УДК 342.9
DOI https://doi.org/10.24144/2788-6018.2023.05.62

ПРАВОВЕ РЕГУЛЮВАННЯ СФЕРИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Крупнова А.О.,
аспірант Міжнародного економіко-гуманітарного університету імені Степана Дем'янчука,
адвокат.
ORCID ID: https://orcid.org/0009-0007-7819-9813

Крупнова А.О. Правове регулювання сфери забезпечення інформаційної безпеки в Україні.

Стаття присвячена дослідженню системи правового регулювання сфери забезпечення інформаційної безпеки в Україні. Встановлено, що фундаментом системи правових актів, яка є основою правового регулювання забезпечення інформаційної безпеки в Україні, є Конституція. Після неї слідують Закони України: Про інформацію, Про захист інформації в інформаційно-комунікаційних системах, Про захист персональних даних, Про державну таємницю, Про національну безпеку України, Про основні засади забезпечення кібербезпеки України, Про електронні комунікації, Про медіа, Про авторське право і суміжні права, Про охорону прав на компонування напівпровідникових виробів, Про охорону прав на винаходи і корисні моделі, Про державну таємницю та ін. Норми, що визначають інформаційну безпеку України, знайшли подальший розвиток на підзаконному рівні. Підзаконні акти спрямовані на деталізацію окремих положень Конституції України та законів. Вони мають предметний напрямок та регламентують конкретну сферу суспільних відносин чи напрями роботи органів державного управління. На рівні центральних органів виконавчої влади у якості підзаконних актів видаються накази, інструкції та розпорядження. До складу документів, що визначають нормативно-технічну базу захисту інформації в Україні, входять також стандарти та галузеві матеріали. Вони мають ключове значення, оскільки забезпечують однаковість в галузі інформаційної безпеки, стандартизують процедури для захисту інформації, методи забезпечення конфіденційності, цілісності та доступності даних, а також заходи щодо запобігання та реагування на інформаційні інциденти. До системи правових актів, що становлять основу правового регулювання забезпечення інформаційної безпеки в Україні нами також були віднесені міжнародні акти: конвенції, декларації, резолюції та ін.

Зроблено висновок, що на сьогоднішній день нормативно-правова основа забезпечення інформаційної безпеки – це розгалужена мережа вітчизняних та міжнародних норм різної юридичної сили та спрямованості, яка у своїй сукупності забезпечує комплексне функціонування всієї системи забезпечення інформаційної безпеки в Україні.

Ключові слова: інформація, інформаційна безпека, правове регулювання, національна безпека, міжнародна інформаційна безпека.

Krupnova A. Legal regulation of information security in Ukraine.

The article is devoted to the study of the system of legal regulation of information security in Ukraine. It has been established that the Constitution is the foundation of the system of legal acts, which is the basis of legal regulation of information security in Ukraine. It is followed by the Laws of Ukraine: On Information, On Protection of Information in Information and Communication Systems, On Protection of Personal Data, On State Secrets, On National Security of Ukraine, On Basic Principles of Ensuring Cyber Security of Ukraine, On Electronic Communications, On Media, On Copyright and related rights, On the protection of rights to the composition of semiconductor products, On the protection of rights to inventions and utility models, On state secrets, etc. Norms defining information security of Ukraine have found further development at the sub-legal level. By-laws are aimed at detailing individual provisions of the Constitution of Ukraine and laws. They have a subject direction and regulate a specific sphere of social relations or areas of work of state administration bodies. At the level of central executive bodies, orders, instructions and orders are issued as by-laws. The documents defining the regulatory and technical basis of information protection in Ukraine also include standards and industry materials. They are of key importance because they ensure uniformity in the field of information security, standardize procedures for protecting information, methods for ensuring confidentiality, integrity and availability of data, as well as measures for preventing and responding to information incidents. We also included international acts: conventions, declarations, resolutions, etc.,

in the system of legal acts that constitute the basis of legal regulation of information security in Ukraine. It was concluded that today the normative and legal basis of ensuring information security is an extensive network of domestic and international norms of different legal force and focus, which in its totality ensures the comprehensive functioning of the entire system of ensuring information security in Ukraine.

Key words: information, information security, legal regulation, national security, international information security.

Постановка проблеми. Правове регулювання забезпечення інформаційної безпеки посідає важливе місце в контексті забезпечення національної безпеки кожної держави. Це пояснюється не лише тим, що інформація є фундаментальним елементом життєдіяльності сучасних соціальних систем, а й тим, що, подібно до того, як рух енергії та матерії визначає роботу біологічних і технічних систем, так і інформація є рушійною силою в сучасному світі. Правове регулювання інформаційної безпеки України є складною системою актів різної юридичної сили, що регулюють відносини у сфері протидії загрозам в інформаційній сфері. Ця система також включає активну діяльність органів державної влади та місцевого самоврядування, спрямовану на постійний розвиток та вдосконалення сфери інформаційної безпеки.

Вклад у дослідження правового регулювання сфери забезпечення інформаційної безпеки внесли: І. Арістова, О. Баранов, В. Брижко, О. Довгань, О. Золотар, І. Корж, Р. Калюжний, Б. Кормич, В. Ліпкан, А. Марущак, В. Пилипчук, В. Рубан, Г. Сащук, Я. Собків, С. Феденько, Л. Харченко, В. Шамрай та ін.

Метою статті є дослідження системи правового регулювання сфери забезпечення інформаційної безпеки в Україні.

Виклад основного матеріалу. Відомо, що ключовий аспект забезпечення інформаційної безпеки України пов'язаний із покращенням законодавчого регулювання даної сфери суспільних відносин. На сьогодні існує безліч правових актів, включаючи закони, акти Президента України, Верховної Ради України, Кабінету Міністрів України та центральних органів виконавчої влади, що регулюють питання, пов'язані з: інформаційною боротьбою; управлінням інформаційною безпекою; загрозами інформаційній безпеці держави, суспільства та людини; захистом прав і свобод людини в інформаційній сфері; видами захисту інформаційної безпеки держави, суспільства та людини; джерелами загроз інформаційній безпеці тощо. Вони також спрямовані на реалізацію мети та завдань, визначених Стратегією інформаційної безпеки.

Систему правових актів, що становлять основу правового регулювання забезпечення інформаційної безпеки в Україні, можна поділити і класифікувати:

1. Залежно від обсягу приписів, які містяться в актах, ступеня і характеру регульованих відносин:

— акти, що не містять прямих регламентуючих положень, щодо забезпечення інформаційної безпеки, проте прямо або опосередковано регулюють інформаційні відносини;

— акти, які безпосередньо регламентують забезпечення інформаційної безпеки в Україні.

2. Залежно від юридичної сили актів:

– Конституція України;

– Закони України, в тому числі «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про національну безпеку України», «Про захист персональних даних» та ін.;

– підзаконні акти – це нормативні акти Президента України, Кабінету Міністрів України, Державної служби спеціального зв'язку та захисту інформації України та ін.;

– нормативні документи в галузі технічного захисту інформації та державні стандарти України стосовно створення і функціонування комплексної системи захисту інформації;

– міжнародні акти.

Забезпечення інформаційної безпеки спирається на широкий спектр норм, що становлять правову основу даної галузі суспільних відносин. З усіх існуючих норм найбільший вплив і важливість, на нашу думку, мають норми адміністративного права. Вони охоплюють безліч ключових аспектів, пов'язаних із забезпеченням інформаційної безпеки, таких як: формування та організаційна структура системи інформаційної безпеки, взаємодія органів та структур, задіяних у забезпеченні інформаційної безпеки, адміністративна відповідальність суб'єктів, що займаються забезпеченням безпеки тощо. Поряд із адміністративним правом, важливе значення мають також норми кримінального права. Вони регулюють відносини, пов'язані з можливими кримінальними правопорушеннями у сфері інформаційної безпеки. Ці норми встановлюють повноваження та обов'язки державних органів, що входять до системи забезпечення інформаційної безпеки, а також інших органів, які мають вплив на дану сферу. Важливим аспектом є також норми цивільного права, які регулюють майнові та особисті немайнові відносини у контексті інформаційної безпеки. Ці норми визначають права та обов'язки сторін щодо власності, використання інформації, а також компенсації збитків у разі порушення інформаційної безпеки. Загалом, правова база забезпечення інформаційної безпеки в Україні включає різноманітні норми

різних галузей права, які в сукупності формують комплексний підхід до регулювання та забезпечення безпеки в інформаційній сфері.

Розглянемо детальніше нормативно-правові акти, що лежать в основі правового регулювання забезпечення інформаційної безпеки в Україні, а також визначимо специфіку регулювання ними даного виду суспільних відносин. Найважливішим правовим актом в системі правових актів, що становлять основу правового регулювання забезпечення інформаційної безпеки в Україні, є Конституція України від 28.06.1996 р. № 254к/96-ВР, будучи найвищим актом у сфері захисту інформації. У ній визначено конституційні засади права на інформацію, деякі конкретні джерела інформації, доступ до яких гарантовано державою, низку інших важливих позицій для розвитку законодавства у сфері забезпечення інформаційної безпеки. Так, згідно зі ст. 34 Конституції України: кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань [1]. Ч. 2 ст. 34 Конституції України чітко визначає, що кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. Інші інформаційні права та свободи також знайшли відповідне закріплення у статтях Конституції України: цензура заборонена (ст. 15); кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31); 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 (ст. 32); 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 (ст. 34); кожен має право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності (ст. 41); кожному гарантується право вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення. Така інформація ніким не може бути засекречена (ст. 50) [1] та ін. Значна кількість закріплених у Конституції України прав та свобод мають яскраво виражений інформаційний характер. Загалом, інформаційні права та свободи становлять цілісний екзистенційний феномен, який можна впізнати винятково крізь призму його системних властивостей і який знаходить свій прояв у наявності прав та свобод інформаційного характеру в різних сферах життєдіяльності суспільства. Можна стверджувати, що інформаційні права та свободи притаманні будь-якій сфері життєдіяльності суспільства [2; 3]. Підкреслимо, що Основний Закон відносить інформаційну безпеку до переліку найважливіших функцій держави. Так, згідно ст. 17 Конституції України: захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [1]. Як бачимо, вітчизняний законодавець на найвищому рівні прирівняв інформаційну безпеку держави до таких невід'ємних характеристик державності, як суверенітет та збереження територіальної цілісності. Це означає, що забезпечення захисту інформації та безпеки України в інформаційному середовищі розглядається як один із ключових елементів національної ідентичності та суверенних прав держави. Можна посилити дане твердження, додавши, що в сучасному інформаційному столітті, коли цифрові технології проникають у всі сфери життя, інформаційна безпека стає невід'ємною частиною державної політики та стратегії розвитку держави і суспільства.

Після Конституції законодавчу основу сфери забезпечення інформаційної безпеки в Україні становлять: Закон України «Про інформацію», Закон України «Про захист інформації в інформаційно-комунікаційних системах», Закон України «Про захист персональних даних», Закон України «Про державну таємницю», Закон України «Про національну безпеку України», Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про електронні комунікації» та ін. Так, Закон України «Про інформацію» від 02.10.1992 р. № 2657-XII регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації [4]. Він визначає основні принципи інформаційних відносин, встановлює суб'єктів і об'єкт інформаційних відносин, право на інформацію та її гарантії, поділяє інформаціє на види, окреслює загальні положення відповідальності за порушення законодавства про інформацію та ін.

Наступний рівень регулювання сфери забезпечення інформаційної безпеки в Україні становлять підзаконні акти, основна роль яких полягає у запровадженні відповідних механізмів інформаційної безпеки, які стосуються низки основних аспектів даного виду державної діяльності, а саме – стану захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії на-

несенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом. Дані акти мають важливе значення для безперебійного функціонування механізму, метою якого є забезпечення інформаційної безпеки в Україні.

Підзаконні акти спрямовані на деталізацію окремих положень Конституції України та законів. Вони мають предметний напрямок та регламентують конкретну сферу суспільних відносин або напрями роботи органів державного управління. Так, Президент України видає укази та розпорядження, де, зазвичай, укази мають загальний, а розпорядження – більш індивідуальний характер.

Особлива роль серед підзаконних актів належить Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28.12.2021 р. № 685/2021. Вона визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних [5]. Стратегія інформаційної безпеки, незважаючи на свою концептуальність, була прийнята до повномасштабного вторгнення Російської Федерації в Україну, тому даний частково є застарілим. Стратегія є документом, який був прийнятий на певному історичному етапі розвитку держави. У тому вигляді, в якому вона існує сьогодні, вона не відповідає сучасним вимогам щодо забезпечення інформаційної безпеки. Але саме цьому документу надається особливе значення при визначенні стратегічних напрямів щодо вдосконалення інформаційної безпеки України. Саме Стратегія інформаційної безпеки має виступати найвищим нормативним актом та окреслювати забезпечення інформаційної безпеки в країні за різними напрямами.

Серед важливих указів Президента України у сфері забезпечення інформаційної безпеки ми можемо виділити: Про Положення про технічний захист інформації в Україні: Указ Президента України від 27.09.1999 р. № 1229/99; Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України»: Указ Президента України від 01.05.2014 р. № 449/2014; Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 р. № 96/2016; Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України»: Указ Президента України від 01.02.2022 р. № 37/2022; Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки»: Указ Президента України від 16.02.2022 р. № 56/2022 та ін.

Чималу роль у забезпеченні інформаційної безпеки відіграє нормотворча діяльність Кабінету Міністрів України. Важливими документами у цьому напрямі стали такі постанови та розпорядження: Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах: Постанова Кабінету Міністрів України від 29.03.2006 р. № 373; Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України: Постанова Кабінету Міністрів України від 16.11.2016 р. № 821; Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова Кабінету Міністрів України від 12.03.2022 р. № 263; Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Розпорядження Кабінету Міністрів України від 04.04.2023 р. № 299; Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: Розпорядження Кабінету Міністрів України від 30.03.2023 р. № 272-р; Про затвердження плану заходів з реалізації Стратегії забезпечення державної безпеки: Розпорядження Кабінету Міністрів України від 18.04.2023 р. № 328-р та ін.

На рівні центральних органів виконавчої влади у якості підзаконних актів видаються накази, інструкції та розпорядження. Такі акти виконують функцію конкретизації та деталізації норм, встановлених законами. Вони служать для більш детального регулювання й уточнення технічних та організаційних моментів, пов'язаних із забезпеченням інформаційної безпеки в Україні. Центральні органи виконавчої влади додатково видають правила, стандарти та інструкції, яких організації та громадяни повинні дотримуватись у сфері інформаційної безпеки. Такі підзаконні акти можуть стосуватися багатьох питань, включаючи: стандарти шифрування, процедури автентифікації, вимоги до захисту даних, процедури обробки інформації, заходи щодо запобігання кібератакам та багато іншого. Вони допомагають забезпечити більш ефективне виконання нормативів, пов'язаних з інформаційною безпекою, а також забезпечують більш точне керівництво

для дій суб'єктів у даній галузі суспільних відносин.

До складу документів, що визначають нормативно-технічну базу захисту інформації в Україні, входять також стандарти та галузеві матеріали. Вони є нормативними документами, розробленими й затвердженими державними органами або спеціальними організаціями, які визначають обов'язкові вимоги до інформаційної безпеки в різних галузях діяльності. Стандарти мають ключове значення, оскільки забезпечують однаковість в галузі інформаційної безпеки, стандартизують процедури для захисту інформації, методи забезпечення конфіденційності, цілісності та доступності даних, а також заходи щодо запобігання та реагування на інформаційні інциденти. На сьогоднішній день в Україні діють наступні нормативні документи та державні стандарти, пов'язані із забезпеченням інформаційної безпеки: Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (НД ТЗІ 3.7-001-99); Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 1.1-002-99); Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 1.1-003-99); Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 2.5-004-99); Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (НД ТЗІ 2.5-005-99); Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу»; Типове положення про службу захисту інформації в автоматизованій системі (НД ТЗІ 1.4-001-2000); Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 (НД ТЗІ 2.5-008-02); Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу (НД ТЗІ 2.5-010-03); Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі (НД ТЗІ 3.7-003-05); Захист інформації. Технічний захист інформації. Порядок проведення робіт (ДСТУ 3396.1-96) та ін.

Аналіз вищенаведених стандартів показав, що у сфері інформаційної безпеки вони також включають різні питання, що стосуються криптографії, захисту мереж та інформаційних систем, вимог, що висуваються до захисту персональних даних, забезпечення безпеки при роботі з інформацією, включаючи класифікацію та маркування конфіденційних даних. Ми вважаємо, що стандарти набувають особливого значення в умовах зростаючих загроз у сфері інформаційної безпеки в Україні. Вони є основою для подальшого розвитку нормативної бази, спрямованої на впровадження ефективних заходів щодо безпеки інформації в різних секторах.

Одним із важливих завдань розвитку правової бази захисту є відповідність вітчизняних стандартів міжнародним. Розуміючи важливість даного питання, законодавець розробив Закон України «Про внесення змін до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації» від 04.06.2020 р. № 681-IX [6]. Закон був прийнятий з метою інтеграції європейських вимог та критеріїв оцінки захисту інформації від кіберзагроз з українською законодавчою системою захисту даних. Він визначив необхідність відповідності вітчизняних стандартів вимогам європейських стандартів системи управління інформаційною безпекою (Information Security Management System, ISMS) для окремих категорій інформації. В подальшому, на вимогу закону, Державною службою спеціального зв'язку та захисту інформації України був розроблений ряд стандартів, які відповідають європейським вимогам та критеріям оцінки захисту інформації від кіберзагроз, а саме: Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці (НД ТЗІ 3.6-004-21); Порядок категоріювання безпеки інформаційної системи та інформації (НД ТЗІ 3.6-005-21); Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем (НД ТЗІ 3.6-006-21); Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем (НД ТЗІ 3.6-007-21); Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем (НД ТЗІ 2.3-025-21 Т1); Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем (НД ТЗІ 2.3-025-21 Т2); Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем (НД ТЗІ 2.3-025-21 Т3); Порядок авторизації безпеки інформаційних систем (НД ТЗІ 2.6-004-21); Порядок моніторингу безпеки інформаційних систем (НД ТЗІ 3.6-008-21).

Але це лише перший крок, оскільки необхідна систематична робота щодо приведення вітчизняних стандартів у сфері інформаційної безпеки у відповідність до європейських та міжнародних стандартів. Це дозволить забезпечити більш ефективний захист інформації [7]. Адаптація вітчизняних стандартів до європейських та міжнародних має низку переваг. По-перше, вона сприяє підвищенню конкурентоспроможності та привабливості нашої країни для бізнесу та інвестицій, оскільки міжнародні компанії та організації воліють працювати в середовищі, що відповідає світовим стандартам інформаційної безпеки. По-друге, узгодження стандартів покращить співпрацю та обмін інформацією між Україною та іншими країнами, особливо з членами Європейського Союзу та іншими міжнародними організаціями, дозволить більш ефективно боротися з транскордонними загрозами та кіберзлочинністю. Також важливо відзначити, що швидкоплинна природа кіберзагроз і технологічні інновації вимагають постійного оновлення та вдосконалення стандартів. Тому перегляд вітчизняних стандартів, більшість із яких ухвалено на межі тисячоліття, є невід'ємною частиною забезпечення інформаційної безпеки в Україні. Загалом, адаптація національних стандартів інформаційної безпеки України до світових нормативів та перегляд старих норм є важливими кроками у напрямку забезпечення більш надійної та сучасної системи інформаційної безпеки для нашої країни.

Міжнародні акти також складають правову основу забезпечення інформаційної безпеки. Зазначимо, що міжнародна інформаційна безпека є одним із компонентів внутрішньої інформаційної безпеки держави. Підтримка стабільності у сфері міжнародної інформаційної безпеки є незамінним фактором для нормального розвитку міждержавних відносин у контексті обміну інформацією та використання кіберпростору. Міжнародна інформаційна безпека уособлює важливий стовп світової політики, її підтримка є не опціональною, а швидше, непорушною умовою для спокійного співіснування держав в епоху цифрової революції.

На міжнародному рівні встановлено заборону на вороже використання інформаційних технологій, наслідки якого можуть бути порівнянні з реальною озброєною агресією, також відомою як кіберагресія. Інакше кажучи, правила заборони застосування сили чи загрози силою також поширюються на інформаційний простір. Крім того, використання інформаційних технологій для підриву соціально-політичної ситуації, здійснення деструктивного інформаційного впливу та формування громадської думки шляхом поширення певної інформації також заборонено. Заборонено негативний вплив на суспільно-політичну свідомість населення, що може розглядатися як втручання у внутрішні справи держави відповідно до п. 7 ст. 2 Статуту ООН [8]. Неприпустимість такої діяльності підтверджується численними актами міжнародних організацій та конференцій, а також міжнародною судовою практикою (Декларація про неприпустимість втручання у внутрішні справи держав, про запобігання їх незалежності та суверенітету від 21.12.1965 р., Декларація про принципи міжнародного права від 24.10.1970 р., Декларація про неприпустимість інтервенції та втручання у внутрішні справи держав від 09.12.1981 р., Заключний акт Наради з безпеки і співробітництва в Європі від 01.08.1975 р., Справа про військову і воєнізовану діяльність в Нікарагуа і проти неї (Рішення «Нікарагуа проти США» від 27.06.1986 р.) та ін.). Більше того, неприпустимість деструктивного інформаційного впливу на світовому рівні також випливає з положень низки міжнародних договорів (Статут Організації Об'єднаних Націй від 26.06.1945 р., Міжнародна конвенція про ліквідацію всіх форм расової дискримінації від 21.12.1965 р., Міжнародний пакт про громадянські і політичні права від 16.12.1966 р. та ін.) та резолюцій Генеральної Асамблеї ООН (Резолюція 110 (II) від 03.11.1947 р., Резолюція 2625 (XXV) від 24.10.1970 р., Резолюція 67/154 від 20.12.2012 р., Резолюція 67/178 від 20.12.2012 р. та ін.). Питання, пов'язані з нормами, правилами та принципами відповідальної поведінки держав у кіберпросторі, а також заходами щодо зміцнення довіри в інформаційному середовищі, підвищення потенціалу держав у даній сфері, порушувалися в Резолюції 58/32 від 08.12.2003 р., Резолюції 63/70 від 02.12.2008 р., Резолюції 68/243 від 27.12.2013 р. та ін. Однак, слід зазначити, що існуюча співпраця у сфері забезпечення міжнародної інформаційної безпеки має певні труднощі, що не може не впливати на забезпечення внутрішньої інформаційної безпеки держав. На сьогодні відсутні всеосяжні універсальні міжнародні угоди, пов'язані з інформаційною сферою, які б регулювали співпрацю держав: а) у сфері забезпечення міжнародної інформаційної безпеки; б) у боротьбі з кіберзлочинністю. Це означає, що зберігається потреба в подальшому розвитку та зміцненні міжнародного правового інструментарію, здатного ефективно регулювати та координувати дії держав у забезпеченні надійного захисту інформаційної сфери та боротьби з кіберзагрозами.

В нинішній час договірно-правове співробітництво у боротьбі зі злочинністю в галузі високих технологій здійснюється на основі міжнародних угод, які спрямовані на боротьбу з окремими видами злочинів. Прикладами таких угод можуть бути Конвенція ООН проти транснаціональної організованої злочинності від 15.11.2000 р., Фа-

культативний протокол до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії від 01.01.2000 р. Крім того, існують точкові конвенції, укладені під егідою регіональних міжнародних організацій, спрямовані на координацію міжнародної боротьби зі злочинністю у сфері інформаційних технологій (Конвенція про кіберзлочинність від 23.11.2001 р. та Додатковий протокол від 28.01.2003 до цієї Конвенції, Конвенція про боротьбу із злочинами у сфері інформаційних технологій Ліги арабських держав від 21.12.2010 р., Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 р., Африканська конвенція про кібербезпеку та захист персональних даних від 27.06.2014 р. та ін.).

На нашу думку, акти Генеральної Асамблеї ООН та конвенції, укладені під егідою регіональних міжнародних організацій, є базисом, спираючись на який можливе створення універсального набору міжнародних актів, що регулюють питання співробітництва та взаємодії держав у сфері забезпечення інформаційної безпеки. Вважаємо, що наявність таких актів буде важливим кроком у напрямку встановлення загальновизнаних стандартів для забезпечення безпеки в інформаційній сфері, а приєднання до них України сприятиме забезпеченню інформаційної безпеки всередині країни. Слід наголосити, що питання укладання таких універсальних міжнародних угод активно обговорюються як у науковій спільноті, так і на такій міжнародній платформі, як ООН. Це свідчить про нагальну необхідність розробки загальновизнаних стандартів для ефективного співробітництва та взаємодії держав з метою забезпечення інформаційної безпеки.

Висновки. Підсумовуючи вищевикладене, зазначимо, що правова база в галузі забезпечення інформаційної безпеки характеризується повнотою та розгалуженістю, не вимагаючи суттєвих коригувань. Незважаючи на це, подальше її вдосконалення залишається однією з фундаментальних складових, що забезпечують національну безпеку України. Здійснення державної політики на рівні законодавчих актів має спиратися на такі пріоритети:

1. Ухвалення нових законів, які враховують інтереси всіх учасників інформаційних відносин. Дані акти повинні прагнути до вдосконалення нормативно-правової бази та врахування динамічної природи інформаційних технологій та процесів.

2. Інтеграція України у світовий правовий простір [9]. Це означає приведення національного законодавства у відповідність до міжнародних актів (у першу чергу тих, що діють на території ЄС), що дозволить більш ефективно взаємодіяти з іншими європейськими країнами в галузі інформаційної безпеки та забезпечення цифрової безпеки.

3. Врахування сучасного стану інформаційних технологій. В умовах швидкого розвитку цифрової сфери необхідне постійне оновлення та адаптація законодавства до нових викликів та загроз. Це передбачає не лише вдосконалення правових норм, а й створення механізмів моніторингу та реагування на інциденти в інформаційному середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Конституція України від 28.06.1996 р. № 254к/96-ВР. *Відомості Верховної Ради України (ВВР)*, 1996. № 30. Ст. 141.
2. Собкив Я. Информационные права и свободы человека и гражданина: особенности украинского нормативно-правового регулирования. *LEGEA ŞI VIAŢA*, 2014. С. 180–184.
3. Боднарчук О.В., Габрелян А.Ю. Розвиток системи страхування банківських вкладів України. *Економіка. Фінанси. Право*, 2023. № 6. С. 50–55.
4. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. *Відомості Верховної Ради України (ВВР)*, 1992. № 48. Ст. 650.
5. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 03.09.2023).
6. Про внесення змін до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації: Закон України від 04.06.2020 р. № 681-IX. *Відомості Верховної Ради (ВВР)*, 2020. № 42. Ст. 349.
7. Габрелян А.Ю. Недоліки законопроекту № 3139. *Верховенство Права*, 2020. № 1. С. 36–43.
8. Статут Організації Об'єднаних Націй від 26.06.1945 р. URL: https://www.un.org/ru/about-us/un-charter/full-text (дата звернення: 07.09.2023).
9. Габрелян А.Ю. Вектор розвитку України: дилема вибору. *Матеріали конференцій МЦНД*, 2021. URL: https://doi.org/10.36074/mcnd-19.02.2021.lawgov.02 (дата звернення: 30.09.2023).