпеки в Україні

«Погоджуємось з професором Ліпканом у твердженні, що «право не зводиться до норм».

На думку Остроухова В.В. нормативна база інформаційної безпеки повинна виконувати в першу чергу три основні функції:

1. Регулювати взаємовідносини між суб'єктами інформаційної безпеки, визначати їх права, обов'язки та відповідальність.

2. Нормативно забезпечувати дії суб'єктів інформаційної безпеки на всіх рівнях, а саме – людини, суспільства, держави.

3. Встановлювати порядок застосування різних сил і засобів забезпечення інформаційної безпеки.

На нашу думку, важливим є створення правової бази на основі поєднання основоположних ідей правового регулювання інформаційної сфери та принципів забезпечення національної безпеки. Адже інформаційна безпека є складовою системи національної безпеки і водночас виступає властивістю інформаційної сфери суспільства» [39].

На думку багатьох дослідників нормативно-правове забезпечення інформаційної безпеки України становлять:

Конституція України,

Міжнародні договори і угоди ратифіковані або парафовані Україною:

Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони

Конвенція про кіберзлочинність [40].

Додатковий протокол до Європейської конвенції про інформацію щодо іноземного законодавства [41].

закони України:

Про національну безпеку України;

Про основні засади забезпечення кібербезпеки України [42];

Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки;

Про державну таємницю [43];

Про Національну програму інформатизації;

Про Концепцію Національної програми інформатизації;

Про захист інформації в інформаційно-телекомунікаційних системах;

Про інформацію;

Про доступ до публічної інформації;

Про радіочастотний ресурс;

Про телекомунікації;

Про захист суспільної моралі.

До перелічених вище можна віднести й закони, які теж визначають окремі положення інформаційної безпеки, зокрема закони «Про оборону України», «Про Збройні Сили України», «Про Службу безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації», «Про національну поліцію», «Про прокуратуру», «Про надзвичайний стан» інші закони та інформативно-правові акти, а також: Доктрина інформаційної безпеки України тощо.

У *Конституції України* наведені основні положення інформаційної безпеки:

Стаття 17. «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу».

Стаття 31. Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції.

Стаття 32. Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України [44].

Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею.

Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації.

Стаття 34. Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань.

Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір [44].

Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [45].

Глава 14 Інформаційне суспільство

Стаття 389

Сторони зміцнюють своє співробітництво щодо розвитку інформаційного суспільства на користь приватних осіб і бізнесу через забезпечення загальнодоступності інформаційно-комунікаційних технологій (ІКТ) та через кращу якість послуг за доступними цінами. Це також полегшить доступ до ринків послуг електронних комунікацій, що сприятиме конкуренції та надходженню інвестицій в цю галузь.

Стаття 390

Співробітництво має на меті імплементацію національних стратегій інформаційного суспільства, розвиток всеохоплюючої нормативно-правової бази для електронних комунікацій та розширення участі України у дослідній діяльності ЄС у сфері ІКТ.

Стаття 391

Співробітництво охоплює такі сфери:

а) сприяння широкосмуговому доступу, поліпшення *безпеки мереж* та широкому використанню ІКТ приватними особами, бізнесом та адміністративними органами шляхом розвитку локальних ресурсів Інтернет і впровадження онлайн-послуг, зокрема електронного бізнесу, електронного уряду, електронної охорони здоров'я і електронного навчання;

«Про національну безпеку України»:

Стаття 3. Принципи державної політики у сферах національної безпеки і оборони

4. Державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо.

Стаття 19. Служба безпеки України

1. Служба безпеки України є державним органом спеціального призначення з правоохоронними функціями, що забезпечує державну безпеку, здійснюючи з неухильним дотриманням прав і свобод людини і громадянина:

3) контррозвідувальний захист державного суверенітету, конституційного ладу і територіальної цілісності, оборонного і науково-технічного потенціалу, кібербезпеки, економічної та інформаційної безпеки держави, об'єктів критичної інфраструктури;

Стаття 22. Державна служба спеціального зв'язку та захисту інформації України

1. Державна служба спеціального зв'язку та захисту інформації України є державним органом, призначеним для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного

зв’язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв’язку спеціального призначення, урядового фельд’єгерського зв’язку, а також інших завдань відповідно до закону.

Про основні засади забезпечення кібербезпеки України [46].

Закон визначає 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.

Стаття 8. Національна система кібербезпеки

1. Національна система кібербезпеки є сукупністю суб’єктів забезпечення кібербезпеки та взаємопов’язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об’єктів критичної інформаційної інфраструктури.

2. Основними суб’єктами національної системи кібербезпеки є Державна служба спеціального зв’язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які відповідно до Конституції і законів України виконують в установленому порядку такі основні завдання:

Про Національну програму інформатизації [47].

Стаття 5. Головна мета та основні завдання Національної програми інформатизації

Головною метою Національної програми інформатизації є створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави.

Стаття 6. Функції державних органів у реалізації Національної програми інформатизації

Державні органи, в межах їх компетенції, здійснюють такі функції у процесі інформатизації:

забезпечення інформаційної безпеки держави.

Про Концепцію Національної програми інформатизації [48].

Бюджетні кошти повинні бути спрямовані насамперед на реалізацію загальнодержавних проектів інформатизації:

Першочергові пріоритети надаються створенню нормативно-правової бази інформатизації, включаючи систему захисту авторських прав і особистої інформації, розробленню національних стандартів у галузі інформатизації; формуванню телекомунікаційної інфраструктури, перш за все оптимізації діючої мережі магістралей передачі даних, будівництву нових сучасних каналів, включаючи волоконно-оптичні та супутникові системи зв'язку; формуванню комп'ютерної мережі освіти, науки та культури як частини загальносвітової мережі INTERNET; здійсненню заходів щодо інформаційної безпеки.

Головною метою Програми є забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією на основі широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави.

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. Результатом виконання Програми буде комплект нормативних документів з усіх аспектів використання засобів обчислювальної техніки для оброблення та зберігання інформації обмеженого доступу; комплекс державних стандартів із документування, супроводження, використання, сертифікаційних випробувань програмних засобів захисту інформації; банк засобів діагностики, локалізації і профілактики вірусів, нові технології захисту інформації з використанням спектральних методів, високонадійні криптографічні методи захисту інформації тощо.

Про захист інформації в інформаційно-телекомунікаційних системах [49].

Стаття 8. Умови обробки інформації в системі

Умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством.

Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності комплексної системи захисту інформації здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому законодавством.

Державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, службової інформації та державних і єдиних реєстрів, створення та забезпечення функціонування яких визначено законами, можуть оброблятися в системі без застосування комплексної системи захисту інформації у разі виконання всіх таких умов: підтвердження відповідності системи управління інформаційною безпекою за результатами

процедури з оцінки відповідності національним стандартам України щодо систем управління інформаційною безпекою, яка проведена органом з оцінки відповідності, акредитованим національним органом України з акредитації чи національним органом з акредитації іншої держави, якщо і національний орган України з акредитації, і національний орган з акредитації такої держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності;

Доктрина інформаційної безпеки України [50].

Доктрина спрямована на захист українського суспільства від агресивного інформаційного впливу, що спрямований на розпалювання національної та релігійної ворожнечі, зміни конституційного ладу та порушення суверенітету і територіальної цілісності держави. Завдання щодо перевірки українського сегмента Інтернету та засоби масової інформації на предмет забороненої інформації покладено на Міністерство інформаційної політики. Служба безпеки України також братиме участь у перевірці, але сфера її діяльності – це моніторинг спеціальними методами й способами вітчизняних та іноземних ЗМІ й Інтернету. Кабінет Міністрів України має координувати роботу міністерств (та інших органів виконавчої влади) і фінансувати програми, які пов’язані з інформаційною безпекою [51].

Доктрина має наступну структуру:

1. Загальні положення

2. Мета та принципи Доктрини

3. Національні інтереси України в інформаційній сфері

4. Актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері

5. Пріоритети державної політики в інформаційній сфері

6. Механізм реалізації Доктрини

1. Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні

технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України.

Комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації.

Принципи, пріоритети та напрями забезпечення кібербезпеки України визначені Стратегією кібербезпеки України, затвердженою Указом Президента України від 15 березня 2016 року № 96 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України».

Доктрина інформаційної безпеки України (далі - Доктрина) визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері.

Правовою основою Доктрини є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України», а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

2. Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни.

Рекомендації парламентських слухань на тему: «Законодавче забезпечення розвитку інформаційного суспільства в Україні» [52].

У переліку пріоритетів стратегічного розвитку України особливе місце повинні займати захист прав, свобод і безпеки громадян в інформаційній сфері,

відмова від ідей тотального інформаційного контролю та розвиток інноваційних галузей економіки, зокрема вітчизняної індустрії інформаційних технологій, надання послуг та виробництво програмної продукції.

Всебічної громадської і державної підтримки також потребує виробництво вітчизняної інформаційно-аналітичної, кіно- та медіапродукції, насамперед в умовах інформаційної агресії проти України. Вкрай актуальною за цих умов є проблема розробки дієвої інформаційної політики та системи забезпечення інформаційної безпеки України.

З метою забезпечення розвитку інформаційного суспільства в Україні, враховуючи низку наявних проблем в інформаційній сфері, зокрема необхідність розвитку інформаційного законодавства, проведення системної кореляції з вирішення питань захисту та забезпечення основних прав, цінностей і соціально-економічних інтересів людини, суспільства і держави, побудови в умовах відкритого суспільства ефективної системи інформаційної безпеки України, а також стан виконання Рекомендацій парламентських слухань з питань розвитку інформаційного суспільства в Україні, що відбулися 21 вересня 2005 року, схвалених Постановою Верховної Ради України від 1 грудня 2005 року № 3175-IV, вважаємо за доцільне рекомендувати:

«2. Щодо інформаційної безпеки України

Верховній Раді України:

– законодавчо визначити засади державної політики щодо забезпечення інформаційної безпеки України як однієї з основних конституційно визначених функцій держави;

Кабінету Міністрів України:

– сформувати ефективну систему забезпечення інформаційної безпеки України та її складової - кібернетичної безпеки;

– утворити державний орган чи координаційний центр для здійснення контролю та регуляції політики в галузі інформаційної безпеки України;

– розробити проект Закону України про кібернетичну безпеку у системній кореляції з вирішенням питань захисту та забезпечення прав і свобод громадян, конституційних засад української держави;

– розробити нормативну базу та здійснити організаційно-технічні заходи, необхідні для фіксування та використання у цивільному і кримінальному процесі даних, відомостей і матеріалів, у тому числі і доказових, що були отримані за допомогою засобів ІКТ;

– з'ясувати та оприлюднити структуру власності компанії "Зеонбуд", "Київстар", "МТС", зокрема, розглянувши потенційні загрози інформаційному простору країни у зв'язку з монопольним становищем цих компаній;

– забезпечити координацію діяльності органів державної влади, їх ефективну взаємодію із засобами масової інформації та інститутами громадянського суспільства щодо розвитку вітчизняного інформаційного простору і захисту національних інтересів в інформаційній сфері;

– забезпечити розробку та обов'язкове впровадження програмного забезпечення вітчизняного виробництва (зокрема вітчизняної операційної системи, антивірусного програмного забезпечення) в органах влади з метою забезпечення кібернетичної безпеки в Україні;

– забезпечити наявність та розвиток сучасної системи оперативного зв'язку між державними органами влади та органами місцевого самоврядування;

– спростити запровадження комплексної системи захисту інформації (КСЗІ) в державних органах влади та органах місцевого самоврядування, підвищити прозорість процедури отримання сертифікатів відповідності вимогам КСЗІ та зниження вартості її впровадження;

– забезпечити захист від кіберзагроз критично важливих об'єктів національної інфраструктури, зокрема атомних електростанцій, гідроелектростанцій, трубопроводів тощо шляхом проведення аудиту інформаційної безпеки і запровадження відповідних вимог, обов'язкових для підприємств усіх форм власності;

– створити єдиний національний ІТ-депозитарій (резервну копію "бекапу" критично важливих інформаційних ресурсів для держави);

– адаптувати системи захисту державних інформаційних ресурсів до вимог та стандартів Європейського Союзу з проведенням тестів на проникнення критично важливих об’єктів національної інфраструктури;

Національній раді України з питань телебачення і радіомовлення з’ясувати обставини отримання окремими телевізійними компаніями множинних ліцензій на здійснення мовлення.

Навели основні положення законодавства, що безпосередньо означає правові основи інформаційної безпеки, необхідні для подальшого аналізу та визначення напрямків розвитку правового забезпечення інформаційної діяльності.

2.2. Правове регулювання сфери інформаційної безпеки в США та ЄС

Варто відзначити, що в останні 30-40 років за кордоном сформувалися наукові школи, які займалися інформаційними проблемами. Визнаним авторитетом, який вперше обґрунтував теоретичні засади діяльності держави в інформаційній сфері був відомий американський вчений Г. Ласуел. У 1950-1960-х рр. технології впливу держави на громадську думку досліджували німецькі дослідники Т. Адорно і Г. Маркузе. У 1970-80-х рр. 3 Зовнішня політика та національна безпека механізми захисту засобами масової комунікації існуючих соціальних відносин вивчалися французькими вченими П. Флішем, А. Матларом, Б. М’єжем, П. Бодом. Американці М.-Мак Комбс і Д. Шоу розробили наукові підходи щодо формування та реалізації інформаційних стратегій. У роботах Д. Белла, М. Кастельса, М. Портера, Й. Масуди, А. Турена, Ф. Вебстера, Е. Гіденса, Ю. Хабермаса, Ф. Фукуяма, Дж. Нейсбіта приділено увагу передумовам, що призвели до формування інформаційного суспільства, його особливостей порівняно з попередніми вехами розвитку людства.

В останні 10-15 років у західних країнах було видано велику кількість робіт, присвячених аналізу ролі держави у сфері розподілу інформаційних ресурсів, захисту національного інформаційного простору, налагодженню комунікації в інформаційній сфері, розвитку інформаційно-комунікативних технологій тощо. Особливу увагу науковців викликають проблеми формування та реалізації інформаційних стратегій держави в умовах швидкого розвитку інформаційного суспільства [53].

Основний зміст інформаційної політики в розвинених країнах складають планомірні дії органів публічної влади щодо удосконалення інформаційних відносин. Серед таких дій основними є: розвиток електронного урядування та електронної держави, модернізація інформаційного законодавства, захист свого інформаційного простору та протидія інформаційним агресіям з боку інших держав, боротьба з кіберзлочинністю [53].

Розробки науковців показують, що першість у забезпеченні інформаційної безпеки у світі належить США. Так, навіть Японія, яка вважається меккою виробництва цифрової техніки та використання найсучасніших ІТ-технологій, відстає від США більше ніж на п’ять років у сфері розповсюдження персональних комп’ютерів, кабельного телебачення, цифрової телефонії та в інших аспектах інформаційної політики [51].

США

Сьогодні законодавство США у сфері забезпечення інформаційної безпеки складається з федеральних законів та законів штатів, які створили правову основу для формування єдиної державної політики в галузі захисту інформації для забезпечення інтересів національної безпеки. Це насамперед, такі закони: «Про інформаційну безпеку», «Про удосконалення інформаційної безпеки» (1997 р.), «Про комп’ютерне шахрайство та зловживання» (1986 р.), «Про свободу інформації» (1967 р.), «Про висвітлення діяльності уряду», «Про охорону особистих таємниць», «Про таємницю» (1974 р.), «Про право на фінансову таємницю» (1978 р.), «Про доступ до інформації про діяльність ЦРУ» (1984 р.), «Про безпеку комп’ютерних систем» (1987 р.).

Національна політика США в галузі захисту інформації формується Агентством національної безпеки (АНБ), а найважливіші стратегічні питання інформаційної безпеки розглядаються Радою національної безпеки з виданням директив Президента США, серед яких: PD/NSC-24 «Політика в галузі захисту систем зв'язку» (1977 р.), у якій вперше зазначено про необхідність захисту важливої несекретної інформації для забезпечення національної безпеки; SDD – 145 «Національна політика США в галузі безпеки систем зв'язку в автоматизованих інформаційних системах (1984 р.), якою на АНБ покладено функції із захисту інформації і контролю за безпекою у каналах зв'язку, обчислювальних та інформаційно-телекомунікаційних системах, а також сертифікації технологій, систем і устаткування із захисту інформації в інформаційно-телекомунікаційних системах, а також ліцензування діяльності в галузі захисту інформації [54].

Тенденцію до надання пріоритетної ролі інформаційній безпеці наочно демонструють резолюції Генеральної асамблеї ООН: «Роль науки і техніки в контексті міжнародної безпеки, роззброєння та інших, пов'язаних з цим сфер» № 53/576 (1998 р.); «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки» № 54/49 (1999 р.); № 55/28 (2000 р.); № 60/45 (2005 р.) [51].

Уже в 1992 р. у США було прийнято програми «Національна інформаційна політика» та «Глобальна інформаційна політика» (GII).

За 1997–2001 рр. на законодавчому рівні у сфері інформаційної безпеки США було зроблено чимало: пом'якшені експортні обмеження на криптографічні продукти, сформована інфраструктура з відкритими ключами, розроблено ряд стандартів на кшталт електронного цифрового підпису – FIPS 186-2 (2000 р.). Усе це дало змогу зосередитися на одному з її найважливіших додатків – аутентифікації, що проводиться за відпрацьованою на криптографічних засобах методикою. На базі цих законів у США сформована загальнонаціональна інфраструктура електронної аутентифікації.

Крім того, у законодавстві США діють як положення обмежувальної спрямованості, так і директиви, які захищають інтереси таких державних відомств, як Міністерство оборони, АНБ, ФБР, ЦРУ.

Тож США розроблено та реалізуються програми, спрямовані на розширення можливостей розвідки з добування й обробки інформації щодо загроз національній інформаційній інфраструктурі з боку інших держав [51].

У 2009 р. конгресмени США О. Сноу та Д. Рокфеллер підготували та ініціювали проект закону США «Акт про кібербезпеку» *(The Cybersecurity Act Of 2009.*

У 2010 р. з метою реалізації захисту держави та уряду від кібератак та хакерів президентом США було затверджено «Ініціативу зі всеосяжної національної кібербезпеки» Ради національної безпеки США, яка містить дванадцять загальних положень. Ця ініціатива є складовою частиною розділу Військової доктрини США, що стосується кібернетичної оборони. Документом передбачено створення єдиної федеральної мережі, пов'язаної захищеними каналами зв'язку, який у свою чергу, має здійснюватися через контрольовані точки доступу. Крім того, ініціатива передбачає об'єднання всіх наявних у США центрів оперативного реагування на кіберзлочини з метою підвищення ефективності їх діяльності та проведення більш глибокого аналізу щодо хакерських атак. Також, з метою протидії іноземним кібершпигунам документом передбачено створення підрозділів кібер контррозвідки в державних органах США, зокрема для захисту секретних внутрішніх мереж Міністерства оборони США від терористичних атак.

У Стратегії кібербезпеки США (2011 р.), запропонований президентом США Б. Обамою, передбачено право держави приймати заходи у відповідь на ворожі дії у кіберпросторі, розглядаючи їх як будь-які інші загрози. Тобто, хакерські атаки прирівняні до оголошення війни США.

У кінці квітня 2012 р. сенат США прийняв Закон CISPA *(Cyber Intelligence Sharing And Protection Act)*, який дає можливість уряду США, приватним агентствам безпеки та будь-яким приватним компаніям за наявності

підозри про вчинення кіберзлочину отримувати доступ до конфіденційної інформації користувачів і комерційних організацій.

Нормативно-правовими документами США, які регулюють безпеку кіберпростору стали Національна стратегія безпечного кіберпростору (2003 р.), Огляд політики кібербезпеки (2009 р.), Міжнародна стратегія для кіберпростору (2011 р.), Наказ Президента США «Щодо Проекту стратегії покращення кібербезпеки критично важливих об'єктів інфраструктури (2013 р.), Проект стратегії покращення кібербезпеки критично важливих об'єктів інфраструктури (2014 р.), Закон з кібербезпеки та обміну інформацією (2015 р.), Національна стратегія безпеки (2015 р.), Стратегія кібербезпеки Департаменту оборони (2015 р.) [51].

З метою посилення кібербезпеки президент США Д. Трамп 11 травня 2017 р. підписав новий указ про кібернетичний захист федеральних мереж, який має допомогти в захисті від хакерів найбільш важливих об'єктів інфраструктури США.

Аналіз законодавства США у сфері інформаційної безпеки показує, що основними напрямами забезпечення національної кібербезпеки США є захист критично важливих об'єктів інфраструктури, а саме – їх інформаційних систем від кібернетичних атак; вдосконалення засобів виявлення таких атак і оперативного реагування на них; визначення завдань безпеки кіберпростору та способи їх вирішення; підготовка відповідних фахівців з безпеки інформації та взаємодія з приватним сектором; співпраця з міжнародними організаціями з метою забезпечення відкритого, безпечного, надійного кіберпростору.

За останні 35 років у США сформувалася чітка система забезпечення інформаційної безпеки, яка характеризується поступовими тенденціями та, разом з тим, кардинальними заходами. Тож американський досвід державної політики в сфері інформаційної безпеки являється важливим для української зовнішньої та внутрішньої політики. Найціннішим є дієвий підхід до регулювання ринка інформаційних технологій в умовах ринкової економіки [51].

Країни ЄС

В ЄС доволі чітко ідентифікували «гібридні загрози» та визначали заходи протидії. Була розроблена низка документів, включаючи Глобальну стратегію ЄС, Спільний рамковий документ з протидії гібридним загрозам (06.04.2016р.) і Спільна доповідь Європейському парламенту і Європейській Раді з його імплементації (19.07.2017р.), Оперативний протокол ЄС з протидії гібридним загрозам «EU Playbook» (05.07.2016р.), Спільний робочий документ «Східне партнерство – 20 очікуваних досягнень до 2020 року: фокусуючись на головних пріоритетах та реальних результатах» (15.12.2016р.), доповідь Європейського парламенту «Протидія гібридним загрозам: Співпраця ЄС-НАТО» (березень 2017р.).

Позиція, що відображала спільну європейську політику щодо інформаційної безпеки була окреслена Європейською Комісією в документі під назвою «Мережева та інформаційна безпека: європейський політичний підхід» у 2001 році. Під «мережевою та інформаційною безпекою» розуміється здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, які становлять загрозу доступності, аутентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через ці мережі і системи. Більш широкий підхід до розуміння щодо змісту поняття «інформаційна безпека» був висловлений представником Швеції при обговоренні питань міжнародної інформаційної безпеки на 56-й сесії Генеральної Асамблеї ООН, згідно з якою інформаційна та мережева безпека означає захист особистої інформації про відправників і одержувачів, захист інформації від несанкціонованих змін, захист від несанкціонованого доступу до інформації і створення надійного джерела постачання обладнання, послуг та інформації, а також охоплює захист інформації, що стосується військового потенціалу та інших аспектів національної безпеки. При цьому, недостатній захист життєво важливих інформаційних ресурсів та інформаційних і телекомунікаційних систем може створити загрозу міжнародній безпеці.

Базовий міжнародний нормативно-правовий документ, що регулює суспільні відносини у сфері боротьби з кіберзлочинністю – Конвенція Ради Європи «Про кіберзлочинність» від 23 листопада 2001 року, був створений власне під впливом європейської правової думки. Найбільш близьким за змістом до нього є Кримінальний кодекс ФРН [39].

Важливим правовим актом є Резолюція Ради ЄС № 2003/С 48/01 від 18 лютого 2003 року про Європейський підхід до культури мережі та інформаційної безпеки.

Кожна з країн ЄС має власну стратегію кібербезпеки – наприклад, Стратегія безпеки та оборони інформаційних систем Франції, Національна стратегія кібербезпеки Королівства Нідерланди, Стратегія кібербезпеки Німеччини, Політика захисту кіберпростору Республіки Польща та інші.

У 2016 році Європейський парламент прийняв Директиву ЄС щодо мережевої та інформаційної безпеки, метою якої є встановлення загальних стандартів кібербезпеки та покращення співпраці між країнами ЄС [39].

Для країн ЄС важливе значення мають: Резолюції Європейського Союзу «Біла Книга. Зростання, конкурентоспроможність, зайнятість: виклики та стратегії XXI століття», Директиви ЄС «Зелена Книга. Життя і працевлаштування в інформаційному суспільстві» та Рекомендації «Інформаційна магістраль для глобального суспільства».

В 2000 році була підтримана ініціатива Європейської Комісії під назвою «Електронна Європа» (eEurope), яка пізніше була закріплена в документі «Електронна Європа – інформаційне суспільство для всіх». Процес розвитку електронного урядування в Європейському Союзі відображають програмні документи: – План дій «eEurope 2002», План дій «eEurope 2005», План дій «e-Government i-2010», а також Цифровий порядок денний для Європи (Digital agenda for Europe) як складова Стратегії Європа 2020 [39].

Досвід європейських країн свідчить про те, що в них давно законодавчо визначаються обмеження щодо запровадження принципу транспарентності на окремі категорії інформації. Ці обмеження стосуються інформації про захист

національної безпеки і міжнародних відносин, захисту приватного життя, комерційної конфіденційності, правоохоронної діяльності і забезпечення громадського порядку, а також інформації, отриманої конфіденційно [55].

Правовою Основою інформаційної безпеки визнано основні НПА в питаннях національної безпеки, зокрема, у США: «Стратегія національної безпеки», Канаді – «Політика національної безпеки», Італії – «Стратегічна концепція національної оборони», Великій Британії, Китаї – «Біла книга».

Законодавство США у сфері забезпечення інформаційної безпеки складається з федеральних законів та законів штатів, які створили правову основу для формування єдиної державної політики в галузі захисту інформації для забезпечення інтересів національної безпеки. Це насамперед, такі закони: «Про інформаційну безпеку», «Про удосконалення інформаційної безпеки», «Про комп'ютерне шахрайство та зловживання», «Про свободу інформації», «Про висвітлення діяльності уряду», «Про охорону особистих таємниць», «Про таємницю», «Про право на фінансову таємницю», «Про доступ до інформації про діяльність ЦРУ», «Про безпеку комп'ютерних систем». Наприкінці минулого століття міністерствами та відомствами США, які відповідають за національну безпеку, було створено Об'єднану комісію з питань безпеки, яка розробила якісно нові підходи до формування політики інформаційної безпеки [56, с. 45–68].

Особливого значення на сучасному етапі розвитку України набувають питання інтеграції до правової системи ЄС.

У контексті євроінтеграції України актуалізується проблема вивчення досвіду становлення інформаційного суспільства у країнах - членах Європейського Союзу, а також імплементації норм правових актів ЄС в інформаційне законодавство України.

Вищезгадана діяльність відповідає напрямам Програми інтеграції України до ЄС.

2.3. Основи правового регулювання правопорушень в інформаційній сфері

Важливою складовою правового забезпечення інформаційної безпеки є юридична відповідальність за порушення інформаційного законодавства.

Виключний перелік видів юридичної відповідальності за делікти в інформаційній сфері (інформаційно-правової відповідальності), з урахуванням ступеню суспільної небезпеки, пропонується такий: кримінально-правова відповідальність, адміністративно-правова відповідальність, дисциплінарно-правова відповідальність, цивільно-правова відповідальність та міжнародно-правова відповідальність. З наведеного переліку очевидно, що результатом наукової класифікації інформаційно-правової відповідальності за інформаційні делікти є такі її види, які сформувалися відповідно з логікою правового регулювання інформаційних правовідносин.

В контексті формування та розвитку вітчизняного інформаційного законодавства, його залежності від галузевої належності норм, що встановлюють санкції за конкретні інформаційні делікти, поряд з актуальністю розробки Інформаційного Кодексу України, виникає проблема інкорпорації інформаційно-деліктного законодавства [57].

«Для використання інструментарію сприяння законній діяльності громадян потрібно реалізувати в законодавстві кілька принципів, стандартних для законодавства демократичних країн. Головним є не назва принципів, а їх зміст та реалізація в нормах законодавства, які відображаються у співвідношенні правових механізмів реалізації регулятивних та охоронних функцій держави в нормах адміністративної діяльності. Важливим є реалізація одночасно обох функцій за демократичними стандартами. В українському законодавстві є проблеми реалізації за двома напрямками діяльності та їх правового регулювання.

До відповідальності у сфері, пов’язаній з публічним управлінням потрібно підходити за певними принциповими основами, сформованими для

сфер, які потребують стандартизації відносин у певній сфері господарської діяльності. Це здійснюється в межах адміністративного права і адміністративної діяльності» [58]..

«Адміністративне право і стає адміністративним, а не управлінським, коли воно змінює характер на захисний, відносно реалізації прав та інтересів громадян. Сучасне адміністративне право сутнісне залишається поліцейським (управлінським), зважаючи на характер його спрямованості. В першу чергу, спрямованість проглядається за правовими інструментами (засобами), які для цього використовуються. Зокрема, адміністративна відповідальність повинна відігравати роль не покарання, а стимулювання до дотримання норм законодавства, яке визначає позитивний сценарій взаємодії громадян і держави на основі соціальної угоди суспільства і держави. Такий підхід відмінний від радянського карального, де покарання є інструментом реалізації цілей державного апарату, незважаючи на права та інтереси громадян.

Ми вже зазначали, що важливими є обидва напрямки діяльності (регулятивний і охоронний), правове регулювання яких фактично здійснюється в межах однієї норми діяльності в певній сфері зі складною конструкцією.

Гіпотеза та диспозиція регулятивної норми визначають перелік зобов’язань, виконання яких потрібне для реалізації у законний спосіб права або законного інтересу суб’єкта приватного права [58].

У загальній нормі діяльності санкцію відіграє складова, яка визначає, яке зобов’язання, з необхідних в регулятивній частині нормі не виконане і які заходи врегулювання передбачаються для компенсації негативних наслідків.

Порушення регуляторних норм передбачає їх урегулювання різними засобами, не завжди пов’язаними з відповідальністю. Охоронні норми мають свою специфічну конструкцію, відміну від регуляторних норм, але тісно пов’язану із змістовною складовою позитивних зобов’язань, за порушення яких передбачено санкцію. Можна вести мову про повноту правової визначеності регуляторних норм, від якої залежить законність застосування відповідальності.

Законність застосування санкції залежить також від повноти правової визначеності охоронних норм.

Таким чином утворюється конструкція загальної комбінованої норми, яка складається з двох та ефективність якої визначається найслабшою ланкою у зв'язці регулятивної та охоронної складових, тоді властивості законодавства в цілому, визначаються якістю загальної норми.

Якість загальних охоронних норм є більш усталеною в історичному та організаційному плані за існування багаторічного тотального карального права. Щодо якості регуляторних норм існує багато проблем, теоретичного та практичного плану. Проблеми у сфері правової охорони дії регуляторних норм в тому, що регуляторна норма повинна бути частиною диспозиції охоронної, і від якості регуляторної норми залежить загальне регулювання цілої сфери діяльності» [58].

Охарактеризуємо у загальному плані відповідальність за правопорушення в інформаційній сфері, не заглиблюючись у склади кримінальних та адміністративних деліктів, оскільки це є предметом окремих досліджень у сфері кримінальної та адміністративної відповідальності.

Кримінальна відповідальність

Аналіз сучасного стану кримінального законодавства показує, що криміналізація суспільно небезпечних діянь у сфері інформаційної безпеки відбувається переважно шляхом: а) формування в структурі Особливої частини КК України самостійних груп злочинів (розділів), які посягають на однорідні за об'єктом суспільні відносини, цінності та блага; б) конструювання окремих складів злочинів, які розміщуються в інших розділах Особливої частини КК.

У Кримінальному кодексі України існує Розділ XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», який включає шість статей:

Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

Стаття 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут

Стаття 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

Стаття 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

Стаття 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 обробляється.

Стаття 363-1. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку [59].

Об’єктами статей цього розділу є правопорушення у сфері інформаційної безпеки.

На думку В.А. Мисливого наявні у розділі XVI КК України статті не лише не створюють оптимальної системи охорони інформаційної інфраструктури, особливостей порядку доступу до інформації в цій системі, а також незаконного впливу на телекомунікації, але й обумовлюють ситуації суперечливої конкуренції між ними, зокрема між складами злочинів, передбачених статтями 361 та 362 КК України, особливо коли зазначені діяння

вчиняються у співучасті загальними та спеціальними суб'єктами. Не витримує критики, на наш погляд, ускладнене формулювання назви цього розділу КК України, яке, до речі, не дає точного уявлення стосовно родового об'єкта цих злочинів, а також вдаються зайве перевантаженими назви кримінально-правових норм. У всякому разі, на наш погляд, цілком беззастережним та відповідним Конституції України було б погодитись з думкою вчених, які пропонують сформулювати назву відповідного розділу КК України як «Злочини проти інформаційної безпеки та інформаційних технологій.

Для побудови в структурі Особливої частини КК України більш досконалої системи норм, які б забезпечували більш ефективну кримінально-правову охорону суспільних відносин у сфері інформаційної безпеки та інформаційних технологій, вченим цієї галузі разом з представниками юридичної науки необхідно розробити сучасну модель, досконалу парадигму системи інформаційних суспільних відносин та інформаційних технологій, визначити її структуру та основні елементи. Наявність такої моделі дозволить з'ясувати найбільш оптимальні підходи щодо більш цілеспрямованих наукових досліджень потреб криміналізації суспільно небезпечних діянь та формування їх системи у кримінальному законодавстві України» [60].

Для кримінальної відповідальності доцільний підхід, з огляду зв'язку відповідальності з регулятивними нормами у сфері інформаційної безпеки та складів кримінальних правопорушень, передбачених в Конвенції Про кіберзлочинність, в якій теж застосовано підхід за сферами регулювання інформаційних відносин.

Адміністративна відповідальність

Серед заходів юридичного впливу, встановлених різними галузями права, адміністративна відповідальність у сфері забезпечення інформаційної безпеки посідає одне з головних місць поряд із відповідальністю кримінальною, оскільки охоплює доволі значний обсяг суспільних відносин в інформаційній сфері. Єдиним кодифікованим законодавчим актом, який містить склади адміністративних правопорушень у сфері інформаційної безпеки та передбачає

заходи адміністративної відповідальності за її порушення, є Кодекс України про адміністративні правопорушення [61].

Про особливе значення КУпАП [62] у сфері забезпечення інформаційної безпеки говорить О.М. Шевчук, щоправда наголошуючи при цьому на необхідності зосередження на державно-управлінській сфері суспільних відносин, «тобто на тих правопорушеннях, які перешкоджають ефективному забезпеченню інформаційної безпеки органами виконавчої влади» [63, с. 67].

У Кодексі України про адміністративні правопорушення передбачено 49 складів адміністративних проступків в інформаційній сфері, які містяться у різних главах кодексу.

Докладний аналіз, здійснений Т.С. Перуном, складів адміністративних правопорушень у сфері інформаційної безпеки, які містяться в КУпАП дозволив розподілити їх на три групи, а саме: а) забезпечення доступу фізичних та юридичних осіб до публічної інформації, необхідної для реалізації їх прав, свобод та законних інтересів; б) забезпечення обмеження доступу до певних відомостей, розповсюдження яких може спричинити негативний вплив правам та свободам громадян, законній діяльності юридичних осіб, або національній безпеці; в) забезпечення безпеки у сфері медіа-інформації.

Враховуючи той факт, що переважна більшість норм КУпАП у сфері забезпечення інформаційної безпеки мають бланкетний характер, спробуємо дослідити їх юридичний зв'язок з законодавчими актами, що регулюють відносини у галузі інформаційної безпеки.

1. Доступ фізичних та юридичних осіб до публічної інформації, необхідної для реалізації їх прав, свобод та законних інтересів має конституційну основу та забезпечується низкою законодавчих актів, провідне місце серед яких посідає Закон України від 02.10.1992 «Про інформацію» та Закон України від 13.01.2011 «Про доступ до публічної інформації».

Частина 1 статті 34 Конституції України закріплює право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір. Пошук інформації становить ключовий елемент в

системі заходів щодо реалізації конституційних прав в інформаційній сфері. Цей висновок підтверджує й Л.В. Кузенко, який зазначає, що пошук тієї або іншої необхідної громадянинові інформації і складає значну частину офіційних взаємин, які виникають між ним і державою.

У той же час, Закон України «Про інформацію» деталізує конституційні положення. Наприклад, визначаючи у ч.1 ст.1 коментованого закону терміни, що в ньому вживаються, законодавець розтлумачив захист інформації не тільки як сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують її збереження та цілісність, але й передбачив необхідність належного порядку доступу до інформаційних ресурсів.

Таким чином, відповідно до статті 11 Закону України «Про інформацію», кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом.

Однією з гарантій забезпечення права на доступ до публічної інформації, відповідно до статті 3 Закону України «Про доступ до публічної інформації» виступає юридична відповідальність, яка проявляється у адміністративно-правових приписах КУпАП [61].

2. За твердженням Нестеренко О.В. право на доступ до інформації не є абсолютним, але обмеження доступу до інформації можливе лише на підставі закону. Учена визначає вимоги до витребуваної на законних підставах інформації, згідно з якими вона повинна стосуватися легітимної мети, визначеної законом; розголошення цієї інформації мало б завдати суттєвої шкоди цій меті; шкода від розголошення цієї інформації має бути вагомою, ніж суспільний інтерес в отриманні цієї інформації [64, с.11].

Забезпечення обмеження доступу до певних відомостей, розповсюдження яких може спричинити негативний вплив правам та свободам громадян, законній діяльності юридичних осіб, або національній безпеці передбачено низкою законодавчих актів. Наприклад, відповідно до ч.2 ст. 34 Конституції України здійснення прав щодо вільного збирання, зберігання, використання і

поширення інформації може бути обмежене у визначених законом випадках [61].

3. Аналізуючи положення КУпАП, можна виділити наступні склади адміністративних правопорушень у сфері інформаційної безпеки, родовим об'єктом яких є медіа-простір: порушення правил реалізації, експлуатації радіоелектронних засобів та випромінювальних пристроїв, а також користування радіочастотним ресурсом України (ст. 146); порушення правил охорони ліній і споруд зв'язку (ст. 147); порушення Правил надання та отримання телекомунікаційних послуг (ст. 148-1); порушення порядку та умов надання послуг зв'язку в мережах загального користування (ст. 148-2); використання засобів зв'язку з метою, що суперечить інтересам держави, з метою порушення громадського порядку та посягання на честь і гідність громадян (ст. 148-3); використання технічних засобів та обладнання, що застосовуються в мережах зв'язку загального користування, без документа про підтвердження відповідності (ст. 148-4); порушення правил про взаємоз'єднання телекомунікаційних мереж загального користування (ст. 148-5); демонстрування і розповсюдження фільмів без державного посвідчення на право розповсюдження і демонстрування фільмів (ст. 164-6); порушення умов розповсюдження і демонстрування фільмів, передбачених державним посвідченням на право розповсюдження і демонстрування фільмів (ст. 164-7); недотримання квоти демонстрування національних фільмів при використанні національного екранного часу (ст. 164-8); незаконне розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних (ст. 164-9); невиконання законних вимог національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації (ст. 188-7) [61].

Навіть побіжний аналіз зазначених статей КУпАП дає можливість зробити висновок, що законодавець не передбачив норми, що встановлюють адміністративну відповідальність за підставами, зазначеними у ч.2 ст.6 Закону України «Про телебачення і радіомовлення», тобто не приділяв уваги

встановленню адміністративної відповідальності за зміст та якість медіа-контенту телерадіо- організацій.

Таким чином, можемо констатувати, що нормативно-правове забезпечення адміністративної відповідальності у сфері забезпечення інформаційної безпеки проявляється у недостатньому охопленні адміністративно-правовими нормами усієї сукупності суспільних відносин в інформаційній сфері. Також у нормах КУпАП залишаються не врегульованими питання щодо встановлення відповідальності за зміст та якість медіа-контенту телерадіо- організацій [61].

Метою сучасного адміністративно-деліктного права є «виховання особи, яка вчинила адміністративне правопорушення, в дусі додержання законів України, поваги до правил співжиття, а також запобігання вчиненню нових правопорушень як самим правопорушником, так і іншими особами» ст.23. КУпАП.

Властивості законодавства в цілому визначаються якістю загальної правової норми у зв'язці регулятивної та охоронної складових. Якість загальних охоронних норм є більш усталеною в історичному та організаційному плані за існування багаторічного тотального карального права. Щодо якості регуляторних норм та їх правової охорони існує багато проблем, теоретичного та практичного плану. Основні проблеми у сфері охорони регуляторних норм в тому, що регуляторна норма повинна бути частиною диспозиції охоронної, і від якості регуляторної норми залежить загальне регулювання цілої сфери діяльності [58].

Таким чином, розробка і прийняття Інформаційного кодексу України дозволить наблизити зміст норм відповідальності до регулятивних норм, що не тільки підвищить якість норм, що містять склади правопорушень, але й сприятимуть підвищенню ефективності кримінальної та адміністративної відповідальності за інформаційні делікти.

Науковці у сфері інформаційного права вже давно наголошують на необхідності прийняття Інформаційного кодексу України. Провідною ідеєю прийняття такого кодексу повинні бути основні потреби щодо:

– кодифікації основ регулятивного та охоронного інформаційного законодавства;

– підвищення якості дії регулятивних норм, шляхом перенесення в кодекс норм відповідальності за делікти в інформаційній сфері.

2.4. Напрями розвитку правового забезпечення інформаційної безпеки України в умовах гібридної війни

Аналіз стану розвитку інформаційного суспільства повністю відображає і стан розвитку інформаційної безпеки взагалі.

При наявності фахівців найвищої якості відсутнє залучення цих фахівців до підвищення рівня, про це свідчить відсутність програм і виділення необхідних грошей.

Абсолютної безпеки нема рівень безпеки визначається грошима які виділяються на її забезпечення.

«Поглиблення міжнародного співробітництва для консолідованого протистояння гібридній агресії РФ є вкрай важливим, але ключові причини його успішності знаходяться всередині держави. А тому й зусилля з розбудови державних можливостей України протистояти гібридним загрозам стосуються переважно внутрішнього виміру» [26].

Головною небезпекою гібридної війни РФ на всіх етапах є використання громадськості у процесі досягнення поставлених агресором цілей через інформаційно-пропагандистський вплив на їхню свідомість, стимулювання недовіри до державних і правоохоронних органів, нав’язування переконання, що життя у державі-агресорі краще, у порівнянні з державою-жертвою, та зниження рівня безпеки суспільства в цілому.

Як відзначає Національний інститут стратегічних досліджень у своїй монографії «Світова гібридна війна: Український фронт», вперше Путін випробував контрольований медіаресурс як інформаційну зброю у поєднанні з військовими діями під час агресії Росії проти Грузії у 2008 році. Відпрацьовані інформаційно-пропагандистські механізми потім були використані в Україні: швидке та масштабне наповнення зони бойових дій контрольованими російськими журналістами; спроба монополізувати контроль за наданням контенту із зони бойових дій; продукування фейків; направлення до зони бойових дій російських діячів культури; використання найманих іноземних журналістів. Кремль зробив висновки з невдач інформаційного висвітлення війни проти Грузії та більш уважно поставився до можливостей і потреб інформаційного інструменту. Бюджет Russia Today був збільшений з 30 до 100 млн. дол. США, а в останні роки він сягнув 250 млн. дол. США. З метою поширення інформаційно-пропагандистського продукту на закордонну аудиторію, на базі «РИА Новости» і радіокомпанії «Голос России» була сформована «МИА Россия сегодня», з бюджетом 99,7 млн. дол. США у 2016 році, у складі якої був створений новий інформаційний інструмент Sputnik, що поширює інформацію більш як 30-ма мовами у десятках країн, переважно Європи, досягнувши рівня місцевого ньюсмейкера [26].

Для протистояння і протидії таким серйозним викликом необхідні державні програми і їх бюджетне забезпечення.

На тлі російської агресії перед Україною постали декілька взаємопов'язаних задач у контексті інформаційних викликів. Потребувала негайного вирішення проблема невідповідності національного законодавства новим викликам інформаційної війни. Незважаючи на велику кількість нормативних актів у інформаційній сфері, не вдалося подолати причини і наслідки інформаційної агресії, яка більшістю (51,4%) українських експертів названа головним фактором уразливості українського суспільства [26].

Важливим при цьому є декілька факторів за можливістю впливу на стан безпеки:

1) Економічна база;
2) Наявність проблем розвитку інформаційного суспільства в цілому;
3) Політична воля для розв'язання проблем;
4) Усвідомлення та знаннєве забезпечення розв'язання проблем;
5) Правове забезпечення розв'язання проблем;
6) Організаційно-кадрове забезпечення реалізації правових норм.

Якість правового забезпечення в першу чергу залежить в першу чергу від чотирьох перших критеріїв, оскільки якість правове забезпечення ІБ (якості інформаційного законодавства) є продуктом інформаційної політики держави (діяльності із формування інформаційної політики)..

Загострення інформаційної безпеки і напрямків її реалізації відбулося з 2014 року.

У 2015 році розпочалася робота над концептуальними документами в сфері інформаційної безпеки. У рамках роботи Експертної ради при МІП України було розроблено Доктрину інформаційної безпеки України та Концепцію інформаційної безпеки України. Хоча цей процес носив відкритий та інклюзивний характер, не всі напрацювання вдалося втілити в життя. Наприклад, Концепція інформаційної безпеки так і залишилася на стадії проекту. Схвалена в лютому 2017 року Доктрина інформаційної безпеки визначає пріоритети та національні інтереси України в інформаційній сфері, загрози для їх реалізації. Однак, вона не стала основою для розробки цілісної нормативної системи інформаційної безпеки держави.

Реформування інформаційного та медіа простору відбувається за кількома основними напрямками, що опосередковано впливають на стан інформаційної безпеки. Законом України «Про реформування державних та комунальних друкованих засобів масової інформації» запущено процес роздержавлення та зменшення впливу державних органів влади і місцевого самоврядування на редакційну політику. Іншим напрямом реформування стало створення суспільного мовлення в Україні. Нині ці реформи ще не досягли завершальної стадії.

Закон України «Про систему іномовлення України» дав старт роботі над створенням українського інформаційного контенту для закордонного споживача. 1 жовтня 2015 року відбувся запуск Мультимедійної платформи іномовлення України, що об'єднав ресурси телеканалу UA|TV та «Укрінформу». З квітня 2016 року почалася активна фаза переформатування.

У жовтні 2016 року уряд схвалив розроблену МІП Концепцію популяризації України у світі та просування інтересів України у світовому інформаційному просторі. Концепція базується на системному підході та максимальному залученні всіх зацікавлених сторін. У 2017 році був розроблений План заходів на виконання Концепції із залученням профільних міністерств і відомств. У 2017 році при МІП була створена міжвідомча комісія з популяризації України у світі. Втім, на сьогодні вона фокусується на питаннях розробки національного бренду.

Українське громадянське суспільство відіграє важливу роль у реалізації політики інформаційної безпеки — від участі у громадських та експертних радах до реалізації конкретних проектів інформаційного спротиву та популяризації України. Деякі громадські активісти в інформаційній сфері навіть пішли на державну службу для продовження і посилення цієї діяльності [26].

Загалом на законодавчому та інституційному рівнях робота з формування відповідної системи захисту кіберпростору розпочалася ще в 2014 році. Тривала розробка Стратегії забезпечення кібернетичної безпеки України, законопроекту «Про кібернетичну безпеку України», було розпочато створення національного центру кіберзахисту та протидії кіберзагрозам, національного центру оперативно-технічного управління мережами телекомунікацій України для забезпечення потреб обороноздатності держави в особливий період 79. У Стратегії національної безпеки України 2015 року вперше сформульовано загрози кібербезпеці та безпеці інформаційних ресурсів, а також визначено пріоритети забезпечення кібербезпеки. Втім, робота просувається повільно.

У березні 2016 року Президент України П. Порошенко підписав указ, яким увів у дію рішення РНБОУ від 27 січня 2016 року «Про Стратегію кібербезпеки України». Кабінету міністрів, СБУ та СЗР було доручено розробляти і виконувати щорічні плани заходів із реалізації цієї Стратегії. На її виконання у червні 2016 року в РНБОУ був створений Національний координаційний центр кібербезпеки. Серед значимих заходів Центру є розгортання національної телекомунікаційної мережі та створення захисного ІТ-контуру для захисту державних інформаційних ресурсів та об'єктів критичної інфраструктури.

23 серпня 2016 року була ухвалена постанова КМУ №563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави». У лютому 2017 року указом Президента введено в дію рішення РНБОУ «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації».

У вересні 2017 року Верховна Рада України схвалила закон «Про основні засади забезпечення кібербезпеки України». Закон розширює та уточнює положення Стратегії кібербезпеки України, визначає терміни у сфері кіберзахисту із врахуванням термінології ЄС і НАТО. Зокрема, визначено, що основними суб'єктами з кіберзахисту є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, СБУ, Міноборони та Генеральний штаб ЗСУ, розвідувальні органи і Національний банк України. Ці стратегічні документи визначають досягнення відповідних стандартів у сфері кібербезпеки стандартам ЄС і НАТО [26].

На початку липня 2017 року між НАТО та СБУ підписано угоду «Про реалізацію Трастового фонду Україна — НАТО з питань кібербезпеки». Допомога спрямована на побудову мережі ситуаційних центрів реагування на комп'ютерні інциденти і розгалуженої мережі автоматизованих датчиків подій, інтегрованих в інформаційні мережі об'єктів критичної інформаційної структури.

План заходів на 2017 рік з реалізації Стратегії кібербезпеки України передбачив імплементацію Директиви 2008/114/ЄК щодо захисту критичної інфраструктури, зокрема, з питань кібербезпеки та кіберзахисту об'єктів критичної інфраструктури. Крім того, заплановано розроблення проекту Дорожньої карти з наближення законодавства України до законодавства ЄС у сфері телекомунікацій. У вересні 2017 року, під час першого двостороннього діалогу щодо кібербезпеки між Україною та США, Вашингтон оголосив про намір виділити понад 5 млн. доларів у рамках нової допомоги Україні в галузі кібербезпеки [26].

У протистоянні інформаційним загрозам Україна досягла значних успіхів, навіть зважаючи на низький рівень початкової готовності до відсічі агресії. Втім, досягнуті позитивні трансформації не можуть гарантувати надійну захищеність національних інтересів України від майбутніх проявів російської інформаційної агресії, адже російська сторона має значну перевагу в засобах ведення інформаційної війни та постійно адаптує нові інструменти і технології підривної діяльності [26].

У процесі оборонного планування розвинених країн, зокрема США, Канади, Австралії та НАТО, застосовується програмно-цільовий метод, орієнтований на можливості. Під терміном «можливості» при розробці оборонних планів, наприклад, Австралії розуміють досягнення бажаного ефекту в певному середовищі протягом конкретного періоду часу і підтримання цього ефекту протягом встановленого періоду часу.

Вже було узагальнено закордонний досвід, який дозволив визначити такі пріоритетні напрями реалізації державної інформаційної політики в Україні:

– модернізація інфраструктури національного інформаційного простору Україні;

– впровадження системи електронного урядування; інформатизація діяльності державного апарату та процесу підготовки і прийняття найважливіших соціально значущих управлінських рішень; створення електронних баз даних, корпоративних та політико-управлінських мереж;

– гармонізація вітчизняних стандартів та норм в інформаційній сфері зі світовими стандартами;

– розвиток системи інформаційної безпеки України, включаючи удосконалення форм, методів і засобів виявлення, оцінки та прогнозування загроз інформаційній безпеці України, а також системи протидії цим загрозам;

– розширення взаємодії з міжнародними органами і організаціями щодо боротьби з кіберзлочинністю;

– забезпечення умов для активної участі України в процесах створення і використання глобальних інформаційних мереж і систем;

– підвищення інформаційної культури громадян;

– створення єдиної системи підготовки кадрів в сфері інформаційної безпеки та інформаційних технологій [65]..

С. Гордієнко справедливо вважає, що в Україні на сьогодні відсутні ознаки політики інформаційної безпеки України, хоча теоретико-прикладних та науково-обґрунтованих теорій її забезпечення існує чимало. Тобто влада на свій розсуд приймає правові положення без їх теоретичного обґрунтування, що й призводить до появи зазначених міністерств та еклектичних нормативно-правових актів [66].

Відсутність політичної волі у прийнятті законодавства про інформаційну безпеку та підтверджена рівнем розвитку інформаційного суспільства (80 місце у світі), дивись вище.

Під час гібридної війни, потрібно приділити значну увагу розвитку інформаційної безпеки, в першу чергу, визначивши та уніфікувавши загальні положення інформаційної безпеки держави та низки правових норм, які охоплюють такі надважливі її складові:

1) наукові й політичні основи теорії інформаційної безпеки;

2) концепції як система поглядів на зміст і напрямки розвитку інформаційної безпеки;

3) загальний план реалізації концепції в діяльності із забезпечення інформаційної безпеки, який охоплює тривалий період, спосіб досягнення

складної мети;

4) конкретний план етап реалізації загального плану в діяльності із забезпечення інформаційної безпеки;

5) трансформація положень плану розвитку інформаційної безпеки в нормативно-правові акти, які регламентують діяльність у різних галузях суспільної діяльності та сферах національної безпеки;

6) забезпечення державою стратегічних і тактичних напрямів розвитку і захисту національного інформаційного простору, цілісної державної інформаційної політики;

Такий системний підхід може бути реалізований в межах одного нормативно-правового акта, зокрема, в «Концепції інформаційної безпеки», або у низці нормативно-правових актів. Такі заходи і правові норми повинні бути узгоджені з правовим забезпеченням розвитку інформаційного суспільства в Україні.

Висновок до розділу 2

На думку Остроухова В.В. нормативна база інформаційної безпеки повинна виконувати в першу чергу три основні функції:

1. Регулювати взаємовідносини між суб'єктами інформаційної безпеки, визначати їх права, обов'язки та відповідальність.

2. Нормативно забезпечувати дії суб'єктів інформаційної безпеки на всіх рівнях, а саме – людини, суспільства, держави.

3. Встановлювати порядок застосування різних сил і засобів забезпечення інформаційної безпеки.

На нашу думку, важливим є створення правової бази на основі поєднання основоположних ідей правового регулювання інформаційної сфери та принципів забезпечення національної безпеки. Адже інформаційна безпека є

складовою системи національної безпеки і водночас виступає властивістю інформаційної сфери суспільства.

Навели основні положення законодавства, що безпосередньо означає правові основи інформаційної безпеки, необхідні для подальшого аналізу та визначення напрямків розвитку правового забезпечення інформаційної діяльності.

Особливого значення на сучасному етапі розвитку України набувають питання інтеграції до правової системи ЄС.

У контексті євроінтеграції України актуалізується проблема вивчення досвіду становлення інформаційного суспільства у країнах - членах Європейського Союзу, а також імплементації норм правових актів ЄС в інформаційне законодавство України.

Вищезгадана діяльність відповідає напрямам Програми інтеграції України до ЄС.

Важливою складовою правового забезпечення інформаційної безпеки є юридична відповідальність за порушення інформаційного законодавства.

Для кримінальної відповідальності доцільний підхід, з огляду зв'язку відповідальності з регулятивними нормами у сфері інформаційної безпеки та складів кримінальних правопорушень, передбачених в Конвенції Про кіберзлочинність, в якій теж застосовано підхід за сферами регулювання інформаційних відносин.

Таким чином, розробка і прийняття Інформаційного кодексу України дозволить наблизити зміст норм відповідальності до регулятивних норм, що не тільки підвищить якість норм, що містять склади правопорушень, але й сприятимуть підвищенню ефективності кримінальної та адміністративної відповідальності за інформаційні делікти.

Науковці у сфері інформаційного права вже давно наголошують на необхідності прийняття Інформаційного кодексу України. Провідною ідеєю прийняття такого кодексу повинні бути основні потреби щодо:

– кодифікації основ регулятивного та охоронного інформаційного законодавства;

– підвищення якості дії регулятивних норм, шляхом перенесення в кодекс норм відповідальності за делікти в інформаційній сфері.

Аналіз стану розвитку інформаційного суспільства повністю відображає і стан розвитку інформаційної безпеки взагалі.

При наявності фахівців найвищої якості відсутнє залучення цих фахівців до підвищення рівня, про це свідчить відсутність програм і виділення необхідних грошей.

Абсолютної безпеки нема рівень безпеки визначається грошима які виділяються на її забезпечення.

С. Гордієнко справедливо вважає, що в Україні на сьогодні відсутні ознаки політики інформаційної безпеки України, хоча теоретико-прикладних та науково-обґрунтованих теорій її забезпечення існує чимало. Тобто влада на свій розсуд приймає правові положення без їх теоретичного обґрунтування, що й призводить до появи зазначених міністерств та еклектичних нормативно-правових актів [66].

Відсутність політичної волі у прийнятті законодавства про інформаційну безпеку та підтверджена рівнем розвитку інформаційного суспільства (80 місце у світі), дивись вище.

Під час гібридної війни, потрібно приділити значну увагу розвитку інформаційної безпеки, в першу чергу, визначивши та уніфікувавши загальні положення інформаційної безпеки держави та низки правових норм, які охоплюють такі надважливі її складові:

1) наукові й політичні основи теорії інформаційної безпеки;

2) концепції як система поглядів на зміст і напрямки розвитку інформаційної безпеки;

3) загальний план реалізації концепції в діяльності із забезпечення інформаційної безпеки, який охоплює тривалий період, спосіб досягнення складної мети;

4) конкретний план етап реалізації загального плану в діяльності із забезпечення інформаційної безпеки;

5) трансформація положень плану розвитку інформаційної безпеки в нормативно-правові акти, які регламентують діяльність у різних галузях суспільної діяльності та сферах національної безпеки;

6) забезпечення державою стратегічних і тактичних напрямів розвитку і захисту національного інформаційного простору, цілісної державної інформаційної політики;

Такий системний підхід може бути реалізований в межах одного нормативно-правового акта, зокрема, в «Концепції інформаційної безпеки», або у низці нормативно-правових актів. Такі заходи і правові норми повинні бути узгоджені з правовим забезпеченням розвитку інформаційного суспільства в Україні.

ВИСНОВКИ

У дипломній роботі наведено теоретичне узагальнення й вирішення поставленого наукового завдання, що полягає у визначенні основ правового забезпечення інформаційної безпеки в умовах гібридної війни. За результатами дисертаційної роботи сформульовано такі основні висновки:

1. Розглянуто основні проблеми безпеки соціальних систем, які дають підстави зробити висновок про те, що їх теоретичний аналіз і розробка розпочалися нещодавно. Донині у спеціальній літературі триває несистемний розгляд базових законів та закономірностей функціонування й розвитку соціальних систем, формулюються та уточнюються основні категорії, поняття й терміни.

2. Удосконалено основні поняття сфери інформаційної безпеки, серед яких:

Інформаційна безпека – це стан систем, пов’язаних з обігом (створенням, поширенням, перетворенням і використанням) інформації, формуванням і використанням інформаційних ресурсів, функціонування інформаційних систем, при якому забезпечено якості таких систем, необхідні для реалізації інтересів і задоволення потреб фізичних та юридичних осіб в інформаційній сфері.

Забезпечення інформаційної безпеки – вжиття заходів щодо зменшення загального рівня небезпеки систем, пов’язаних з обігом інформації за рахунок передбачення умов, коли може бути завдана шкода, розробка та вжиття заходів і засобів, які зменшать або ліквідують ризик завдання шкоди.

Інформаційна безпека держави – це стан інститутів держави і суспільства в структуру яких входять підсистеми, пов’язані з обігом (створенням, поширенням, перетворенням і використанням) інформації, формуванням і використанням інформаційних ресурсів, функціонування інформаційних

систем, необхідні для реалізації інтересів і задоволення потреб фізичних та юридичних осіб в інформаційній сфері.

Інформаційне законодавство – сукупність нормативно-правових актів, окремих норм (іноді їх називають інформаційно-правовими нормами), положень міжнародних договорів, які регулюють відносини, пов'язані з реалізацією конституційного права кожного на інформацію, зі здійсненням інформаційної діяльності та її публічно-правовим регулюванням.

4. Під час розгляду питань інформаційної безпеки держави в Україні визначено сукупність проблем, серед яких такі:

1) недостатня теоретична розробленість категорій безпеки, методології її дослідження та забезпечення у сфері державно-правової організації соціальних систем;

2) визначення інформаційної безпеки держави пов'язане з визначенням пріоритетності завдань держави (реальних, а не фіктивних, що тільки декларуються), на які будуть спиратися при визначенні ефективності забезпечення національної безпеки;

3) безпека – категорія конкретна, треба визначати підстави й умови результативного функціонування тієї чи іншої інформаційної системи за всіма напрямками діяльності, а у сфері правової організації публічної діяльності не дуже прагнуть розраховувати комплексні показники на сучасному етапі розвитку держави;

4) інформаційна система держави – система стосовно якої традиційно не прийнято розглядати ефективність її роботи багатоаспектно, тобто ефективність виконання системою усіх суспільних функцій інформаційної політики України і правової забезпеченості її виконання на необхідному для держави рівні, що мається на увазі при визначенні інформаційної безпеки держави як складової національної безпеки;

5) практична реалізація заходів безпеки передбачає побудову зрозумілої та обґрунтованої структури забезпечення безпеки (правової, кадрової, інформаційної, матеріально-технічної) за всіма напрямками діяльності, що є

достатньо складним завданням не тільки для окремого державного органу, але і для держави в цілому.

5. Визначено, що предмет правового забезпечення інформаційної безпеки утворюється сукупністю суспільних відносин, пов'язаних з інформацією, інформаційною діяльністю, інформаційною інфраструктурою і правовим статусом суб'єктів інформаційної сфери, що належать до об'єктів національних інтересів, а також із проявом загроз безпеці цих об'єктів.

6. Правове забезпечення інформаційної безпеки держави є складовою предмету інформаційного права, зокрема, як складової адміністративного права.

Інформаційно-адміністративне право – сукупність правових норм, що регулюють інформаційно-адміністративну діяльність, пов'язану з правовим регулюванням приватної інформаційної діяльності, інформаційну діяльність публічної адміністрації з реалізації основних функцій держави, особливості юрисдикційної діяльності органів публічної адміністрації з питань правопорушень у сфері обігу інформації, формування і використання публічних інформаційних ресурсів, функціонування публічних інформаційних систем з метою забезпечення інтересів і задоволення потреб фізичних та юридичних осіб.

Фактично діяльність із забезпечення інформаційної безпеки є складовою інформаційної діяльності за усіма рівнями і сферами та норми з правового забезпечення інформаційної діяльності є складовими адміністративного права, як інформаційно-адміністративного, яке регулює правовими нормами діяльності пов'язані із забезпеченням інформаційної безпеки.

7. Проблема забезпечення інформаційної та кібербезпеки загострюється під час зовнішніх загроз, зокрема, інформаційної війни. Тобто звичайні засоби і способи інформаційної діяльності використовуються стандартні, але важливість їх передбачення у правовому регулюванні і загостренням і урахуванням зовнішніх загроз значно зростає за всіма напрямами інформаційної діяльності.

Головне завданням правового забезпечення інформаційної безпеки є перетворення змісту інформаційної політики з питань забезпечення інформаційної безпеки в якості інформаційного законодавства.

8. Визначено, що предметом розгляду правового забезпечення інформаційної безпеки є не тільки сама діяльність але й елементи, включені до системного подання цієї діяльності, тобто повна схема кооперації діяльностей учасників взаємодії при здійсненні такої діяльності – це, зокрема:

– правотворча діяльність з питань формування та реалізації інформаційної політики щодо забезпечення інформаційної безпеки;

– правозастосовча діяльність органів державної виконавчої влади на які покладено завдання із забезпечення інформаційної безпеки, які виконують її основні функції;

– діяльність суб'єктів діяльності із забезпечення інформаційної безпеки, яка залучається до системи діяльності органів державної виконавчої влади на які покладено завдання із забезпечення інформаційної безпеки;

– діяльність фахівців, які виконують забезпечувальні (ресурсні) функції із забезпечення інформаційної безпеки;

– діяльність адміністрації органів державної виконавчої влади на які покладено завдання із забезпечення інформаційної безпеки з організування, керівництва та управління діяльністю їх органів та підрозділів на різних рівнях системи.

9. Аргументовано, що важливим є створення правової бази на основі поєднання основоположних ідей правового регулювання інформаційної сфери та принципів забезпечення національної безпеки. Адже інформаційна безпека є складовою системи національної безпеки і водночас виступає властивістю інформаційної сфери суспільства.

10. Визначено, що важливою складовою правового забезпечення інформаційної безпеки є юридична відповідальність за порушення інформаційного законодавства.

Для кримінальної відповідальності доцільний підхід, з огляду зв'язку відповідальності з регулятивними нормами у сфері інформаційної безпеки та складів кримінальних правопорушень, передбачених в Конвенції Про кіберзлочинність, в якій теж застосовано підхід за сферами регулювання інформаційних відносин.

Таким чином, розробка і прийняття Інформаційного кодексу України дозволить наблизити зміст норм відповідальності до регулятивних норм, що не тільки підвищить якість норм, що містять склади правопорушень, але й сприятимуть підвищенню ефективності кримінальної та адміністративної відповідальності за інформаційні делікти.

11. Запропоновано за ідею прийняття Інформаційного кодексу України. вважати потреби щодо:

– кодифікації основ регулятивного та охоронного інформаційного законодавства;

– підвищення якості дії регулятивних норм, шляхом перенесення в кодекс норм відповідальності за делікти в інформаційній сфері.

12. Під час гібридної війни, потрібно приділити значну увагу розвитку інформаційної безпеки, в першу чергу, визначивши та уніфікувавши загальні положення інформаційної безпеки держави та низки правових норм, які охоплюють такі надважливі її складові:

1) наукові й політичні основи теорії інформаційної безпеки;

2) концепції як система поглядів на зміст і напрямки розвитку інформаційної безпеки;

3) загальний план реалізації концепції в діяльності із забезпечення інформаційної безпеки, який охоплює тривалий період, спосіб досягнення складної мети;

4) конкретний план етап реалізації загального плану в діяльності із забезпечення інформаційної безпеки;

5) трансформація положень плану розвитку інформаційної безпеки в нормативно-правові акти, які регламентують діяльність у різних галузях

суспільної діяльності та сферах національної безпеки;

6) забезпечення державою стратегічних і тактичних напрямів розвитку і захисту національного інформаційного простору, цілісної державної інформаційної політики;

Такий системний підхід може бути реалізований в межах одного нормативно-правового акта, зокрема, в «Концепції інформаційної безпеки», або у низці нормативно-правових актів. Такі заходи і правові норми повинні бути узгоджені з правовим забезпеченням розвитку інформаційного суспільства в Україні.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Заплатинський В. М. Логіко-детермінантні підходи до розуміння поняття «Безпека». Вісник Кам'янець-Подільського національного університету імені Івана Огієнка. Фізичне виховання, спорт і здоров'я людини. / [редкол.: П. С. Атаманчук (відп. Ред..) та ін.]. – Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2012. – Випуск 5. – 336 с. – С. 90-98.

2. Кунєв Ю. Д. Діяльність митної служби України : проблеми правової організації : [монографія] / Ю. Д. Кунєв. – Дніпропетровськ : Академія митної служби України, 2009. – 242 с.

3. Про національну безпеку України: закон України // Відомості Верховної Ради (ВВР), 2018, № 31, ст.241. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2469-19#n355.

4. Коваленко, Ю. О. (2010). Забезпечення інформаційної безпеки на підприємстві. Економіка промисловості (3). – С. 123–129.

5. Гурковський В.І. Безпека як об’єкт правовідносин в умовах глобального інформаційного суспільства. Правова інформатика. 2010. No 2(26). – С. 72-77

6. Калюжний Р. Питання концепції реформування інформаційного законодавства України. Правове, нормативне та метрологічне забезпечення системи інформації в Україні: Тематичний збірник праць учасників Другої науково-технічної конференції. – К., 2000. – С.17-21.

7. Кочубей Л.О. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно комунікаційних технологій у сучасному Донбасі. Наукові записки Інституту політичних і етнонаціональних досліджень імені І. Ф. Кураса. 2015. – Вип. 3. – С. 220–237.

8. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: [навчальний посібник]. – Київ: Кондор, 2004. – 382 с.

9. Корж І.Ф. Внутрішні фактори загроз і викликів інформаційній безпеці України. Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти : матеріали наук.-практ. конф. 06 жовтня. 2016 р. Упоряд. : В. М. Фурашев. – Київ : НТУУ «КПІ імені Ігоря Сікорського», Вид-во «Політехніка», 2016. – 204 с

10. Князев А. А. Информационная война. // Энциклопедический словарь СМИ. – Бишкек: Издательство КРСУ, 2002.

11. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: закон України від 09.01.2007 р. № 537-V // Відомості Верховної Ради України (ВВР), 2007, № 12, ст.102.

12. Бакалінська О., Бакалінський О. Правове забезпечення кібербезпеки в Україні // Підприємство, господарство і право. – №9. – 2019. – С. 100-108.

13. Селезньова О.М. Теоретико-методологічне трактування окремих засадничих категорій інформаційного права // ІТ право: проблеми і перспективи розвитку в Україні: збірник матеріалів науково-практичної конференції. – Львів: НУ «Львівська політехніка», 2016. – 396 с. – С. 136–142.

14. Про інформацію : закон України // Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2657-12#Text

15. Турукало Андрій. Аналіз рівня розвитку інформаційного суспільства в Україні. – Режим доступу : https://www.slideshare.net/Andrey_Turukalo/ss-76838396

16. Кунєв Ю. Д. Об’єкт правознавства: системодіяльнісний підхід // Право України. 2008. – № 3. – С. 35–38.

17. Калюжний Р.А., Марценюк О.Г. Предмет та методи інформаційного права // Правова інформатика. 2008. – № 3. – С. 5–9.

18. Красноступ Г.М. Проблема визначення об’єкта та предмета інформаційного права. Режим доступу : https://minjust.gov.ua/m/str_7949.

19. Селезньова О.М. Специфіка природи інформаційного права в контексті галузевої приналежності // Науковий вісник Ужгородського національного університету. 2014 Серія ПРАВО. Випуск 26. – С. 178–180.

20. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право / Под. ред. Б. Н. Топорнина. – СПб: Юрид. центр Пресс, 2001.

21. Yuriy Kuniev, Iryna Sopilko, Valerii Kolpakov: Object and subject of information law. Journal of law and political sciences scientific and academy journal. Vol. 23, issue 2/ 2020 P. ISSN 2222-7288 E. ISSN 2518-5551. P. 9–41. https://orcid.org/0000-0002-5952-2052

22. Шмідт-Ассманн Е. Загальне адміністративне право як ідея врегулювання: основні засади та завдання систематики адміністративного права / Ебергард Шмідт-Ассманн ; [пер. з нім. Г. Рижков, І. Сойко, А. Баканов] ; відп. ред. О. Сироїд. – К. : К.І.С., 2009. – 552 с.

23. Daniel T. Lasica. Strategic Implications of Hybrid War: A Theory of Victory — School of Advanced Military Studies, 2009.

24. Кравчук О. Ю. загрози та виклики політичній безпеці України в умовах гібридної війни. Дисертація на здобуття науково ступеня кандидата політичних наук за спеціальністю 23.00.02 «Політичні інститути та процеси» – Державний заклад «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського». – Одеса, 2019. – 221 с. – С. 111.

25. Світова гібридна війна: український фронт: монографія. – Київ: НІСД, 2017. – 496 с.

26. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і східного партнерства. Аналітичний документ. – Київ. – 2018. – 106 с.

27. Кравчук О. Ю. загрози та виклики політичній безпеці України в умовах гібридної війни. Дисертація на здобуття науково ступеня кандидата політичних наук за спеціальністю 23.00.02 «Політичні інститути та процеси» – Державний заклад «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського». – Одеса, 2019. – 221 с. – С. 119.

28. John R. Davis Jr. Defeating Future Hybrid Threats // Military Review, September-October 2013.

29. Бєлоусова Н.Б., Афанасьєва П.А. Основні вимоги НАТО щодо забезпечення безпеки інформаційного простору // Актуальні проблеми міжнародних відносин. Випуск 102 (Частина І), 2011. – С.195–202.

30. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. – Режим доступу : www.justinian.com.ua/article.php.

31. Martin C. Libicki. What is Information Warfare? United States Government Printing, Washington DC, 1995. . – Режим доступу : http://www.dodccrp.org/files/Libicki_What_Is.pdf (дата звернення: 16.12.2017).

32. Гриняев С. Взгляды военных экспертов США на ведение информационного противоборства // Зарубежное военное обозрение. – 2001. – № 8.

33. Кравчук О. Ю. загрози та виклики політичній безпеці України в умовах гібридної війни. Дисертація на здобуття науково ступеня кандидата політичних наук за спеціальністю 23.00.02 «Політичні інститути та процеси» – Державний заклад «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», – Одеса, 2019. – 221 с.

34. Tisdall S. Result of Macedonia’s referendum is another victory for Russia. The Guardian. 2018. Oct. 1. – Режим доступу : https://www.theguardian.com/world/2018/oct/01/result-of-macedonia-referendum-isanother-victory-for-russia

35. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України. Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 — адміністративне право і процес; фінансове право; інформаційне право (081 — Право). – ДВНЗ «Ужгородський національний університет», Ужгород, 2019. – 487 с.

36. Штогрін І. Називай агресію “захистом”: принципи інформаційної війни проти Росії [Електронний ресурс] / Ірина Штогрін. — Режим доступу : www.radiosvoboda.org/cntent/article/25293307.html.

37. Інформаційна війна коштує Росії 4$ мільярди. – Режим доступу : www.ukrinform.ua/ukr.news/2030605.

38. Малик Я. Інформаційна війна і Україна // Науковий вісник. – 2015. – Вип. 15 Демократичне врядування. . – Режим доступу : http://lvivacademy.com/vidavnitstvo_1/visnyk15/fail/Malyk.pdf.

39. Золотар О.О. Інформаційна безпека людини: теорія і практика : монографія. – Київ : Видавничий дім АртЕк, 2018 – 446 с. С 180-182.

40. Конвенція про кіберзлочинність. Конвенцію ратифіковано із застереженнями і заявами Законом N 2824-IV (2824-15) від 07.09.2005, ВВР, 2006, – № 5-6, – ст.71.

41. Додатковий протокол до Європейської конвенції про інформацію щодо іноземного законодавства. Про приєднання до Додаткового протоколу див. Постанову ВР N 3386-XII (3386-12) від 14.07.93. Дата набуття чинності для України: 14.09.1994.

42. Про основні засади забезпечення кібербезпеки України: закон України // Відомості Верховної Ради, 2017, № 45, ст.403.– Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19#Text

43. Про державну таємницю: закон України // Відомості Верховної Ради України (ВВР), 1994, № 16, ст.93. – Режим доступу : https://zakon.rada.gov.ua/laws/show/3855-12?find=1&text=%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86+%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA

44. Конституція України: закон України // (Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141) . – Режим доступу : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

45. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Угоду ратифіковано Законом № 1678-VII від 16.09.2014. – Режим доступу : https://zakon.rada.gov.ua/laws/show/984_011?find=1&text=%D1%96%D0%BD%D

1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0+%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0#w1_23

46. Про основні засади забезпечення кібербезпеки України: закон України // (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) . – Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19#Text

47. Про Національну програму інформатизації (Відомості Верховної Ради України (ВВР), 1998, № 27-28, ст.181) . – Режим доступу : https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80?find=1&text=%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86+%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA#w2_2

48. Концепція Національної програми інформатизації: схвалено законом України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 року № 75/98-ВР . – Режим доступу : https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80?find=1&text=%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86+%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA#w2_3.

49. Про захист інформації в інформаційно-телекомунікаційних системах: закон України // (Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286) https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80?find=1&text=%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86+%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA#w2_4.

50. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25 лютого 2017 року № 47/2017. – Режим доступу : https://zakon.rada.gov.ua/laws/show/47/2017#Text.

51. Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України. . – Режим доступу :

http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350.

52. Рекомендації парламентських слухань на тему: «Законодавче забезпечення розвитку інформаційного суспільства в Україні» : схвалено Постановою Верховної Ради України від 3 липня 2014 року № 1565-VII . – Режим доступу : https://zakon.rada.gov.ua/laws/show/1565-18#Text.

53. Пахнін М. Л. особливості державної інформаційної політики в розвинених країнах світу. Теорія та практика державного управління. – Вип. 4 (47). 2014. – С.1–9.

54. Брижко В. До питання сучасної інформаційної політики. Вісн. Академії управління МВС. 2009. – № 2. – С. 32–36.

55. Тихомирова Є.Б. Комунікативна політика ЄС: інформаційна безпека vs транспарентність. Актуальні проблеми міжнародних відносин: зб. наук. пр. Вип. 102. Ч.1. – К.: КНУ ім. Т. Шевченка, 2011. – С. 22-28.

56. Гуменюк Б. І. Сучасна дипломатична служба / Б. І. Гуменюк, О. В. Щерба. – К.: Либідь, 2001. – 255 с.

57. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / І. В. Арістова, О. А. Баранов, О. П. Дзьобань та ін.; за заг. ред. проф. К. І. Бєлякова. – Київ: КВІЦ, 2019. – 344 с. – С. 204.

58. Кунєв Ю.Д. Основи адміністративного урегулювання митних правопорушень // Юридичний вісник 2 (55) 2020. – С. 86-93.

59. Кримінальний Кодекс України // (Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131) . – Режим доступу : https://zakon.rada.gov.ua/laws/show/2341-14#n2523

60. Мисливий В.А. Кримінальна відповідальність за злочини в інформаційній сфері // Теорія і практика юридичної відповідальності за правопорушення в інформаційній сфері: Матеріали науково-практичної конференції / 08 червня 2016 р., м.Київ / Упоряд. : В.М.Фурашев, С.Ю.Петряєв.

– К.: НДІІП НАПрН України, Апарат РНБО України, КНДІСЕ Мінюсту України, НТУУ «КПІ», 2016. – 200с. – С.104–107.

61. Перун Т.С. Адміністративна відповідальність в системі заходів забезпечення інформаційної безпеки // ІТ право: проблеми і перспективи розвитку в україні (друга міжнародна щорічна конференція) . – Режим доступу : http://aphd.ua/publication-358/

62. Кодекс України про адміністративні правопорушення : Закон України. // Відомості Верховної Ради Української РСР (ВВР) 1984, додаток до № 51, ст.1122.

63. Шевчук О.М. Адміністративно-правове регулювання у сфері забезпечення інформаційної безпеки: дис. …канд. юрид. наук : спец. 12.00.07 / Шевчук Олексій Миколайович. – Класичний приватний університет, 2011. – 210 с.

64. Нестеренко О.В. Право на доступ до інформації в Україні: конституційно-правовий аспект: автореф. дис. …канд. юрид. наук: спец. 12.00.02 / О.В. Нестеренко. – Х., 2008. – 22 с.

65. Пахнін М. Л. Особливості державної інформаційної політики в розвинених країнах світу. Теорія та практика державного управління. – Вип. 4 (47), 2014. – С.1-9.

66. Гордієнко С. Доктринальні положення інформаційної безпеки України в умовах сучасності. // Юридичний вісник України від 24.03.2019.