МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Кваліфікаційна наукова
праця на правах рукопису

КРИВОЛАП Євгеній Володимирович

УДК 342.9:351.746.2 (043.5)

ДИСЕРТАЦІЯ

АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ У СФЕРІ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

12.00.07 – адміністративне право і процес;
фінансове право; інформаційне право
(081 Право)

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Є.В. Криволап

Науковий керівник: Кунєв Юрій Дем’янович,
доктор юридичних наук, професор, професор кафедри
конституційного і адміністративного права

Київ – 2025

АНОТАЦІЯ

Криволап Є. В. – Адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії зі спеціальності 081 «Право». – Державне некомерційне підприємство «Державний університет «Київський авіаційний інститут», Київ, 2025.

У дисертаційному дослідженні вперше здійснений комплексний аналіз і отримані наукові результати у сфері теоретичних і методологічних основ наук адміністративного та інформаційного права та на засадах міждисциплінарного підходу у галузі інформаційної та кібернетичної безпеки; отримані нові науково обґрунтовані результати у галузі адміністративно-правового забезпечення діяльності у сфері кібернетичної безпеки України. Отримані результати становлять інтерес для науки і практики адміністративного права, інформаційного права, кібернетичного права, теорії психології впливів, деліктології.

Констатується, що у сучасних реаліях широкого впровадження нових інформаційно-комунікаційних технологій, з одного боку, і тенденцій їх використання для завдання шкоди особам, підприємствам, суспільству, державі, з іншого боку, перед державою постає завдання надійного захисту кібернетичної безпеки суб’єктів. В дисертації запропонований, обґрунтовується і досліджується міждисциплінарний підхід до вивчення та реалізації ефективних засобів правового забезпечення інформаційної й кібер-безпеки, який полягає у поєднанні засобів, методів і правил адміністративного права, інформаційного права, пра́ва кібербезпеки, теорії психології впливів, деліктології. Вперше узагальнені встановлені Кодексом України про адміністративні правопорушення делікти у сфері обігу інформації і використання інформаційно-комунікаційних систем.

Удосконалене розуміння адміністративно-правового забезпечення діяльності у сфері кібернетичної безпеки України, яке полягає у поєднанні

засобів і методів адміністративного права з урахуванням технічних аспектів і технологічних небезпек в кіберпрострі, включаючи протидію вразливостям, кіберінцедентам, кіберконлфктам.

Введено в український правовий науковий оборот Закон ЄС про кіберстійкість (The Cyber Resilience Act (CRA)) щодо покращення кібербезпеки та кіберстійкості шляхом встановлення стандартів кібербезпеки для продуктів з цифровими елементами в ЄС, досліджені його основні положення, якими запропоновано доповнити Закон України «Про основні засади забезпечення кібербезпеки України».

Досліджені особливості концептів «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті особливої уваги до «когнітивної безпеки»; сформульовані положення, що у сучасному інформаційному просторі актуальною стає не тільки захист інформації, але й захист від інформації.

У дисертації запропонована і досліджена авторська структура інформаційних прав громадян. Виходячи з того, що «інформаційні права» не тотожні «праву на інформацію», запропонована і розглянута наступна структура інформаційних прав: свобода слова; право на доступ до інформації, у тому числі право на звернення; захист персональних даних; захист інформаційної безпеки; захист прав інтелектуальної власності; право на захист від кримінальних посягань у кіберпросторі. Розкриті особливості забезпечення кожного із видів прав.

Запропоновано і обґрунтовано необхідність поширити вимоги Закону України «Про основні засади забезпечення кібербезпеки України» на соціальні мережі та/або приватні електронні інформаційні ресурси в мережі Інтернет як потенційні точки входу для кібератаки.

Системно досліджені дії російських/проросійських пропагандистів щодо маскування фейкової інформації під зовнішнє оформлення відомих та авторитетних українських інформаційних сайтів, наприклад, «Обозреватель», УНІАН. Проаналізовані приклади фактичних фейкових повідомлень (сайтів)

від російської федерації, які можуть становити небезпеку для когнітивного самопочуття громадян.

Запропоновано і обґрунтовано необхідність включити законодавче регулювання сутності і змісту Стратегії зовнішньополітичної діяльності України, Стратегії інформаційної безпеки, Стратегії забезпечення державної безпеки, Стратегії енергетичної безпеки в Закон «Про національну безпеку України».

Доведено, що українська система безпекових стратегій побудована за моделлю НАТО та ЄС, яка (модель) розглядає інформаційну безпеку (information security) і кіберзахист (cyber defence) як єдиний операційний домен.

Здійснені системні дослідження з питань кіберконфліктів. Проаналізована сутність поняття «кіберконфлікт» як цілісного концепту (булінг, фішинг, картинг, кеш-трапінг, сталкінг, кібершпигунство, кібервандалізм, кібертероризм тощо). Розглянутий взаємозв’язок між поняттями «кіберконфлікт», з одного боку, та кіберінцидент і кіберзлочин, з іншого боку. Встановлено, що інцидент кібербезпеки – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора), спрямованих проти систем електронних комунікацій, систем управління технологічними процесами, а негативні прояви «кіберконфліктів» спрямовані проти інтересів осіб. Тобто, без врахування людського фактору як об’єкту негативного впливу розгляд проблематики кіберінцидентів є недостатнім та неповним.

Сформульовані рекомендації для підвищення ступеня інформаційної безпеки: використання надійних паролів, регулярне оновлення програмного забезпечення, використання антивірусного програмного забезпечення та брандмауера, уникнення відкриття підозрілих електронних листів, завантаження неперевіреного вмісту та переходів за сумнівними посиланнями, активація двофакторної аутентифікації, створення резервних

копії, використання тільки ліцензійних та офіційних програм.

Доведена необхідність впровадження Рекомендацій Комітету міністрів РЄ № R (89) 7 від 27.04.1989 р. «Про принципи поширення відеозаписів насильницького, жорстокого чи порнографічного змісту», № R (97) 19 від 30.10.1997 р. «Про показ насильства електронними ЗМІ», № R (97) 20 від 30.10.1997 р. «Про розпалювання ненависті» як документів щодо реалізації заходів забезпечення когнітивної безпеки від інформаційно-психологічного впливу електронних засобів комунікації.

Наведені обґрунтування, з точки зору Конвенції Ради Європи про захист прав людини і основоположних свобод 1950 року, заходів керівництва України щодо обмежень в інформаційно-комунікаційному середовищі країни: заборона російських соціальних мереж і сайтів; запровадження санкцій проти засобів масової інформації із забороною їх трансляції в умовах агресивної інформаційної війни і інших ворожих дій рф проти України.

Розглянуті правові засади застосування методу пошуку вразливостей на засадах системи Bug Bounty – це тестування електронних сервісів із залученням зовнішніх фахівців, яке дає можливість виявити вразливі місця і недоліки в програмних продуктах. Виконана періодизація офіційного правового запровадження даної системи в Україні, виділено 2 етапи: 1-й етап – запровадження відповідних змін до Кримінального кодексу України, 2-й етап – запровадження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, затвердженого Постановою КМУ від 16.05.2023 № 497 «Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж». Розглянуті принципи взаємодії між замовником і виконавцем (цями) при пошуку вразливостей, зокрема, висунення публічній пропозиції, підготовка звітів, виплата винагороди тощо.

Отримано розуміння логіки побудови структури підзаконних нормативно-правових актів України у сфері кіберзахисту.

Встановлено, що сукупність нормативних приписів у сфері забезпечення кібербезпеки та протидії кіберзлочинності доповнена також таким специфічним актом, як Типологія легалізації (відмивання) доходів, одержаних злочинним шляхом, у 2013 році, затверджені Наказом від 25.12.2013 № 157 Державної служба фінансового моніторингу України.

Запропонована і досліджена сфера застосування поняття «презумпція достовірності інформації», під якою розуміється відсутність необхідності додатково перевіряти достовірність інформації, розміщеної в легалізованих (зареєстрованих) ЗМІ. Європейський Суд з прав людини не вважає прийняття національних нормативних актів щодо державної реєстрації Інтернет-видань порушенням свободи слова. Навпаки, Європейський Суд з прав людини висновував, що принцип презумпції достовірності інформації, яка розміщена в Інтернеті, може бути застосований тільки щодо інформації, розміщеної в легалізованих (зареєстрованих) ЗМІ.

За наслідками виконаного дослідження запропоновано внести такі зміни і доповнення до законодавства у сфері інформаційної і кібер- безпеки:

– доповнити Закон України «Про основні засади забезпечення кібербезпеки України» положеннями нормативного акту ЄС – Закону про кіберстійкість (The Cyber Resilience Act (CRA)), серед яких (положень) – встановлення стандартів кібербезпеки для продуктів з цифровими елементами в ЄС, зокрема обов'язкові звіти про інциденти та автоматичні оновлення безпеки;

– поширити вимоги Закону України «Про основні засади забезпечення кібербезпеки України» на соціальні мережі та/або приватні електронні інформаційні ресурси в мережі Інтернет навіть якщо вони не містять інформацію, необхідність захисту якої встановлена законом, оскільки ці системи за визначенням взаємодіють із публічними мережами електронних комунікацій, зокрема, Інтернет, тому, вони є потенційною точкою входу для

кібератаки;

– доповнити Закон України «Про основні засади забезпечення кібербезпеки України» визначенням поняття «вразливості», згідно із міжнародним стандартом інформаційної безпеки ISO 27005;

– доповнити Закон України «Про основні засади забезпечення кібербезпеки України» визначенням поняття «кіберконфлікт» як зіткнення різноманітних інтересів в кіберпросторі;

– реалізувати у текстах законів напрями термінологічного узгодження у ч. 2 ст. 8 та абз. 2 ч. 4 ст. 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах» та у ч. 3 ст. 6 Закону України «Про основні засади забезпечення кібербезпеки України» (слова «інформаційної безпеки» замінити словами «безпеки інформації»);

– доповнити Закон України «Про захист персональних даних», визначенням «персональні дані» з Регламенту Європейського парламенту і Ради ЄС 2016/679 від 27.04.2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних: це «будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи»;

– доповнити Закон України «Про національну безпеку України» нормами щодо правового регулювання сутності і змісту Стратегії зовнішньополітичної діяльності України, Стратегії інформаційної безпеки, Стратегії забезпечення державної безпеки, Стратегії енергетичної безпеки

Ключові слова: кіберпростір, електронний кіберпростір, кібербезпека, кібертероризм, кіберзлочинність, захист інформації, інформаційна безпека,

адміністративне правопорушення, адміністративна відповідальність, булінг, фішинг, сталкінг, інтелектуальна власність, інтелектуальна власність у кіберпросторі, захист прав інтелектуальної власності, захист прав інтелектуальної власності в кіберпросторі, порушення прав інтелектуальної власності, дезінформація, російська федерація, інформаційні права, права людини, інформаційний вплив, обмеження прав людини

ABSTRACT

Kryvolap E. V. – Administrative and legal support of activities in the field of cyber security of Ukraine. – Qualification scientific work in the form of a manuscript.

Dissertation for the degree of Doctor of Philosophy in the specialty 081 «Law». – State Non-profit Enterprise “State University «Kyiv Aviation Institute», Kyiv, 2025.

In the dissertation study, a comprehensive analysis was first carried out and scientific results were obtained in the field of theoretical and methodological foundations of the sciences of administrative and information law and on the basis of an interdisciplinary approach in the field of information and cyber security, new scientifically substantiated results were obtained in the field of administrative and legal support of activities in the field of cyber security of Ukraine. As a result of the research, new scientifically substantiated results were obtained, which are of interest for the science and practice of administrative law, information law, cyber law, the theory of the psychology of influences, and torts.

It is stated that in the modern realities of the widespread introduction of new information and communication technologies, on the one hand, and the trends of their use to cause harm to individuals, enterprises, society, and the state, on the other hand, the state is faced with the task of reliably protecting the cyber security of entities. The dissertation proposes, justifies and investigates an interdisciplinary approach to the study and implementation of effective means of legal support for information and cyber security, which consists of combining the means, methods and rules of administrative law, information law, cybersecurity law, theories of psychology of influences, torts. For the first time, the torts established by the Code of Ukraine on Administrative Offenses in the field of information circulation and use of information and communication systems are generalized.

Improved the understanding of the administrative and legal support of activities in the field of cybersecurity of Ukraine, which consists of using the means and methods of administrative law, taking into account technical aspects

and technological dangers in cyberspace, including countering vulnerabilities, cyber incidents, and cyber conflicts.

The Cyber Resilience Act (CRA) has been introduced into Ukrainian legal scientific circulation – an EU regulatory act to improve cybersecurity and cyber resilience by establishing common cybersecurity standards for products with digital elements in the EU. Its main provisions are studied, which are proposed to supplement the Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity of Ukraine».

The features of the concepts of «information security», «security of information», «cybersecurity» are studied in the context of special attention to «cognitive security»; the provisions are formulated that in the modern information space not only information protection, but also protection from information is becoming relevant.

The dissertation proposes and investigates the author's structure of citizens' information rights. Based on the fact that «information rights» are not identical to the «right to information», the following structure of information rights is proposed and considered: freedom of speech; the right to access information, including the right to appeal; protection of personal data; protection of information security; protection of intellectual property rights; the right to protection from criminal encroachments in cyberspace. The features of ensuring each type of rights are revealed.

The need to extend the requirements of the Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity of Ukraine» to social networks and/or private electronic information resources on the Internet as a potential entry point for cyberattacks is proposed and substantiated

The actions of russian/pro-russian propagandists to disguise fake information under the external design of well-known and reputable Ukrainian information sites, for example, «Obozrevatel», UNIAN, are systematically investigated. Examples of actual fake messages (sites) from the russian federation that may pose a danger to the cognitive well-being of citizens are analyzed.

The need to include legislative regulation of the essence and content of such security strategies as the Strategy of Foreign Policy Activities of Ukraine, the Strategy of Information Security, the Strategy of Ensuring State Security, and the Strategy of Energy Security in the Law "On National Security of Ukraine" is proposed and substantiated.

It is proven that the Ukrainian system of security strategies is built on the model of NATO and the EU – NATO considers information security and cyber defense as a single operational domain. The EU in its «Cybersecurity Strategy for the Digital Decade» (2020) also emphasizes the interdependence of information resilience, digital sovereignty, and cyber defense.

Systematic research on cyber conflicts has been carried out. The essence of the concept of «cyber conflict» as a holistic concept is analyzed (bullying, phishing, carting, cash trapping, stalking, cyber espionage, cyber vandalism, cyber terrorism, etc.). The relationship between the concepts of «cyber conflict», on the one hand, and cyber incident and cyber crime, on the other hand, is considered. It is established that a cybersecurity incident is an event or a series of adverse events of an unintentional nature (natural, technical, technological, erroneous, including as a result of the action of the human factor), directed against electronic communications systems, technological process control systems, and the negative manifestations of «cyber conflicts» are directed against the interests of individuals. That is, without taking into account the human factor as an object of negative influence, consideration of the issues of cyber incidents is insufficient and incomplete.

Recommendations have been formulated to increase the level of information security: using strong passwords, regularly updating software; using antivirus software and a firewall; avoiding opening suspicious emails, downloading unverified content, and clicking on dubious links; activating two-factor authentication; creating backups to avoid data loss; using only licensed software.

The need for the implementation of Recommendations of the Committee of Ministers of the Council of Europe No. R (89) 7 of 27.04.1989 «On the principles

of distribution of video recordings of violent, cruel or pornographic content», No. R (97) 19 of 30.10.1997 «On the display of violence by electronic media», No. R 20 of 30.10.1997 «On incitement to hatred» as documents on the implementation of measures to ensure cognitive security from the informational and psychological impact of electronic means of communication has been proven.

The justifications, from the point of view of the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms of 1950, of the measures of the Ukrainian leadership regarding restrictions in the country's information and communication environment are given: the ban on russian social networks and websites; the introduction of sanctions against the media with the prohibition of their broadcast in the conditions of aggressive information warfare and other hostile actions of the rf against Ukraine.

The legal principles of applying the method of finding vulnerabilities based on the Bug Bounty system are considered – this is testing of electronic services with the involvement of external specialists, which makes it possible to identify vulnerabilities and shortcomings in software products. Was performed periodization of official legal implementation of this system in Ukraine, 2 stages have been identified: Stage 1 – introduction of relevant amendments to the Criminal Code of Ukraine, Stage 2 – introduction of the Procedure for searching and identifying potential vulnerabilities of information (automated), electronic communication, information and communication systems, electronic communication networks, approved by the Resolution of the Cabinet of Ministers of Ukraine dated 16.05.2023 No. 497 "On approval of the Procedure for searching and identifying potential vulnerabilities of information (automated), electronic communication, information and communication systems, electronic communication networks". The principles of interaction between the customer and the contractor (s) when searching for vulnerabilities have been considered, in particular, submitting a public offer, preparing reports, paying a reward, etc.

An understanding of the logic of building the structure of subordinate regulatory legal acts of Ukraine in the field of cyber protection has been obtained.

It has been established that the set of regulatory requirements in the field of ensuring cybersecurity and combating cybercrime is also supplemented by such a specific act as the Typology of legalization (laundering) of proceeds from crime in 2013, approved by Order No. 157 of the State Financial Monitoring Service of Ukraine dated 25.12.2013.

The scope of application of the concept of "presumption of reliability of information" is proposed and investigated, which means the absence of the need to additionally verify the reliability of information posted in legalized (registered) media. The European Court of Human Rights does not consider the adoption of national regulatory acts on the state registration of Internet publications to be a violation of freedom of speech. On the contrary, the European Court of Human Rights concluded that the principle of presumption of reliability of information posted on the Internet can be applied only to information, placed in legalized (registered) media.

As a result of the research, it is proposed to make the following changes and additions to the legislation in the field of information and cyber security:

– to supplement the Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity in Ukraine» with the provisions of the EU regulatory act – the Cyber Resilience Act (CRA), including (provisions) – establishing cybersecurity standards for products with digital elements in the EU, in particular mandatory incident reports and automatic security updates;

– to extend the requirements of the Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity in Ukraine» to social networks and/or private electronic information resources on the Internet even if they do not contain information the need for protection of which is established by law, since these systems by definition interact with public electronic communications networks, in particular the Internet, therefore, they are a potential entry point for a cyberattack;

– to supplement the Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity in Ukraine» with the definition of the concept of «vulnerability», in accordance with the international information security standard ISO 27005;

– to supplement the Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity of Ukraine" with a definition of the concept of "cyber conflict» as a clash of various interests in cyberspace;

– to implement in the texts of laws the directions of terminological harmonization in Part 2 of Article 8 and Paragraph 2 of Part 4 of Article 8 of the Law of Ukraine «On Information Protection in Information and Communication Systems» and in Part 3 of Article 6 of the Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity of Ukraine» (replace the words «information security» with the words «security of information»);

– to supplement the Law of Ukraine «On Personal Data Protection» with the definition of «personal data» from Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data: this is «any information relating to an identified or identifiable natural person («data subject»); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person»;

– to supplement the Law of Ukraine «On National Security of Ukraine» with norms on legal regulation of the essence and content of the Strategy of Foreign Policy Activities of Ukraine, the Strategy of Information Security, the Strategy of Ensuring State Security, and the Strategy of Energy Security.

Keywords: cyberspace, electronic cyberspace, cybersecurity, cyberterrorism, cybercrime, information protection, information security, administrative offense, administrative liability, bullying, phishing, stalking, intellectual property, intellectual property in cyberspace, protection of intellectual property rights, protection of intellectual property rights in cyberspace, violation of intellectual property rights, disinformation, russian federation, information rights, human rights, information influence, restriction of human right

СПИСОК ПРАЦЬ, ОПУБЛІКОВАНИХ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України:

1. Бєлкін Л.М., Юринець Ю.Л., Бєлкін М.Л., Криволап Є.В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020-2021 років. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2022. № 3 (64). С. 78-86. DOI: https://doi.org/10.18372/2307-9061.64.16893

2. Guoqiang Fu, Криволап Є.В. Особливості термінології в англомовній літературі у сфері кібербезпеки. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2023. № 1 (66). С. 63-71. DOI: https://doi.org/10.18372/2307-9061.66.17419

3. Криволап Є.В., Юринець Ю.Л., Бєлкін Л.М. Питання нейтралізації вразливостей інформаційно-комунікаційних систем цивільної авіації: правовий аспект. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2023. № 3 (68). С. 16-23. DOI: https://doi.org/10.18372/2307-9061.68.17969

4. Криволап Є.В., Юринець Ю.Л. Взаємозв'язок безпекових стратегій України з інформаційною безпекою та кібербзпекою. *Актуальні питання у сучасній науці*. 2023. № 8 (14). С. 477-487. DOI: https://doi.org/10.52058/2786-6300-2023-8(14)-477-487

5. Криволап Є.В. Адміністративно-правове регулювання заходів протидії кіберзагрозам актами європейського рівня. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2024. № 3 (72). С. 84-92. DOI: https://doi.org/10.18372/2307-9061.72.19064

6. Юринець Ю.Л., Криволап Є.В. Соціальні мережі як чинник впливу

на формування іміджу закладу вищої освіти. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2025. № 2 (75). С. 201-210. DOI: https://doi.org/10.18372/2307-9061.75.20235

7. Криволап Є.В. Публічно-правове регулювання підвищення рівня кібербезпеки в Європейському Союзі на підставі акту про кіберстійкість (The Cyber resilience Act). *Наукові інновації та передові технології (Серія «Управління та адміністрування», Серія «Право», Серія «Економіка», Серія «Психологія», Серія «Педагогіка»)*: журнал. 2025. № 3 (43). С. 516-526. DOI: https://doi.org/10.52058/2786-5274-2025-3(43)-516-526

8. Юринець Ю.Л., Криволап Є.В., Сопілко І.М., Бєлкін Л.М., Бєлкін М.Л. Проблеми формування державної політики у сфері кіберконфліктів. *Успіхи і досягнення у науці* (Серія «Право», Серія «Освіта», Серія «Управління та адміністрування», Серія «Соціальні та поведінкові науки»), 2025. № 6 (16). С. 249-270. DOI: https://doi.org/10.52058/3041-1254-2025-6(16)-249-270

Наукові праці, які засвідчують апробацію дисертації:

9. Криволап Є.В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека». «Когнітивна безпека» як стійкість проти інформаційно-психологічних впливів на людину і суспільство. *Свобода, безпека та незалежність: правовий вимір*: [Матеріали XIII Міжнародної науково-практичної конференції, м. Київ, Національний авіаційний університет, 24 лютого 2023 р.]. С. 195-197.

10. Криволап Є.В. Питання застосування механізмів забезпечення інформаційної безпеки і кібербезпеки в реалізації безпекових стратегій України. *Наукові дослідження та інновації*: Матеріали 2-ї Міжнар. науково-практичної інтернет-конференції 3-4 квітня 2023 р. ФОП Марениченко В.В., Дніпро, Україна, С. 216-218.

11. Криволап Є.В. Засади правового регулювання заходів забезпечення

кібербезпеки актами європейського рівня. *Глобальні проблеми та рішення*: Матеріали 2-го Міжнародного науково-практичного Інтернет-конгресу, 10-11 квітня 2023 р. ФОП Марениченко В.В., Дніпро, Україна, С. 42-45.

12. Криволап Є.В. Вплив стратегій інформаційної та кібербзпеки на інші безпекові стратегії України. *VI Міжнародний молодіжний науковий юридичний форум*: [Матеріали форуму, м. Київ, Національний авіаційний університет, 18 травня 2023 р.]. С. 119-121.

13. Криволап Є.В., Юринець Ю.Л. До питання вразливості інформаційно-комунікаційних систем цивільної авіації: правовий аспект. *АЕРО-2023. Повітряне і космічне право*: [Матеріали Всеукраїнської конференції здобувачів вищої освіти і молодих учених, м. Київ, Національний авіаційний університет, 23 листопада 2023 р.]. Тернопіль: Вектор. С. 118-120.

14. Криволап Є.В. Підвищення рівня контролю і протидії вразливостям інформаційно-комунікаційних систем в аспекті відновлення України. *Правова парадигма відновлення України: проблеми та перспективи*: [Матеріали XIV Міжнародної науково-практичної конференції, м. Київ, Національний авіаційний університет, 23 лютого 2024 р.]. Тернопіль: Вектор, 2024. с. 220-223.

15. Криволап Є.В., Бєлкін Л.М., Юринець Ю.Л. Правові засади виявлення та протидії вразливостям інформаційно-комунікаційних систем на підставі методів bug bounty (білий хакінг) в Україні. *Впровадження інноваційних технологій та модернізація технічної складової сектору безпеки і оборони як вагомий чинник у боротьбі з агресором*: зб. матеріалів міжвідомчої науково-практичної конференції, 27 березня 2024 р., Київ / [відп. ред. Парфило О.А.] ; Укр. наук.-дослід. ін.-т спец. техніки та судових експертиз Служби безпеки України. Київ : ІСТЕ СБУ, 2024. С. 99-103.

16. Криволап Є.В. Адміністративно-правові засади виявлення та протидії вразливостям інформаційно-комунікаційних систем на підставі методів bug bounty (білий хакінг) в Україні. *VII Міжнародний молодіжний*

науковий юридичний форум: [Матеріали форуму, м. Київ, Національний авіаційний університет, 16-17 травня 2024 р.] С. 145-147.

17. Бєлкін М.Л., Криволап Є.В., Юринець Ю.Л. Адміністративно-правове регулювання нейтралізації вразливостей інформаційно-комунікаційних систем. *Збірник матеріалів «Актуальні питання забезпечення кібербезпеки» IX Міжнародної науково-практичної конференції* (м. Київ, 13 листопада 2024 року). Київ. МАУП. 13 листопада 2024 року. С 38-42.

18. Криволап Є.В. Правові підходи до підвищення рівня кібербезпеки в Європейському Союзі (the Cyber Resilience Act, CRA). *Правова система України: європейський вектор розвитку в умовах воєнного стану*: [Матеріали XV Міжнародної науково-практичної конференції, м. Київ, Державний університет «Київський авіаційний інститут», 21 лютого 2025 р.]. Тернопіль: Вектор, 2025. С. 201-204.

19. Криволап Є., Юринець Ю., Бєлкін Л., Бєлкін М. Поняття «кіберконфлікти» в системі термінології з кібербезпеки. *Innovations and New Directions in Scientific Research*: Proceedings of the 2nd International Scientific Conference (Manchester, United Kingdom, 20September2025). Lulu Press, Inc., 2025. P. 191-195.

20. Криволап Є.В. Використання фейкових сайтів в російській пропаганді. *АЕРО-2024. Повітряне і космічне право*: [Матеріали Всеукраїнської конференції, м. Київ, Державне некомерційне підприємство «Державний університет «Київський авіаційний інститут», 20 листопада 2024 р.]. Тернопіль. «Вектор». С. 113-115.

21. Юринець Ю.Л., Криволап Є.В., Бєлкін Л.М. Використання соціальних мереж для формування іміджу закладів вищої освіти. *Соціально-економічний розвиток у контексті викликів сьогодення*: матеріали III Міжнародної науково-практичної конференції / Східноєвропейський центр наукових досліджень (Одеса, 16 серпня 2025 р). Research Europe, 2025. С. 123-127.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ВРУ – Верховна Рада України

ГШ (Генштаб) – Генеральний штаб

ЄКПЛ – Конвенція Ради Європи про захист прав людини і основоположних свобод 1950 року

ЄС – Європейський Союз

ЄСПЛ – Європейський Суд з прав людини

ЗМІ – засоби масової інформації

ЗСУ – Збройні Сили України

ІКТ – інформаційно-комунікаційні технології

ІТ – інформаційні технології

КК – Кримінальний кодекс [України]

КУпАП – Кодекс України про адміністративні правопорушення

ООН – Організація Об’єднаних Націй

ПАРЄ – Парламентська Асамблея Ради Європи

РЕ – Рада Європи

РНБО – Рада Національної безпеки і оборони [України]

рф – російська федерація

США – Сполучені Штати Америки

ЦРУ – Центральне розвідувальне управління [США]

ВСТУП

Обґрунтування вибору теми дослідження. Стаття 17 Конституції України спеціально передбачає, що забезпечення інформаційної безпеки України є однією з найважливіших функцій держави.

Таким чином, Конституція України ставить досягнення інформаційної безпеки держави конституційним завданням. І це є невипадковим, оскільки у сучасній ситуації цілеспрямовані інформаційні впливи здатні спонукати населення до вчинення таких дій, на які б воно самостійно не наважилося і об’єктивно не хотіло. Яскравим прикладом цього є масові антиукраїнські акції населення Донбасу 2014 р., які були здійсненні під впливом російської пропаганди, яке (населення) на даний час не у захваті від життя під окупацією рф. Зокрема, за даними берлінського Центру східноєвропейських та міжнародних досліджень, станом на серпень 2019 року мало місце збільшення підтримки повернення до становища цих територій ***перед війною***. Загалом і в 2016-му, і в 2019-му роках близько 55 % жителів непідконтрольних Уряду України територій висловилися за повернення цих територій під контроль українського уряду.

Як зазначає луганський журналіст Є. Соломін, проімперська риторика росіян в українському регіональному ефірі спричинила те, що в головах багатьох луганчан сформувалося схвальне ставлення до путінсько-російської політики. Отже, убезпечення населення від негативних інформаційних впливів тісно поєднане із інформаційною безпекою держави як такої.

Важливо зазначити, що сучасні засоби масової комунікації (Інтернет, радіомовлення, телебачення, супутниковий зв'язок,) є транскордонними. Як зазначав італійський вчений Умберто Еко, «інформація допускає ворога в чужі тили…». Зокрема, агресія рф проти України, важливою складовою якої була та є інформаційна війна, поставила перед науковцями та практиками нові завдання у галузі протидії інформаційним операціям та інформаційним війнам. Самим обґрунтуванням широкомасштабної військової агресії рф проти України 24.02.2022 року є (були) пропагандистські штампи, які

створили для керівництва рф «віртуальну реальність», у межах якої і приймалося рішення про вторгнення.

Із загостренням воєнної ситуації наростають і ризики у кіберпросторі. Наприклад, за звітом компанії Microsoft, з початку широкомасштабного російського вторгнення 24.02.2022 року російські хакери скоїли майже 240 кібератак проти України. Атаки були спрямовані на знищення комп'ютерних систем, збирання розвідувальних даних або поширення дезінформації.

Таким чином, поняття інформаційної безпеки нерозривно пов'язане з поняттям кібербезпеки. З точки зору національної (інформаційної) безпеки держави слід підкреслити, що кібервійна стає все більш важливою складовою гібридної війни. Отже, дослідження аспектів забезпечення кібернетичної безпеки як чинника інформаційної безпеки України є актуальними.

Науково-теоретичною основою дисертаційного дослідження є наукові праці вітчизняних і зарубіжних учених у галузі адміністративного права, інформаційного права, кібернетичної безпеки. Значну увагу приділено технологічним аспектам виникнення кіберзагроз і вирішенню проблем протидії цим загрозам, а також інформаційно-психологічним проблемам забезпечення когнітивної безпеки.

До переліку використаних джерел увійшли праці таких науковців, як Р.А. Калюжний, Ю.Д. Кунєв, С.Я. Лихова, В.В. Філінович, О.О. Тихомиров, Н.Б. Новицька, М.І. Легенький, І.М. Сопілко, А.І. Марущак, В.Ю. Богданович, В.А. Ліпкан, інші автори. Використано також законодавство України, міжнародні правові акти, зокрема документи НАТО, Європейського Союзу, Ради Європи, матеріали судової практики та офіційні інформаційні ресурси центральних органів виконавчої влади

Зв’язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження здійснене відповідно до тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2023 року, затверджених постановою КМУ від 07.09.2011 № 942 (із змінами, внесеними постановою КМУ від 09.05.2023 № 463); Переліку пріоритетних тематичних

напрямів наукових досліджень і науково-технічних розробок на період до 31 грудня року, наступного після припинення або скасування воєнного стану в Україні**,** затверджених постановою КМУ від 30.04.2024 № 476; Указу Президента України «Про цілі сталого розвитку України на період до 2030 року» від 30.09.2019 № 722/2019, а також у межах плану наукових досліджень Факультету права та міжнародних відносин Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут» (при виконанні робіт – Національний авіаційний університет), зокрема, кафедри конституційного та адміністративного права, теми: «Забезпечення конституційних прав громадян в контексті конвенційних зобов'язань України» (державний реєстраційний номер 0119U103091); «Людиноцентричність публічного права України» (державний реєстраційний номер 0124U003363) та держбюджетної науково-дослідної роботи № 312-ДБ20 «Проблеми формування та реалізації державної політики у сфері інформаційної безпеки України: теорія і практика» (державний реєстраційний номер 0120U102136).

Тема дисертації відповідає освітньо-науковій програмі «Право» за спеціальністю 081 «Право» 08 «Право» в КАІ (зокрема, ОК 1.3.1, ОК 1.3.2, ОК, 1.3.3. та ОК 1.3.4).

Мета і завдання дослідження. Метою дисертаційного дослідження є розкриття сутності і змісту адміністративно-правових засад спрямування методів і засобів забезпечення кібернетичної безпеки на вирішення завдань забезпечення інформаційної та кібер- безпеки, поставлених у Стратегії від 15.10.2021 р. інформаційної безпеки та Стратегії від 14.05.2021 р. кібербезпеки України, затверджених Указами Президента України від 28.12.2021 р. № 685/2021 та від 26.08.2021 р. № 447/2021 відповідно.

Сформульована мета дослідження обумовила необхідність вирішення наступних ***завдань***:

– здійснити системний аналіз наукового доробку вітчизняних та зарубіжних учених за темою дисертаційного дослідження;

– визначити засадничі вимоги безпекових Стратегій 2020-2021 років в Україні (Стратегія національної безпеки України від 14.09.2020 р.; Стратегія воєнної безпеки України від 25.03.2021 р.; Стратегія кібербезпеки України від 14.05.2021 р.; Стратегія інформаційної безпеки від 15.10.2021 р.);

– уточнити та розширити понятійно-категорійні концепти «безпека інформації», «інформаційна безпека», «кібербезпека» в контексті безпекових стратегій України 2020-2021 років;

– обґрунтувати наукове визначення категорії «когнітивна безпека» як складової протидії інформаційно-психологічним операціям ворога;

– дослідити особливості правового регулювання заходів забезпечення кібербезпеки правовими актами європейського рівня;

– розкрити особливостей правового регулювання заходів забезпечення кібербезпеки актами національного права;

– обґрунтувати форми та визначити особливості методів забезпечення кібербезпеки як чинників забезпечення інформаційної безпеки;

– узагальнити повноваження суб'єктів кіберзахисту у сфері забезпечення кібербезпеки як чинників забезпечення інформаційної безпеки;

– розкрити систему прав і свобод людини і громадянина, що забезпечуються в межах кібербезпеки, здійснивши їх класифікацію за видами та окресливши організаційно-правові й технологічні механізми гарантування;

– обґрунтувати потенціал та необхідність міждисциплінарного підходу у сфері інформаційної та кібер- безпеки, що базується на інтеграції доктринальних положень адміністративного та інформаційного права, з одного боку, та наукових здобутків та практичного досвіду інформаційних технологій – з іншого.

Об'єктом дослідження є теорія й практика організації діяльності у сфері забезпечення інформаційної і кібернетичної безпеки України.

Предметом дослідження є адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України.

Методи дослідження. Методологічну основу дисертаційного

дослідження становить сукупність взаємопов’язаних методів наукового пізнання, що забезпечили системний підхід до вирішення поставлених завдань, єдність юридичної форми і правового змісту отриманих результатів (усі розділи роботи). Застосовується міждисциплінарний підхід у сфері інформаційної та кібер- безпеки, який полягає у поєднанні засобів, методів і правил адміністративного права (принципи діяльності публічної адміністрації і організації публічного управління в демократичному суспільстві), інформаційного права (поєднання свободи інформаційної діяльності із захистом національного інформаційного простору України від розповсюдження ворожої інформаційної продукції, створення та використання інформаційних технологій), пра́ва кібербезпеки (врахування конкретних ситуацій прийняття рішень публічною адміністрацією), теорії психології впливів (захист осіб від шкідливих інформаційних впливів, забезпечення когнітивної безпеки), деліктології (вивчення заходів державного примусу адміністративно-правового і кримінально-правового характеру для забезпечення встановлених правил у сфері інформаційної та кібр- безпеки) (підрозділи 1.1 + 1.2 + 1.3 + 3.1 + 3.2). Важливе місце у роботі займає використання принципу аналізу-синтезу як методу діалектичного мислення (підрозділ 2.3). Системний метод застосовано для упорядкування емпіричної інформації та проведення класифікації досліджуваних правових явищ (підрозділ 2.3). Документальний аналіз дозволив послідовно дослідити документальні джерела правових явищ, які використані у даній роботі, зокрема, міжнародні акти, акти органів української влади, рішення судів тощо (підрозділи 2.1 + 2.2). Метод абстрагування дозволив залишати на певних етапах дослідження поза увагою конкретні численні сторони і ознаки відповідного явища, але виявити у ньому найбільш характерне, тобто розкрити останнє як наукову категорію (підрозділ 3.3). Компаративний метод (метод порівняння) застосовано для порівняння, з одного боку, законодавства України, а з іншого боку, законодавства Європейського Союзу і Ради Європи (підрозділи 2.1 + 2.2). Використання методу об’єктивної істини здійснено

шляхом перехресної перевірки даних, використаних при дослідженні, дослідження із декількох джерел, опори на статистичні дані та судову практику (усі розділи роботи).

Науково-теоретичне підґрунтя для виконання дисертації становлять наукові праці фахівців у галузі адміністративного права, інформаційного права, теорії держави і права, інших галузевих юридичних наук, інформаційно-комунікаційних технологій та кібербезпеки, у тому числі робіт зарубіжних дослідників.

Нормативну основу дослідження становлять Конституція України, чинні законодавчі та підзаконні нормативно-правові акти України, а також міжнародно-правові акти та законодавство зарубіжних країн, приписи якого можуть бути імплементовані у законодавство України. Використані також наукові аналітичні публікації, публікації у засобах масової інформації, інші інформаційні джерела, не заборонені законодавством.

Наукова новизна одержаних результатів полягає в тому, що вперше за напрямком досліджень теоретичних і методологічних основ наук адміністративного та інформаційного права та на засадах міждисциплінарного підходу у галузі інформаційної та кібер- безпеки отримані нові науково обґрунтовані результати у галузі адміністративно-правового забезпечення діяльності у сфері кібернетичної безпеки України. Як результат проведеного дослідження його наукову новизну відображають основні положення за ступенями новизни:

вперше:

– системно обґрунтовано проблеми адміністративно-правового забезпечення діяльності у сфері кібербезпеки України на засадах міждисциплінарного підходу, що інтегрує засоби, методи та принципи адміністративного права, інформаційного права, права кібербезпеки, теорії психологічних впливів та деліктології;

– розкрито реалізацію владних повноважень публічної адміністрації у сфері кібербезпеки крізь призму адміністративно - правових зобов'язань, що

охоплюють здійснення публичного управління, надання адміністративних послуг, визначення відповідності публічної адміністрації у разі неправомірних дій чи порушення діяльності за її діяльністю, а також відповідальності суб'єктів суспільства;

– введено в український правовий науковий обіг Закон Європейського Союзу про кіберстійкість (Cyber Resilience Act, CRA), спрямований на підвищення рівня кібербезпеки та кіберстійкості шляхом встановлення єдиних стандартів захисту продуктів із цифровими елементами; здійснено дослідження його ключових положень та визначено їх значення для формування національної правової доктрини у сфері кібербезпеки;

– уточнено та розширено понятійно-категорійні характеристики категорій «безпека інформації», «інформаційна безпека» та «кібербезпека» в контексті акцентованої уваги на феномені «когнітивної безпеки», що дозволило сформулювати положення, згідно з якими в сучасному інформаційному просторі актуалізується не лише завдання захисту інформації, а й необхідність захисту від деструктивного інформаційного впливу;

– запропоновано поширити вимоги Закону України від 05.10.2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» на соціальні мережі та/або приватні електронні інформаційні ресурси в мережі Інтернет як потенційні точки входу для кібератаки;

– запропоновано включити законодавче регулювання сутності і змісту Стратегії зовнішньополітичної діяльності України, Стратегії інформаційної безпеки, Стратегії забезпечення державної безпеки, Стратегії енергетичної безпеки в Закон України «Про національну безпеку України»;

удосконалено:

– підходи до вивчення кіберконфліктів, розуміння сутності поняття «кіберконфлікт», взаємозв’язку між поняттями «кіберконфлікт», з одного боку, та кіберінцидент і кіберзлочин, з іншого боку;

– розуміння адміністративно-правового забезпечення діяльності у сфері

кібернетичної безпеки України, яке полягає у поєднанні засобів і методів адміністративного права з урахуванням технічних аспектів і технологічних небезпек в кіберпрострі, включаючи протидію вразливостям, кіберінцедентам, кіберконлфктам;

– рекомендації для підвищення ступеня інформаційної безпеки: використання надійних паролів, регулярне оновлення програмного забезпечення, використання антивірусного програмного забезпечення та брандмауера, уникнення відкриття підозрілих електронних листів, завантаження неперевіреного вмісту та переходів за сумнівними посиланнями, активація двофакторної аутентифікації, створення резервних копії, використання тільки ліцензійних та офіційних програм;

– розуміння Рекомендацій Комітету міністрів РЄ № R (89) 7 від 27.04.1989 р. «Про принципи поширення відеозаписів насильницького, жорстокого чи порнографічного змісту», № R (97) 19 від 30.10.1997 р. «Про показ насильства електронними ЗМІ», № R (97) 20 від 30.10.1997 р. «Про розпалювання ненависті» як документів щодо впровадження заходів забезпечення когнітивної безпеки від інформаційно-психологічного впливу електронних засобів комунікації;

– структура інформаційних прав громадян: свобода слова; право на доступ до інформації, у тому числі право на звернення; захист персональних даних; захист інформаційної безпеки; захист прав інтелектуальної власності; право на захист від кримінальних посягань у кіберпросторі. Розкриті особливості забезпечення кожного із видів прав;

– обґрунтування заходів керівництва України щодо обмежень в інформаційно-комунікаційному середовищі країни: заборона російських соціальних мереж і сайтів; запровадження санкцій проти засобів масової інформації із забороною їх трансляції в умовах агресивної інформаційної війни рф проти України;

дістали подальшого розвитку:

– розуміння сучасних викликів у зв’язку із широкомасштабною

агресією рф проти України, яке (розуміння) полягає у тому, що у сучасних реаліях широкого впровадження нових інформаційно-комунікаційних технологій, з одного боку, і тенденцій їх використання у гібрідних війнах для завдання шкоди суб'єктам інформаційних відносин, з іншого боку, перед державою постає завдання надійного захисту кібернетичної безпеки суб'єктів та їх прав у кіберпросторі;

– періодизація запровадження системи пошуку вразливостей Bug Bounty, яка полягає у контрольованих кібератаках певних інформаційно-комунікаційних систем з метою перевірки їх стійкості до таких атак і пошуку вразливостей;

– розуміння, що українська система безпекових стратегій побудована за моделлю НАТО та ЄС, відповідно до якої (моделі) НАТО розглядає інформаційну безпеку (information security) і кіберзахист (cyber defence) як єдиний операційний домен;

– узагальнення встановлених Кодексом України про адміністративні правопорушення деліктів у сфері обігу інформації і використання інформаціонно-комунікаційних систем;

– уявлення про дії російських/проросійських пропагандистів щодо маскування фейкової інформації під зовнішнє оформлення відомих та авторитетних українських інформаційних сайтів, наприклад, «Обозреватель», УНІАН. Проаналізовані приклади фактичних фейкових повідомлень (сайтів);

– обгрунтування правового регулювання Інтернет-ресурсів як ЗМІ; запропоноване поняття «презумпція достовірності інформації», під якою розуміється відсутність необхідності додатково перевіряти достовірність інформації, розміщеної в легалізованих (зареєстрованих) ЗМІ.

Практичне значення одержаних результатів дослідження полягає у можливості їх використання:

– Секретаріатом Касаційного цивільного суду у складі Верхового Суду дозволить організувати та планувати роботу з протидії правопорушенням у кібермережі (довідка про впровадження від 05.12.2025);

– ДНП «Державний університет «Київський авіаційний інститут» у науково-дослідній сфері основні положення та висновки дисертації можуть бути основою для подальшої розробки адміністративно-правових питань комплексного забезпечення інформаційної і кібер- безпеки (акт про впровадження від 01.12.2025);

– Комітетом Верховної Ради України з питань правоохоронної діяльності при формуванні та обґрунтуванні пропозицій щодо вдосконалення нормативно-правових актів у сфері забезпечення інформаційної та кібербезпеки (довідка про впровадження №04-27/12-2022/214837 від 13.12.2022).

– Київським національний університетом будівництва і архітектури у навчальному процесі матеріали дисертації використовуватимуться під час проведення занять із дисципліни «Цифрові трансформації у суспільстві та електронне урядування», «Захист персональних даних», «Адміністративне право і процес», «Конституційне право України», «Верховенство права через призму конституційного та адміністративного права та процесу» (акт про впровадження від 24.11.2025);

– Українською асоціацією інвестиційного бізнесу для забезпечення підвищення рівня захисту інформаційних баз даних (довідка про впровадження від 01.12.2025).

Особистий внесок здобувача. У межах дисертаційного дослідження здійснено формулювання теоретичних положень, узагальнень і висновків, що мають наукове та прикладне значення. Розроблені практичні рекомендації та пропозиції ґрунтуються на самостійному комплексному аналізі чинного законодавства, спеціальної наукової літератури та адміністративно-правової практики у сфері забезпечення кібербезпеки. Висвітлені положення є результатом системного осмислення правових механізмів забезпечення кібербезпеки, інформаційних права громадян. у дисертації не використовуються наукові ідеї та розробки, що належать співавторам опублікованих робіт. Висновки та положення дисертації обґрунтовані автором особисто. Використані в дисертації ідеї, положення чи гіпотези

інших авторів мають відповідні посилання і використані лише для підкріплення ідей здобувача.

Апробація результатів дисертації. Результати дослідження, його основні висновки та рекомендації оприлюднені на 13 наукових конференціях, а саме: «Свобода, безпека та незалежність: правовий вимір» (Київ, 2023), «Наукові дослідження та інновації» (Дніпро, 2023), «Глобальні проблеми та рішення» (Дніпро, 2023), «VI Міжнародний молодіжний науковий юридичний форум» (Київ, 2023), «AEPO-2023. Повітряне і космічне право» (Київ, 2023), «Правова парадигма відновлення України: проблеми та перспективи» (Київ, 2024); «Впровадження інноваційних технологій та модернізація технічної складової сектору безпеки і оборони як вагомий чинник у боротьбі з агресором» (Київ, 2024), «VII Міжнародний молодіжний науковий юридичний форум» (Київ, 2024), «Актуальні питання забезпечення кібербезпеки» (Київ, 2024), «Правова система України: європейський вектор розвитку в умовах воєнного стану» (Київ, 2025), «Інновації та нові напрямки в наукових дослідженнях» (Манчестер, Велика Британія, 2025), «AEPO-2024. Повітряне і космічне право» (Київ, 2024), «Соціально-економічний розвиток у контексті викликів сьогодення» (Одеса, 2025).

Публікації. Основні положення дисертаційного дослідження відображено у 19,5[1] наукових працях, зокрема у 6,5 наукових статтях, опублікованих у фахових виданнях України з юридичних наук, а також у 13 тезах, опублікованих за результатами участі в науково-практичних конференціях, у тому числі міжнародних, всеукраїнських і зарубіжних.

Список опублікованих праць за темою дисертації

Статті у наукових фахових виданнях України:

1. Бєлкін Л.М., Юринець Ю.Л., Бєлкін М.Л., Криволап Є.В.

[1] Згідно пп. 1 п. 8 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого Постановою КМУ від 12.01.2022 № 44 (із змінами), якщо число співавторів у статті, опублікованій у співавторстві (разом із здобувачем), становить більше двох осіб, така стаття прирівнюється до 0,5 публікації

Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020-2021 років. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2022. № 3 (64). С. 78-86. DOI: https://doi.org/10.18372/2307-9061.64.16893

Особистий внесок Бєлкіна Л.М. – постановка завдання,

Особистий внесок Юринець Ю.Л. – огляд стану розроблення питання,

Особистий внесок Бєлкіна М.Л. – підбір літератури,

Особистий внесок Криволапа Є.В. – розмежування понять «інформаційна безпека» і «безпека інформації», виділення поняття «когнітивна безпека».

2. Guoqiang Fu, Криволап Є.В. Особливості термінології в англомовній літературі у сфері кібербезпеки. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2023. № 1 (66). С. 63-71. DOI: https://doi.org/10.18372/2307-9061.66.17419

Особистий внесок Фу Г. – підбір ключової англомовної термінології з питання,

Особистий внесок Криволапа Є.В. – тлумачення деяких англомовних термінів українською мовою.

3. Криволап Є.В., Юринець Ю.Л., Бєлкін Л.М. Питання нейтралізації вразливостей інформаційно-комунікаційних систем цивільної авіації: правовий аспект. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2023. № 3 (68). С. 16-23. DOI: https://doi.org/10.18372/2307-9061.68.17969

Особистий внесок Криволапа Є.В. – вперше виконав адміністративно-правовий аналіз процедури Bug Bounty, проаналізував її правовий аспект,

Особистий внесок Юринець Ю.Л. – огляд напрямів застосування процедури,

Особистий внесок Бєлкіна Л.М. – постановка завдання.

4. Криволап Є.В., Юринець Ю.Л. Взаємозв’язок безпекових стратегій

України з інформаційною безпекою та кібербзпекою. *Актуальні питання у сучасній науці*. 2023. № 8 (14). С. 477-487. DOI: https://doi.org/10.52058/2786-6300-2023-8(14)-477-487

Особистий внесок Криволапа Є.В. – встановлення логіки взаємозв'язків і взаємовпливів інформаційної безпеки та кібербезпеки з іншими компонентами національної безпеки,

Особистий внесок Юринець Ю.Л. – постановка завдання.

5. Криволап Є.В. Адміністративно-правове регулювання заходів протидії кіберзагрозам актами європейського рівня. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2024. № 3 (72). С. 84-92. DOI: https://doi.org/10.18372/2307-9061.72.19064

6. Юринець Ю.Л., Криволап Є.В. Соціальні мережі як чинник впливу на формування іміджу закладу вищої освіти. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2025. № 2 (75). С. 201-210. DOI: https://doi.org/10.18372/2307-9061.75.20235

Особистий внесок Юринець Ю.Л. – постановка завдання,

Особистий внесок Криволапа Є.В. – аналіз властивостей соціальних мереж як чинника формування іміджу.

7. Криволап Є.В. Публічно-правове регулювання підвищення рівня кібербезпеки в Європейському Союзі на підставі акту про кіберстійкість (The Cyber resilience Act). *Наукові інновації та передові технології (Серія «Управління та адміністрування», Серія «Право», Серія «Економіка», Серія «Психологія», Серія «Педагогіка»)*: журнал. 2025. № 3 (43). С. 516-526. DOI: https://doi.org/10.52058/2786-5274-2025-3(43)-516-526

8. Юринець Ю.Л., Криволап Є.В., Сопілко І.М., Бєлкін Л.М., Бєлкін М.Л. Проблеми формування державної політики у сфері кіберконфліктів. *Успіхи і досягнення у науці (Серія «Право», Серія «Освіта», Серія «Управління та адміністрування», Серія «Соціальні та поведінкові науки»)*, 2025. № 6 (16).

С. 249-270. DOI: https://doi.org/10.52058/3041-1254-2025-6(16)-249-270.

Особистий внесок Юринець Ю.Л. – постановка завдання,

Особистий внесок Криволапа Є.В. – формування переліку видів кіберконфліктів та аналіз їх властивостей,

Особистий внесок Сопілко І.М. – підбір правових актів,

Особистий внесок Бєлкіна Л.М. – генезис понять «кіберінцедент» та «кіберконфлікт»,

Особистий внесок Бєлкіна М.Л. – підбір літератури.

Наукові праці, які додатково відображають наукові результати дисертації:

9. Криволап Є.В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека». «Когнітивна безпека» як стійкість проти інформаційно-психологічних впливів на людину і суспільство. *Свобода, безпека та незалежність: правовий вимір*: матеріали XIII Міжнародної науково-практичної конференції, м. Київ, Національний авіаційний університет, 24 лютого 2023 р. С. 195-197.

10. Криволап Є.В. Питання застосування механізмів забезпечення інформаційної безпеки і кібербезпеки в реалізації безпекових стратегій України. *Наукові дослідження та інновації*: матеріали 2-ї Міжнар. науково-практичної інтернет-конференції, 3-4 квітня 2023 р. ФОП Марениченко В.В., Дніпро, Україна, С. 216-218.

11. Криволап Є.В. Засади правового регулювання заходів забезпечення кібербезпеки актами європейського рівня. *Глобальні проблеми та рішення*: матеріали 2-го Міжнародного науково-практичного Інтернет-конгресу, 10-11 квітня 2023 р. ФОП Марениченко В.В., Дніпро, Україна, С. 42-45.

12. Криволап Є.В. Вплив стратегій інформаційної та кібербзпеки на інші безпекові стратегії України. *VI Міжнародний молодіжний науковий юридичний форум*: матеріали форуму, м. Київ, Національний авіаційний університет, 18 травня 2023 р. С. 119-121.

13. Криволап Є.В., Юринець Ю.Л. До питання вразливості інформаційно-комунікаційних систем цивільної авіації: правовий аспект. *АЕРО-2023. Повітряне і космічне право*: матеріали Всеукраїнської конференції здобувачів вищої освіти і молодих учених, м. Київ, Національний авіаційний університет, 23 листопада 2023 р. Тернопіль: Вектор. С. 118-120.

14. Криволап Є.В. Підвищення рівня контролю і протидії вразливостям інформаційно-комунікаційних систем в аспекті відновлення України. *Правова парадигма відновлення України: проблеми та перспективи*: матеріали XIV Міжнародної науково-практичної конференції, м. Київ, Національний авіаційний університет, 23 лютого 2024 р. Тернопіль: Вектор, 2024. с. 220-223.

15. Криволап Є.В., Бєлкін Л.М., Юринець Ю.Л. Правові засади виявлення та протидії вразливостям інформаційно-комунікаційних систем на підставі методів bug bounty (білий хакінг) в Україні. *Впровадження інноваційних технологій та модернізація технічної складової сектору безпеки і оборони як вагомий чинник у боротьбі з агресором*: зб. матеріалів міжвідомчої науково-практичної конференції, 27 березня 2024 р., Київ / [відп. ред. Парфило О.А.] ; Укр. наук.-дослід. ін.-т спец. техніки та судових експертиз Служби безпеки України. Київ : ІСТЕ СБУ, 2024. С. 99-103.

16. Криволап Є.В. Адміністративно-правові засади виявлення та протидії вразливостям інформаційно-комунікаційних систем на підставі методів bug bounty (білий хакінг) в Україні. *VII Міжнародний молодіжний науковий юридичний форум*: матеріали форуму, м. Київ, Національний авіаційний університет, 16-17 травня 2024 р. С. 145-147.

17. Бєлкін М.Л., Криволап Є.В., Юринець Ю.Л. Адміністративно-правове регулювання нейтралізації вразливостей інформаційно-комунікаційних систем. *Збірник матеріалів «Актуальні питання забезпечення кібербезпеки» IX Міжнародної науково-практичної конференції*, м. Київ, 13 листопада 2024 року. Київ. МАУП. 13 листопада 2024 року. С. 38-42.

18. Криволап Є.В. Правові підходи до підвищення рівня кібербезпеки в Європейському Союзі (the Cyber Resilience Act, CRA). *Правова система*

України: європейський вектор розвитку в умовах воєнного стану: матеріали XV Міжнародної науково-практичної конференції, м. Київ, Державний університет «Київський авіаційний інститут», 21 лютого 2025 р. Тернопіль: Вектор, 2025. С. 201-204.

19. Криволап Є., Юринець Ю., Бєлкін Л., Бєлкін М. Поняття «кіберконфлікти» в системі термінології з кібербезпеки. *Innovations and New Directions in Scientific Research*: Proceedings of the 2nd International Scientific Conference, Manchester, United Kingdom, 20 September 2025. Lulu Press, Inc., 2025. P. 191-195.

20. Криволап Є.В. Використання фейкових сайтів в російській пропаганді. *АЕРО-2024. Повітряне і космічне право*: матеріали Всеукраїнської конференції, м. Київ, Державне некомерційне підприємство «Державний університет «Київський авіаційний інститут», 20 листопада 2024 р. Тернопіль. «Вектор». С. 113-115.

21. Юринець Ю.Л., Криволап Є.В., Бєлкін Л.М. Використання соціальних мереж для формування іміджу закладів вищої освіти. *Соціально-економічний розвиток у контексті викликів сьогодення*: матеріали III Міжнародної науково-практичної конференції / Східноєвропейський центр наукових досліджень (Одеса, 16 серпня 2025 р). Research Europe, 2025. С. 123-127.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, які містять 9 підрозділів, висновків, списку використаних джерел (366 найменувань) і 3 додатків. Загальний обсяг дисертації становить 343 сторінки, з них основний текст – 229 сторінок.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ КРАЇНИ: АДМІНІСТРАТИВНО-ПРАВОВИЙ ВИМІР

1.1. Правове забезпечення інформаційної та кібер- безпеки як предмет адміністративного права: засади міждисциплінарного підходу

У сучасному світі свобода слова перетворюється на грізну зброю ворожих впливів – інформаційну зброю. Зазначене у повній мірі проявилося у період широкомасштабної агресії рф проти України: велика кількість населення, піддалася інформаційним впливам російської пропаганди і стала на бік агресора. Володіння в сучасних умовах інформаційною зброєю і засобами захисту від неї є одним із пріоритетних напрямів забезпечення національної безпеки в інформаційній сфері [311, с. 305].

Впровадження нових інформаційно-комунікаційних технологій є основою соціально-економічного та науково-технічного прогресу – інформатизації суспільства [66]. Натомість, як зазначає професор Г. Почепцов, інформаційна цивілізація змінює не тільки статус інформації, тобто її позитивну роль, а й різко розширює негативні можливості. Інформація, яка поширюється через інформаційно-комунікаційні системи, стає потужним інструментом, який діє практично без обмежень. Інформаційні війни різної інтенсивності стали явною ознакою наших днів [234]. Ця проблема є особливо актуальною з огляду на великий потенціал впливу інформаційних мереж на державу суспільство, зокрема, на інформаційну безпеку [115, 259]. Так, у пункті 20 Стратегії національної безпеки України від 14.09.2020 р. № 392/2020 наголошується [22], що деструктивна пропаганда розпалює ворожнечу, підриває суспільну єдність, провокує конфлікти.

Глобальний інформаційний простір як середовище віртуального «перебування» великої кількості людей по всьому світу дало людству багато,

одночасно ставши об’єктом постійних ризиків і кібернетичних загроз… Тому протидія цим ризикам і кіберзагрозам, у вказаній сфері стало сьогодні першочерговим завданням для держави і окремих організацій [256, с. 105].

В наш час практично кожна сфера людської діяльності послуговується інформаційними технологіями, що, в свою чергу, створює для зловмисників приводи атакувати комп’ютерні системи. В результаті кібератаки стали звичайною справою [290, с. 41-42].

В статті [347] автори висновують, що можливості кіберпростору підвищили ризики кіберзагроз, спричинили масований та різноманітний вплив на людей, а також мають здатність підривати фундаментальні демократичні цінності та свободи. Вони можуть спричиняти та загострювати ескалацію воєнних дій у кіберпросторі, провокувати та поширювати інноваційні форми агресії. Таким чином, у ході гібридної війни в Україні кіберзагрози мали найвищий рівень негативного впливу на державні органи та критичну інфраструктуру [347, с. 334].

В статті [212] О.В. Мітенко наголошує на практичній безмежності глобального інформаційного простору поширювати та доставляти будь-яку інформацію, у тому числі і таку, що спрямовується проти безпеки суспільства, громадян, держави.

В Резолюції Європарламенту [16, п.п. 3, 4] зазначається, що анти-європейська пропаганда та дезінформація охоплює різні сфери, включаючи традиційні ЗМІ, соціальні мережі як у ЄС, так і за його межами. У пунктах 7-14 Резолюції наголошується саме на російських ворожих антиєвропейських діях.

Проф. В.Ю. Богданович наголошує, що інформаційний вплив є найпотужнішим чинником забезпечення воєнної безпеки України [84, с. 47].

Отже, відносини у сфері інформаційної безпеки стають чинниками відносин військових, що стало в повній мірі усвідомлюватися українським суспільством тільки після того, як широкомасштабна війна в Україні стала реальністю.

В українській науковій літературі питанням інформаційної й кібер-безпеки присвячені праці низки відомих вчених, серед яких Р.А. Калюжний [140-143], Ю.Д. Кунєв [179-182], С.Я. Лихова [188-190, 262, 351], І.М. Сопілко [255-262], В.В. Філінович [289-292, 339-340], О.О. Тихомиров [274-276, 321, 343, 346, 362], Н.Б. Новицька [209, 219, 222], М.І. Легенький [182, 347], А.І. Марущак [206, 207], В.Ю. Богданович [84-86], В.А. Ліпкан [191-201], інші автори [65, 74, 79, 80, 117, 119, 183, 202, 240, 251, 288, 308, 314 та ін.]. Натомість зміни інформаційної конфігурації світу вимагають від дослідників розробки нових підходів до розвитку інформаційного суспільства, з'ясування меж впливу закону на зв'язки з громадськістю.

Як зазначено вище, в сучасних умовах у здійсненні інформаційних атак і спеціальних інформаційних операцій провідну роль відіграють сучасні електронні засоби масової комунікації (Інтернет, радіомовлення, телебачення, супутниковий зв'язок,). Вади розвитку інформаційного суспільства породжують серйозні проблеми щодо запобігання негативним тенденціям, зокрема: протидії негативним ворожим інформаційним впливам – як на українську аудиторію, так і за кордонами України; забезпечення об'єктивності й достовірності інформації; унормування поширення інформації в Інтернеті [79, 240, 259, 308 та ін.].

Таким чином, поняття інформаційної безпеки нерозривно пов'язане з поняттям кібербезпеки. З точки зору національної (інформаційної) безпеки держави слід підкреслити, що кібервійна стає все більш важливою складовою гібридної війни. На основі теоретичного аналізу роботи вчених можна зробити висновок, що кібервійна – це протистояння в інформаційному (кібернетичному) просторі, мета якого – діяти на комп'ютерні мережі ворога. Кібервійна є невід'ємною частиною інформаційної війни [251].

У пункті 52 Стратегії національної безпеки України [22] основним завданням розвитку системи кібербезпеки визнане гарантування кібербезпеки національної інформаційної інфраструктури, її кіберстійкості, зокрема при цифровій трансформації [22].

Як наголошує проф. Ю.Д. Кунєв [180], проблема забезпечення інформаційної та кібер- безпеки стає особливо актуальною під час зовнішніх загроз, зокрема, гібридної війни. Правове забезпечення інформаційної безпеки є складовою інформаційно-адміністративного права [180, с. 101].

Відповідно до теоретичних поглядів проф. В.М. Торяника [281], забезпечення інформаційної безпеки держави як важливої складової національної безпеки України – важлива функція держави [281, с. 153-154]. Отже, участь держави у створенні механізмів забезпечення інформаційної і кібер- безпеки, правовому регулюванні цих механізмів покладає певні зобов'язання на публічну адміністрацію держави, вимагає здійснення регуляторних функцій у цій сфері і обумовлює створення правового регулювання. Зокрема, як констатують Ю.Д. Кунєв, Є.О. Легеза [181, с. 184-185], предметом розгляду заходів забезпечення інформаційної безпеки є як сама діяльність, так і елементи цієї діяльності, тобто повна схема взаємодії учасників такої діяльності із забезпечення належного та безпечного обігу інформації. Уся ця діяльність опосередковується засобами адміністративного права.

Як зазначає німецький вчений Е Шмідт-Ассманн [302], адміністративне право має захищати права громадянина в його взаємовідносинах з органами публічної адміністрації, але при цьому й врегульовувати права і обов'язки публічної адміністрації так, щоб вона могла ефективно виконувати свої повноваження. Реалізації такого подвійного замовлення слугує багатоманітність норм права, юридичних інститутів, процедурних й організаційних форм, які утворюють структуру регулювання адміністративного права. Наука адміністративного права повинна не тільки надійно продемонструвати цю багатоманітність і прокоментувати її. Вона має також напрацювати завдання та напрями розвитку, показати взаємозв'язки та поміркувати над потрібними змінами; нові форми врегулювання та виклики європеїзації публічно-адміністративної діяльності мають бути порівняні з панівною нині догматикою [301, передмова].

Безсумнівно, у воєнний час технічні елементи інформаційної безпеки мають першорядне значення. Саме вони дозволяють нам швидко реагувати на атаки та пом'якшувати їх наслідки. Водночас технічні рішення не можуть бути ефективними без відповідної правової бази. Закон визначає відповідальних суб'єктів, встановлює стандарти, регулює обмін інформацією та координацію дій. Саме це дає технічним спеціалістам чіткі правила та можливість швидко діяти [319, 350].

Системне дослідження структури і властивостей публічної адміністрації виконано в роботах В.К. Колпакова. Відповідно до концепції «публічної адміністрації» В.К. Колпакова [152, с. 31-32; 184, с. 23-24], правова категорія «публічна адміністрація» має два виміри: функціональний (діяльність певних владних структур, спрямована на реалізацію публічного інтересу – «публічне адміністрування») і організаційно-структурний (це сукупність органів, які утворюються для здійснення такої діяльності). Отже, аналогічний висновок щодо системної діяльності на реалізацію публічного інтересу слід зробити, зокрема, щодо виконання функцій «публічного адміністрування» у сфері забезпечення інформаційної та кібер- безпеки.

На публічну адміністрацію при її створенні покладаються зобов’язання, спрямовані на задоволення інтересів суспільства і громадян. Ці зобов’язання носять публічний характер, їх виконання потребує використання публічною адміністрацією владних повноважень. При їх реалізації виникають так звані «відносини адміністративних зобов’язань», а саме [184, с. 24]:

– публічного управління;

– адміністративних послуг;

– встановленої правовими нормами відповідальності публічної адміністрації у випадку їх неправомірних дій або бездіяльності;

г) відповідальності суб’єктів суспільства за порушення порядку і правил, встановлених публічною адміністрацією у межах її повноважень.

Характерною ознакою усіх вказаних адміністративно-правових відносин є владний характер діяльності публічної адміністрації, яка має

право на прийняття владного рішення, обов'язкового для виконання [184, с. 24].

Разом із тим, слід враховувати, що наведені принципи діяльності публічної адміністрації мають загальний характер і мусять переломлюватися крізь призму специфіки тої чи іншої сфери управлінської діяльності. Зокрема, з цього приводу згаданий вище німецький вчений Е Шмідт-Ассманн [302] висновує, що для того, щоб адміністративне право ефективно виконувало свої регулятивні функції в суспільстві, державі й економіці, наука адміністративного права повинна враховувати досягнення інших наук. Перш за все це стосується природничих і технічних наук. Так, право, що регулює публічне адміністрування інформації й адміністрування ризиків, не може розвиватися без інтенсивного вивчення відповідних фахових дисциплін. Право лише тоді спроможне протиставити щось динаміці розвитку самої техніки, коли воно розуміє її рушійні сили та механізми [302, с. 31].

Далі Е Шмідт-Ассманн [302] вказує, що будь-яка методологія адміністративного права повинна виходити з конкретної ситуації прийняття рішення виконавчою владою. Детальний аналіз показує, що ці ситуації мають різну форму прояву залежно від того, який вид права застосовується органом публічної адміністрації, у якому організаційному контексті це відбувається і якою мірою це пов'язано з виконанням певних завдань [302, с. 33].

За таких умов виникає необхідність «наведення мостів» між різними науками, яка полягає у застосуванні принципу міждисциплінарності [150, с. 19]. Всебічний аналіз підходів до визначення явища міждисциплінарності виконаний у роботі [158, с. 26], серед яких одним з ключових слід визнати взаємопроникнення, взаємозбагачення методів і підходів різних наук (дисциплін).

Таким чином, як інструмент публічного адміністрування у сфері інформаційної та кібер- безпеки суспільство послуговується методами і засобами адміністративного права, але для вирішення конкретних питань

правового забезпечення інформаційної та кібер- безпеки адміністративне право користується законами і правилами із сфери інформаційної та кібер-безпеки. У межах такого взаємозбагачення підходів і взаємопроникнення методів різних наук вдається досягнути ефективних результатів у сфері публічного адміністрування у даній сфері.

Натомість, як наголошується у статті [319], більшість сучасних правових підходів зосереджені або на кібербезпеці, або на протидії дезінформації, нехтуючи їхньою взаємозалежністю.

Закон України «Про правотворчу діяльність» [58] (ч. 2 ст. 9 Закону) офіційно встановлює сукупність і ієрархію актів публічної адміністрації, які охоплюються поняттям «законодавство України»: Конституція (Основний Закон) України; закони України; підзаконні нормативно-правові акти, що містять норми права, а саме: постанови Верховної Ради України, укази Президента України, що містять норми права; постанови КМУ; накази міністерств); акти інших державних органів, що містять норми права; накази і постанови суб'єктів публічної адміністрації, створених в Автономній Республіці Крим (АРК) – Верховної Ради АРК, Ради міністрів АРК, накази міністерств АРК; акти уповноважених керівників місцевих державних адміністрацій; акти органів місцевого самоврядування.

Частиною законодавства України визначені міжнародні правові акти, належним чином легітимізовані і Україні.

Варто зазначити, що як вказується у підручнику [81], адміністративне право розглядається як сукупність правових норм, спрямованих на регулювання суспільних відносин в сфері державного управління [81, с. 24]. У звіті СИГМА [126] зауважується, що хоча прояв і концепції адміністративного права (Verwal-tungsrecht, droit administrativ) різняться у різних національних системах, можна домовитися про універсальні визначення адміністративного права як про сукупність правил, що застосовуються до здійснення «публічного адміністрування» та до взаємин між адміністрацією і громадянами [126, с. 8].

Так, згідно пункту 18 ст. 106, ч.ч. 3, 7 ст. 107 Конституції України, Президент України очолює РНБО України є Головою РНБО України. Рішення РНБО України вводяться в дію указами Президента. Зокрема, з метою інституалізації положень, пов'язаних з національною безпекою України, протягом 2020-2021 рр. в Україні схвалена рішенням РНБО України та затверджена Указом Президента України низка безпекових стратегій, у тому числі: Стратегія національної безпеки України від 14.09.2020 р., схвалена рішенням РНБО України від 14.09.2020 р. та затверджена Указом Президента України від 14.09.2020 р. № 392/2020 [22]; Стратегія воєнної безпеки України від 25.03.2021 р., схвалена рішенням РНБО України від 25.03.2021 р. та затверджена Указом Президента України від 25.03.2021 р. № 121/2021 [23]; Стратегія кібербезпеки України від 14.05.2021 р., схвалена рішенням РНБО України від 14.05.2021 р. та затверджена Указом Президента України від 26.08.2021 р. № 447/2021 [24]; Стратегія розвитку оборонно-промислового комплексу України від 18.06.2021 р., схвалена рішенням РНБО України від 18.06.2021 р. та затверджена Указом Президента України від 20.08.2021 р. № 372/2021 [25]; Стратегія зовнішньополітичної діяльності України від 30.07.2021 р., схвалена рішенням РНБО України від 30.07.2021 р. та затверджена Указом Президента України від 26.08.2021 р. № 448/2021 [26]; Стратегія інформаційної безпеки від 15.10.2021 р., схвалена рішенням РНБО України від 15.10.2021 р. та затверджена Указом Президента України від 28.12.2021 р. № 685/2021 [28]; Стратегія забезпечення державної безпеки від 30.12.2021 р., схвалена рішенням РНБО України від 30.12.2021 р. та затверджена Указом Президента України від 16.02.2022 р. № 56/2022. [29]. Ці документи являють собою комплексне нормативно-правове упорядкування засад публічно-правової діяльності у безпекових сферах Держави.

Ключовим правовим актом України у сфері забезпечення кібербезпеки є Закон від 05.10.2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» (далі – Закон № 2163-VIII).

Так, у преамбулі цього Закону наголошено, що 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.

В контексті організаційно-структурного підходу до поняття «публічна адміністрація» Закон визначає основні суб'єкти національної системи кібербезпеки, а саме: Державна служба спеціального зв'язку та захисту інформації України, Міністерство оборони України та Генеральний штаб Збройних Сил України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи України, Міністерство закордонних справ України, які відповідно до Конституції і законів України виконують у встановленому порядку завдання, встановлені Законом (стаття 8 Закону № 2163-VIII).

Слід звернути увагу, що у Законі № 2163-VIII міститься поняття кіберзлочин (комп'ютерний злочин) – це суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України (пункт 8 статті 1 Закону № 2163-VIII).

Отже, потенційна можливість здійснення у кіберпросторі злочинів, а також залучення до забезпечення кібербезпеки органів боротьби із злочинністю, ставить питання про зв'язок адміністративно-правового регулювання з кримінальним правом. Сучасні погляди на адміністративне право свідчать про те, що такий зв'язок існує [63, с. 61], оскільки кримінальне право надає заходи кримінально-правового захисту норм, встановлених публічною адміністрацією. Найпоширеніше в юридичній і спеціальній літературі визначення поняття адміністративної діяльності органів внутрішніх справ сформульовано в такий спосіб: адміністративна діяльність

органів внутрішніх справ (поліції) – це виконавчо-розпорядницька діяльність щодо організації роботи служб і підрозділів зазначених органів і практичного здійснення адміністративно-правовими способами охорони громадського порядку, забезпечення громадської безпеки і боротьби зі злочинністю [63, с. 259].

Як зазначалося у Вступі до цієї дисертаційної роботи, ворожі інформаційні впливи несуть небезпеки як інформаційно-комунікаційним системам, так і безпосередньо особам, оскільки використовуються для доставляння небажаної інформації в обхід запобіжників її отримання.

Вирішення питання захисту суспільства і особи від інформації необхідне тому, що інформація формує у людській свідомості систему поглядів чи переконань, якими людина керується у своїх вчинках, зокрема, ворожих по відношенню до оточення, суспільства, держави. Інформація може змінювати поведінку людей. Зокрема, проф. Г.Г. Почепцов вважає, що у сфері інформаційної і кібер- безпеки традиційно багато уваги приділяється кібербезпеці і мало тому́, що можна позначити поняттям «***когнітивна безпека***». У кібербезпеці захищають кіберресурси, у когнітивній безпеці – розум людини. Ми живемо у світі пропаганди, яка, як правило, спотворює реальність [235]. Пропаганда робить ментальну операцію, замінюючи одні сенси на інші, причому робить це непомітно для «пацієнта»… [236]. Тобто, когнітивна операція спрямована на зміну моделі світу людини [237, с. 170].

Професор М.В. Маркова зазначає, що інформаційно-психологічний вплив може викликати зрушення в цінностях, життєвих позиціях, орієнтирах, світогляді особистості. Такі зміни зумовлюють вияви девіантної антисоціальної поведінки й становлять небезпеку вже для суспільства й держави [205, с. 7]. Медіа-аналітик К. Ілюк [136] також наголошує, що інформаційно-психологічний вплив завжди здійснюється з метою зміни поведінки. Тобто кожен фейк, провокація чи спекуляція у своїй сукупності має штовхати до дії.

Водночас, Інтернет створює для поширення небажаного контенту

незрівнянно більші можливості, ніж радіо та телебачення: мова йде про значно більший спектр можливостей з розміщення та доставки інформації до адресата найрізноманітнішого характеру (відео, картинки, світлини, текст, аудіо), ніж радіо та телебачення, про значну більшу швидкість поширення інформації; значно менші витрати трудових і матеріальних ресурсів на створення контенту [93, 311]. Отже, інформаційно-комунікаційні мережі сприяють ефективній доставці і навіть нав’язуванню ворожого культурного та/або інформаційного контенту.

Окремо слід зазначити такий аспект адміністративного права, як регулювання відносин відповідальності суб’єктів суспільства за порушення порядку і правил, встановлених публічною адміністрацією у межах її повноважень – у разі порушення заборон, встановлених КУпАП та іншими нормативними актами. Розвиток таких відносин завершується притягненням винних осіб до адміністративної відповідальності і застосуванням до таких осіб заходів впливу, встановлених законом [184, с. 31]. Основні риси адміністративної відповідальності полягають у тому, що її підставою є адміністративне правопорушення (проступок). Велику увагу проблемам адміністративної відповідальності приділяли В.К. Колпаков [151], Ю.П. Битяк [81], С.Т. Гончарук [108] та інші вчені-адміністративісти. Більшість досліджень у цій сфері спрямовується на регулювання відносин в певній сфері публічного управління і, як засіб, розглядається адміністративна відповідальність за правопорушення в певній сфері правового регулювання [182, с. 92].

Зв'язок теорії адміністративної відповідальності з забезпеченням кібер-безпеки пов'язаний із тим, що така відповідальність передбачена відповідними нормами Закону № 2163-VIII. Згідно ч. 1 ст. 6 цього Закону, посадові особи операторів критичної інфраструктури, власників або розпорядників об’єктів критичної інформаційної інфраструктури… несуть відповідальність за невиконання вимог з захисту інформації та кіберзахисту… згідно із законом. Аналогічна норма міститься у ст. 12 цього

Закону.

Автором цього дисертаційного дослідження систематизовані норми деліктів у сфері обігу інформації та інформаційної й кібер- безпеки за КУпАП. Результати аналізу узагальнені в таблиці додатку А1. З таблиці, наведеною в додатку А1, видно, що адміністративна відповідальність передбачена, зокрема, за порушення у сфері використання телекомунікаційних мереж; у сфері порушень авторського права в мережі Інтернет; незаконне зберігання спеціальних технічних засобів негласного отримання інформації; невиконання законних вимог посадових осіб відповідних регуляторних органів; відмова у наданні або, навпаки, незаконне поширення інформації всупереч вимогам законодавства; здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах, зокрема, незаконний збут такої інформації.

Наприклад, Постановою від 18.07.2018 року у справі № 758/9072/18 Подільського районного суду м. Києва адміністратор безпеки державного ресурсу Міністерства фінансів України «minfin.gov.ua», який здійснював, через мережу Інтернет з використанням сервісу Ubuntu apt-get несанкціонований доступ до державного ресурсу Міністерства фінансів України «minfin.gov.ua», притягнутий до адміністративної відповідальності за ч. 1 ст. 212-6 КУпАП [127, № 75396749].

Разом із тим, як зазначено вище, захист суспільних відносин у сфері обігу інформації та інформаційної й кібер- безпеки здійснюється також через встановлення кримінальної відповідальності [139, 190]. Основним критерієм розмежування адміністративного правопорушення та злочину є суспільна небезпека [116]. Окремі аспекти кримінальної відповідальності у сфері обігу інформації та інформаційної й кібер- безпеки розглядаються автором у подальших розділах цієї дисертаційної роботи.

Таким чином, міждисциплінарний підхід як він запропонований і використовується у даній дисертаційній роботі, полягає у поєднанні засобів,

методів і правил адміністративного права, інформаційного права, права кібербезпеки, теорії психології впливів, деліктології. Ефективність та перспективність міждисциплінарного підходу обґрунтована дисертантом у статті [319].

1.2. Технологічні аспекти виникнення кіберзагроз і проблеми протидії цим загрозам

Інтенсивний розвиток інформаційних систем та технологій всебічно впливає на всі сфери діяльності суспільства. Переважна кількість сучасних державних та приватних підприємств використовує інформаційні системи для управління виробничими процесами, підтримки прийняття рішень, пошуку необхідних даних тощо. Це забезпечує їм низку переваг, пов’язаних з: підвищенням продуктивності праці і мобільності працівників; високою оперативністю доступу до інформації та послуг; можливостями віддаленого управління ресурсами і процесами тощо. Разом з цим збільшується кількість вразливостей та загроз інформаційних систем і тому для забезпечення їх нормального функціонування та попередження вторгнень необхідні спеціалізовані засоби безпеки [154, с. 5].

Стратегія національної безпеки України (п. 47) [22] визначає, що Україна запровадить національну систему стійкості … що, зокрема, передбачатиме: оцінку ризиків, визначення ***вразливостей***, своєчасну ідентифікацію загроз.

Вразливість – це нездатність системи протистояти певним впливам (випадковим або навмисним). Основні причини появи вразливостей пов'язані з використанням комп'ютерних мереж у цілому та Інтернету зокрема [273, с. 1-2].

Інформатизація та її розвиток є характерною рисою сучасного суспільства. Нові інформаційні технології (ІТ) впроваджуються в усі сфери діяльності суспільства й держави. Інформаційні системи (ІС) управляють

космічними об’єктами, розподіляють електроенергію, контролюють роботу атомних електростанцій й обслуговують банківські системи. Інформаційно-комунікаційні системи стають основою обміну інформаційними ресурсами суспільства, вони здійснюють зберігання, передачу й обробку інформації, надання послуг споживачам з впровадженням найсучасніших технологій [304, с. 6].

Сучасні організації та підприємства усе ширше впроваджують корпоративні інформаційно-комунікаційні системи й мережі у свою діяльність. Це дозволяє підвищити ефективність діяльності компанії завдяки використанню більш актуальної й повної інформації, а також відкриває нові можливості для взаємодії з контрагентами за допомогою загальнодоступних глобальних інформаційних мереж [304, с. 6].

Новітні інформаційно-комунікаційні технологій об'єднали окремі мережі в глобальне інформаційне середовище, що призвело до появи глобальних мережі передачі даних та інформаційні системи [304, с. 6].

Однак разом із перевагами, з'являються й небезпечні ризики стосовно взаємодії інформаційно-комунікаційних систем з неконтрольованим зовнішнім інформаційним середовищем [304, с. 6]. Вказані системи стають вразливими для негативного впливу зовнішнього інформаційного середовища, негативними наслідками чого є [155, 332]:

– виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону);

– негативний вплив на стан енергетичної безпеки держави (регіону);

– негативний вплив на стан економічної безпеки держави;

– негативний вплив на стан обороноздатності, забезпечення національної безпеки та правопорядку у державі;

– негативний вплив на систему управління державою;

– негативний вплив на суспільно-політичну ситуацію в державі;

– негативний вплив на імідж держави;

– порушення сталого функціонування фінансової системи держави;

– порушення сталого функціонування транспортної інфраструктури держави (регіону);

– порушення сталого функціонування інформаційної й телекомунікаційної інфраструктури держави (регіону), зокрема, її взаємодії з інфраструктурами інших держав.

Для зниження цих ризиків необхідно приділяти все більш уваги побудові, впровадженню й супроводу комплексних систем безпеки, згідно вимог державних і міжнародних стандартів. Актуальність і важливість проблеми забезпечення безпеки інформаційних технологій, обумовлені наступними причинами [304, с. 7]:

– збільшення обчислювальної потужності сучасних автоматизованих комплексів при одночасному спрощенні їхньої експлуатації;

– різке збільшення обсягів інформації, що обробляється та передається каналами зв’язку;

– різке зростання кількості розподілених баз даних та їх стандартизація й інтеграція до сучасного інформаційного простору;

– високі темпи росту використання інформаційних технологій в діяльності суспільства;

– різке розширення кількості джерел інформації та кола користувачів інформаційними ресурсами і широкого спектра послуг, що надаються інформаційними системами;

– поширення сучасних мережних технологій [304, с. 7].

Об’єктивна необхідність захисту інформації в інформаційних системах обумовлена низкою факторів, які сприяють підвищенню вразливості комп’ютерної інформації, зокрема: різке збільшення обсягів інформації, що накопичується, обробляється та зберігається за допомогою комп’ютерів; значне розширення кола користувачів, допущених до інформаційних ресурсів в системах і мережах; зосередження в єдиних базах даних інформації великого обсягу, різного призначення і різної приналежності; ускладнення режимів функціонування комп’ютерних систем; автоматизація обміну

комп’ютерною інформацією; широке впровадження багатопрограмного режиму тощо. У цих умовах виникає вразливість двох видів: з одного боку, можливість несанкціонованого використання інформації (небезпека витоку комп’ютерної інформації обмеженого користування), а з іншого – можливість спотворення або знищення комп’ютерної інформації (порушення її фізичної цілісності), [236]. Тому важливого значення набуває вирішення проблем захисту інформації в персональних комп’ютерах, що широко увійшли в нашу повсякденну діяльність [236].

Розглянемо окремі технологічні аспекти виникнення кіберзагроз і правові шляхи протидії цим загрозам.

Питання нейтралізації вразливостей: нормативно-правовий аспект.

Стратегія кібербезпеки України [24] (розділ 1) визначає, що поширення кіберзагроз вимагає максимально швидкого виявлення кібератак і ***вразливостей***, реагування та поширення відомостей про них для мінімізації можливої шкоди.

В розділі 6 «Стратегічні завдання» щодо розбудови національної системи кібербезпеки виділені, між іншим, такі важливі напрями [24]:

запровадження на постійній основі оцінки стану захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів на ***вразливість***, … стимулювання участі у цих заходах фахівців з кібербезпеки приватного сектору;

запровадження скоординованого виявлення та розкриття ***вразливостей*** інформаційно-комунікаційних систем.

В публікаціях [330, 364] аналізуються підходи щодо визначення вразливості комп’ютерних систем до кібератак. Вразливості – слід розглядати як недоліки в комп’ютерній системі, що послаблюють загальну безпеку пристрою/системи. Вразливості можуть бути слабкими місцями як в апаратному забезпеченні, так і в програмному забезпеченні. Вразливості можуть бути використані зловмисником для виконання неавторизованих

(несанкціонованих) дій у комп'ютерній системі. Щоб використати вразливість, зловмисник повинен мати принаймні один відповідний інструмент, який може підключитися до слабкої сторони системи.

Управління вразливістю – це циклічна практика, яка містить процеси, що включають: виявлення всіх активів, визначення пріоритетів активів, оцінку або виконання повного сканування вразливостей, звіт про результати, усунення вразливостей, перевірку виправлення – повторення. Ця практика, як правило, стосується вразливостей програмного забезпечення в обчислювальних системах. Гнучке управління вразливістю означає запобігання атакам шляхом якнайшвидшого виявлення всіх вразливостей [315].

Офіційне міжнародне визначення поняття «вразливість» міститься в міжнародному стандарті інформаційної безпеки ISO 27005 (в Україні має назву *ДСТУ ISO/IEC 27005:2015 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT)*). Стандарт визначає вразливість як слабкість активу або групи активів, які можуть бути використані однією або декількома загрозами, де активом є все, що має цінність для організації, її бізнес-операцій та їх безперервності, у тому числі інформаційні ресурси, які підтримують місію організації [364].

Необхідно зазначити, що поняття «вразливість» згадується також в Законі № 2163-VIII [51], де, зокрема, вказується, що функціонування національної системи кібербезпеки забезпечується, в тому числі, за рахунок впровадження організаційно-технічної моделі національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію ***вразливості*** комунікаційних систем (пункт 15 ч. 3 ст. 8 Закону). Згідно ч. 5 ст. 8 цього Закону, впровадження організаційно-технічної моделі кібербезпеки … здійснюється Державним центром кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного доступу

державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, системи виявлення ***вразливостей*** і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту... Цим же Законом частина 1 статті 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» [45] доповнена пунктом 91, яким до обов'язків Служби віднесені «координація, організація та проведення аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на ***вразливість***».

Таким чином, в законодавстві України питанням нейтралізації вразливостей приділяється певна увага як важливому чиннику кібербезпеки, *однак універсального юридичного визначення цьому поняттю не надано*. Натомість, на офіційному рівні визначення «вразливість системи» («system vulnerability») наведене у Нормативному документі НД ТЗІ 1.1-003-99 Служби безпеки України «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» [62]. За пунктом 4.2.11 цього документу, вразливість системи – це нездатність системи протистояти реалізації певної загрози або сукупності загроз. Це визначення визначає «вразливість» більш вузько, ніж міжнародний стандарт ISO 27005.

Водночас, у «Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж», затвердженому постановою КМУ від 16.05.2023 р. № 497 (далі – Порядок № 497) [59], поняття «вразливість системи» вживається в такому значенні – це «властивість системи, через використання якої створюється загроза для її безпеки, порушується сталий, надійний та штатний режим функціонування системи, здійснюється несанкціоноване втручання в її роботу, створюється загроза для безпеки (захищеності) електронних інформаційних ресурсів, конфіденційності, цілісності, доступності таких ресурсів». Зазначається, що

цей термін використовується конкретно для цілей цього Порядку.

Окремі питання правового регулювання процедур виявлення вразливостей розглянуті автором цього дисертаційного дослідження у його роботах [77, 160, 166, 170, 172, 179, 342].

Як зазначено вище, одним із основних суб'єктів національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку), яка, зокрема, «забезпечує формування та реалізацію державної політики з кіберзахисту державних інформаційних ресурсів та інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, активної протидії агресії в кіберпросторі, кіберзахисту критичної інфраструктури, здійснює державний контроль у зазначених сферах».

Держспецзв'язку в публікації [279] звернув увагу на необхідність систематичної протидії вразливостям інформаційно-комунікаційних систем, виділив ключові вразливості інформаційно-комунікаційних систем за даними Державного центру кіберзахисту Держспецзв'язку (ДЦКЗ Держспецзв'язку). Підсистема Оперативного центру реагування на кіберінциденти ДЦКЗ Держспецзв'язку є центральною складовою системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Вона забезпечує централізований збір та накопичення інформації про мережеві події інформаційної безпеки, централізоване управління усіма підсистемами системи виявлення ***вразливостей*** і реагування на кіберінциденти та кібератаки, а також проводить моніторинг та обробку в режимі реального часу кіберзагроз і кіберінцидентів. З-поміж усіх видів вразливостей, виявлених внаслідок моніторингу, ДЦКЗ виокремлює найбільш поширені, якими користуються зловмисники для атак на інформаційно-комунікаційні системи [279]:

– *використання застарілого (вразливого) програмного забезпечення та/або операційних систем*;

– *надмірна кількість відкритих сервісів*;

– *недоліки у налаштуваннях мережевого обладнання, зокрема порушення контролю доступу*;

– *недотримання вимог кібергігієни*;

– *особливості використання віддаленого доступу*.

Сутність вказаних вразливостей описана в таблиці додатку Б4 [279].

В навчальному посібнику [272, с. 20] також вказується, що вразливість може виникати в результаті допущених помилок програмування, недоліків, допущених під час проектування системи, ненадійних паролів, вірусів та інших шкідливих програм, скриптових і SQL-ін’єкцій. Деякі уразливості відомі тільки теоретично, інші ж активно використовуються і мають відомі експлойти. Вразливості класифікуються відповідно до класу активів, до яких вони належать:

– апаратне забезпечення**:** сприйнятливість до вологості; сприйнятливість до пилу; сприйнятливість до забруднень; сприйнятливість до незахищеного зберігання**;**

– програмне забезпечення: недостатнє тестування; відсутність аудиту;

– комп’ютерна мережа: незахищені лінії зв’язку; незахищена мережева архітектура;

– персонал: недоліки найму працівників; недостатня поінформованість про небезпеку;

– сайт**:** ненадійне джерело живлення**;**

– організація: відсутність регулярних перевірок; відсутність планів безперервності; відсутність безпеки**.**

Зазвичай вразливість дає змогу атакуючому «обдурити» додаток – змусити його вчинити дію, на яку у нього не повинно бути прав. Це робиться шляхом впровадження будь-яким чином у програму даних або коду в такі місця, які програма сприйме як «свої». Деякі вразливості з’являються через недостатню перевірку даних, що вводяться користувачем, і дозволяють вставити в інтерпретований код довільні команди (SQL-ін’єкція, XSS). Інші вразливості з’являються через більш складні проблеми, такі як запис даних у

буфер без перевірки його меж (переповнення буфера).

Для аналізу захищеності операційних систем Microsoft Baseline Security Analyzer (MBSA) 2.0 може використовуватися база National Vulnerability Database (NVD) [272, с. 6]. База розроблена National Institute of Standards and Technology (NIST) Computer Security Division, Information Technology Laboratory за підтримки Department of Homeland Security's National Cyber Security Division. Вона є державним сховищем даних США, яке засноване на стандартах управління вразливостями. Такі дані дозволяють автоматизувати процеси управління вразливостями, вимірювати стан інформаційної безпеки і визначати його відповідність. База NVD включає в себе базу даних контрольних списків безпеки, недоліків PIC, неправильних конфігурацій, PIC і показників впливу. База даних – репозитарій основних стандартів управління даними вразливостей, розроблений на основі протоколу автоматизації контенту безпеки – Security Content Automation Protocol (SCAP) [272, с. 6].

Директива Європейського Парламенту і Ради ЄС 2022/2555 від 14.12.2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту ЄС 910/2014 та Директиви ЄС 2018/1972 та скасування Директиви ЄС 2016/1148 (Директива NIS 2) (далі – Директива 2022/2555) [14] передбачає створення Європейської бази даних про вразливості. Ця база даних містить:

– інформацію, що описує вразливість;

– уражені продукти ІКТ чи послуги ІКТ та серйозність вразливості з точки зору обставин, за яких її може бути експлуатовано;

– наявність пов'язаних патчів (часткових змін в програмному забезпеченні) і, за відсутності доступних патчів, інструкції, надані компетентними органами чи групами реагування на інциденти комп'ютерної безпеки (CSIRT) користувачам вразливих продуктів ІКТ та послуг ІКТ щодо можливих способів пом'якшення ризиків, спричинених відомими вразливостями.

Для підвищення ефективності виявлення вразливостей в Україні протягом 2022-2023 рр. офіційно запроваджена так звана система bug bounty – це тестування електронних сервісів із залученням зовнішніх фахівців, яке дає можливість виявити вразливі місця і недоліки в програмних продуктах. Процедура широко застосовується у всьому світі [233]**.** Процедура по суті заохочує так званих «білих» хакерів атакувати певні системи на договірній основі з метою перевірки їх стійкості до таких атак і пошуку вразливостей. За знайдені помилки пропонується винагорода. Це дозволяє розробникам усунути помилки, запобігаючи випадкам масових зловживань і не допускаючи дискредитації застосованих технічних (апаратних і програмних) рішень серед широкої громадськості. Програми Bug bounty були реалізовані в компаніях Mozilla, Facebook, Yahoo!, Reedit, Google, Square і Microsoft [322]. Безпечність застосунку «Дія» тестувалася також за допомогою програми Bug bounty [123]. «Біли хакери» зі всього світу підтвердили надійність «Дії» під час проведення програми Bug Bounty. Повідомляється, що у грудні 2020 року команда Міністерства цифрової трансформації на платформі Bugcrowd за підтримки агентства з міжнародного розвитку США (USAID) провела тестування на знаходження можливих помилок у «Дії». У застосунку не виявили вразливостей, які б впливали на безпеку. Знайдено два технічні баги найнижчого рівня, які одразу були виправлені спеціалістами проекту «Дія».

Офіційне запровадження системи Bug Bounty в Україні здійснювалося у два етапи. На першому етапі були внесені відповідні зміни у КК України. Суть цих змін полягала у тому, що стаття 361 КК України, яка передбачала кримінальну відповідальність за «несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж», була доповнена частиною 6, відповідно до якої ці дії не тягнули кримінальну відповідальність, «***якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж***» (Закон

від 24.03.2022 року № 2149-IX [54]).

На другому етапі запровадження системи Bug Bounty КМУ затвердив Порядок № 497 [59], згаданий вище. Порядок визначає механізм пошуку та виявлення потенційних вразливостей в інформаційних, електронних комунікаційних системах та мережах. Він встановлює правила та процедури для здійснення цієї діяльності, яка є важливим елементом забезпечення кібербезпеки, щоб протидіяти загрозам та порушенням цілісності систем. Мета порядку – створити формалізований підхід до пошуку вразливостей у системах, що є критично важливим для захисту від навмисних або випадкових впливів. Порядок не поширюється на інформаційно-комунікаційні системи, інформаційні (автоматизовані), електронні комунікаційні системи та мережі, в яких обробляється службова інформація та/або інформація, що становить банківську таємницю, державну таємницю, розвідувальну таємницю.

Відповідальність за безпеку інформації в системах відповідальність несе власник або розпорядник системи, тому пошук вразливостей є їхньою прямою відповідальністю. Тому організація пошуку потенційної вразливості системи, згідно Порядку, здійснюється її власником, який за необхідності може прийняти рішення про залучення, на договорінй основі, координатора для організації пошуку потенційної вразливості системи. Пошук потенційної вразливості здійснюється на підставі публічної пропозиції. Публічна пропозиція оприлюднюється власником системи на власному офіційному веб-сайті, а при залученні для пошуку вразливості координатора – на веб-сайті останнього. У такому разі власник системи оприлюднює на своєму офіційному веб-сайті посилання на відповідну сторінку веб-сайта координатора. Публічна пропозиція викладається українською мовою і – додатково – може бути викладена власником системи та/або координатором офіційною мовою Ради Європи.

Публічна пропозиція розробляється власником системи або координатором згідно примірної публічної пропозиції, затвердженої

Адміністрацією Держспецзв’язку. Така «Примірна публічна пропозиція», а також Методичні рекомендації з розроблення публічної пропозиції, затверджені Наказом від 14.07.2023 № 599 Адміністрації Держспецзв’язку [61]. У публічній пропозиції визначаються, зокрема: інформація про систему, яка перевіряється на вразливість; заборонені дії дослідника; вимоги до звіту дослідника і порядок його подання; відомості про винагороду дослідника та/або моральне захочення у вигляді публічного висловлювання подяки; період нерозголошення інформації про вразливість системи (не більше шести місяців з дати реєстрації звіту); додаткові умови.

Під час виконання роботи з пошуку потенційної вразливості системи дослідник може: здійснювати збір інформації у відкритих джерелах про систему та умови її використання, про інфраструктуру та інтерфейси системи; аналізувати та вивчати оприлюднену власником системи або власником прав інтелектуальної власності на систему документацію щодо роботи системи; сканувати мережу, хости і сервіси без подолання систем логічного захисту; проводити інші дії за згодою власника системи та власника прав інтелектуальної власності на систему та її компоненти.

Загальна логіка пошуку і виявлення вразливостей у системах грунтується на аналізі їхньої архітектури, конфігурації та програмного забезпечення, а також за допомогою тестування, яке може включати сканування на наявність вразливостей, проникнення та інші методи. Основна мета – знайти недоліки, які можуть бути використані для порушення цілісності, доступності чи конфіденційності інформації. Для цього використовують спеціалізовані інструменти та дотримуються процедур, що включають такі етапи: ідентифікація об'єктів, аналіз загроз, моделювання атак та оцінка ризиків.

Етапи пошуку та виявлення вразливостей:

– ідентифікація системи: визначення меж системи, включаючи апаратне та програмне забезпечення, мережеві компоненти, а також взаємодію з іншими системами;

– складання переліку всіх компонентів системи та їхніх функцій;

– аналіз загроз: визначення потенційних загроз для системи, що можуть призвести до її компрометації;

– аналіз векторів атак, які можуть бути використані зловмисниками (вектор атаки – це послідовність дій або засіб для отримання неавторизованого доступу до захищеної інформаційної системи [92]). Методичні рекомендації, затверджені Наказом від 14.07.2023 № 599 Адміністрації Держспецзв'язку [61], передбачають можливість не виплачувати винагороду дослідникові у випадку відсутності у звіті детального опису векторів атак;

– моделювання атак: використання спеціалізованих інструментів для моделювання атак на систему;

– імітація дій зловмисників для перевірки стійкості системи: тестування на проникнення (pentest); проведення тестування, яке імітує реальну атаку на систему, з метою виявлення вразливостей; виявлення слабких місць у програмному забезпеченні та конфігурації;

– виявлення та документування вразливостей: збір та аналіз даних, отриманих під час тестування, для виявлення всіх знайдених вразливостей, складання звіту з детальним описом кожної вразливості, її впливу та рекомендаціями щодо її усунення, розробка та впровадження заходів для усунення виявлених вразливостей;

– оцінка ризиків та пріоритезація – оцінка ймовірності використання зловмисником кожної вразливості.

– усунення вразливостей.

Після завершення пошуку потенційної вразливості дослідник подає йому звіт. Власник системи та/або координатор перевіряє звіт на відповідність вимогам публічної пропозицією, наявність в ньому інформації про вразливість системи, виявлену раніше іншими дослідниками, вивчає умови та можливі ризики використання зловмисниками виявленої вразливості, приймає рішення щодо внесення/невнесення змін до системи.

Якщо прийняте рішення про внесення змін до системи, про таке рішення та відповідну виявлену вразливість повідомляється урядова команда реагування на комп'ютерні надзвичайні події України CERTUA, а в разі наявності – галузева команда реагування на комп'ютерні надзвичайні події. Власник системи, в якій обробляються державні інформаційні ресурси, оператор критичної інфраструктури повідомляє також Національній поліції та СБУ.

Протягом 30 робочих днів з дати реєстрації звіту власник системи або координатор повідомляє досліднику про прийняте рішення щодо внесення/невнесення змін до системи. У разі отримання повідомлення щодо невнесення змін до системи дослідник має право оприлюднити інформацію про виявлену вразливість та її технічні особливості.

У випадку прийняття рішення про внесення змін до системи власник системи вживає заходів щодо запобігання можливим наслідкам у разі використання вразливості. Власник системи може прийняти рішення про оприлюднення інформації про виявлену вразливість до внесення змін до системи.

Крім інформації та положень, які передбачені безпосередньо Порядком № 497 [59], у Методичних рекомендаціях передбачені підходи до визначення винагороди дослідника, яку визначає власник системи і якщо така винагорода передбачається, у системному зв'язку із виявленими вразливостями системи. Винагородою може бути: матеріальний подарунок, певна сума коштів у національній валюті; інше. Винагорода встановлюється згідно категорії виявленої вразливості. Приклад визначення категорії вразливості відповідно до BugCrowd Vulnerability Rating Taxonomy наведено в таблиці додатку Б2.

Методичні рекомендації, затверджені Наказом від 14.07.2023 № 599 Адміністрації Держспецзв'язку [61], дозволяють не передбачати виплату винагороди, але заохочувати дослідника будь-яким іншим способом. Як зазначено вище, у виплаті винагороди може бути відмовлено у випадку

некоректних випадків опису вразливості у звіті без детального опису вектора атаки та доказів потенційного завдання збитку або шкоди.

Практичне значення нормативно-правових актів про Bug Bounty полягає у тому, що це правове регулювання служить для розробки та впровадження заходів безпеки, що допомагають запобігти несанкціонованому доступу та іншим видам атак.

Забезпечення належного рівня кібербезпеки Інтернет-речей (IoT): нормативно-правовий аспект.

Сьогодні багато пристроїв можуть підключатися до мережі Інтернет, отримуючи і відправляючи певну інформацію. Така здатність робить пристрій «розумним» (тобто «старт» – від англ. Smart) забезпечує його більшу ефективність. Інтернет речей (також IoT, від англ. Internet of Things) став буденністю, частиною нашого повсякденного життя. Прикладами подібного є «розумні» годинники, системи «розумний будинок», «розумне авто» розумні лічильники, розумні роботи, Wi-Fi роутери тощо.

При цьому сама така річ (пристрій) не повинна бути зверх-високотехнологічною, досить того, щоб вона могла підключатися до серверів такого «надкомп'ютера». Але із безсумнівними благами Інтернет речей приніс нам і велику кількість негативних моментів, пов'язаних із «ударами» по кібербезпеці: використання його елементів нерідко призводить до зростання ризиків, пов'язаних із кібербезпекою, оскільки кожен із нас може стати жертвою кіберзлочинців, всього лише використовуючи звичні речі [291, с. 122].

Так, в літературі описаний випадок, коли пасажир, який презентував себе як дослідник з безпеки One World Labs, зламав розважальну систему під час польоту (IFE) літака та перезаписав код на комп'ютері керування тягою літака, перебуваючи на борту. У публікації йдеться, що він зміг видати команду на підйом і змусити літак ненадовго змінити курс. Він отримав фізичний доступ до мереж через електронний блок сидіння (SEB). Вони встановлені по два в ряд, з кожного боку проходу під пасажирськими

сидіннями, на певних літаках. Після зняття кришки SEB шляхом «похитання та стиснення блоку», він підключив кабель Ethernet Cat6 з модифікованим роз'ємом до блоку та до свого ноутбука, а потім використав ідентифікатори та паролі за замовчуванням, щоб отримати доступ до бортової розважальної системи. ***Підключившись до цієї мережі, він зміг отримати доступ до інших систем на літаках*** [366]. Отже, система розваг літака, яка, на перший погляд, не мла відношення до захищених систем управління літаком, стала провідником негативного впливу.

Як визначає В. Муравський, [213], технологія Інтернету речей – це сукупність знань про використання програмно-технічного комплексу, який містить технологічні датчики, виконавчі механізми, сенсорні монітори та мікрокомп’ютери у формі елементів одягу, побутової техніки, транспортних засобів, виробничого обладнання тощо, які з’єднані з мережею Інтернет для взаємодії з навколишнім світом чи комунікацій між собою та людиною [213, с. 91].

На думку В.В. Філінович, Інтернет речей – це технологічна концепція підключення пристроїв по всьому світу до мережі Інтернет з метою управління ними віддалено. Здійснюватися це може як через сервер, так і безпосередньо шляхом використання спеціального програмного забезпечення і обміну даними в режимі real time, тобто реального часу [291, с. 123].

Надання масового відкритого Інтернет-доступу до побутових та господарських пристроїв створює загрози функціонуванню підприємств. Кіберзагрози пов’язані з можливістю витоку конфіденційної облікової інформації, інформаційного шпіонажу, кібератак, кібертероризму, що визначає актуальність організації ефективної системи кіберзахисту в умовах застосування IoT-технологій [291, с. 92]. Глобальні загрози та проблеми безпеки в Інтернеті речей (IoT) наведені у таблиці додатку Б3.

В науковому просторі присутні численні праці, присвячені забезпеченню кіберзахисту інформаційно-комунікаційних систем з використанням технології IoT. Більшість з них ґрунтуються на імплементації

блоково-ланцюгового структурування даних (технології блокчейн в обробці інформації). Водночас науковці проводять оригінальні наукові дослідження щодо перспективних варіантів кіберзахисту підприємств в умовах застосування IoT-пристроїв. Зокрема, Kumar Gautam, Singh Om Prakash та Saini, Hemraj Sikanjic обгрунтували вплив Індустрії 4.0 на кібербезпеку підприємств, що потребує застосування новітніх комунікаційних технологій, серед яких важливе місце займає IoT. Також Sikanjic Nedeljko, Avramovic Zoran та Marinkovic Drazen запропонували структуру IoT інфраструктури, використання якої мінімізує кіберризики та кіберзагрози функціонування підприємства. Аналогічно й Henry Matey Akwetey та інші дослідили перспективи використання технології IoT для кіберзахисту об'єктів критичної інфраструктури держав. Aisenberg Michael й інші визначили напрямки державної та місцевої політики у сфері кібербезпеки через поєднання технологій IoT, хмарної обробки інформації та блоково-ланцюгового структурування даних. Аналогічно й Smith Kane, Dhillon Gurpreet та Carter Lemuria розробили напрямки держаної політки у сфері кіберзахисту IoT-технологій на основі позиціонування «користувацьких цінностей (інформаційних потреб користувачів). Rohan Rohani, Funilkul Suree, Pal Debajyoti та Thapliyal Himanshu пояснили вплив технології IoT в споживчому використанні на мінімізацію чинника людського ресурсу. Роль штучного інтелекту в кіберзахисті IoT-технології також дослідили Kuzlu Murat, Fair Corinne та Güler Özgiir. Продовжили дослідження Chesney Steve, Roy Kaushik і Khorsandroo Sajad, які запропонували алгоритми машинного навчання для превентивного попередження активних кіберзагроз у сфері IoT. У той же час Djenna Amir, Saidouni Djamel Eddine та Wafia Abada запропонувати прагматичні стратегії кіберзахисту підприємств від прояву кібератак з використанням IoT. Іншу стратегію організації кібербезпеки у сфері IoT, що орієнтується на перманентній змін безпекових налаштувань, запропонували Mercado-Velazquez Andres, Escamilla-Ambrosio P. Jorge і Ortiz-Rodriguez Floriberto [213, с. 93].

Окремою групою Інтернет-речей є цифрові мобільні пристрої. Згідно з визначенням Національного інституту стандартів і технологій США (NIST), розміщеному у звіті Guidelines for Managing and Securing Mobile Devices in the Enterprise (NIST Special Publication 800-124 Revision 1), мобільними вважаються пристрої з малими габаритами та вагою, як мінімум одним безпроводовим інтерфейсом доступу до мережі мобільного зв'язку або (Інтернет), вбудованою (незнімною) пам'яттю, операційною системою, яка не є повноцінною ОС настільних комп'ютерів і ноутбуків, можливістю встановлення програм різними способами, що мають вбудовані засоби синхронізації даних із віддаленим джерелом. Крім цього, пристрій може мати інші, необов'язкові властивості, зокрема, мати не менше одного безпроводового персонального мережевого інтерфейсу типу Bluetooth або NFC, а також не менше одного безпроводового мережевого інтерфейсу для голосового зв'язку, наприклад стільниковий модуль; оснащуватися системою глобального позиціонування; мати одну або кілька цифрових камер, а також засоби зберігання даних (підтримка знімних носіїв, підтримка використання самого пристрою як знімного носія інформації) [75, с. 6].

В.В. Філінович звертає увагу на такі чинники, що можуть являти собою загрозу кібербезпеці: «дірки» у безпеці, тобто низька стійкість існуючих цифрових мобільних пристроїв до зовнішнього вторгнення; застарілі формати даних. Зараз все ще функціонують системи, впроваджені ще близько 3-4 десятиліть назад, які (системи) користувачі не поспішать замінювати, зокрема, і у зв'язку із браком коштів [291, с. 123]. Вказані загрози потребують належної уваги до кібергігієни у користуванні такими мобільними пристроями, особливо, коли вони підключені до інформаційно-комунікаційних систем. Адже цифрові апаратні та програмні продукти є одним із основних шляхів для успішних кібератак. У підключеному середовищі інцидент кібербезпеки в одному продукті може вплинути на всю організацію або весь ланцюг постачання, часто поширюючись через кордони внутрішнього ринку за лічені хвилини.

У цьому сенсі слід зазначити, що згідно ч. 1 ст. 2 Закону № 2163-VIII [51], цей Закон не поширюється на:

3) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет, … якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів;

4) комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій, … не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем).

У цих нормах абсолютно правильно наголошено, що вимоги цього Закону не поширюються на комунікаційні системи, які ***НЕ взаємодіють*** з публічними мережами електронних комунікацій…, ***НЕ підключені*** до мережі Інтернет та/або інших глобальних мереж передачі даних, бо таке підключення вимагає суворого дотримання встановлених законодавством правил кіберзахисту.

Разом із тим, не можна погодитися із не поширенням вимог закону на соціальні мережі та/або приватні електронні інформаційні ресурси в мережі Інтернет навіть якщо вони не містять інформацію, необхідність захисту якої встановлена законом, оскільки ці системи за визначенням взаємодіють із публічними мережами електронних комунікацій, зокрема, Інтернет. Де-факто інтереси інформаційного захисту потребують такого регулювання. Так, за результатами опитування, яке провела Громадянська мережа ОПОРА (з 06.05 до 04.06.2024) [252], 73,4 % опитаних для отримання новин використовують соціальні мережі. Саме соціальні мережі зберігають лідерство в інформуванні українців. Рейтинг найпопулярніших соціальних мереж у нашій країні протягом останніх трьох років залишається практично незмінним: його очолюють Telegram (, 78,1 %), YouTube (, 59,5 %) та Facebook (, 44,6 %). Трохи більш ніж 42 % респондентів отримують новини з Viber ( ), 29,6 % – з Instagram (), 26,8 % – з TikTok (), 7,8 % – з X

(Twitter). Іншими соціальними мережами для отримання інформації користуються лише 1,2 % респондентів.

Разом із тим, попри популярність месенджера Telegram, слід мати на увазі, що 19.09.2024 року Національний координаційний центр кібербезпеки при РНБО України ухвалив рішення обмежити використання месенджера Telegram у державних органах, військових формуваннях та на об’єктах критичної інфраструктури. Рішення було прийняте з метою мінімізації кіберзагроз. Представники СБУ та ГШ ЗСУ зазначили, що Telegram активно використовується ворогом для кібератак, розповсюдження фішингу та шкідливого програмного забезпечення, встановлення геолокації користувачів, корегування ракетних ударів тощо [176].

У розвиток цієї позиції в Національному авіаційному університеті прийнятий документ СМЯ НАУ ПВМ 26(01)-01-2024 «Система менеджменту якості. Політика щодо використання месенджера Telegram у Національному авіаційному університеті», введений в дію наказом в.о. директора НАУ від 31.10.2024 року № 574/од. Зокрема, цим документом встановлені обмеження на використання месенджера Telegram в НАУ. Визначено, що забороняється: передавати інформацію, яка використовується в роботі, через месенджер Telegram (фінансові дані, інформацію про умови співпраці з контрагентами, особисті дані співробітників та інформацію про студентів, контрагентів, партнерів, тощо); здійснення комунікацій зі службовою метою з використанням месенджера Telegram, крім комунікації осіб, яким згідно з посадовими обов'язками належить використання Telegram у службовій діяльності; встановлення клієнта Telegram та/або використання вебверсії Telegram на службових комп’ютерах (пристроях); використання месенджера Telegram на особистих комп’ютерах, які використовуються для виконання службових обов'язків, оскільки це може привести до небажаних наслідків для інформаційної безпеки організації. Повідомляється також про запровадження аналогічних обмежень в інших університетах країни [285] Разом із цим, ці обмеження не стосуються використання месенджера Telegram студентами та

працівниками, якщо таке здійснюється в позаробочий час з використанням особистих засобів комунікації та не стосується службової діяльності. Разом із тим, таке обмеження слід визнати недостатньо жорстким з точеи зору забезпечення кібербезпеки – забороненими месенджерами не можна користуватися у будь-який час і для будь-якої діяльності на комп'ютері, який підключений до інформаційно-комунікаційної системи установи.

Крім того, варто мати на увазі, що суттєві претензії до месенджера Telegram висловлюються і у спеціальній технічній літературі [75]. Зауважується, що якщо потрібен безпечний мобільний месенджер, то краще не обирати Telegram. І основна причина полягає в тому, що він не відповідає базовим вимогам захищеного інструменту для комунікацій – мова йде про наскрізне шифрування. Інша проблема цього інструменту – збереження повідомлень користувачів на серверах компанії-розробника, що означає потенційний доступ до них. Ще одна проблема Telegram – до цього часу так і не відомі зв'язки його засновника, Павла Дурова, із російськими спецслужбами та владою країни-загарбника [75, с. 85].

Вказані питання обмежень використання небажаних месенджерів розглядалося автором дисертації у його публікації [309].

Незважаючи на гостру проблематику, питання правового регулювання питань, пов'язаних з використанням технології Інтернет-речей, до останнього часу не знаходило належного правового регулювання ані в України, ані в ЄС [291, с. 125]. Разом із тим з вересня 2021 року ЄС розпочав розробку Закону про кіберстійкість (The Cyber Resilience Act (CRA)) – це нормативний акт ЄС щодо покращення кібербезпеки та кіберстійкості в ЄС шляхом встановлення спільних стандартів кібербезпеки для продуктів з цифровими елементами в ЄС, таких як обов'язкові звіти про інциденти та автоматичні оновлення безпеки [333]. Продукти з цифровими елементами – це переважно апаратне та програмне забезпечення, «передбачуване та цільове використання якого включає пряме або непряме підключення даних до пристрою або мережі [338].

Подальшим розвитком загальноєвропейського правового регулювання у сфері кібербезпеки є The Cyber Resilience Act (Акт CRA).

Як зазначається у публікації [335], цей нормативний акт вимагатиме від виробників підключених пристроїв належного захисту їх перед доставкою, негайного виявлення та усунення недоліків, а гарантія на виправлення надходитиме протягом п’яти років [335]. Необхідність такого акту для європейських споживачів викликана тим, що споживачі все частіше стають жертвами недоліків безпеки, пов'язаних з цифровими продуктами, такими як дитячі монітори, робопилососи, Wi-Fi маршрутизатори та системи сигналізації. Для бізнесу важливість забезпечення безпеки цифрових продуктів у ланцюжку поставок стала ключовою, враховуючи, що три з п'яти постачальників вже втратили гроші через прогалини в безпеці продуктів [338].

До Акту CRA різноманітні акти та ініціативи, вжиті на рівні ЄС та національному рівні, лише частково вирішували виявлені проблеми та ризики, пов’язані з кібербезпекою, створюючи законодавчу мозаїку на внутрішньому ринку. Це збільшило правову невизначеність як для виробників, так і для користувачів цих продуктів і додало непотрібного тягаря для компаній щодо дотримання низки вимог до подібних типів продуктів. Кібербезпека цих продуктів має особливо сильний транскордонний вимір, оскільки продукти, вироблені в одній країні, часто використовуються організаціями та споживачами на всьому внутрішньому ринку. Акт вирішує дві основні проблеми:

1. Подолання низького рівня кібербезпеки продуктів із цифровими елементами, що відображається широко поширеними вразливими місцями та недостатнім і непослідовним наданням оновлень для їх усунення.

2. Недостатнє розуміння та доступ до інформації користувачам, що заважає їм вибрати продукти з відповідними властивостями кібербезпеки або використовувати їх у безпечний спосіб.

За певних умов усі продукти з цифровими елементами, інтегровані у

велику електронну інформаційну систему або підключені до неї, можуть служити вектором атаки для зловмисників. Як наслідок, навіть апаратне та програмне забезпечення, які вважаються менш критичними, можуть полегшити початкову компрометацію пристрою чи мережі, дозволяючи зловмисникам отримати привілейований доступ до системи або переміщатися між системами (як це, наприклад, відзначилося в описаній вище історії з доступом до системи управління літаком [366]).

Прикладами виробів з цифровими елементами можуть бути [360]:

– кінцеві пристрої: ноутбуки, смартфони, датчики та камери, розумні роботи, смарт-карти, розумні лічильники, мобільні пристрої, розумні колонки, маршрутизатори, перемикачі, промислові системи управління;

– програмне забезпечення, прошивка, операційні системи, мобільні додатки, настільні програми, відеоігри;

– компоненти (як апаратні, так і програмні); блоки обробки комп’ютера; відеокарти; програмні бібліотеки.

У публікаціях [96, 149, 354, 360] наведені приклади кібератак, які використали недостатню кібербезпеку продуктів із цифровими елементами: шпигунська програма Pegasus, яка використовувала вразливості в мобільних телефонах [354]; програма-вимагач WannaCry, яка використовувала вразливість Windows, яка вразила комп’ютери в 99 країнах [94]; атака на ланцюг поставок Kaseya VSA, яка використовувала програмне забезпечення для адміністрування мережі для атаки на понад 1000 компаній [149].

«Комп’ютери, телефони, побутова техніка, … іграшки… кожен із цих сотень мільйонів підключених продуктів є потенційною точкою входу для кібератаки», – пояснив Тьєррі Бретон, єврокомісар з питань внутрішнього ринку. «І все ж сьогодні більшість апаратних і програмних продуктів не підлягають жодним зобов’язанням щодо кібербезпеки» (цитується за публікацією [335]).

Занепокоєння Комісії виходить за рамки злому самого продукту та впливу, який один інцидент може мати на весь ланцюг постачання.

Організація назвала можливі наслідки як «серйозні порушення економічної та соціальної діяльності на внутрішньому ринку, що підриває безпеку або навіть стає небезпечним для життя» [335].

Законопроект, який розробляється з вересня 2021 року, «запроваджує обов'язкові вимоги до кібербезпеки продуктів із цифровими елементами протягом усього життєвого циклу». Закон містить вимоги до інформаційної безпеки, яких необхідно виконати, перш ніж продукти зможуть потрапити на європейські ринки, деякі з них стосуються їх проектування, розробки та виробництва. Після того, як продукти надійдуть у продаж, Закон зобов'яже виробників розкривати інциденти протягом 24 годин після того, як їм стало відомо про них, і усувати вразливості за допомогою підтримки безпеки та оновлень програмного забезпечення. Виробники зобов'язані вирішувати проблеми кібербезпеки протягом п'яти років або очікуваного терміну служби продукту. «Нові правила перебалансують відповідальність перед виробниками», – заявили в Комісії. Після ухвалення закону виробники матимуть пільговий період у два роки, щоб адаптуватися до нових вимог. Для звітів про вразливості та інциденти пільговий період становить лише один рік. Невиконання вимог може призвести до штрафів у розмірі до 15 мільйонів доларів США (15 мільйонів євро) або 2,5 відсотка від загального світового річного обороту порушника за попередній фінансовий рік. Щоб ніхто не припустив, що законодавство вплине лише на Європу, Комісія не соромилася заявити, що вона має потенціал для встановлення глобальних стандартів, назвавши це, «ймовірно, стати міжнародною точкою відліку». Комісія не заперечуватиме, якщо це станеться, оскільки вона вже очолила світ із Загальним регламентом захисту даних (GDPR) і діями проти технічних гігантів через їх бізнес-практику та використання даних [335].

В публікації [355] наголошується, що Акт CRA є першим нормативним актом ЄС щодо кібербезпеки продуктів із цифровими елементами. Це стосується не лише програмних продуктів, а й розумних пристроїв – від підключених холодильників до комп'ютерних мережевих пристроїв.

Безпека програмного забезпечення, вказується у [355], була постійною проблемою з самого початку Інтернету. Щомісяця виявляються нові вразливості системи безпеки, які постраждалі організації намагаються усунути якомога швидше. Якщо системи безпеки виходять з ладу або вони недоступні, хакерам легко скомпрометувати уражені системи. Оскільки сучасні електронні пристрої – від іграшок до пральних машин і автомобілів – також містять багато різних програмних продуктів, проблема незахищеного програмного забезпечення впливає не лише на традиційну індустрію програмного забезпечення, але й на значну частину промисловості.

Щоб вирішити ці виклики, ЄС прийняв новий Закон про кібернетостійкість (Акт CRA). Цей регламент ЄС поширюється на всі продукти з цифровими елементами. Він охоплює не лише традиційні програмні продукти та комп'ютерне обладнання, а й інші інтелектуальні пристрої. Крім того, Акт охоплює будь-які онлайн-сервіси, пов'язані з регульованим продуктом і без яких продукт не може виконувати одну зі своїх функцій. Таким чином, Закон про кібернетостійкість є не лише інструментом регулювання безпеки продуктів, але й охоплює багато типів онлайн-сервісів. Наприклад, якщо онлайн-сервіс супроводжується програмою, яка полегшує використання онлайн-сервісу на мобільному пристрої, Закон про кібернетостійкість, ймовірно, застосовуватиметься до всього онлайн-сервісу.

Закон про кібернетостійкість набуде чинності поетапно, із зобов'язанням сповіщати про активно використовувані вразливості для продуктів, що входять до сфери дії, набуде чинності з 11 вересня 2026 року, а решта зобов'язань – з 11 грудня 2027 року. За стандартами нещодавнього законодавства ЄС, організації мають більш розумні часові рамки для впровадження; однак, оскільки Закон про кібернетостійкість, ймовірно, вимагатиме від багатьох організацій внести значні зміни в те, як вони запускають і обслуговують відповідні продукти в ЄС, не можна втрачати час.

Основні вимоги Акту полягають у наступному [355].

Виробники, які розглядають розробку продукту з цифровими елементами, повинні будуть провести оцінку ризиків кібербезпеки, пов’язаних з продуктом. Результат цієї оцінки необхідно враховувати при подальшому плануванні, проектуванні, розробці та виробництві продукту, а також при його доставці та обслуговуванні. За результатами цієї оцінки ризику виробник несе низку зобов’язань щодо забезпечення належного рівня кібербезпеки.

Виробникам забороняється пропонувати на ринку продукти з відомими вразливими місцями, які можна використовувати, або продукти без конфігурації безпеки за замовчуванням. У разі виявлення вразливості безпеки виробники також зобов’язані негайно та безкоштовно надати оновлення безпеки. Крім того, виробники також повинні надавати автоматичні оновлення безпеки, які встановлюються протягом відповідного періоду часу, увімкненого як налаштування за замовчуванням. Відповідно до Закону про кіберстійкість, період підтримки для продуктів із цифровими елементами, тобто період, протягом якого користувачі можуть очікувати надання оновлень безпеки, має відображати очікуваний час використання продукту.

Відповідно до Закону про кіберстійкість, виробники повинні прозоро вказати дату закінчення цього періоду підтримки. Це також має на меті допомогти користувачам порівнювати продукти та приймати більш обґрунтовані рішення про покупку. Крім того, на виробників буде покладено низку додаткових інформаційних зобов’язань. Наприклад, виробники повинні будуть надати перелік обставин, які можуть призвести до значних ризиків кібербезпеці, запровадити скоординовану політику розкриття вразливостей і створити єдину контактну точку, куди можна повідомити інформацію про вразливості, виявлені в продукті.

Усі виробники повинні будуть піддавати свою продукцію з цифровими елементами процедурі оцінки відповідності та видати декларацію про відповідність, яка підтверджує, що продукт відповідає основним вимогам

Закону про кіберстійкість. Цю декларацію про відповідність і технічну документацію також можуть вимагати для перевірки національні органи влади. Виробник повинен нанести маркування «CE», тим самим заявляючи, що продукт відповідає вимогам Закону про захист від кібернетичної інформації.

Відповідно до Закону про кіберстійкість, виробники також будуть зобов'язані вилучати або відкликати продукти з ринку, якщо вони знають або мають підстави вважати, що певний продукт має очевидні вразливості.

Таким чином, визначені особливості правового регулювання заходів забезпечення кібербезпеки на підставі акту ЄС про кіберстійкість (The Cyber Resilience Act). Акт спрямований на подолання низького рівня кібербезпеки продуктів із цифровими елементами, що відображається широко поширеними вразливими місцями та недостатнім і непослідовним наданням оновлень для їх усунення. Передбачена низка зобов'язань виробників, які розглядають розробку продукту з цифровими елементами, зокрема, здійснити оцінку ризиків кібербезпеки, пов'язаних з продуктом, та враховувати результат цієї оцінки при подальшому плануванні, проектуванні, розробці та виробництві продукту, а також при його доставці та обслуговуванні. За результатами цієї оцінки ризику виробник несе низку зобов'язань щодо забезпечення належного рівня кібербезпеки. Враховуючи перспективу інтеграції України з ЄС, Україні необхідно враховувати наявність такого Акту ЄС і таких вимог. Зокрема, пропонується доповнити Закон № 2163-VIII [51] положеннями щодо вимог до технологій Інтернет-речей, аналогічним The Cyber Resilience Act. Аналізу акту ЄС про кіберстійкість (The Cyber Resilience Act) і перспектив використання таких напрацювань в Україні присвячені роботи автора дисертації [159, 167, 168].

Коли дисертація вже була підготовлена до друку, стало відомо, що Постановою КМУ від 03.12.2025 № 1580 внесені зміни до Постанови КМУ від 16.05.2023 р. № 497 (щодо застосування системи Bug Bounty (додаток Б13).

1.3. Особливості концептів «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020-2021 років. Когнітивна безпека

Як зазначено вище, з метою інституалізації положень, пов'язаних з національною безпекою України, протягом 2020-2021 рр. в Україні схвалена рішенням РНБО України та затверджена Указом Президента України низка безпекових стратегій, зокрема: Стратегія національної безпеки України від 14.09.2020 р. [22]; Стратегія воєнної безпеки України від 25.03.2021 р. [23]; Стратегія кібербезпеки України від 14.05.2021 р. [24]; Стратегія розвитку оборонно-промислового комплексу України від 18.06.2021 р. [25]; Стратегія зовнішньополітичної діяльності України від 30.07.2021 р. [26]; Стратегія інформаційної безпеки від 15.10.2021 р. [28]; Стратегія забезпечення державної безпеки від 30.12.2021 р. [29]. Ці документи являють собою комплексне нормативно-правове упорядкування засад публічно-правової діяльності у безпекових сферах Держави.

Однією із цілей прийняття аналізованих Стратегій є інституалізація термінології у сфері безпеки. Однак це питання у повній мірі не вирішене, тому що не усунені певні суперечності у термінології в правових актах, практиці та науці.

Натомість, як зазначається у статті [135], термінологія займає особливе місце в збереженні та передаванні знань, оскільки саме на неї припадає основне інформаційне навантаження. Разом із тим у статті [70, с. 7] констатується, що з поняттям «інформаційна безпека» склалася парадоксальна ситуація. З одного боку, термін «інформаційна безпека» широко використовується в наукових публікаціях, навчальній літературі та законодавчих документах різного рівня, з іншого боку, це поняття досі не має однозначного розуміння. У публікації [359] вказано, що «є досить мало розуміння» поняття «кібербезпека», що потенційно може викликати суттєві проблеми в контексті комунікації між зацікавленими особами. Таким чином,

дана проблема є актуальною.

Як зазначено вище (див. «Вступ»), стаття 17 Конституції України захист ***інформаційної безпеки країни*** визнає́ однією з найважливіших функціяй держави.

Натомість, відома велика кількість робіт, в яких поняття «інформаційна безпека» фактично спрямовуються на певні локальні питання, зокрема: «інформаційна безпека» бібліотеки [83], «інформаційна безпека» підприємств і господарської діяльності [64, 221, 250, 303], «інформаційна безпека» в органах внутрішніх справ [113], «інформаційна безпека» страхових компаній [128] та ін. Очевидно, ці види «інформаційних безпек» не відповідають конституційному рівню правового регулювання і захисту.

В окремих роботах аналіз «інформаційної безпеки» зводиться до проблематики «кібербезпеки» [67, 90]. В статті [99] розглядається співвідношення понять «інформаційна безпека» та «безпека інформації» в сучасному науковому просторі [99, с. 55]. Зазначається, що «на перший погляд, "інформаційна безпека" "безпека інформації" тотожні за змістом, але це не відповідає істині». В статті [311] «інформаційна безпека» розглядається як в контексті «захисту інформації», так і в контексті «захисту від інформації» [311, с. 301]. В.М. Фурашев вважає, що немає принципової різниці, чому споживач отримав недостовірну або спотворену інформацію: чи внаслідок викривлення інформації чи внаслідок порушення її цілісності. Результат один: споживач одержав неповну інформацію, наслідком чого може бути викривлення висновків на основі цієї інформації [294].

Таким чином, викладені різні підходи потребують узагальнення.

У Стратегії інформаційної безпеки України надано визначення «інформаційна безпека України» – це складова частина національної безпеки України, стан 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 нанесенню 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.

Аналогічне визначення надає Стратегія забезпечення державної безпеки України.

Отже, маємо офіційне визначення «інформаційна безпека України». Це поняття є комплексним і враховує забезпечення прав і свобод людини на збирання, зберігання, використання та поширення інформації; запобігання негативним інформаційним впливам; запобігання поширенню недостовірної, необ'єктивної інформації, деструктивній пропаганді, іншим інформаційним операціям; захист цілісності інформації, запобігання її перекрученню та несанкціонованому поширенню.

Ю.Д. Кунєв, Є.О. Легеза [181] вважають, що забезпечення інформаційної безпеки – це вжиття заходів зменшення рівня небезпеки систем, розробка та вжиття заходів, що зменшать або ліквідують ризик завдання шкоди [181, с. 183]. І.М. Сопілко констатує, що загрозами інформації у кіберпросторі є кіберзагрози, тому заходами протидії цим загрозам є забезпечення кібербезпеки [254]. В цьому контексті зазначимо, що Стратегія інформаційної безпеки України не заперечує важливість кібербезпеки в гарантуванні інформаційної безпеки. Цей контекст враховується шляхом відсилання до Стратегії кібербезпеки України.

Розглядаючи особливості категорії «інформаційна безпека» у міжнародному контексті, В. Котляров [157] констатує, що «інформаційна безпека є складовою національної безпеки в цілому. Суть цього інституту інформаційного права полягає у здійсненні правових, організаційних, технічних заходів, спрямованих на безпечний стан … інформаційно-

комунікаційного комплексу держави, окремих організацій та кожної людини» [67; 157, с. 21].

Отже, «інформаційна безпека» не означає безпеки окремих інформаційних систем, чи окремої сукупності даних, чи до кібербезпеки, хоча ці терміни пов'язані між собою. Є.О. Архипова у згаданій вище статті [70] констатує, що «інформаційна безпека» є ширшим поняттям, ніж «безпека інформації», включаючи в себе останню. Ототожнення цих понять вона пояснює тим, що вітчизняні дослідники не враховують, що міжнародні стандарти, з яких запозичується визначення поняття *information security,* належать до сфери безпеки інформаційних технологій, де об'єктом захисту виступає саме інформація (а не держава, суспільство чи людина). Вказане формальне запозичення призводить до плутанини щодо термінологічних визначень [70, с. 8]. Зокрема, дослідниця вказує, що у стандарті ISO/IEC 17799 *Information security* характеризується забезпеченням конфіденційності, доступності та цілісності інформації, а в стандарті ISO/IEC 27001 – як всі аспекти, що пов'язані з визначенням, досягненням та підтримкою доступності, конфіденційності, цілісності, підзвітності, невідмовності, достовірності та автентичності інформації або засобів її обробки. Дж. Фрулінгер (J. Fruhlinger) [341] також вказує на так звану тріаду ЦРУ як складові безпеки інформації: цілісність, конфіденційність, доступність. Усі ці міркування стосуються безпосередньо поняття «безпека інформації».

Згідно ч. 1 ст. 1 Закону України «Про інформацію», інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [36].

Отже, захисту підлягає інформація як в електронному вигляді, так і на будь-якому носії. Так, у публікації [317] наголошується, що «***незалежно від того, як зберігається ваша інформація***, вашій організації потрібні засоби контролю безпеки, щоб перешкодити несанкціонованому доступу» [317]. Таким чином, кібербезпека є окремим випадком загального поняття безпеки інформації, однак такої інформації, яка обертається у кіберпросторі. При

цьому причиною підвищеної уваги саме до кіберзагрозам і кібербезпеки є дедалі зростаюча роль обігу інформації в комп'ютерних системах і електронно-комунікаційних мережах.

Таким чином, поняття «інформаційна безпека ***держави***» не є тотожним поняттю «інформаційна безпека», яка розуміється як досягнення та підтримка доступності, конфіденційності, цілісності, підзвітності, невідмовності, достовірності та автентичності інформації або засобів її обробки. У цьому випадку слушно казати саме про «безпеку інформації».

Варто при цьому зазначити, що вказані термінологічні невідповідності мають місце не тільки в науковій літературі і практиці, але й у законотворчості. Так, згідно ч. 2 ст. 1 Закону «Про національну безпеку України» [52], інші терміни, ніж ті, що прямо визначені у цій статті, вживаються у цьому Законі в значенні, наведеному в інших законах України.

Однак аналіз, наприклад, Закону України «Про захист інформації в інформаційно-комунікаційних системах» [38], який (Закон) вважається чинним і останні зміни до якого вносилися 16.12.2020 року, свідчить про те, що у цьому Законі поняття «інформаційна безпека» використовується не у розумінні Стратегії інформаційної безпеки України, а у розумінні «безпека інформації». Про це свідчать наступні формулювання Закону [38]:

– «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 (частина друга статті 8)

– «підтвердження відповідності системи управління ***інформаційною безпекою*** за результатами процедури з оцінки відповідності національним стандартам України щодо систем управління ***інформаційною безпекою***… (абзац другий частини 4 статті 8)».

З іншого боку, відсилаючи до термінів у значенні, наведеному «в інших законах України», Закон «Про національну безпеку України» закладає суперечність із Стратегією інформаційної безпеки України. Тобто, необхідні

зміни в законах з метою термінологічного узгодження їх із Стратегією інформаційної безпеки України.

У ч. 3 ст. 6 відносно нового Закону № 2163-VIII [51] також використано поняття «інформаційна безпека» не у розумінні Стратегії інформаційної безпеки України. Зокрема, у цій нормі Закону зазначено: «Вимоги і порядок проведення незалежного аудиту ***інформаційної безпеки*** на об'єктах критичної інфраструктури встановлюються відповідними нормативно-правовими актами з аудиту ***інформаційної безпеки***, що затверджуються КМУ. Розроблення нормативно-правових актів з незалежного аудиту ***інформаційної безпеки*** на об'єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів ЄС та НАТО з обов'язковим залученням представників основних суб'єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій».

В Стратегії від 14.05.2021 р. кібербезпеки України загрози кібербезпеці України конкретизовані так: агресія рф проти України у кіберпросторі; кіберзлочинність; кібератаки, поєднані з кібершпигунством; кібертероризм, фінансова та інша підтримка терористичної діяльності.

У статті 1 Закону № 2163-VIII [51] кібербезпека визначена як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі (пункт 5); кіберзагроза визначена як наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів (пункт 6).

В американській (США) доктрині кібербезпеки остання розуміється ширше. Так, Matt Rosenthal [352] визначає п'ять основних типів кібербезпеки

і описує їх наступним чином.

А. ***Безпека критичної інфраструктури*** – зосереджена на захисті кіберфізичних систем, мереж і активів, що використовують сучасні суспільства. Безпека та стійкість критичної інфраструктури життєво важливі для безпеки й добробуту сучасного суспільства. Наводяться типові приклади критичної інфраструктури: водопостачання; електрична мережа; торгові центри; світлофори; лікарні. Організаціям, яким доручено захистити критично важливу інфраструктуру, необхідно виявити вразливі місця цієї інфраструктури, і створити план запобігання майбутнім збиткам. Компанії, що не відповідають за критичну інфраструктуру, але залежать від неї, також повинні розробити план дій на випадок надзвичайних ситуацій, оцінивши вплив можливих атак на них [352].

В Україні на законодавчому рівні також запроваджене визначення об'єктів критичної інфраструктури. За статтею 10 Закону «Про критичну інфраструктуру» (частина 4) [55], до життєво важливих функцій та/або послуг… належать, зокрема: 1) урядування та надання найважливіших публічних (адміністративних) послуг; 2) енергозабезпечення (у тому числі забезпечення тепловою енергією); 3) водопостачання та водовідведення; 4) продовольче забезпечення; 5) охорона здоров'я; 6) фармацевтична промисловість; 7) виготовлення вакцин, функціонування біолабораторій; 8) інформаційні послуги; 9) електронні комунікації; 10) фінансові послуги; 11) транспортне забезпечення; 12) оборона, державна безпека; 13) правопорядок, здійснення правосуддя, тримання під вартою; 14) цивільний захист населення та територій, служби порятунку; 15) космічна діяльність; 16) хімічна промисловість; 17) дослідницька діяльність. Натомість слід зазначити, що, за цитованою вище американською доктриною, цей перелік повинен окремо включати торгові центри та засоби забезпечення дорожнього руху (світлофори).

В. ***Безпека комп'ютерних програм*** – забезпечує захист програмного коду і даних від зломів і кіберзагроз. Він використовує апаратні і програмні

методи для боротьби із зовнішніми загрозами. Оскільки додатки доступніші через мережі, важливо запровадити негайно стандарти безпеки, системи, процедури та інструменти, щоб захистити додатки, що використовуються, на всіх етапах розробки. Способи забезпечення безпеки комп'ютерних програм: авторизація; аутентифікація; антивірусні програми; антишпигунське програмне забезпечення; програми шифрування; брандмауери; тестування безпеки програми. Перелічені заходи безпеки допомагають запобігти несанкціонованому доступу до програм, що використовуються, і захистити активи конфіденційних даних за допомогою спеціальних процесів безпеки програми [352]. Брандмауер – це програмне забезпечення або пристрій, які контролюють вхідний і вихідний мережевий трафік, блокують або пропускають дані відповідно до набору правил безпеки, захищають комп'ютерну мережу від несанкціонованого доступу, шкідливих програм і мережевих атак.

C. ***Безпека мережі*** – захищає від несанкціонованого вторгнення у використовувані внутрішні мережі через зловмисний намір. Заходи безпеки мережі гарантують безпеку внутрішніх мереж шляхом захисту інфраструктури та блокування доступу до неї. На даний час команди безпеки використовують автоматичний контроль, щоб в реальному часі розпізнавати ненормальний трафік і своєчасно сповіщати про загрози задля кращого керування моніторингом безпеки мережі. Необхідно впроваджувати процедури щодо запобігання неавторизованому доступу, модифікації та експлуатації мережі. Загальні приклади реалізації безпеки мережі: нові паролі; додаткові логіни; антивірусні програми; антишпигунське програмне забезпечення; брандмауери, шифрування; контрольований доступ до Інтернету [352].

D. ***Хмарна безпека*** – це програмний інструмент безпеки, що контролює та захищає дані у хмарних ресурсах користувача. Хмарні постачальники постійно впроваджують нові інструменти безпеки, щоб допомогти корпоративним користувачам краще захистити свою інформацію. Не

відповідають дійсності уявлення, що хмарні обчислення менш безпечні, ніж традиційні, коли користувач безпосередньо володіє та керує ресурсами. Однак було практично доведено, що контроль не гарантує безпечність. Зокрема, користувачі локального середовища зазнають у середньому у 2,2 рази більше 61,4 атак, ніж клієнти хмарного середовища середовища [352].

Е. ***Безпека пристроїв, підключених до комп'ютерних мереж, у тому числі до системи Інтернет*** – це захист мереж, від вразливості пристроїв, підключених до мереж. Ця проблема розглянута вище (див. підрозділ 1.2 цієї роботи). Зокрема, з'ясовано, що для нормативного подолання цієї проблеми у ЄС прийнятий акт, спрямований на забезпечення безпеки технології Інтернет-речей (Акт CRA).

Alison Grace Johansen [318] вказує, що кібербезпека – це стан або процес захисту та відновлення мереж, пристроїв і програм від кібератак. Кібербезпека – це практика захисту використовуваних електронних систем, мереж, комп'ютерів, мобільних пристроїв, даних і програм від ворожих цифрових атак. Кіберзлочинці можуть застосовувати різноманітні атаки проти окремих жертв. Ці атаки можуть включати доступ, видалення або зміну конфіденційних даних; втручання в бізнес-процеси, вимагання платежу. Кібератаки становлять небезпеку для організацій, співробітників і споживачів. Фактично ці атаки можуть зруйнувати бізнес і завдати шкоди особистому життю та/або фінансовому стану, особливо якщо особа стала жертвою крадіжки особистих даних.

Кібербезпека – це безпека інформаційних технологій, відома також як безпека електронної інформації або InfoSec, тобто це захист інформації – як там, де вона зберігається, так і під час її переміщення через мережу. Кібербезпека захищає інформацію як у цифровій, так і фізичній формі, тобто дані в будь-якій формі, від несанкціонованого доступу, використання, розголошення, видалення, зміни або інших форм зловмисного наміру з боку зловмисників.

Безпека мережі, як і безпека комп'ютера, є підмножиною кібербезпеки.

Цей тип безпеки спрямований на програмне та/або апаратне забезпечення для захисту будь-яких даних, що надсилаються через комп'ютер та/або інші пристрої в мережу. Безпека мережі спрямована на захист інформаційної інфраструктури та захист від зміни, викрадення чи перехоплення інформації кіберзлочинцями.

Alison Grace Johansen [318] визначає в цілому ті ж 5 основних напрямів забезпечення кібербезпеки, що і Matt Rosenthal [352]. Натомість Alison Grace Johansen [318] виділяє три види кіберзагроз: атаки на цілісність, атаки на конфіденційність і атаки на доступність.

A. ***Атаки на цілісність***. Можуть бути спрямовані на особистий або корпоративний саботаж, часто називаються витоками. Зловмисник отримує доступ до конфіденційної інформації та оприлюднює її з метою впливу на суспільство, щоб воно втратило довіру до організації чи особи.

Типом атаки на цілісність вважаються так звані розширені постійні загрози (APT – advanced persistent threats), коли неавторизований користувач проникає в мережу непоміченим і залишається в мережі протягом тривалого часу. Метою цього типу кібератак є викрадення даних, а не шкода мережі. APT часто відбуваються у сферах з високою цінністю інформації, зокрема, національна оборона, виробництво та фінансова галузь.

B. ***Атаки на конфіденційність***. Ці атаки можуть бути спрямовані на викрадення ідентифікаційної інформації щодо особи: номер особи в системі соціального страхування та/або дані кредитної картки та/або банківський рахунок. У випадку успіху атаки ця інформація може бути передана (продана) стороннім особам для використання із зловмисними цілями.

Тип атаки на конфіденційність – так звана соціальна інженерія. Це психологічне маніпулювання людьми, спрямоване на змушування їх виконувати дії та/або передавати інформацію. Найпоширеніша форма соціальної інженерії – фішингові атаки. Вони нерідко здійснюються у вигляді оманливого електронного листа, спрямованого на змушування одержувача надати особисту інформацію чи перехувати кошти [352] (див. також

підрозділ 2.3 цієї дисертаційної роботи).

Наприклад, наприкінці 2025 року податкова служба України попередила про фішингові листи, що імітують офіційні повідомлення від Державної податкової служби (ДПС) та сервісу «Дія». Шахраї надсилають листи з підозрілими вкладеннями (наприклад, у форматі .pdf.js) або посиланнями на підроблені сайти, щоб виманити особисті дані, банківські реквізити або перехопити управління комп'ютером. Податкова закликає українців не відкривати подібні вкладення та перевіряти офіційні джерела інформації, а також звертати увагу на доменну адресу електронної пошти – офіційні листи ДПС надходять з домену tax.gov.ua [283].

С. ***Атаки на доступність***. Ці атаки можуть бути спрямовані на блокування доступу користувачів до їхніх даних, доки ці користувачі не виконають умови вимагачів, наприклад, сплатити гроші або передати дані, або виконати інші дії на шкоду користувачу та в інтересах зловмисника(ів). Такі атаки, як правило, здійснюються з використанням шкідливого програмного забезпечення. Зловмисник проникає в мережу й позбавляє законних користувачів доступу до важливих даних, висуваючи певні умови. Користувачі виконують ці умови, а потім виправляють кібервразливість з метою уникнення аналогічних кіберконфліктів в майбутньому [352].

Як зазначено вище (див. «Вступ»), загострення воєнної ситуації тягне і ризики у кіберпросторі. Кібервійна реально стає невід’ємною частиною інформаційної війни [251]. Наприклад, за звітом компанії Microsoft, з початку широкомасштабного російського вторгнення 24.02.2022 року російські хакери скоїли майже 240 кібератак проти України. Атаки були спрямовані на знищення комп'ютерних систем, збирання розвідувальних даних або поширення дезінформації [245].

В подальшому хакерські кібератаки з території рф постійно збільшувалися. Відомості про наймасштабніші кібератаки в Україні наведені на рисунку у додатку Б5 [247]. Наведені відомості свідчать про те, що у період широкомасштабного вторгнення рф кількість кіберинцидентів,

спрямованих на критичну інфраструктуру України, постійно зростала: якщо у 2022 та 2023 році фахівці урядової команди реагування на комп'ютерні надзвичайні події України відреагували на 2,2 тисячі та 2,5 тисячі кіберинцидентів відповідно, то у 2024 році їх було вже 4,3 тисячі.

Ці та інші аналогічні епізоди підтверджують, зокрема, думку Ю.С. Размєтаєвої, яка вважає, що запобігання кіберзагрозам можливе завдяки поєднанню національної й міжнародної систем кіберзахисту [241]. Можна цілком погодитись із тезою, що і захист програмного забезпечення і захист устаткування є головним завданням кібербезпеки. Разом із тим, ці види захисту повинні бути реалізовані та вбудовані до міжнародної та національної стратегій (регулювання), щоб досягти своїх цілей» [353, с. 22].

Україна інтегрована у світовий інформаційно-комунікативний простір, і зазна́є різних негативних впливів та загроз, які виходять з кіберпростору. Це гостро актуалізує питання кібербезпеки на загальнодержавному рівні. Тому виникає необхідність зрозуміти нову безпекову (кібербезпекову) реальність й вирішити практичні питання впорядкування внутрішнього нормативно-правового регулювання, зон відповідальності суб'єктів публічної адміністрації у сфері кібербезпеки держави, та весь комплекс питань розбудови національної системи кібербезпеки [125, с. 11].

Як зазначалося вище, ворожі інформаційні впливи можуть бути небезпечними не тільки для інформаційних (комп'ютерних) систем, але й безпосередньо для осіб, оскільки можуть бути використані для доставляння шкідливої інформації в обхід запобіжників отримання (доставляння) цієї інформації.

Як наголошує професор Г.Г. Почепцов [235], у сфері інформаційної і кібер- безпеки традиційно багато уваги приділяється кібербезпеці і мало тому́, що можна позначити поняттям «***когнітивна безпека***». У кібербезпеці захищають кіберресурси, у когнітивній безпеці – розум людини. Ми живемо у світі пропаганди, яка, як правило, спотворює реальність [235]. Цей вплив створює загрози ***інформаційно-психологічній безпеці особи («когнітивній***

безпеці»). Навпаки, забезпечення такої безпеки – це забезпечення захищеності психіки осіб від впровадження у її свідомість (підсвідомість) деструктивної інформації, що викликає неадекватне сприйняття людиною дійсності [138, с. 105].

Як зазначає проф. В.А. Ліпкан, з урахуванням сучасних інформаційних заходів, сучасна пропаганда виступає формою систематичного цілеспрямованого переконування, що спрямоване на емоції, думки, погляди й дії цільової аудиторії з політичною, ідеологічною, іншою метою через контрольовану передачу пропагандистами односторонніх повідомлень, в яких зацікавлені останні, – безпосередньо або каналами мас-медіа [194].

Найбільш небезпечною загрозою ***інформаційно-психологічній безпеці особи*** є така складова частина пропаганди, як інформаційно-психологічний вплив [138, с. 12]. Базовими методами інформаційно-психологічних впливів є переконання й навіювання. При цьому переконання звернене до власного сприйняття дійсності об’єктом впливу. Навіювання є основним способом маніпулювання свідомістю, прямим вторгненням у психічне життя людей. Маніпулятивний вплив організується так, щоб думка, уявлення, образ безпосередньо входили у сферу свідомості та закріплювалися в ній як дані безперечні й уже доведені [138, с. 12-13].

Так колишній донеччанин Ю. Протасенко розповів журналістам, що люди на референдумі[2] переказували один одному абсурдні новини, почуті в ефірі російського телебачення[3]: «Я помню этот "референдум". За несколько дней до этого по одному из российских телеканалов ведущая новостей рассказала, что в Донецке ставят метки на домах русскоговорящих граждан. Мы с женой хихикнули тогда. Какая чушь! На каждом доме надо метку ставить, коль на то пошло. Потом эту чушь всерьез пересказывали друг другу люди на референдуме. И мы вдруг поняли, что народ массово начал сходить

[2] Незаконний «референдум» 11.05.2014 про так звану «державну незалежність Донецької області», організований проросійськими сепаратистами. У той же день аналогічний «референдум» проводився у Луганській області.
[3] Мовою оригіналу.

с ума. Слухи, даже самые идиотские, перемалывались и становились чуть ли не официальными новостями. Все что связано с Украиной сразу стало плохо и гадко, и все начали говорить, что это "страна 404"», – розповідав Протасенко [215]. Цей приклад наочно підтверджує справедливість тези про те, що інтенсивний інформаційно-психологічний вплив може перевести великі маси людей на протилежну картину світу.

У листопаді 2025 року Генштаб ЗС Польщі повідомив про підсилення розпалювання антиукраїнських настроїв у Польщі. Спостерігається активізація психологічних операцій проти України. Ведеться інтенсивна наративна діяльність в Інтернеті, де пропагується ненависть до України. Зокрема, росія спекулює на проблематиці Волинської трагедії[4]. Особливо активно це здійснюється у центрах допомоги воюючій Україні, зокрема, щодо переправляння зброї. У Генштабі ЗС Польщі називають ці дії «саботажними», що спрямовані на підрив підтримки України та суперечать державній політиці [103].

У цих умовах актуальним стає не захист інформації, а захист від інформації.

Український політик О.В. Турчинов наголошує, що парадигма гібридної війни спрямована на підрив і руйнування усього комплексу суспільних відносин у об'єкта агресії, знищення волі до опору, у тому числі і за рахунок інформаційних операцій. Застосовані під час гібридної війни засоби є вельми латентними, їх складно ідентифікувати, а ще складніше завдати удару у відповідь [284, с. 27].

Антонова С.Є., Мартинюк Г.Ф. наголошують, що «2014-2015 рр. стали надзвичайно важкими для забезпечення інформаційної безпеки України. Україна зіткнулася з використанням проти неї роками вибудуваної у рф пропагандистської системи. Дії противника направлені на … знищення української політичної нації, прославляння сепаратизму, штучне посилення

[4] Обопільні етнічні чистки польського та українського населення під час Другої світової війни, що відбулися на Волині

реальних і вигаданих внутрішніх протиріч, створення атмосфери недовіри до дій і намірів влади, провокування актів громадянської непокори, формування у громадян України та міжнародної спільноти викривленого бачення подій в Україні, перекручення української історії та маніпулювання історичними фактами» [66].

Як зазначає Ю.О. Горбань [109, с. 140], в інформаційній війні проти України рф застосовує практично усі можливості впливу на свідомість людей. В публікації [220] відзначається, що, наприклад, антиукраїнська пропаганда велася на кримському телебаченні усі 23 роки незалежності України [220].

Як зазначає згаданий вище луганський автор, журналіст Є. Соломін (див. «Вступ»), рф, прагнучи домінувати в українському телевізійному просторі, поряд із покриттям власним сигналом прикордонних територій, свій продукт поширювала через супутникове мовлення, українських операторів кабельного ринку та увійшла з власним продуктом через регіональні ТРК. Так, партнером росіян у поширенні її продукції через кабельні мережі у Луганську стало ЛКТ та близько двох десятків кабельних операторів на території області. У час, коли «русская весна» вже стукала в українські двері і проти російського продукту повстали українські глядачі, менеджери луганських кабельних каналів продовжували трансляцію Першого каналу, НТВ, РТР і «Росії 24», ігноруючи заборону Національної ради з питань телебачення та радіомовлення та відповідне рішення окружного адміністративного суду Києва [253, с. 69].

Необхідно також згадати, що Стратегія від 15.10.2021 р. інформаційної безпеки [28] надає таке визначення «інформаційна загроза» і частині саме впливу на людину: це «потенційно або реально негативні явища, тенденції і чинники ***інформаційного впливу на людину***, суспільство і державу, що застосовуються в інформаційній сфері…». Тобто, наголошується на недопустимості негативних інформаційних впливів на людину і суспільство.

У статті [312] авторка зазначає, що В.О. Голубєв [106] вважає

інформаційною безпекою держави, суспільства, людини стан їх інформаційної озброєності…, за якого ***ніякі інформаційні впливи*** на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів. Ця слушна точку зору є абсолютно справедливою відносно стану когнітивної безпеки.

На рисунку додатку Б6 наводиться схема запропонованої структури інформаційної безпеки. Зв'язок «кібербезпека» → «когнітивна безпека» пов'язаний із тим, що, як зазначено у Стратегії від 14.05.2021 р. кібербезпеки України, «кібератаки також активно використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення». Роль кібербезпеки у забезпеченні заходів когнітивної безпеки буде предметом подальших досліджень.

Висновки до Розділу 1

У сучасних реаліях широкого впровадження нових інформаційно-комунікаційних технологій, з одного боку, і тенденцій їх використання для завдання шкоди особам, підприємствам, суспільству, державі, з іншого боку, перед державою постає завдання надійного захисту кібернетичної безпеки суб'єктів. В даному розділі запропонований, обґрунтовується і досліджується міждисциплінарний підхід до вивчення та реалізації ефективних засобів правового забезпечення інформаційної й кібер- безпеки, який полягає у поєднанні засобів, методів і правил адміністративного права (принципи діяльності публічної адміністрації і організації публічного управління в демократичному суспільстві), інформаційного права (поєднання свободи інформаційної діяльності із захистом національного інформаційного простору України від розповсюдження ворожої інформаційної продукції, створення та використання інформаційних технологій), пра́ва кібербезпеки (врахування конкретних ситуацій прийняття рішень публічною

адміністрацією), теорії психології впливів (захист осіб від шкідливих інформаційних впливів, забезпечення когнітивної безпеки), деліктологія (вивчення заходів державного примусу адміністративно-правового і кримінально-правового характеру для забезпечення встановлених правил у сфері інформаційної та кібр- безпеки). Вперше узагальнені встановлені КУпАП делікти у сфері обігу інформації і використання інформаційно-комунікаційних систем.

В контексті необхідності врахування конкретних ситуацій прийняття рішень публічною адміністрацією щодо ключових аспектів забезпечення кібербезпеки розглянуті окремі технологічні аспекти виникнення ризиків у кіберпросторі і кіберзагроз, а також проблеми протидії цим ризикам та загрозам. Для зниження цих ризиків і рівня загроз необхідно приділяти все більш уваги побудові, впровадженню й супроводу комплексних систем безпеки, згідно вимог державних і міжнародних стандартів, зокрема, вибудовування систем протидії вразливостям.

Наголошено, що на необхідність системної нейтралізації вразливостей вказується у Стратегії кібербезпеки України, міжнародному стандарті ISO 27005, рекомендаціях Держспецзв'язку, відомчих нормативних документах, наприклад, Нормативному документі НД ТЗІ 1.1-003-99 Служби безпеки України «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу». Разом із тим, у Законі України «Про основні засади забезпечення кібербезпеки України» не надається визначення цього терміну, що обмежує уніфікацію робіт у цій сфері. Пропонується доповнити цей Закон визначенням поняття «вразливості», згідно із міжнародним стандартом інформаційної безпеки ISO 27005.

Пропонується авторське розуміння адміністративно-правового забезпечення діяльності у сфері кібернетичної безпеки України, яке полягає у використанні засобів і методів адміністративного права (публічне адміністрування, нормативно-правове регулювання, встановлення відповідальності за порушення встановлених нормативних правил), з

урахуванням технічних аспектів і технологічних небезпек в кіберпросторі, включаючи протидію вразливостям, кіберінцедентам, кіберконлфктам.

Розглянуті правові засади застосування методу пошуку вразливостей на засадах системи Bug Bounty – це тестування електронних сервісів із залученням зовнішніх фахівців, яке дає можливість виявити вразливі місця і недоліки в програмних продуктах. Виконана періодизація офіційного правового запровадження даної системи в Україні, виділено 2 етапи: 1-й етап – запровадження відповідних змін до Кримінального кодексу України, 2-й етап – запровадження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, затвердженого Постановою КМУ від 16.05.2023 № 497 «Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж». Розглянуті принципи взаємодії між замовником і виконавцем (цями) при пошуку вразливостей, зокрема, висунення публічній пропозиції, підготовка звітів, виплата винагороди тощо. Постановою КМУ від 03.12.2025 № 1580 у цей Порядок внесені зміни. Основна ідея змін полягає у тому, що Постанова № 1580 затверджує новий Порядок пошуку та/або виявлення потенційних вразливостей в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, де обробляються ***державні інформаційні ресурси або інформація з обмеженим доступом, а також на об'єктах критичної інформаційної інфраструктури***. Цей Порядок встановлює організаційно-технічний механізм для здійснення пошуку вразливостей, включно з легальними програмами Bug Bounty, а також уніфікує підходи до сканування, оцінки захищеності та обміну інформацією про вразливості.

Сформульовано положення про те, що загальна логіка пошуку і виявлення вразливостей у системах на засадах системи Bug Bounty

грунтується на аналізі архітектури систем, конфігурації та програмного забезпечення, а також за допомогою тестування, яке може включати сканування на наявність вразливостей, проникнення та інші методи, у тому числі імітацію дій зловмисників для перевірки стійкості системи, з метою виявлення вразливостей; виявлення слабких місць у програмному забезпеченні та конфігурації. Практичне значення нормативно-правових актів про Bug Bounty полягає у тому, що це правове регулювання служить для розробки та впровадження заходів безпеки, що допомагають запобігти несанкціонованому доступу та іншим видам атак.

Встановлено, що Директива Європейського Парламенту і Ради ЄС 2022/2555 від 14.12.2022 року передбачає створення Європейської бази даних про вразливості. Ця база даних включає: (a) інформацію, що описує вразливість; (b) уражені продукти ІКТ чи послуги ІКТ та серйозність вразливості з точки зору обставин, за яких її може бути експлуатовано; (c) наявність пов’язаних патчів і, за відсутності доступних патчів, інструкції, надані компетентними органами чи групами CSIRT користувачам вразливих продуктів ІКТ та послуг ІКТ щодо можливих способів пом’якшення ризиків, спричинених відомими вразливостями.

Розглянуті правові засади забезпечення належного рівня кібербезпеки Інтернет-речей (IoT) – електронно-цифрових пристроїв, приєднаних до інформаційно-комунікаційних систем: «розумні» годинники, «розумні» лічильники, системи «розумний будинок», «розумне авто», розумні роботи, Wi-Fi роутери, ноутбуки, смартфони, датчики та камери, розумні роботи, смарт-карти, мобільні пристрої, розумні колонки, маршрутизатори, перемикачі, промислові системи управління, програмне забезпечення, прошивка, операційні системи, мобільні додатки, настільні програми, відеоігри; компоненти (як апаратні, так і програмні); блоки обробки комп’ютера; відеокарти; програмні бібліотеки тощо. Небезпека цих пристроїв, коли вони приєднані до інформаційно-комунікаційних систем, полягає у тому, що вони є потенційною точкою входу для кібератаки. У

підключеному середовищі інцидент кібербезпеки в одному продукті може вплинути на всю організацію або весь ланцюг постачання, часто поширюючись через кордони внутрішнього ринку за лічені хвилини.

Незважаючи на гостру проблематику, питання правового регулювання питань, пов’язаних з використанням технології Інтернет-речей, до останнього часу не знаходило належного правового регулювання ані в України, ані в ЄС. Разом із тим з вересня 2021 року ЄС розпочав розробку Закону про кіберстійкість (The Cyber Resilience Act (CRA)) – це нормативний акт ЄС щодо покращення кібербезпеки та кіберстійкості в ЄС шляхом встановлення спільних стандартів кібербезпеки для продуктів з цифровими елементами в ЄС, таких як обов'язкові звіти про інциденти та автоматичні оновлення безпеки. Цей нормативний акт вимагатиме від виробників підключених пристроїв належного захисту їх перед доставкою, негайного виявлення та усунення недоліків, а гарантія на виправлення надходитиме протягом п’яти років. У Розділі наголошено не необхідності прийняття аналогічного акту (закону) або доповнення до Закону № 2163-VIII. Одночасно запропоновано поширити вимоги цього Закону на соціальні мережі та/або приватні електронні інформаційні ресурси в мережі Інтернет навіть якщо вони не містять інформацію, необхідність захисту якої встановлена законом, оскільки ці системи за визначенням взаємодіють із публічними мережами електронних комунікацій, зокрема, Інтернет. Де-факто інтереси інформаційного захисту потребують такого регулювання.

Проаналізовані особливості концептів «інформаційна безпека», «безпека інформації», «кібербезпека», «когнітивна безпека» в контексті безпекових стратегій України 2020-2021 років. Наголошується, що в сучасному інформаційному просторі актуальною стає не тільки захист інформації, але й захист від інформації. Це поділяє поняття «інформаційна безпека» на підмножини «безпека інформації» та «когнітивна безпека», тобто «інформаційно-психологічна безпека особи». Крім того, у якості підмножини «безпека інформації» слід розглядати поняття «кібербезпека» як захищеність

життєво важливих інтересів держави, суспільства, людини і громадянина під час використання кіберпростору. У кібербезпеці захищають кіберресурси, у когнітивній безпеці – розум людини. Ворожі інформаційні впливи можуть нести небезпеки не тільки інформаційним (комп'ютерним) системам, але й безпосередньо особам, оскільки можуть бути задіяні для доставляння небажаної інформації в обхід запобіжників отримання (доставляння) цієї інформації. Інформація формує у свідомості людини систему знань, поглядів, смислів, якими людина керується у своїх вчинках – не тільки лояльних по відношенню до оточення, суспільства, держави, але й ворожих по відношенню до них. Інформаційний вплив може змінювати поведінку людей, нав'язувати їм цілі, які об'єктивно не входять в число їх інтересів. Отже, необхідно враховувати зворотній вплив кібербезпеки на когнітивну безпеку. Кібератаки активно використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення.

Запропоновано напрями термінологічного узгодження у ч. 2 ст. 8 та абз. 2 ч. 4 ст. 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах» та у ч. 3 ст. 6 Закону України «Про основні засади забезпечення кібербезпеки України» («слова «інформаційної безпеки» замінити словами «безпеки інформації»).

РОЗДІЛ 2. АДМІНІСТРАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХОДІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

2.1. Правове регулювання заходів забезпечення кібербезпеки актами європейського рівня

Проблеми врегулювання і унормування діяльності у кіберпросторі вже давно стали ключовими у політиці багатьох держав світу. Всі вони однозначні у твердженні, що кіберпростір – це міжнародний простір, і діяльність держав у кібепросторі повинна в першу чергу відповідати нормам міжнародного права. Як зазначено вище, Україна інтегрована у світовий цифровий простір, тому запобігання кіберзагрозам можливе завдяки поєднанню національної та міжнародної стратегій кіберзахисту [71, 94, 125, 138, 241, 243, 353 та ін.].

Так, Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII [51], який є ключовим у сфері кібербезпеки і кіберзахисту в Україні та визначає правові та організаційні основи кібербезпеки, орієнтований на застосування, поряд із національним, міжнародного права у сфері кібербезпеки. Закон встановив принципи, цілі та заходи захисту від кіберзагроз, визначив основні напрямки державної політики у цій сфері. Він також закладає правову основу для захисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. Відповідно до Закону, забезпечення кібербезпеки базується на Конституції України, законах щодо національної безпеки, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, а також на міжнародних документах, зокрема, таких як Конвенція про кіберзлочинність [6] (буде аналізуватися нижче). Закон встановлює загальні принципи формування та реалізації державної політики у сфері кібербезпеки, включаючи: захист прав громадян на доступ до інформації та захист від несанкціонованого доступу; захист державних інформаційних ресурсів та

критичної інформаційної інфраструктури; протидія кіберзлочинності та кібертероризму; створення безпечного інформаційного простору. Ці завдання вирішуються на підставі принципів і стандартів міжнародного права, пріоритету норм міжнародних договорів (ст. 3 Закону, ч.ч. 1, 2); міжнародного співробітництва та вироблення спільних підходів щодо протидії кіберзагрозам, зміцнення взаємної довіри, протидії злочинній діяльності у міжнародному кіберпросторі (пункт 9 ч. 1 ст. 7 Закону); функціонування національної системи кібербезпеки з урахуванням ***міжнародних*** стандартів безпеки та системи індикаторів кіберзагроз (пункт 13 ч. 2 ст. 7 Закону).

Тому необхідно вивчати і знати норми міжнародного права у цій сфері, застосовувати їх у правотворенні і практичній діяльності, на що також звертається увага у статті [267, с. 67-73]. Окремі питання правового регулювання заходів забезпечення кібербезпеки актами європейського рівня досліджувалися автором цієї дисертаційної роботи у його працях [159, 163, 164, 174], а також у статті М.І. Легенького [347].

Як зазначено в огляді статті [347], кібербезпека вже давно є на порядку денному НАТО та Європейського Союзу. Вони мали чітке розуміння того, що будь-яким гібридним загрозам необхідно запобігати, а у разі гібридних атак необхідно застосовувати як м’які, так і жорсткі заходи протидії. У 2002 році Празький саміт розширив механізми кібербезпеки та заклав основу для ініціатив у сфері кібербезпеки в рамках НАТО, відомих як Агентство з питань зв’язку та інформації («перша лінія оборони» НАТО проти кібертероризму) та Технічний центр інформаційної безпеки, який відповідає за зв’язок та комп’ютерну безпеку. Варто наголосити, що 20.12.2002 року Генеральна Асамблея ООН ухвалила Резолюцію 57/239 «Елементи глобальної культури кібербезпеки», яка ввела поняття «кібербезпека» в юридичну термінологію [363]. У цьому документі визначено, що глобальна культура кібербезпеки включає такі взаємопов’язані елементи, як усвідомлення, відповідальність, реагування, етика, демократія, оцінка

ризиків, розробка та впровадження заходів безпеки, а також переоцінка [336].

Після кібератаки на Естонію в 2007 році НАТО почало активно працювати над вирішенням проблеми, і було створено низку органів з кібербезпеки. У 2008 році, в результаті Бухарестського саміту та для об'єднання основних органів НАТО, що займаються кібербезпекою, було створено Орган з управління кібербезпекою, який застосовує гнучкий підхід до розуміння кібербезпеки, а не приймає стабільний та фіксований набір правил і рекомендацій [348]. Стратегічні рамки НАТО чітко окреслюють покрокові заходи організації для підвищення стійкості до зовнішніх факторів та посилення національних стандартів кібербезпеки для держав-членів [348].

Слід зазначити, що з 2010-х років увага зосереджувалася на питаннях політики національної безпеки, а вектор уваги спрямовувався на захист фізичних активів, таких як супутники, глибоководні кабелі та інші засоби зв'язку. У 2012 році Міжнародний центр кримінології також визначив вісім ключових інновацій, які окреслюють майбутні ризики та загрози у сфері кібербезпеки. Вони включають: хмарне середовище; великі дані, мобільний Інтернет, нейронний інтерфейс, безконтактні платежі, мобільні роботи, квантові обчислення та мілітаризацію кіберпростору [337].

ЄС визначив пріоритетом протидію гібридним загрозам та подальший розвиток системи кібербезпеки на найближчі роки. Ці аспекти чітко визначені в низці документів, зокрема у спільних документах Європейського Парламенту й Європейської Ради відносно впровадження заходів протидії гібридним загрозам у ЄС. Аналіз цих документів свідчить про те, що вони окреслюють реалістичне бачення гібридних кіберзагроз та визначають основні напрямки правового забезпечення кібербезпеки в ЄС. Вони також представляють Європейському Співтовариству досягнення та поетапність подальших дій для їх реалізації у сферах, запропонованих у спільних діях, а саме: підвищення обізнаності про ситуацію; стійкість суспільства; зміцнення можливостей запобігання кризам та реагування на них; координація відновлення та розширення співпраці з НАТО для забезпечення

взаємодоповнюваності діяльності. Запропоновані заходи зосереджені на підвищенні обізнаності про гібридні кіберзагрози, виявленні суспільних вразливостей до них та координації спільних заходів для оцінки цих загроз. Для виявлення суспільних вразливостей та врахування реальних гібридних особливостей проводиться аналіз можливих ризиків, які кіберзагрози можуть становити для установ та мереж як пріоритетний компонент та сприяє усвідомленню вразливостей системи у кібербезпеці [347, с. 336].

Історично на європейському рівні слід виокремити такі акти загальноєвропейського правового регулювання:

– Директива 2016/1148 від 06.07.2016 Європейського парламенту й Ради ЄС року про заходи високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу [11]. Директива була замінена Директивою 2022/2555 від 14.12.2022 року [14], яка набрала чинності 16.01.2023 року;

– Директива Ради від 08.12.2008 2008/114/ЄС про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту [9]. Директива була замінена Директивою 2022/2557 від 14.12.2022 року [15], яка набрала чинності 16.01.2023 року;

– Директива від 24.10.1995 95/46/ЄС Європейського Парламенту й Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» [8]. Директива замінена Регламентом від 27.04.2016 Європейського парламенту й Ради ЄС 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) [10], яка набрала чинності 24.05.2016 року;

– Директива від 11.12.2018 Європейського Парламенту й Ради ЄС 2018/1972 про запровадження Європейського кодексу електронних комунікацій [12];

– Регламент від 17.04.2019 Європейського парламенту й Ради ЄС

2019/881 про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту № 526/2013 ЄС (Акт про кібербезпеку) [13];

– Конвенція від 23.11.2001 Ради Європи «Про кіберзлочинність» [6]; в Україні ратифікована Законом від 07.09.2005 № 2824-IV «Про ратифікацію Конвенції про кіберзлочинність» [43]. Конвенція набрала чинності для України 01.07.2006;

– Додатковий протокол від 28.01.2003 до Конвенції від 23.11.2001 про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [7]; протокол ратифіковано Законом України від 21.07.2006 № 23-V [44]. Набрання чинності в Україні – 01.04.2007;

Рекомендація від 30.10.1997 р. № R (97) 19 Комітету міністрів РЄ «Про показ насильства електронними ЗМІ» [19];

Рекомендація від 30.10.1997 р. № R (97) 20 Комітету міністрів РЄ «Про розпалювання ненависті» [20];

Рекомендація від 27.04.1989 р. № R (89) 7 Комітету міністрів РЄ «Про принципи поширення відеозаписів насильницького, жорстокого чи порнографічного змісту» [18].

Даний перелік не є вичерпним. Сюди ж слід віднести розглянутий вище Закон ЄС про кіберстійкість (The Cyber Resilience Act (CRA)).

Перші 5 перелічених (чинних) документів (Директива 2022/2555 від 14.12.2022; Директива 2022/2557 від 14.12.2022; Регламент 2016/679 від 27.04.2016; Директива 2018/1972 від 11.12.2018; Регламент 526/2013 від 17.04.2019) підлягають імплементації у законодавство України відповідно до Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, Розділ III «Юстиція, свобода та безпека». При цьому вважається [244], що прийняття Закону України від

16.12.2020 року № 1089-IX «Про електронні комунікації» [53] є імплементацією Директиви ЄС 2018/1972 від 11.12.2018 про запровадження Європейського кодексу електронних комунікацій [12].

Директива 2016/1148

Директива 2016/1148 [11] – це законодавчий акт ЄС з кібербезпеки, який встановлює єдиний високий стандарт безпеки для мережевих та інформаційних систем у всіх країнах-членах. Директива 2016/1148 називається ще Директивою NIS («Network and Information Security»; «мережева та інформаційна безпека»). Директива спрямована на створення загального стандарту кібербезпеки у всіх країнах ЄС, на підвищення кібербезпеки в усьому ЄС шляхом встановлення жорсткіших вимог до держав-членів та організацій.

У Директиві 2016/1148 від 06.07.2016 відзначається, що вона прийнята, між іншим, виходячи з наступних міркувань:

(1) Мережеві та інформаційні послуги та системи відіграють важливу роль в державі. Надійність та безпека таких послуг та систем є суттєвою для економічної та соціальної діяльності.

(2) Вплив кіберінцидентів зростає та становлять велику загрозу для мережевих та інформаційних систем. Такі системи стають об’єктом умисних шкідливих дій, які здійснюються з метою пошкодження таких систем або перешкоджання їх експлуатації. Такі інциденти можуть завдавати значних фінансових збитків, перешкоджати здійсненню економічної діяльності, підривати довіру користувачів.

(3) Мережеві та інформаційні системи, зокрема, Інтернет, сприяють транскордонному руху товарів, людей та послуг.

(63) Набуло широкого поширення викрадення персональних даних у результаті кіберінцидентів. Тому необхідна постійна протидія витокам персональних даних.

Директива вимагає від країн-членів мати національні стратегії кібербезпеки та національні групи реагування на інциденти комп'ютерної

безпеки (CSIRT), а також стандартизує режими санкцій та наглядові заходи. Національні стратегії та групи реагування: Директива вимагає, щоб держави-члени розробили національну стратегію кібербезпеки та призначили CSIRT для реагування на інциденти. Згідно з Директивою створюється єдина контактна особа (SPoC) для забезпечення транскордонної співпраці між національними органами влади. Вводяться більш суворі наглядові заходи та вимоги до забезпечення дотримання законодавства, а також гармонізуються санкції по всьому ЄС. Директива спрямована на підвищення стійкості та можливостей реагування на кіберінциденти як у державному, так і в приватному секторах, а також загалом в ЄС.

З метою захисту критичної інфраструктури Директива зобов’язує організації вводити заходи щодо забезпечення безпеки своїх мережевих та інформаційних систем, особливо в критично важливих секторах, таких як енергетика, транспорт, банківська справа, охорона здоров’я та цифрові послуги.

Користувачі інформаційно-комунікаційними системами чи приєднаними до них приладами повинні здійснювати управління ризиками, тобто повинні керувати ризиками, впроваджувати відповідні заходи безпеки та створювати плани забезпечення безперервного розвитку бізнесу на випадок кіберінцидентів. Від компаній, що підпадають під дію директиви, вимагається запровадити адекватні та співрозмірні заходи безпеки, провести навчання керівництва та співробітників, а також забезпечити безпеку всього ланцюгу поставок. Компанії зобов’язані повідомляти компетентні національні органи про серйозні інциденти кібербезпеки. Введено суворі вимоги щодо звітності про кіберінцеденти і посилення відповідальності щодо невиконання вимог кібербезпеки.

Хоча директива набула чинності в 2023 році, країни-члени ЄС повинні були адаптувати своє національне законодавство до 17 жовтня 2024 року, а організації повинні були розробити стратегії відповідності новим вимогам.

В Директиві наголошується, що вона поважає фундаментальні права,

визнані в ЄС, зокрема права на захист персональних даних, на повагу особистого життя, права власності, свободи підприємництва, права дієвого правового захисту.

Директива 2022/2555

Директива 2016/1148 про мережеву та інформаційну безпеку (NIS) була першим загальноєвропейським законодавчим актом щодо кібербезпеки, а його конкретною метою було досягнення високого спільного рівня кібербезпеки в державах-членах. Хоча вона підвищила можливості держав-членів у сфері кібербезпеки, її впровадження виявилося складним, що призвело до фрагментації на різних рівнях внутрішнього ринку [361, с. 1].

Тому, наприкінці 2022 року – початку 2023 року було визнано, що Директива 2016/1148 від 06.07.2016 [11] вичерпала себе. На заміну була прийнята Директива 2022/2555 [14], яка набрала чинності 16.01.2023 року. У цій Директиві віддавалося належне надбанням, що досягнуті у період дії Директиви 2016/1148 від 06.07.2016 [11]. Зокрема, зазначається, що завдяки впровадженню Директиви 2016/1148 вдалося досягнути суттєвого прогресу в підвищенні кіберстійкості ЄС. Зокрема, на підставі Директиви була створена Група співробітництва NIS та мережа команд реагування на інциденти комп'ютерної безпеки (CSIRT) для забезпечення як обміну інформацією про кібербезпеку, так і співпраці щодо конкретних інцидентів кібербезпеки [361, с. 3]. Директива послужила каталізатором регуляторного та інституційного підходу до кібербезпеки, забезпечила остаточне формування національних заходів щодо безпеки інформаційних й мережевих систем шляхом запровадження національних стратегій безпеки мережевих та інформаційних систем та розбудови національних спроможностей щодо реалізації регуляторних заходів у сфері критичної інфраструктури та важливих суб’єктів, що визначаються кожною державою-членом.

Разом із тим, зазначається, що у період дії Директиви 2016/1148 не вдалося досягнути належного рівня уніфікації вимог до стану кібербезпеки. Наявні розбіжності розбіжності могли б призвести до підвищеної вразливості

окремих держав до кіберзагроз із поширенням негативних наслідків в інші країни ЄС. Отже, метою нової Директиви 2022/2555 було усунути такі значні розбіжності, зокрема, шляхом уніфікації вимог.

Таким чином, Директива 2022/2555, відома як NIS2, набула чинності в 2023 році. Директива спрямована на посилення кібербезпеки в ЄС, встановлюючи високий спільний рівень безпеки мережевих та інформаційних систем. Вона замінила попередню Директиву 2016/1148 (NIS 2016 року), розширила сферу застосування на нові сектори та організації, уніфікувала вимоги та посилила відповідальність організацій за порушення у сфері управління ризиками та звітування про інциденти. Нова директива охоплює ширше коло секторів, включаючи енергетику, транспорт, охорону здоров'я, банківську справу, цифрову інфраструктуру, а також виробництво, космічну галузь та послуги IT-постачальників. Директива NIS2 посилює вимоги до кібербезпеки для критично важливих секторів в ЄС, вимагаючи проактивного управління ризиками, за яким (управлінням) організації зобов'язані впроваджувати відповідні технічні, операційні та організаційні заходи для управління ризиками кібербезпеки. Це включає: політики інформаційної безпеки (наявність затверджених документів, що визначають заходи, обов'язки та контроль); оцінки ризиків (регулярний аналіз ризиків, що стосуються ключових активів та процесів); шифрування (використання шифрування для захисту критичних та персональних даних); багатофакторна автентифікація (MFA) (обов'язкове використання MFA для доступу до мереж та систем); безпека ланцюга постачання (директива вимагає від компаній оцінювати та контролювати кібербезпеку своїх постачальників та сервісних провайдерів); звітність про інциденти (вимагається обов'язкова та своєчасна звітність про значні кіберінциденти, як правило, у три фази: попередня звітність (24 години), повне повідомлення (72 години) та фінальний звіт (один місяць)); безперервність бізнесу (необхідно мати плани для забезпечення безперервності бізнесу та кризового управління, що дозволяють швидко відновити роботу після інциденту); фізична безпека (для деяких

секторів можуть бути встановлені вимоги щодо фізичної безпеки, такі як камери відеоспостереження для контролю доступу до чутливих зон); санкції (невиконання вимог може призвести до значних штрафів). Зокрема, за порушення вимог щодо заході управління ризиками кібербезпеки та/або правил звітування можуть стягуватися адміністративні штрафи у розмірі не менше 10.000.000 євро або не менше 2 % загального річного світового обороту суб'єкта господарювання, якому належить цей основний суб'єкт, залежно від того, яка сума більша.

Отже, вказане свідчить про те, що ЄС твердо стоїть на позиції уніфікації і інтеграції систем забезпечення кібербезки, що висуває відповідні вимоги і перед Україною, яка має Угоду про асоціацію з ЄС і прагне вступу до ЄС. Зокрема, у статті 1 Директиви 2022/2555 наголошується, що ця Директива встановлює інструменти, що мають на меті досягти високого спільного для країн ЄС рівня кібербезпеки задля того, або покращити функціонування внутрішнього ринку. Задля цього Директива встановлює:

(a) обов'язки, що вимагають від держав-членів ухвалити національні стратегії кібербезпеки і призначити чи створити компетентні органи, органи управління кіберкризами, єдині контактні пункти з питань кібербезпеки (єдині контактні пункти) та групи реагування на інциденти в сфері комп'ютерної безпеки (CSIRT);

(b) обов'язки щодо звітування та заходи управління ризиками у сфері кібербезпеки;

(c) правила і обов'язки щодо обміну інформацією щодо кібербезпеки;

(d) наглядові та правозастосовні обов'язки держав-членів.

У статті 7 Директиви 2022/2555 вимагається, що кожна держава-член ухвалює стратегію кібербезпеки. Національна стратегія кібербезпеки включає:

(a) цілі й пріоритети стратегії кібербезпеки держави-члена;

(b) управлінську систему для досягнення цілей стратегії;

(c) управлінську систему, що роз'яснює функції та обов'язки

відповідних стейкхолдерів на національному рівні, закладаючи основу для співпраці та координації між компетентними органами та групами CSIRT за цією Директивою, а також координації та співпраці між національними органами та компетентними органами за секторальними правовими актами Союзу[5];

(d) механізм ідентифікації відповідних активів і оцінювання ризиків у державі-члені;

(e) визначення інструментів, що забезпечують підготованість до інцидентів, реагування на них й відновлення після них, у тому числі співпрацю між приватним і державним секторами;

(f) перелік різних органів влади та стейкхолдерів, що беруть участь у реалізації національної стратегії кібербезпеки;

(g) політичні рамки для посиленої координації між компетентними органами за Директивою ЄС 2022/2557 та компетентними органами за цією Директивою з метою обміну інформацією щодо кіберзагроз, інцидентів ризиків, включаючи ризики, що не відносяться до ризиків у сфері кібербезпеки, загроз та інцидентів та виконання наглядових завдань, залежно від випадку;

(h) план, у тому числі необхідні заходи, для посилення загального рівня обізнаності про кібербезпеку серед громадян.

Тут слід принагідно наголосити, що Україна має таку розроблену Стратегію кібербезпеки 14.05.2021 р. [24], яка неодноразово згадувалася і аналізувалася у цій роботі.

У статті 8 Директиви 2022/2555 передбачається, що кожна держава призначає (створює) компетентний(і) орган(и), відповідальний(і) за кібербезпеку.

Слід зазначити, що це є ті са́мі суб’єкти публічної адміністрації,

[5] Стейкхолдери (від англ. *stakeholders*) – зацікавлені сторони, зацікавлені особи, заінтересовані сторони, причетні сторони – фізичні та/або юридичні особи, які мають легітимний інтерес у діяльності організації, тобто певною мірою залежать від неї або можуть впливати на її діяльність [216].

загальні принципи діяльності яких у сфері публічного адміністрування розглянуті у підрозділі 1.1 цієї дисертації і які визначені такими у сфері кібербезпеки згідно ч. 2 ст. 8 Закону № 2163-VIII [51].

У статті 10 Директиви 2022/2555 на Держави-члени покладається обов’язок створювати Групи реагування на інциденти комп’ютерної безпеки (CSIRT). Згідно ч. 3 ст. 9 Закону № 2163-VIII [51], в Україні це CERT-UA – національна команда реагування на кібератаки, кіберінциденти, кіберзагрози (національний CSIRT), діяльність якої забезпечується службою Держспецзв’язку, а також галузеві команди реагування на надзвичайні комп’ютерні події.

Як зазначалося вище, у підрозділі 1.1 цієї дисертаційної роботи, стаття 12 Директиви 2022/2555 передбачає ведення Європейської бази даних про вразливості, а також скоординоване оприлюднення інформації про вразливості. Організації, які постраждали від кіберінцидентів (кібератак), повинні повідомляти про будь-який «значний інцидент» своїй CSIRT (групі реагування на інциденти комп’ютерної безпеки) або компетентному органу наступним чином: раннє попередження протягом 24 годин; повідомлення про інцидент протягом 72 годин; проміжний звіт на запит; та остаточний звіт протягом одного місяця. Фізичні та юридичні особи також зобов’язані повідомляти CSIRT про нещодавно виявлені вразливості. Агентство ЄС з кібербезпеки (ENISA) має розробити та підтримувати базу даних вразливостей ЄС (див. також [356]).

Директива 2022/2555 безпосередньо поширюється на основні суб'єкти господарювання: енергетика (електроенергетика, централізоване опалення та охолодження, нафта, газ та водень); транспорт (повітряний, залізничний, водний та автомобільний); банківська справа; інфраструктура фінансового ринку; охорона здоров'я, включаючи виробництво фармацевтичної продукції, включаючи вакцини; питна вода; стічні води; цифрова інфраструктура (точки обміну інтернетом; реєстри імен TLD; постачальники послуг DNS; постачальники послуг центрів обробки даних; постачальники послуг

хмарних обчислень; постачальники довірчих послуг; мережі доставки контенту; постачальники мереж загальнодоступного електронного зв'язку та загальнодоступних послуг електронного зв'язку); управління послугами ІКТ (постачальники керованих послуг та постачальники керованих послуг безпеки), державне управління та космос, а також на «важливі суб'єкти господарювання»: поштові та кур'єрські послуги; управління відходами; хімічні речовини; харчові продукти; виробництво медичних виробів, комп'ютерів та електроніки, машин та обладнання, автомобілів, причепів та напівпричепів, а також іншого транспортного обладнання; цифрові постачальники (онлайн-майданчики, платформи соціальних мереж; онлайн-пошукові системи) та дослідницькі організації.

Директива 2022/2555 визначила за необхідне, щоб національні стратегії кібербезпеки вирішували потреби у сфері кібербезпеки середніх і малих підприємств, які все частіше стають мішенями атак на ланцюжки постачання у зв’язку з менш жорсткими заходами управління ризиками кібербезпеки.

Директива 2022/2555 також передбачає, що національні стратегії кібербезпеки мають містити політики щодо сприяння кіберзахисту як частині ***оборонної стратегії***, що також стає все більш актуальним. Зокрема, повідомляється [226], що НАТО пропонує включити кібербезпеку в нову ціль оборонних витрат. Згідно з документом НАТО, який цитує Bloomberg, в Альянсі пропонують включити в пов’язані з обороною витрати кібербезпеку, охорону кордонів, захист критичної інфраструктури, невійськові розвідувальні служби та діяльність, пов'язану з космосом.

Директива 2022/2557 в контексті війни у кіберпросторі

Директива 2022/2557 від 14.12.2022 року [15] присвячена вирішенню питань стійкості критично важливих суб’єктів, оскільки ця проблема стає вкрай актуальною не тільки в Україні, але й на Заході через протиборство у кіберсередовищі, нав’язаному диктаторськими режимами. Так, британський та канадський політолог українського походження наводить спостереження [178], що сподівання на те, що Путін обмежить своє втручання діями проти

країн, котрі не належать до НАТО, як-от Грузія чи Україна, було ілюзорним. Росія вдалася до гібридної та інформаційної війни й війни в кіберпросторі проти багатьох членів Альянсу: Естонії, Великої Британії, Німеччини, Норвегії, Нідерландів, Франції, Греції, Угорщини, Болгарії, Туреччини, а також Чорногорії, яка була кандидатом на вступ до НАТО [178, с. 53]. До трійки країн, на які найчастіше спрямовані російські кібератаки, належать США, Україна та Велика Британія ([349], публікація 2023 року).

Так, у грудні 2022 року Клінт Воттс, генеральний менеджер центру аналізу цифрових загроз Microsoft у дописі в блозі компанії «On the Issues» повідомляв, що росія активізує свої кіберзусилля, щоб тиснути на джерела військової та політичної підтримки України, як внутрішні, так і зовнішні. Поряд з майже двома місяцями ракетних ударів та ударів безпілотників по цивільній інфраструктурі України, відбувалися «додаткові» кібератаки на українські та іноземні ланцюги поставок, а також «кібероперації впливу», додав він [357].

У вересні 2022 року стало відомо, що російські хакери атакували Генеральний штаб Збройних Сил Португалії, в результаті чого до мережі потрапили секретні документи НАТО. Про вразливість португальського Генерального штабу місцевий уряд дізнався лише після отримання повідомлення від США через посольство у Лісабоні [146].

У січні 2023 року російські хакери (лояльне до Путіна російське хакерське угруповання Killnet) атакували Німеччину у зв’язку з її рішенням передати танки Україні [102].

У березні 2023 року повідомлялося про хвилю кібератак проросійської хакерської групи noname057(16) на італійські сайти; під ударом у тому числі опинилися кілька урядових структур. Серед них – сторінки міністерства транспорту, Регуляторної служби з питань транспорту, Atac (Римське муніципальне агентство залізничного транспорту). У своєму Telegram група noname057(16) пояснила атаку останніми новинами про те, що 20 українських військових пройшли в Італії навчання на системах ППО SAMP-

Т, та що прем’єрка Джорджія Мелоні не бачить передумов для початку перемовин про завершення війни в Україні [88]. Одночасно повідомлялося, що на початку березня 2023 року також повідомляли про кібератаку на німецький концерн Rheinmetall, який хоче виробляти танки в Україні [88].

У січні 2024 року пов'язане з Росією хакерське угруповання NoName атакувало кілька урядових сайтів Швейцарії через участь Президента України Володимира Зеленського на Всесвітній економічний форум у Давосі. У результаті хакерської DDoS-атаки низка урядових сайтів були недоступними. Про це повідомляла пресслужба уряду Швейцарії. За інформацією відомства, в результаті DDoS-атаки було тимчасово перервано доступ до низки сайтів, у тому числі до сайтів Федеральної адміністрації [100].

У жовтні 2025 року міністр цифровізації Польщі Кшиштоф Гавковський в інтерв'ю Reuters повідомив про значне збільшення кількості кібератак, спрямованих проти критичної інфраструктури країни. За його словами, російська військова розвідка утричі збільшила свої ресурси для проведення зловмисних дій проти Польщі у 2025 році. Загалом упродовж перших трьох кварталів року зафіксовано понад 170 тисяч кіберінцидентів, значна частина яких пов'язана з російськими структурами. Міністр також наголосив, що іноземні хакери розширюють діяльність за межі систем водопостачання та каналізації, переходячи до атак на енергетичний сектор [185].

У лютому 2024 року Нідерланди звинуватили Китай у кібершпигунстві: хакери залізли в мережу військових. Китайські кібершпигуни, яких підтримує держава, отримали доступ до нідерландської військової мережі, заявили нідерландські спецслужби. Агентства країни, відомі під абревіатурами MIVD і AIVD, заявили, що хакери розмістили шкідливе програмне забезпечення, яке приховувало їхню діяльність, в мережі збройних сил, яку використовували 50 осіб для проведення несекретних досліджень [217].

Нову хакерську групу в межах розвідувального агентства формує Північна Корея. Новий підрозділ, відомий як Research Center 227, зосередиться на розробці «наступальних технологій і програм для злому». Про це пише TechCrunch, посилаючись на Daily NK. За інформацією джерела, Research Center 227 вивчатиме ***західні системи кібербезпеки та комп'ютерні мережі***, розширюючи можливості режиму для крадіжки цифрових активів. Також він працюватиме над розробкою методів, заснованих на штучному інтелекті, для викрадення інформації та координуватиме роботу з іншими північно-корейськими хакерськими угрупованнями за кордоном. Останнім часом північно-корейські хакери активно атакують криптовалютні біржі та компанії по всьому світу. Однією з найбільших крадіжок став нещодавній злам біржі Bybit на суму $1,4 млрд. Раніше ФБР і Агентство національної безпеки США неодноразово звинувачували розвідувальні агентства Північної Кореї у кібератаках і шпигунстві [282].

Виходячи з фактичних реалій кібер-протиборства, Директива 2022/2557:

(a) встановлює обов'язки держав-членів щодо вжиття конкретних заходів, спрямованих на забезпечення надання послуг, які є важливими для підтримання життєво важливих суспільних функцій або економічної діяльності у сфері застосування статті 114 Договору про функціонування Європейського Союзу, безперешкодно на внутрішнього ринку, зокрема обов'язки з визначення критично важливих суб'єктів, підтримувати критично важливі суб'єкти щодо задоволення покладених на них обов'язків;

(b) встановлює обов'язки критично важливих суб'єктів, спрямовані на посилення їхньої стійкості та здатності надавати послуги, згадані в пункті (a), на внутрішньому ринку;

(c) встановлює правила:

(i) щодо нагляду за критично важливими суб'єктами;

(ii) щодо правозастосування;

(iii) щодо визначення критично важливих суб’єктів, що мають особливе значення для Європи, та щодо дорадчих місій для оцінювання заходів, які такі суб’єкти запровадили для виконання своїх обов’язків відповідно до глави III;

(d) встановлює спільні процедури співпраці та звітування щодо застосування цієї Директиви;

(e) встановлює заходи з метою досягнення високого рівня стійкості критично важливих суб’єктів, щоб забезпечити надання основних послуг у межах Союзу та для покращення функціонування внутрішнього ринку.

Зокрема Директива визначає [218]:

– необхідність ухвалення державами-членами ЄС стратегії підвищення кіберстійкості операторів критичної інфраструктури з надання життєво важливих послуг;

– вимоги щодо проведення аналізу ризиків стійкості критичної інфраструктури за всіма секторами та підсекторами критичної інфраструктури, визначеними Директивою;

– зобов’язання щодо застосування операторами критичної інфраструктури планів стійкості, які (плани) включають без пекові, технічні, та організаційні заходи, з урахуванням визначеного рівня загроз, їхнього впливу;

– створення Групи стійкості операторів критичної інфраструктури як консультативно-координаційного механізму підтримки Єврокомісії та підготовки методичних та нормативних матеріалів для операторів критичної інфраструктури та держав – членів ЄС в цілому;

– інститут «консультативної місії» для оцінки обов’язкових заходів, вжитих оператором критичної інфраструктури, для забезпечення стійкості функціонування критичної інфраструктури;

– вимоги щодо визначення уповноваженого органу для взаємодії між Єврокомісією, іншими інституціями ЄС, державами – членами ЄС, операторами критичної інфраструктури, а також оцінювання стану

імплементації державами положень Директиви, підготовки звітів для подання Єврокомісії;

– підготовку методичних та інструктивних матеріалів, сприяння в організації та проведенні колективних навчань, консультування, запровадження програм підвищення кваліфікації персоналу операторів критичної інфраструктури.

Директива приділяє увагу розбудові спроможності ЄС й держав-членів бути заздалегідь підготовленими до кризових ситуацій. Наголошується на необхідності мати максимально повну, точну й актуальну інформацію про загрози критичної інфраструктури, з якими можуть зіткнутись оператори критичної інфраструктури, можливі негативні наслідки реалізації цих загроз.

Вказується, що підвищення стійкості європейської критичної інфраструктури до цілеспрямованих зловмисних дій повинно бути пріоритетом щодо ключових секторів критичної інфраструктури, а саме: цифрова інфраструктура, енергетика, транспорт і космос. Щодо критичної інфраструктури, основна увага повинна зосереджуватися на інфраструктурі надання послуг транскордонного характеру.

Відповідно до вказаних пріоритетів, Директива 2022/2557 запроваджує необхідні інструменти та механізми забезпечення стійкості надання послуг, формулює вимоги до залучених суб'єктів. Директива 2022/2557 встановлює вимоги до операторів критичної інфраструктури щодо забезпечення ними стійкості надання послуг, способи взаємодії між операторами критичної інфраструктури та уповноваженими державними органами, повноваження Єврокомісії щодо координації національних зусиль та інституцій ЄС на рівні Союзу тощо.

Отже, Директива 2022/2557 створює цілісну систему взаємодії операторів критичної інфраструктури, інституцій ЄС та держав-членів щодо забезпечення стійкості надання основних послуг на внутрішньому ринку ЄС. Разом із тим, особливістю такої системи є максимальне використання зацікавленості операторів критичної інфраструктури у сталості надання ними

послуг та безперервності бізнес-процесів.

Конвенція Ради Європи «Про кіберзлочинність»

Конвенція Ради Європи «Про кіберзлочинність» (Будапештська конвенція) [6] з Додатковим протоколом до неї [7] вважається універсальним міжнародним документом, що спрямований на боротьбу з інтернет-злочинністю та комп'ютерною злочинністю (кіберзлочинністю) [144], й встановлює і класифікує злочини у сфері кіберзлочинності [94, с. 70]. На квітень 2023 року Конвенцію ратифікували 68 країн (як зазначено вище, Україна ратифікувала Конвенцію 07.09.2005 року; проти Конвенції виступає рф, яка, как правило, уникає співпраці з правоохоронними органами у питаннях розслідування кіберзлочинів) [144]. Просуваючи загальні стандарти розслідування та судового переслідування кіберзлочинів Конвенція ставить за мету:

– збалансувати ефективну правоохоронну діяльність із захистом фундаментальних прав людини;

– установити рамки для взаємодопомоги між країнами у сфері кібербезпеки;

– дозволяти країнам обмінюватися інформацією та ресурсами у процесі розслідування кіберзлочинів;

– гармонізувати національне законодавство та посилити співпрацю у транснаціональних відносин у контексті кібербезпеки.

Основні положення Конвенції про кіберзлочинність зосереджені на криміналізації певних видів правопорушень, пов'язаних з комп'ютерами та Інтернетом, та створенні міжнародної правової бази для співпраці між державами. Головні положення охоплюють криміналізацію злочинів проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, а також встановлюють процедури для доступу до цифрових доказів та транскордонної співпраці правоохоронних органів.

Конвенція визначає та криміналізує такі види злочинів:

– злочини проти конфіденційності, цілісності та доступності

комп'ютерних даних і систем, включає незаконний доступ до комп'ютерних систем та даних, втручання в роботу систем;

– комп'ютерне шахрайство, включає злочини, пов’язані з обманом за допомогою комп'ютерних систем;

– злочини, пов’язані з контентом, зокрема, дитяча порнографія та порушення авторських прав;

– злочини, пов’язані з порушенням безпеки мережі, включає незаконне перехоплення даних та інші злочини, що стосуються безпеки комп’ютерних мереж.

Додаткові підстави відповідальності співучасть та/або корпоративна відповідальність.

Конвенція встановлює рамки для міжнародної співпраці, покладаючи на держави обов’язок допомагати одна одній у розслідуванні кіберзлочинів.

Конвенція регламентує доступ до доказів – вона передбачає процедури для правоохоронних органів щодо можливості отримувати цифрові докази, в тому числі ті, що знаходяться за кордоном.

Усього серед перелічених можна виділити 2 групи кіберзлочинів: які вчиняються у кіберпросторі та які вчиняються з використанням останнього.

До першої групи злочинів можна віднести три категорії кіберзлочинів:

– злочини проти конфіденційності, цілісності і працездатності комп'ютерних даних і систем – незаконний доступ, незаконне перехоплення, створення перешкод для обміну даними, створення перешкод для функціонування систем, неправомірне використання апаратних пристроїв;

– комп'ютерні злочини – фальсифікація і підробка, що здійснюються з використанням комп'ютерної техніки;

– злочини, пов'язані з контентом, – виготовлення, поширення і зберігання дитячої порнографії.

Об’єктом таких кіберзлочинів може стати будь-який користувач Інтернету.

Разом із тим, до другої групи злочинів можна віднести дві категорії

кіберзлочинів:

– злочини, пов’язані з порушенням авторського права і суміжних прав; встановлення таких правопорушень віднесено до компетенції національних законодавств держав;

– кіберзлочини як акти ксенофобії та расизму, скоєні за допомогою комп’ютерних мереж.

Об’єктом таких кіберзлочинів може стати не тільки і навіть не стільки будь-який користувач Інтернету, але й особа, яка не є користувачем Інтернету. Наприклад об’єктом злочину у вигляді поширення контрафактної продукції через мережу Інтернет може стати суб’єкт авторського права, який не є користувачем Інтернету.

Як зазначається у дисертації [94, с. 71], деякі кіберзлочини нормами Конвенції не виділено в окремі групи. До таких кіберзлочинів відноситься «кібертероризм», тобто використання кіберпростору в терористичних цілях. Державами та міжнародними організаціями докладаються зусилля по протидії терористичним організаціям, що використовують кіберпростір. Як приклад, можна навести проект Clean IT, який існує на рівні ЄС та метою якого є боротьба з кібертероризмом.

Зокрема, «Clean IT» – це онлайн-проект, ініційований ЄС, спрямований на зменшення або запобігання онлайн-тероризму та подальшій незаконній діяльності через Інтернет. Його метою є створення документа, який зобов’язує інтернет-індустрію допомагати урядам виявляти контент, що підбурює до актів тероризму. Основними посередниками, які взялися за цей проект, були Нідерланди, Німеччина, Велика Британія, Бельгія та Іспанія. Є багато інших членів ЄС, які підтримують проект, таких як Угорщина, Румунія та нещодавно Італія, але основними країнами, які розпочали проект, є 5 перелічених вище [329].

Не можна залишити поза увагою ще одну категорію кіберзлочинів – крадіжка і використання персональних даних з метою вчинення злочинів (identity theft), яка безпосередньо не включена в Конвенцію про

кіберзлочинність, однак отримала поширення після прийняття цього міжнародного документа. Деякі країни виділяють ці правопорушення в окрему категорію, однак інші вважають, що ці правопорушення підпадають під кілька статей кримінального законодавства [71, с. 33], що спонукає до виділення даного діяння в окрему групу та гармонізації міжнародного законодавства у цій сфері.

Метою Додаткового протоколу [7] до Конвенції «Про кіберзлочинність» [6] є внесення доповнень до положень Конвенції, які стосуються криміналізації дій ксенофобного та расистського характеру, які вчинені через комп'ютерні системи. Для цілей цього Протоколу «ксенофобний та расистський матеріал» означає будь-який письмовий матеріал, будь-яке зображення чи будь-яке інше представлення ідей або теорій, які захищають, сприяють або підбурюють до ненависті, дискримінації чи насильства проти будь-якої особи або групи осіб за ознаками раси, кольору шкіри, національного або етнічного походження, а також віросповідання, якщо вони використовуються як привід для будь-якої з цих дій.

Отже, цей Протокол повинен забезпечити кримінально-правовий захист когнітивної безпеки осіб та суспільства в частині запобігання проявам дій ксенофобного та расистського характеру.

Важливість цього напряму захисту когнітивної безпеки наочно ілюструє історія з радіо «Тисячі пагорбів» (Radio Télévision Libre des Mille Collines, RTLM, RTLMC) – руандійською радіостанцією, яка мовила з 08.07.1993 по 31.07.1994, що розпалювала міжнаціональну ворожнечу і підбурювала до геноциду в Руанді в 1994 році і відповідальність пропагандистів якої за геноцид доведена юридично – Міжнародним трибуналом з Руанди. Конкретними підрахунками впливу радіо на різанину між тутсі та хуту зайнявся доцент-економіст Гарвардського університету Девід Янагізава-Дротт. Ґрунтуючись на фізичних законах поширення радіохвиль, він встановив, що оскільки в розпорядженні RTLM було два

передавача – один в Кігалі, другий на гірському піку Муе, а Руанда геть уся покрита горами, то вони (гори) перекривають шлях радіосигналу. Тому в деяких селищах немає прийому, або ж покриття часткове. За допомогою карти рельєфу учений розрахував рівень сигналу в кожній точці країни. Виходячи з даних, скільки саме людей у кожному селищі було засуджено за геноцид, він виявив, що в зоні впевненого прийому радіо їх число було набагато більше, ніж у тих місцях, де сигналу не було. Таким чином, економіст публічно довів негативний вплив радіопропаганди на виникнення різанини між тутсі та хуту. За підрахунками Янагізави, на дикторах та редакторах RTLM лежить відповідальність приблизно за 45-50 тис. убивств. Таким чином, десятки тисяч людей залишилися б живими, якби зламалася вся пара радіопередавачів [232, 313]. Таким чином, математично доведено, що пропаганда вбиває.

За Протоколом, визнано необхідним криміналізувати таки діяння:

– поширення ксенофобного та расистського матеріалу через комп'ютерні системи (стаття 3);

– погроза з ксенофобних та расистських мотивів, зроблена через комп'ютерну систему (стаття 4);

– [публічна] обра́за з ксенофобних та расистських мотивів, зроблена через комп'ютерну систему (стаття 5);

– заперечення, значна мінімізація, схвалення або виправдання геноциду чи злочинів проти людства, як це визнано заключними та обов'язковими рішеннями Міжнародного військового трибуналу, заснованого згідно з Лондонською угодою від 08.08.1945 року або будь-якого іншого міжнародного суду (стаття 6);

– пособництво та/або підбурювання до вчинення будь-якого з правопорушень, визначених відповідно до цього Протоколу, з наміром вчинити такий злочин (стаття 7).

В публікації [144] С. Карвацька, Р. Іванюк Р. звертають увагу на важливість Конвенції Ради Європи «Про кіберзлочинність» для України в

умовах сучасної злочинної кібервійни рф проти України, у тому числі масової антиукраїнської пропаганди та закликів до геноциду українського народу. Конвенція, вказують автори, залишається в авангарді як основний міжнародно-правовий стандарт щодо кіберзлочинності та електронних доказів. Адже очевидно, що за умов агресії рф проти України загрози кіберзлочинності стають дедалі складнішими, тому вкрай важливо, щоб вітчизняні правові системи були оснащені для ефективного розслідування кіберзлочинів, одночасно забезпечуючи захист прав людини.

Рекомендації Комітету міністрів Ради Європи щодо протидії пропаганді війни, насильства, жорстокості, розпалювання расової, національної, релігійної, міжетнічної, ворожнечі та ненависті

Серед стратегічних цілей реалізації Стратегії інформаційної безпеки України [28] визначена, зокрема, протидія пропаганді війни, насильства, жорстокості, розпалювання расової, національної, релігійної, міжетнічної, ворожнечі та ненависті. Комплекс підходів, що надає уявлення про європейські стандарти обмеження поширення матеріалів, що містять показ насильства та жорстокості, окреслюють Рекомендації Комітету міністрів РЄ від 27.04.1989 р. № R (89) 7 «Про принципи поширення відеозаписів насильницького, жорстокого чи порнографічного змісту» [18], від 30.10.1997 р. № R (97) 19 «Про показ насильства електронними ЗМІ» [19], від 30.10.1997 р. № R (97) 20 «Про розпалювання ненависті» [20]. Базовим принципом підходу до обмежень в даній сфері є положення, передбачені статтею 10 ЄКПЛ. Імплементація цих Рекомендацій також є подальшим впровадженням заходів забезпечення когнітивної безпеки.

У Рекомендації № R (89) 7, враховуючи, зокрема, норми ст.ст. 8 і 10 ЄКПЛ щодо свободи вираження поглядів і безперешкодного поширення інформації та ідей, визнаéться, натомість, важливість консолідації дій, спрямованих проти поширення відеозаписів жорстокого, насильницького й порнографічного змісту, а також проти вживання наркотиків, зокрема задля захисту неповнолітніх. Визнано, що Держави-члени повинні: заохочувати

створення систем саморегулювання, або створювати системи класифікації й контролю відеозаписів за допомогою відповідних професійних секторів чи органів державної влади, або запроваджувати системи, які поєднують саморегулювання з системами класифікації й контролю чи іншими, які не суперечать національному законодавству. В усіх випадках можливе застосовування кримінального законодавства та відповідних заходів впливу фіскального й фінансового характеру. Зокрема, обмеження поширення можуть здійснюватися шляхом: заборони поставок з комерційною метою або пропозицій щодо поставок неповнолітнім; заборони на рекламу; заборони на продаж по пошті. Класифікація кожного відеозапису має бути вказана на упаковці матеріального носія і у відеокаталозі, рекламі та ін.

Рекомендація № R (97) 20 від 30.10.1997 р. виходила з засудження розпалювання ксенофобії, расової ненависті, антисемітизму та всіх форм нетерпимості, оскільки це підриває безпеку демократії, культурну єдність, плюралізм. Зазначається, що окремі випадки розпалювання ненависті можуть бути настільки образливі для окремих осіб і груп населення, що вони вийдуть за рамки правового захисту, що надається статтею 10 ЄКПЛ відносно свободи самовираження. Деякі форми необґрунтованого показу насильства, розпалювання ненависті можуть законним чином бути обмежені, враховуючи обов'язки й відповідальність, що їх несе із собою здійснення права на свободу вираження поглядів, за умови, що такі втручання в свободу вираження поглядів передбачені законодавством і є необхідними в демократичному суспільстві, згідно частини 2 статті 10 ЄКПЛ.

Найбільш докладно аналізована проблема відзеркалена у Рекомендації № R (97) 19. Ця Рекомендація виходила з того, що здійснення свободи вираження поглядів пов'язані з обов'язками і відповідальністю, і що воно може бути законним чином обмежене з метою підтримки рівноваги між здійсненням цього права і дотриманням інших основних прав, свобод і інтересів, які захищає Конвенція. Рекомендація [172] сформулювала способи, якими на фахівців ЗМІ може бути покладена відповідальність за належну

редакційну політику, в тому числі і щодо уникнення «необґрунтованого показу насильства»: i) попередня поінформованість громадськості про повідомлення, слова́ й зображення насильницького характеру, які збираються зробити доступними; ii) запровадження кодексів поведінки, які визначатимуть конкретні обов'язки відповідного професійного сектора; iii) впровадження внутрішніх керівних принципів, у т. ч. стандартів для оцінювання змісту в організаціях електронних ЗМІ; iv) заснування на секторальному рівні та окремими телерадіомовниками відповідних консультативних і контрольних механізмів для моніторингу процесу впровадження стандартів саморегулювання; v) врахування стандартів саморегулювання в контрактах з іншими секторами, наприклад, виробниками аудіовізуальної продукції й відеоігор, рекламними агенціями та ін.; vi) регулярні контакти та обмін інформацією з національними регуляторними органами, а також з органами саморегулювання в інших країнах.

До аналогічних висновків приходила Ю.Л. Юрицень у дисертаційному дослідженні [307, с. 359-361].

2.2. Правове регулювання заходів забезпечення кібербезпеки актами національного права

М.І. Легенький (із співавторами) [347, с. 337] справедливо вважає, що в систему українського законодавства у сфері інформаційної та кібер- безпеки входять, зокрема, Конституція Україна, Кримінальний кодекс України, Закони України «Про основи національної безпеки» [42] (з 08.07.2018 – «Про національну безпеку України» [52]), «Про основні засади забезпечення кібербезпеки України» [51], «Про інформацію» [36], «Про державну таємницю» [37], «Про доступ до публічної інформації» [48], «Про захист інформації в інформаційно-телекомунікаційних системах» [38], «Про наукову та науково-технічну експертизу» [39], «Про технічні регламенти та оцінку відповідності» [49].

До цього ж слід додати Закони України «Про Державну службу спеціального зв’язку та захисту інформації України» [45], «Про авторське право і суміжні права» [57], «Про критичну інфраструктуру» [55], «Про Національну поліцію» [50], «Про захист персональних даних» [47], «Про електронні комунікації» [53], «Про медіа» [56].

Як висновується у статті [319], одним із співавторів якої є дисертант, необхідно відзначити багатогалузевий характер законодавства про інформаційну та кібер- безпеку. Воно охоплює широкий спектр питань, від захисту свободи слова та протидії кіберзагрозам до регулювання діяльності ЗМІ [319]. Загалом, формування українського законодавства у цій сфері розпочалося у 2011 році та триває досі. Його розвиток базувався на принципах міжнародного регулювання інших країн [347, с. 337].

Ключовим правовим актом в Україні щодо забезпечення кібербезпеки слід визнати Закон України від 05.10.2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» [51] (далі – Закон № 2163-VIII).

Мета та цілі прийняття закону:

– забезпечення національної безпеки – захист суверенітету, територіальної цілісності та безпеки держави у кіберпросторі;

– захист громадян – захист прав, свобод та інтересів громадян України в кіберпросторі;

– захист інформації – захист інформаційних ресурсів та систем від несанкціонованого доступу, крадіжки, пошкодження чи руйнування;

– протидія кіберзагрозам – створення ефективної системи протидії кіберзагрозам, включаючи хакерські атаки, віруси, витік даних та інші шкідливі дії;

– координація та управління – в контексті діяльності публічної адміністрації у даній сфері закон передбачає створення Національного координаційного центру кібербезпеки як робочого органу РНБО України. Його основна мета – координація діяльності всіх суб'єктів забезпечення кібербезпеки для вирішення складних завдань у цій сфері.

Закон визначає принципи забезпечення кібербезпеки в Україні, які охоплюють: верховенство права, захист національних інтересів, прозорість і стабільність кіберпростору, державно-приватну взаємодію, пропорційність заходів кіберзахисту, пріоритет запобігання загрозам і невідворотність покарання за кіберзлочини. Також важливе значення мають координація зусиль суб'єктів кібербезпеки, підтримка вітчизняного наукового потенціалу та підвищення обізнаності суспільства. Основні принципи верховенства права та законності: забезпечення кібербезпеки відбувається у межах закону та з повагою до прав людини. Захист національних інтересів здійснюється шляхом надання пріоритету захисту безпеки України у кіберпросторі. Відкритість і доступність кіберпростору – сприяння розвитку кіберпростору та відповідальній поведінці в ньому. Державно-приватна взаємодія – співпраця держави, приватного сектору та громадянського суспільства у сфері кібербезпеки. Пропорційність – заходи кіберзахисту мають відповідати реальним і потенційним ризикам. Закон робить акцент на превентивних заходах для захисту від загроз (пріоритет запобігання). Декларуються: невідворотність покарання – застосування заходів відповідальності до осіб, які вчиняють кіберзлочини; координація та взаємодія – узгодження дій усіх суб'єктів, що забезпечують кібербезпеку, на національному та міжнародному рівнях. В контексті вимог Директиви 2022/2555 ЄС передбачається пріоритетне зосередження зусиль на захисті об'єктів критичної інформаційної інфраструктури; підтримка вітчизняного науково-технічного та виробничого потенціалу у сфері кібербезпеки; адаптація законодавства (приведення законодавства України у відповідність до норм ЄС); підвищення обізнаності (інформування суспільства про кіберризики та загрози).

За змістом Закону № 2163-VIII [51], об'єкти критичної інформаційної інфраструктури – це інформаційні, електронні, комунікаційні системи, які необхідні для функціонування життєво важливих служб та процесів, а також відсутність яких призведе до значних негативних наслідків для суспільства та держави. До них належать системи в таких галузях, як телекомунікації

(оператори мобільного зв'язку, інтернет-провайдери), фінанси (банки), медицина (лікарні, заклади швидкої допомоги), транспорт (залізничні, авіаційні, морські, автомобільні компанії), енергетика та інші стратегічно важливі сектори. Основні характеристики та приклади визначення: інформаційна, електронна комунікаційна, інформаційно-комунікаційна або технологічна система, необхідна для сталого функціонування об'єкта критичної інфраструктури, що істотно впливає на безперервність та стійкість надання життєво важливих функцій. Критеріями віднесення об’єкту захисту до цієї категорії є відсутність альтернативних об'єктів або способів надання послуг. Приклади об'єктів: телекомунікації (оператори мобільного зв'язку, інтернет-провайдери, мережі передачі даних, телефонні мережі; фінанси (банки, платіжні системи, страхові компанії; охорона здоров'я (лікарні, центри швидкої медичної допомоги, системи трансплантації органів); транспорт (системи управління залізничним, авіаційним, морським та автомобільним рухом, аеропорти, вокзали); енергетика (системи управління електромережами, газопостачанням тощо); державне управління (системи, що забезпечують функціонування органів державної влади). Особливості Об'єкти критичної інформаційної інфраструктури мають відповідати підвищеним вимогам до кіберзахисту, включаючи фізичний та логічний контроль доступу. Власники або розпорядники об'єктів призначають відповідальних осіб за кіберзахист або утворюють спеціальні підрозділи.

Порівняння вказаних норм надають підставі вважати, що вони цілком адаптовані до Директиви 2022/2555 ЄС.

За змістом Закону № 2163-VIII [51], об'єктами кіберзахисту та кібербезпеки в цілому є критично важливі інформаційні системи та інфраструктура, зокрема: конституційні права і свободи; держава, її конституційний лад, територіальна цілісність і недоторканність; критична інформаційна інфраструктура, як це описано вище; національні інтереси; сталий розвиток інформаційного суспільства; державні інформаційні ресурси та системи (системи органів державної влади, місцевого самоврядування,

правоохоронних органів та військових формувань); комунікаційні системи всіх форм власності, що використовуються для задоволення суспільних потреб (наприклад, електронне урядування, електронна комерція, електронний документообіг).

Стаття 5 Закону № 2163-VIII [51] визначає суб'єкти влади, які здійснюють функції кіберзахисту в Україні Це є Державна служба спеціального зв'язку та захисту інформації (Держспецзв'язку), Національна поліція (Кіберполіція), Служба безпеки України (СБУ), Збройні Сили України, а також центральні та місцеві органи виконавчої влади. Окрім них, до кіберзахисту залучені інші урядові та державні структури, включно з Національним банком України та операторами критичної інфраструктури.

Основні суб'єкти: Держспецзв'язку – головний орган, відповідальний за формування та реалізацію державної політики у сфері кіберзахисту. Служба, зокрема, забезпечує функціонування Державного центру кіберзахисту та Центру активної протидії агресії у кіберпросторі, урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA; Кіберполіція – підрозділ Національної поліції, який бореться зі злочинами в кіберпросторі; СБУ – забезпечує кібербезпеку держави, включаючи контррозвідувальні заходи та захист інформаційних ресурсів; Збройні Сили України та інші військові формування – здійснюють кіберзахист військових систем та інфраструктури, беручи участь у кібероборонні держави; Національний банк України – відповідає за кіберзахист банківської системи та створення відповідних підрозділів реагування (CSIRT-NBU); центральні та місцеві органи виконавчої влади – Міністерства та інші органи, а також місцеві державні адміністрації, які здійснюють заходи з кібербезпеки в межах своєї компетенції.

Крім того, Закон визначає інші суб’єкти у сфері кіберзахисту: оператори критичної інформаційної інфраструктури – власники або розпорядники об'єктів критичної інфраструктури, які забезпечують захист своїх інформаційних систем; суб'єкти господарювання, громадяни,

громадські об'єднання – всі особи, які займаються діяльністю, пов'язаною з національними інформаційними ресурсами, кіберзахистом та комунікаціями, несуть відповідальність за кібербезпеку.

Згідно ч. 3 ст. 6 Закону № 2163-VIII [51], розроблення нормативно-правових актів в системі безпеки та кібер- безпеки інформації здійснюється здійснюється на основі міжнародних стандартів, стандартів ЄС та НАТО з обов'язковим залученням представників основних суб'єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій.

Міжнародне співробітництво у сфері кіберзахисту включає спільне вироблення норм поведінки у кіберпросторі, посилення захисту критичної інфраструктури, гармонізацію законодавства та координацію дій у боротьбі з кіберзлочинністю через міжнародні організації (як ЄС) та двосторонні угоди. Воно також може включати обмін ресурсами, як-от технологіями та технічною допомогою, для підвищення кіберстійкості.

Закон містить також інші важливі положення щодо основних засад забезпечення кібербезпеки України.

Основні напрями міжнародного співробітництва у сфері кіберзахисту: розробка стандартів та політик – спільне вироблення норм поведінки у кіберпросторі та вдосконалення нормативно-правової бази; технічне співробітництво – посилення захисту критичної інфраструктури та обмін технологіями, наприклад, через співпрацю з ЄС; правове співробітництво – гармонізація законодавства з партнерами (наприклад, з ЄС) та координація дій у боротьбі з кіберзлочинністю, включаючи правову допомогу та екстрадицію; спільні операції та реагування – участь у спільних кібероперaціях та координація реагування на кіберзагрози; обмін досвідом – передача цінних ресурсів, технічної допомоги та обмін досвідом у протидії кібератакам.

Форми міжнародного співробітництва: через міжнародні організації – участь у роботі організацій, таких як ЄС, та спільних ініціативах; через

міжнародні угоди – укладання двосторонніх або багатосторонніх угод; через конференції – співробітництво в рамках міжнародних конференцій; двостороння співпраця – пряма співпраця між державами.

В контексті реалізації «відносини адміністративних зобов'язань» [184, с. 24], які притаманні засобам і способам адміністративного права, у Законі № 2163-VIII послідовно реалізовані усі:

а) відносини публічного управління – управлінські функції і повноваження Президента України, КМУ, міністерств, інших центральних органів виконавчої влади; місцевих державних адміністрацій; органів місцевого самоврядування;

б) відносини адміністративних послуг – кібербезпека та адміністративні послуги пов'язані через цифровізацію державних сервісів, де захист даних стає ключовим завданням. Кібербезпека захищає інформаційні системи, що забезпечують надання електронних адміністративних послуг, а фахівці з кібербезпеки працюють у держорганах, поліції, СБУ, щоб запобігати кіберзагрозам. Фахівці захищають комп'ютерні системи від шкідливого програмного забезпечення, програм-вимагачів, SQL-ін'єкцій та інших кібератак;

в) встановленої правовими нормами відповідальності публічної адміністрації у випадку їх неправомірних дій або бездіяльності – суб'єкти національної системи реагування на кіберінциденти, кіберзагрози, кібератаки … несуть адміністративну, цивільно-правову, кримінальну відповідальність за неправомірне розголошення, неправомірне розкриття, неправомірне використання та інші неправомірні дії з інформацією про кіберінциденти відповідно до закону (ч. 3 ст. 9 Закону № 2163-VIII). Адміністративна відповідальність настає за порушення, передбачені КУпАП (див. також таблицю додатку Б1, стаття 212-6 КУпАП – за здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем та інше);

г) відповідальності суб’єктів суспільства за порушення порядку і правил, встановлених публічною адміністрацією у межах її повноважень – посадові особи власників або розпорядників інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, де обробляються державні інформаційні ресурси та/або службова інформація та інформація, що становить державну таємницю, посадові особи операторів критичної інфраструктури, власників або розпорядників об’єктів критичної інформаційної інфраструктури несуть адміністративну відповідальність відповідно до закону за невиконання або невиконання у встановлені строки обов’язку щодо здійснення обов’язкових повідомлень про кіберінциденти, кібератаки (ч. 6 ст. 9-1 Закону № 2163-VIII).

Натомість крім вказаного Закону окремі питання щодо забезпечення кібербезпеки України вирішуються в окремих інших суміжних законах України, а також у підзаконних актах [223] (перелік Законів неповний):

– «Про основи національної безпеки України»;

– «Про Державну службу спеціального зв’язку та захисту інформації України»;

– «Про телекомунікації»;

– «Про критичну інфраструктуру»;

– «Про захист персональних даних»;

– «Про захист інформації в інформаційно-комунікаційних системах»;

– «Про медіа» (регулює правовідносини, серед іншого, у сфері електронних медіа)

– Указ Президента України від 26.08.2021 року № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» (див. розділ 1 даної праці);

– Положення про проходження військової служби (навчання) військовослужбовцями Державної служби спеціального зв'язку та захисту інформації України, затверджене Указом Президента України від 31.07.2015 року № 463/2015. Основні аспекти Положення охоплюють: порядок прийому,

проходження, звільнення, а також права, обов'язки, соціальні гарантії військовослужбовців, і зарахування часу служби до стажу;

– Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затверджене постановою КМУ від 03.09.2014 р. № 411;

– Порядок формування переліку об’єктів критичної інформаційної інфраструктури, затверджений постановою Кабінету Міністрів України від 09.10.2020 р. № 943. Формування переліку… включає секторальні органи, які складають переліки своїх секторів, затверджують їх та подають до уповноваженого органу, яким є Адміністрація Держспецзв'язку. Натомість основний реєстр об'єктів критичної інформаційної інфраструктури адмініструє саме Держспецзв'язку за даними, отриманими від відповідних секторальних органів;

– Порядок віднесення об’єктів до об’єктів критичної інфраструктури, затверджений постановою КМУ від 09.10.2020 № 1109. Порядок… встановлює КМУ, а рішення приймають секторальні органи на основі критеріїв, визначених у Законі України «Про критичну інфраструктуру» [55]. Власники об'єктів мають звернутися до відповідного секторального органу, який відповідає за їх сектор чи підсектор, для визначення, чи належить об'єкт до критичної інфраструктури. В першу чергу, суб'єкт господарювання повинен звернутися до секторального органу, який відповідає за його сектор (наприклад, енергетика, транспорт, зв'язок тощо). Перелік секторів затверджено Постановою КМУ № 1109;

– Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах, затверджений постановою КМУ від 16.11.2002 № 1772. Порядок… визначається законодавством, зокрема Законом України «Про захист інформації в інформаційно-комунікаційних системах» [38] та Законом України «Про Державну службу спеціального зв'язку та захисту інформації України» [45]. Ключовими аспектами є

координація дій через Систему електронної взаємодії органів виконавчої влади (СЕВ ОВВ) та співпраця з Державною службою спеціального зв'язку та захисту інформації України, яка є головним суб'єктом у сфері кіберзахисту. Взаємодія між органами влади відбувається через електронний формат за допомогою СЕВ ОВВ, що автоматизує обмін електронними документами;

– Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою КМУ від 29.03.2006 № 373. Правила… визначаються законодавством України, зокрема Законом України «Про захист інформації в інформаційно-комунікаційних системах» [38]. Основні принципи включають захист інформації від несанкціонованого доступу (конфіденційність), модифікації (цілісність) та забезпечення доступу до неї (доступність). Відповідальність за захист інформації в системі несе її власник або розпорядник. Захисту підлягає інформація з обмеженим доступом, що циркулює в системах, а також відкрита інформація, яка є державними інформаційними ресурсами. Вимоги до захисту інформації встановлюються відповідними нормативними документами, наприклад, «Критерії оцінки захищеності комп'ютерних систем від несанкціонованого доступу» (НД ТЗІ 2.5-004-99);

– Правила надання та отримання телекомунікаційних послуг, затверджені постановою КМУ від 11.04.2012 № 295, втратило чинність, на заміну прийняті Правила надання та отримання телекомунікаційних послуг, затверджені постановою КМУ від 25.06.2025 № 761. Правила… передбачають укладення договору між споживачем та оператором, а також оплату послуг споживачем. Договір має відповідати вимогам, встановленим Національною комісією, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку. До послуг належать різні види зв'язку та доступу до мереж. Надані визначення: телекомунікації – це передавання або приймання сигналів, зображень, звуків та повідомлень різними системами зв'язку;

оператор телекомунікаційних послуг – це компанія, що надає послуги зв'язку, зокрема традиційні та новітні (інтернет, електронна пошта тощо); телекомунікаційне обладнання – це пристрої, що забезпечують передачу та прийом мережевого трафіку;

– Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури, затверджені Постановою КМУ від 19.06.2019 № 518. Вимоги визначають технологічні, організаційно-методологічні та технічні умови кіберзахисту критичної інфраструктури, що є обов’язковими для виконання підприємствами, установами та організаціями, що віднесені до об’єктів критичної інфраструктури;

– Порядок формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави, затверджений постановою КМУ від 23.08.2016 № 563, втратив чинність, на заміну прийнятий Порядок формування переліку об’єктів критичної інформаційної інфраструктури, затверджений постановою КМУ від 09.10.2020 № 943. Порядок... визначається законодавством України, зокрема Законом України «Про критичну інфраструктуру» [55] та нормативно-правовими актами, що регулюють захист інформації. Процес включає ідентифікацію об'єктів, визначення їхньої критичності, установ та організацій, що є об'єктами критичної інфраструктури в різних секторах (енергетика, фінанси, охорона здоров'я, інформаційні технології тощо), а також подальше включення їхніх інформаційно-телекомунікаційні системи до відповідних переліків, що здійснюється державними органами, які відповідають за безпеку та захист інформації;

– Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, затверджений постановою КМУ від 23.12.2020 № 1295. Порядок визначає засади функціонування системи реагування на кіберінциденти та кібератаки та виявлення вразливостей, які здійснюються щодо об’єктів кіберзахисту, що визначені Законом «Про основні засади забезпечення кібербезпеки України» [51];

– Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджений Наказом Адміністрації Держспецзв'язку[6] від 10.06.2008 за № 94, зареєстрованим в Міністерстві юстиції України 07.07.2008 № 603/15294. Координацію здійснюють КМУ, РНБО України та місцеві державні адміністрації відповідно до їхніх повноважень, як визначено законодавством. Координація на державному рівні здійснюється через центральні органи виконавчої влади, зокрема КМУ та РНБО України. Координацію в галузі цивільного захисту забезпечують КМУ та РНБО України. Координація на місцевому рівні здійснюється місцевими державними адміністраціями та органами місцевого самоврядування. Наприклад, для координації дій громадських формувань з охорони громадського порядку;

– Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджений Наказом Адміністрації Держспецзв'язку від 02.12.2014 за № 660, зареєстрованим в Міністерстві юстиції України 28.01.2015 № 90/26535;

– Порядок сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті, затверджений Наказом Адміністрації Держспецзв'язку від 15.01.2016 № 20, зареєстрованим в Міністерстві юстиції України 05.02.2016 за № 196/28326. Сканування є однією з форм оцінки стану захищеності інформації в інформаційно-комунікаційних системах і полягає у дистанційній перевірці інформаційно-комунікаційної системи, де розміщені державні інформаційні ресурси в Інтернеті щодо виявлення в ній вразливостей;

[6] Державна служби спеціального зв'язку та захисту інформації України

– Положення про територіальний орган Адміністрації Державної служби спеціального зв’язку та захисту інформації України, затверджене Наказом Адміністрації Держспецзв’язку від 01.09.2014 № 432 (у редакції наказу Адміністрації від 08.02.2022 № 66), зареєстрованим в Міністерстві юстиції України 18.09.2014 за № 1142/25919. Положення… визначає основні функції територіального органу, структуру, завдання та порядок діяльності. Ці положення затверджуються керівництвом Держспецзв'язку на основі закону «Про Державну службу спеціального зв’язку та захисту інформації України» [45], а також інших нормативно-правових актів, що регламентують діяльність відомства.

Запропонована логіка побудови структури описаних підзаконних нормативно-правових актів України у сфері кіберзахисту, яка наведена на схемі додатку Б7.

Важливо зазначити, що у пункті 2 ч. 2 ст. 2 Закону № 2163-VIII передбачено, що правозастосування у сфері кібербезпеки та прийняття суб’єктами владних повноважень рішень щодо виконання норм цього Закону здійснюються, зокрема, з максимально можливим застосуванням національного та міжнародного права щодо повноважень і обов’язків суб’єктів забезпечення кібербезпеки, у тому числі як державних, так і приватних. У пункті 3 ч. 2 ст. 2 Закону № 2163-VIII передбачено також принцип забезпечення захисту прав суб’єктів кіберпростору, у тому числі прав на захист персональних даних та невтручання у приватне життя (див. також підрозділ 3.3 цієї роботи).

Отже, хоча законодавство з кіберзахисту звернено, перш за все, до суб’єктів національної системи кібербезпеки, це законодавство покликано також забезпечення безпеки, прав, свобод та інтересів широкого кола користувачів об’єктами кібербезпеки та кіберзахисту, – через належне виконання уповноваженими суб’єктами національної системи кібербезпеки своїх обов’язків та повноважень у сфері кіберзахисту.

Варто зазначити, що питання кіберзлочинності розглядаються також у

такому специфічному акті, як Типології легалізації (відмивання) доходів, одержаних злочинним шляхом, у 2013 році, затверджені Наказом від 25.12.2013 № 157 Державної служба фінансового моніторингу України [60].

У Документі розглядаються наступні питання щодо кіберзлочинності: види кіберзлочинів, загрози та ризики кіберзлочинів, шахрайство з використанням інформаційно-комунікаційних систем та комп'ютерних технологій; кіберзлочинність нефінансового характеру, загальні напрямки протидії кіберзлочинам, виявлення підозрілих фінансових операцій.

Висновується, що правовою основою боротьби з легалізацією доходів, одержавних внаслідок вчинення кіберзлочинів, є Конвенція від 23.11.2001 року Ради Європи «Про кіберзлочинність» [6], яка в аналізованій Типології називається як «Будапештська Конвенція» (див. також підрозділ 2.1 цієї дисертаційної роботи). Конвенція забезпечує основу для співпраці між країнами у розслідуванні злочинів, вчинених за допомогою комп'ютерних систем, що може включати фінансові злочини. Кіберзлочинність часто є джерелом коштів, які потім відмиваються. Наприклад, хакери можуть використовувати незаконно отримані гроші для фінансування або приховування своєї діяльності. Будапештська конвенція може бути використана для розслідування фінансових злочинів, скоєних через Інтернет, оскільки вона встановлює процедури для збору цифрових доказів і допомоги між країнами у розслідуваннях.

Інтернет використовується не тільки як місце вчинення злочину з одержанням незаконного доходу, а місцем легалізації цього доходу. Протидія кіберзлочинам в контексті легалізації незаконних доходів поєднує комплекс технічних, організаційних, інформаційних та правових (законодавчих) заходів.

Так, у Постанові від 21.06.2023 року у справі № 922/4091/19 Верховного Суду у складі колегії Касаційного господарського суду (пункт 9) [127, № 114187019] констатовано:

«Перед Верховним Судом при розгляді справи постали такі питання:

– за яких умов банк зобов`язаний повернути кошти клієнту відповідно до ч. 1 ст. 1073 Цивільного кодексу України, якщо їх несанкціоноване списання здійснене внаслідок злочинних дій?;

– чи поширюється на спірні відносини законодавство про фінансовий моніторинг та кібербезпеку?;

– чи мав Банк правомочності зупинити підозрілі операції, що призвели до несанкціонованого списання коштів з рахунку клієнта?»

Виходячи з цих проблем, у Постанові висновується, зокрема, наступне:

«***121.*** *У Типології легалізації (відмивання) доходів, одержаних злочинним шляхом, … від 25.12.2013 № 157 (далі – Типологія), вказано, що банківська система України є однією зі сфер, де найбільш широко та активно використовуються сучасні можливості інформаційних технологій та мережі Інтернет… Несанкціоноване списання коштів з банківських рахунків, втручання в роботу інтернет-банкінгу, шахрайство з платіжними картками, розповсюдження комп`ютерних вірусів, шахрайство в інформаційних мережах, DDoS атаки на інтернет-ресурси, – це не повний перелік кіберзлочинів, тобто злочинів у сфері інформаційних та комп`ютерних технологій.*

125. *Мета шахраїв – спотворити інформацію і провести платіж, який за змістом не буде виділятися в потоці звичайної діяльності жертви, але переведе гроші на рахунки підставної особи або фіктивної фірми, використовуючи звичайне для даного клієнта призначення платежу.*

126. *У Типології вказано, що індикаторами підозрілості фінансових операцій … для банківських установ … можуть бути, зокрема, наступні фактори:*

– спроба входу із нового або забороненого IP-адресу;

– транзакції в нестандартний час;

– незвичайні умови чи складність операції;

– спроби зняти кошти в день їх зарахування;

– операції не відповідають попереднім операціям клієнта.

127. *Відповідно до ч. 1 ст. 17 Закону № 1702-VII, суб`єкт первинного фінансового моніторингу має право зупинити здійснення фінансової(их) операції(ій), яка(і), зокрема містить(ять) ознаки, передбачені статтями 15 та/або 16 цього Закону.*

128. *Виходячи із вказаних норм права … Верховний Суд зазначає, що Банк після отримання для виконання платіжних доручень про перерахування грошових коштів з рахунку позивача мав здійснити фінансовий моніторинг таких операцій, адже вони мали очевидні ознаки, що вказують на сумнівність (підозрілість)*».

Питання правового регулювання заходів забезпечення кібербезпеки актами національного права досліджувалося, зокрема, у роботі [164] автора цієї дисертаційної роботи.

2.3. Публічне адміністрування у сфері протидії кіберконфліктам

Повсюдне поширення інформаційно-комунікаційних систем, зокрема, Інтернету, призвело до того, що доступ до таких систем став достатньо полегшеним. При цьому одні особи входять у системи з позитивною метою (отримання об’єктивної інформації, спілкування, здійснення законних платежів), а інші особи – із зловмисними цілями (викрадення або спотворення інформації, викрадення грошових коштів, булінг тощо). За таких умов користувачі інформаційно-комунікаційних систем можуть мати різноманітні інтереси, а зіткнення різноманітних інтересів в інформаційній сфері призводить до інформаційних конфліктів. Якщо ці інформаційні конфлікти переносяться у віртуальний простір, такі конфлікти набувають характер кіберконфліктів [299]. Як зазначено у монографії [268], саме прийняття Закону «Про основні засади забезпечення кібербезпеки України» (№ 2163-VIII) означає для України законодавче закріплення понятійного апарату з приставкою «кібер-» і запровадження регулювання в цілому цифрової економіки [268, с. 62].

Закон № 2163-VIII запровадив низку понять. Зокрема, згідно пункту 11 ч. 1 ст. 1 Закону № 2163-VIII, кіберпростір – середовище (віртуальний простір), що надає можливості для здійснення комунікацій чи реалізації суспільних відносин, яке (середовище) утворене в результаті функціонування з'єднаних (сумісних) комунікаційних систем з використанням мережі Інтернет чи інших глобальних мереж передачі даних.

Отже, кіберконфлікти – це конфлікти у кіберпросторі.

Згідно ч. 1 ст. 7 Закону № 2163-VIII, забезпечення кібербезпеки в Україні ґрунтується, зокрема, на принципах: верховенства права, захисту національних інтересів, прозорості і стабільності кіберпростору, пріоритету запобігання загрозам і невідворотність покарання за кіберзлочини. Основні принципи верховенства права та законності: забезпечення кібербезпеки відбувається у межах закону та з повагою до прав людини.

У пункті 70 Преамбули Директиви ЄС 2022/2555 [14] зазначається, що масштабні інциденти та кризи кібербезпеки на рівні Союзу вимагають розвивати і захищати глобальний, відкритий, стабільний і **безпечний кіберпростір**, заснований на правах людини, фундаментальних свободах, демократії та верховенстві права.

Отже, ефективне публічне адміністрування у сфері протидії кіберконфліктам є важливою сферою адміністративно-правового забезпечення діяльності у сфері кібернетичної безпеки України.

Нормативного визначення поняттю «кіберконфлікти» Закон № 2163-VIII не надає. Це поняття у більшій мірі використовується як доктринальне. Тому дослідження підходів до визначення кіберконфліктів є актуальним.

Розвиток техніки та технологій в інформаційній площині вимагає адекватних заходів забезпечення захисту як особистої інформації, так і інформації на державному рівні. Не завжди впровадження захисних програм дозволяє отримати позитивних результатів [299, с. 157]. Несанкціонований доступ до електронному інформації може відбуватися шляхом: зчитування даних у інших користувачів; читання інформації, яка залишилася після

виконання санкціонованих запитів; викрадання паролів, інших аналогічних реквізитів з метою маскування під зареєстрованого користувача; маскування несанкціонованих запитів під запити операційної системи (містифікація); використання програмних пасток, виведення з ладу механізмів захисту. Наведений перелік достатньо повно відображає фактичний стан справ. Особливо небезпечними є шляхи, пов’язані із зміною/викривленням програмного забезпечення [236].

Проведений аналіз літератури [299, с. 154] дозволив визначити наступні підходи до визначення конфліктів у системах безпеки: 1) інформаційні конфлікти як частина конфліктів у різних сферах і галузях, оскільки інформація – стратегічний ресурс, цінність якого набуває особливо у процесі створення, тому потребує забезпечення захисту; 2) інформаційні конфлікти як конфлікти в інформаційних системах між впровадженими програмами або у телекомунікаційних системах між радіоелектронними засобами та системами безпеки; 3) кіберконфлікти – частина міжнародних інформаційних конфліктів і пов’язані найчастіше з інформаційними війнами, кібершпигунством, кібероперацією [299, с. 154].

Отже, систематичні дослідження концепту «кіберконфлікт» на даний момент (кінець 2025 року) відсутні.

До аналогічного висновку можна дійти з аналізу дисертаційного дослідження [120]. Зокрема, дослідник пропонує три ключові рівні кіберконфліктів:

1) перший – «*класичні» кіберзлочини* (здирництво, шахрайство, несанкціонований доступ до автоматизованих баз даних та персональних даних користувачів, поширення порнографії, продаж наркотиків чи зброї тощо) – як оригінальні, так і звичні для нас, для реалізації вони потребують тільки наявності сучасних інформаційних технологій [120, с. 234];

2) другий – *злочини, які характерні для геополітичної боротьби*: політично вмотивовані хакерські атаки; кібердиверсії, кібершпигунство [120, с. 234]. Тут слід пригадати описані вище хакерські атаки хакерських груп,

пов’язаних з російською владою, на країни, що допомагають Україні в її боротьбі з російською агресію – як «покарання» за цю допомогу;

3) третій – ворожі атаки у кіберпросторі, особливістю яких є спрямування на знищення життєво важливої інфраструктури й отримання доступу до військових, оборонних, банківських, комерційних та інших життєво важливих баз даних [120, с. 234].

Однак аналіз концепту «кіберконфлікт» далі не пішов, хоча питанням загальної конфліктології приділена певна увага.

Зазначене підтверджує актуальність дослідження підходів до визначення кіберконфліктів. Це питання досліджувалося, зокрема, у роботах [175, 297, 310] автора цієї дисертаційної роботи.

Поняття «кіберконфлікт», попри те, що воно формально не легітимізоване у спеціальному Законі № 2163-VIII, і при наявності близьких за змістом легітимізованих понять «кіберінцидент» і «кіберзлочин», достатньо широко використовується у науковій літературі [107, 120, 129, 156, 203, 299 деякі інші] і у науково-практичній діяльності [295 та інші]. Зазначене пов’язано, очевидно, із тим, що поняття «кіберконфлікт» дозволяє охопити значну більшу кількість конфліктних явищ, які виникають у кіберпросторі, ніж два інші згадані поняття, взяті разом.

Так, у статтях [70, 101] конфлікт пропонується визначити як оцінку характеру взаємодії. Таке визначення дає змогу зберегти назву конфлікт за ситуаціями протидії сторін одна одній, які ми традиційно називали конфліктом, і водночас поширити це поняття на ситуації несумісності певних елементів у складі цілого [101, с. 41; 299, с. 154]. Тобто несумісність певних елементів у складі цілого необов’язково пов’язано із злочинною поведінкою, але може підпадати під визначення «конфлікт».

Згідно ч. 1 ст. 1 (пункт 3) Закону № 2163-VIII, інцидент кібербезпеки (кіберінцидент) – подія або ряд несприятливих подій ненавмисного характеру (технологічного, природного, технічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки

можливої кібератаки, які становлять загрозу безпеці систем електронних комунікацій, управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем, ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

Це визначення зосереджується на пріоритеті загроз безпеці електронних комунікацій, управління технологічними процесами, електронних інформаційних ресурсів, але не приділяють жодної уваги захищеності окремих людей, людських спільнот, суспільства в цілому. У той же час у статті [299] звертається увага на те, що проблема конфліктів в інформаційній сфері повинна розглядатися через взаємодію площин теорії конфліктології та теорії інформаційної та кібернетичної безпеки у трьох ракурсах: «суб'єкт – суб'єкт» або «людина – людина», можливо «група людей – група людей», «людина – група людей»; «суб'єкт – об'єкт» або «людина – машина»; «об'єкт – об'єкт» або «машина – машина». У преамбулі Закону № 2163-VIII визначається, що Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів **людини і громадянина, суспільства** та держави, національних інтересів України у кіберпросторі…

Тобто, без врахування людського фактору як об'єкту негативного впливу розгляд проблематики кіберінцидентів є недостатнім та неповним.

При цьому, говорячи про негативний вплив на людину, варто врахувати, що при цьому мова йде не тільки і, можливо, не стільки про матеріальні збитки осіб, наприклад, викрадення коштів з рахунку у банку чи з електронного гаманця, але й про шкоду інформаційно-психологічного характеру. Це питання розглядалося нами у підрозділах 1.1, 1.3 цієї дисертаційної роботи і зроблений висновок, що забезпечення захисту розуму людини від інформаційно-психологічних впливів є забезпеченням його «**когнітивної безпеки**». С.К. Костючков [156] використовує поняття нейрокогнітивний хакінг (від слова «хакер», англ. *hacker*, від *to hack* – комп'ютерний зломщик) – процес впливу суб'єкта на окремі ділянки мозку

індивіда через підсвідомі стимули з метою отримання бажаної поведінкової реакції, зокрема – у військовому протистоянні. Інтегруючи в кіберпростір меседжі специфічного змісту, провайдер кіберконфлікту створює загальний символічний простір, де індивідуальні оцінювальні емоції прораховуються, ідентифікуються та спільно проживаються індивідами та соціальними групами. В результаті кумулятивного впливу складових нейрокогнітивного хакінгу активатор кіберконфлікту досягає бажаного ефекту: в об'єктів впливу формується задана поведінкова реакція [156, с. 55].

Далі, згідно ч. 1 ст. 1 (пункт 8) Закону № 2163-VIII, кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке ***передбачена законом України про кримінальну відповідальність*** чи ***визнано злочином*** міжнародними договорами України.

Отже, під злочином розуміється відносно обмежене коло дій, наділених строго формалізованими ознаками. Більше того, згідно ч. 1 ст. 12 Кримінального кодексу (далі – КК) України [34], кримінальні правопорушення поділяються на кримінальні проступки і злочини. Згідно ч. 2 ст. 12 КК України, кримінальним проступком є передбачене цим Кодексом діяння (дія чи бездіяльність), за вчинення якого передбачене основне покарання у вигляді штрафу не більше трьох тисяч неоподатковуваних мінімумів доходів громадян або інше покарання, не пов'язане з позбавленням волі.

Тобто, закон про кримінальну відповідальність навіть кримінальні правопорушення не відносить до злочинів. Таким чином, кіберзлочини є поняттям значно вужчим, ніж кіберконфлікти.

У КК України злочини із групи кіберзлочинів закріплено у розділі 16 «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» і представлено такими нормами:

– ст. 361 – несанкціоноване втручання в роботу інформаційних

(автоматизованих), інформаційно-комунікаційних, електронних комунікаційних систем, електронних комунікаційних мереж (з урахуванням змін, внесених Законом від 24.03.2022 «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» – Закон № 2149-IX [54]);

– ст. 361-1 – створення шкідливих програмних чи технічних засобів з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут, які (засоби) призначені для несанкціонованого втручання в роботу інформаційних (автоматизованих), інформаційно-комунікаційних, електронних комунікаційних систем, електронних комунікаційних мереж (з урахуванням змін, внесених Законом № 2149-IX);

– ст. 361-2 – несанкціоновані збут або розповсюдження створеної та захищеної відповідно до чинного законодавства інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;

– ст. 362 – несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), комп'ютерних мережах, автоматизованих системах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї.

Під несанкціонованими діями з інформацією розуміється несанкціоновані знищення, зміна або блокування інформації (ч. 1 ст. 362 КК), несанкціоновані копіювання або перехоплення інформації (ч. 2 ст. 362 КК);

– ст. 363 – порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), комп'ютерних мереж, автоматизованих систем чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється;

– ст. 363-1 – перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), комп'ютерних мереж, автоматизованих систем чи мереж електрозв'язку шляхом масового розповсюдження повідомлень

електрозв'язку.

Кримінально караним за цією статтею є умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), комп'ютерних мереж, автоматизованих систем чи мереж електрозв'язку.

Крім того, діяльність у сфері кіберзлочинів кваліфікується за ч. 3 ст. 190 КК України «Шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки»; ст. 200 КК України – незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення; ст. 231 КК України «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю» [177].

Також частиною українського законодавства є згадана вище Конвенція від 23.11.2001 року Ради Європи «Про кіберзлочинність» [6] з Додатковим протоколом від 28.01.2003 до цієї Конвенції [7] щодо криміналізації дій ксенофобного та расистського характеру, вчинених через комп'ютерні системи. Обидва документи ратифіковані Україною.

У Конвенції представлена класифікація кіберзлочинів. Усі вони характеризуються наявністю наміру як елемента суб'єктивної сторони. Всього – три категорії кіберзлочинів:

– злочини проти конфіденційності, цілісності і працездатності комп'ютерних даних і систем – незаконний доступ, незаконне перехоплення, створення перешкод для обміну даними, створення перешкод для функціонування систем, неправомірне використання апаратних пристроїв;

– комп'ютерні злочини – фальсифікація і підробка, що здійснюються з використанням комп'ютерної техніки;

– злочини, пов'язані з контентом, – виготовлення, поширення і зберігання дитячої порнографії.

У Додатковому протоколі представлена класифікація кіберзлочинів когнітивного характеру, який спрямований на мозок людини:

– поширення ксенофобного та расистського матеріалу через комп'ютерні системи (стаття 3 Протоколу);

– погроза з ксенофобних та расистських мотивів, зроблена через комп'ютерну систему (стаття 4 Протоколу);

– [публічна] обра́за з ксенофобних та расистських мотивів, зроблена через комп'ютерну систему (стаття 5 Протоколу);

– заперечення, значна мінімізація, схвалення або виправдання геноциду чи злочинів проти людства, як це визнано заключними та обов'язковими рішеннями Міжнародного військового трибуналу, заснованого згідно з Лондонською угодою від 08.08.1945 року або будь-якого іншого міжнародного суду (стаття 6 Протоколу);

– пособництво та/або підбурювання до вчинення будь-якого з правопорушень, визначених відповідно до цього Протоколу, з наміром вчинити такий злочин (стаття 7 Протоколу).

Об’єктом кіберзлочинів може стати будь-який користувач Інтернету.

Окремо слід виділити кібербулінг, який не є злочином за КК України, але за який передбачена адміністративна відповідальність за Кодексом України про адміністративні правопорушення (далі – КУпАП). Згідно статті 173-4 КУпАП, булінг (цькування) учасника освітнього процесу – це діяння учасників освітнього процесу, що полягають у психологічному, економічному, фізичному, сексуальному насильстві, ***у тому числі із застосуванням засобів електронних комунікацій***, що вчиняються стосовно неповнолітньої чи малолітньої особи або такою особою стосовно інших учасників освітнього процесу, внаслідок чого була заподіяна чи могла бути заподіяна шкода фізичному або психічному здоров’ю потерпілого.

Аналогічне визначення міститься у Законі України «Про охорону дитинства» [41]: це «психологічне, економічне, фізичне чи сексуальне насильство, тобто будь-яке умисне діяння (дія або бездіяльність), ***у тому***

числі із застосуванням засобів електронних комунікацій, яке систематично вчиняється особою стосовно дитини, з якою вони є учасниками одного колективу, або дитиною стосовно іншого учасника одного колективу та яке порушує права, свободи, законні інтереси потерпілої особи та/або перешкоджає виконанню нею визначених законодавством обов'язків».

Кібербулінг (кіберзалякування, англ. *cyberbullying*) [147] – умисне цькування щодо певної особи у кіберпросторі, як правило, впродовж тривалого проміжку часу. Особу, яка здійснює *кібербулінг*, називають «булер», вона діє анонімно, – щоб жертва не знала джерела агресивних дій. Існує два поняття: кібермобінг та кібербулінг, дуже схожі за змістом. Перший термін початково стосувався реалізації булінгу лише на одному пристрої – мобільному телефоні. Однак термін кібермобіг не розповсюджений в англомовному середовищі у порівняні з кібербулінгом [147].

Як зазначає проф. М.І. Легенький [187], актуальність наукових досліджень у сфері протидії булінгу визначається, передусім, суспільною небезпекою вказаного явища та його поширеністю. Так, за даними Міністерства освіти і науки України станом на 2024 р. 51,3 % учнів (55,9 %, дівчат і 46,2 % хлопців) коли-небудь стикалися з булінгом, а 24,7 % учнів стали мішенями боулінгу з початку повномасштабного вторгнення [187, с. 12]. Дослідження та аналіз цієї проблеми є важливими для розробки дієвих механізмів запобігання булінгу, захисту постраждалих та формування безпечного освітнього середовища. Це сприятиме не лише дотриманню прав людини в освіті, а й формуванню здорового соціального клімату в суспільстві загалом [187, с. 16].

Виходячи із положень Конвенції про кіберзлочинність, слід визнати, що кількість і різноманіття правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (розділ XVI КК України), які (правопорушення) завдають шкоди користувачам комп'ютерних мереж і які доцільно було б

криміналізувати, є значно більшим. Деякі з цих правопорушень і при даних нормах КК України могли б потрапляти під кримінально-правову кваліфікацію, але дії зловмисників «на межі» допустимого роблять таку кваліфікацію вкрай утрудненою. Розглянемо характер найбільш поширених видів правопорушень у цій сфері, які являють собою типовими кіберконфліктами, що не потрапляють під визначення «кіберінцидент» або «кіберзлочин».

Один з найбільш поширених видів кіберконфліктів слід назвати онлайн-шахрайство – заволодіння коштами громадян через сайти та телекомунікаційні засоби зв'язку, Інтернет-аукціони, Інтернет-магазини, [68, 177]. Для скоєння інтернет-злочинів кіберзлочинці можуть проявляти неабияку винахідливість, коли справа доходить до виманювання грошей у користувачів Інтернету. Для атаки на своїх жертв зловмисники можуть використовувати різні методи – від маскування під державних службовців до створення шахрайських сайтів в Інтернеті, адаптуючи їх до актуальних тем. У період пандемії COVID-19 багато шахраїв видавали себе за органи охорони здоров'я або пропонували продати дефіцитні ліки чи товари для захисту. Варто враховувати, що схеми зловмисників не обмежуються надзвичайними ситуаціями у сфері охорони здоров'я або глобальними подіями. Тому від користувачів Інтернету вимагається бути уважними під час роботи в Інтернеті та перевіряти доступну інформацію, що допоможе своєчасно виявляти будь-які схеми зловмисників.

Фішинг – це сукупність методів виманювання в користувачів Інтернету логінів та паролів, номерів кредитних карток та іншої конфіденційної інформації. Зазвичай власник кредитної картки добровільно повідомляє шахраям необхідну інформацію [78, 177, 270]. Найчастіше зловмисники в електронних листах або телефонних дзвінках видають себе представниками відомих організацій. Поштовий фішинг – один з найпоширеніших типів фішингу, він користується технікою «spray and pray», завдяки якій хакери видають себе за легітимну особу чи організацію, спрямовуючи масові

електронні листи на всі адреси електронної пошти. Їх мета полягає в тому, щоб своєю терміновістю викликати необдумані дії адресата, наприклад, натиснути на шкідливе посилання.

Головною метою шахраїв у таких схемах є забезпечити собі доступ до облікових записів користувача (логін та пароль) з намірами отримання конфіденційної інформації. Найчастіше, зловмисники використовують фішингові сайти з полем логіну та паролю, які повністю ідентичні оригінальним сайтам компаній [246, с. 160]. Відомі численні випадки, коли функціонери російської пропаганди створювали фіктивні інформаційні сайти, маскуючи їх під зовнішнє оформлення відомих та авторитетних українських інформаційних сайтів, наприклад, «Обозреватель», УНІАН [161, с. 114]. Аналогічна інформація надходила від відомих інформаційних агенцій Франції, Ізраїлю тощо [161, с. 113-114]. Тобто, як зазначено вище, кіберконфлікти мають місце не тільки щодо матеріальної складової, але й щодо ментальної.

Фішинг буває кількох видів [68, 177, 246, 270]:

– SMS-фішинг – потенційна жертва отримує від шахраїв повідомлення, що банк заблокував її кредитну картку, і для її розблокування необхідно надати реквізити, або повідомлення, що власник картки отримав виграш, однак потрібно заплатити його доставку цього виграшу. Варіантів SMS-повідомлень за змістом безліч, тому необхідно бути особливо уважними до таких чи аналогічних повідомлень;

– Інтернет-фішинг – шахраї створюють фішингові (підроблені) сторінки, що імітують офіційні сторінки банків, інтернет-магазинів, платіжних сервісів, тощо.

Вішинг – вид кіберзлочинів, при якому в повідомленнях міститься прохання зателефонувати на певний міський номер, а при розмові запитуються конфіденційні реквізити власника картки. Це майже той же фішинг, однак виманювання реквізитів зловмисники здійснюють за допомогою телефонних дзвінків (шахраї нерідко представляються

працівниками банку й намагаються отримати у власника картки ПІН-код чи примусити здійснити певні дії зі своїм рахунком) [68, 101]. «Популярними» схемами вішингу є, наприклад, маскування злочинців під «фахівців» з технічної підтримки. Жертвам телефонують нібито від імені їх провайдера або відомого постачальника програмного чи апаратного забезпечення. Шахраї стверджують, що виявили неіснуючу проблему з вашим комп'ютером, а потім вимагають оплати за її виправлення, іноді завантажуючи шкідливе програмне забезпечення в процесі.

Різновидом такої нібито «технічної підтримки» є так званий SIM-Jacking [246, с. 160]. Суть його проста: зловмисник дзвонить в call-центр вашого оператора, представляючись Вами як власником SIM-карти і стверджуючи, що Ваша SIM-картка зламана і номер потрібно перенести на іншу карту, якою аферист вже володіє. Таким чином, він зможе приймати всі коди підтвердження на свій пристрій, отримуючи доступ до ваших банківських облікових записів, облікових записів у сервісах та багато іншого.

Кардинг – незаконні фінансові операції, які не ініційовані володільцем платіжної картки або не підтверджені ним, з використанням картки або її реквізитів [68, 177]. Реквізити платіжних карт злочинці знаходять на зламаних серверах інтернет-магазинів, платіжних та розрахункових систем, а також – персональних комп'ютерів (через програми віддаленого доступу – «троянці», «боти» – або безпосередньо). Це може бути також незаконне отримання, зокрема, крадіжка, кредитної картки, копіювання даних картки для її подальшого підроблення, копіювання реквізитів картки для здійснення покупок через Інтернет без участі власника картки. У будь-якому випадку метою злочинців є доступ до чужих грошових коштів. Для досягнення цієї мети зловмисники вигадують різноманітні способи отримання потрібної інформації в неуважних і легковірних громадян.

Кеш-трапінг – це викрадення готівки з банкомату через встановлення на шатер банкомату утримуючої накладки спеціальної конструкції [68]. У момент видачі купюр банкомат піднімає захисну металеву «штору» і

виштовхує гроші. Однак, якщо на банкоматі встановлено злочинне обладнання (планка зі стрічкою скотчу), то банкноти приклеюються до стрічки, а шахрайська планка не «випускає» їх з банкомату. Адекватна і швидка реакція банків на небезпеку – установка антикештрепінгових накладок, які застосовують найбільші банки України, масштабна інформаційна кампанія проти банкоматного шахрайства, призвели до значного зменшення такого виду злочинів.

Скімінг – це різновид шахрайства, коли зловмисники встановлюють на банкомат спеціальне обладнання (скімер) і зчитують дані банківської картки разом із PIN-кодом. Зазвичай це відбувається в момент виконання карткових операцій із банкоматами [68, 177]. Дані копіюються за допомогою мінімодуля в картоприймачі, PIN-код отримують через мікрокамеру або накладку на клавіатуру. Потім цю інформацію використовують, щоби створити дублікат картки і списати з неї кошти.

Шимінг – це модернізований різновид скімінгу. В таких випадках шахраї використовують практично непомітний прилад, розміщуваний усередині картридера. У такий спосіб дані картки копіюються непомітно [177].

Найнебезпечнішим видом шахрайства у сфері фішингу є банери-вимагачі, які також належать до категорії вірусів та виду «троянів». Спочатку, вони є невинними листами, наприклад, з проханням «друга» відкрити та перевірити на працездатність програму, яка нібито не відкривається на його комп'ютері. Однак якщо таку програму відкрити, то на екрані комп'ютера «висить» повідомлення з інформацією про те, що ваш комп'ютер заражений вірусом, всі ваші файли зашифровані і розшифрувати ці файли можна тільки відправивши гроші на такий-то гаманець. Закрити таке повідомлення не виходить, оскільки вірус блокує поєднання команд Ctrl+Alt+Delete та Alt+F4; при перезавантаженні комп’ютера нічого не змінюється. Навіть якщо відправити гроші шахраям, то, звичайно, ніякого коду розблокування користувач не отримує, а навпаки, буде внесений до

«білого списку» користувачів, які готові платити за свої дані, тож якщо все-таки гроші шахраям відправлені, але жоден код не отриманий, але комп'ютер розблокуваний, то слід чекати «гостей» знову. [246, с. 160-161].

Проблема з програми-вимагачами стала настільки актуальної в ЄС, що їй присвячено окремий пункт Директиви 2022/2555 від 14.12.2022 року [14] (пункт 54 Преамбули). В документі зазначається, що в останні роки ЄС зіткнувся із дуже швидким зростанням кількості атак за допомогою програм-вимагачів, коли шкідливе програмне забезпечення шифрує дані та системи і вимагає за відновлення доступу сплатити викуп. Держави-члени у рамках національної стратегії кібербезпеки мають розробити політику, яка вирішує проблему зростання кількості атак із застосуванням програм-вимагачів [14].

Інтернет-піратство (цифрове піратство) – незаконне розповсюдження інтелектуальної власності в Інтернеті [68, 177], а також інші види порушень авторських і суміжних прав (див. підрозділ 3.3 цієї дисертаційної роботи). Суть Інтернет-піратства полягає у відтворенні і розповсюдженні мережею Інтернет фільмів, музичних творів, комп’ютерних програм, інших об’єктів інтелектуальної власності, без дозволу автора або іншої особи, яка має авторське право і/або суміжні права, або без виплати винагороди за використання творів у встановленому законом порядку.

Як зазначає В. Філінович [340], у цифрову епоху інтелектуальна власність стикається з новими вразливостями. Хоча матеріальна власність може бути фізично захищена, інтелектуальна власність вимагає складних правових та технологічних гарантій, особливо в кіберпросторі. Швидкісне зростання кількості цифрового контенту в поєднанні із глобалізованим доступом та розповсюдженням посилило проблему забезпечення ефективного захисту прав інтелектуальної власності. Існуючі моделі правозастосування часто не справляються з транскордонними порушеннями та швидким поширенням несанкціонованого контенту в Інтернеті [340, с. 159].

В законодавстві України визначення Інтернет-піратства наведене у

статті 50 Закону України «Про авторське право і суміжні права»: Інтернет-піратство – це вчинення будь-яких дій, які є порушенням авторського права і (або) суміжних прав з використанням мережі інтернет (п. б ст. 50). Інтернет-піратство має глобальний характер, його неможливо побороти в окремій країні. Натомість кожна країна і світова спільнота в цілому намагаються розробити ефективний механізм прискореного та спрощеного захисту авторського права в мережі Інтернет. На це спрямовані такі міжнародні акти як: Директива ЄС «Про електронну комерцію» № 2000/31/ЄС від 08.06.2000 року; Директива ЄС «Про авторське право в єдиному цифровому ринку» № 2019/790/ЄС від 17.04.2019 року.

Кард-шарінг – забезпечення незаконного перегляду супутникового та кабельного TV [145].

Фармінг – перенаправлення жертви на недостовірну IP-адресу. Шахрай встановлює на комп'ютерах шкідливу програму, яка після запуску забезпечує перенаправлення жертви замість справді потрібних жертві сайтів на підроблені сайти [268, 287].

У класичному фішингу зловмисник поширює листи електронної пошти серед користувачів соціальних мереж, онлайн-банкінгу, поштових вебсервісів, заманюючи на підроблені сайти користувачів, що стали жертвою обману, з метою отримання їх логінів і паролів. Багато користувачів, які активно використовують сучасні вебсервіси, не раз стикалися з подібними випадками фішингу та проявляють обережність до підозрілих повідомлень.

У схемі класичного фішингу основною «слабкою» ланкою, що визначає ефективність всієї схеми, є залежність від користувача – повірить він фішеру чи ні. При цьому з плином часу підвищується інформованість користувачів про фішингові атаки. Банки, соціальні мережі, інші вебслужби попереджають про різноманітні шахрайські прийоми з використанням методів соціальної інженерії. Все це знижує кількість відгуків в фішингової схеми – все менше користувачів вдається заманити обманним шляхом на підроблений сайт. Тому зловмисники придумали механізм прихованого

перенаправлення користувачів на фішингові сайти, що отримав назву фармінг («pharming» – похідне від слів «phishing» і англ. «farming» – заняття сільським господарством, скотарством). Зловмисник поширює на комп'ютери користувачів спеціальні шкідливі програми, які після запуску на комп'ютері перенаправляють звернення до заданих сайтів на підроблені сайти. Таким чином, забезпечується висока скритність атаки, а участь користувача зведено до мінімуму – досить дочекатися, коли користувач вирішить відвідати цікаві для зловмисника сайти. Шкідливі програми, що реалізують фармінг-атаку, використовують два основних прийоми для скритного перенаправлення на підроблені сайти – маніпулювання з файлом HOSTS або зміною інформації DNS [268, 287].

Зворотна соціальна інженерія може бути здійснена тільки у випадку, коли шахрай знайомий із жертвою, а остання йому довіряє. За таких умов жертва сама звертається до шахрая (наприклад, системного адміністратора), із проханням допомогти відновити втрачений файл (який заховав сам шахрай). При цьому жертві повідомляється, що таку дію можна зробити якнайшвидше, зайшовши у її обліковий запис. У такий спосіб жертва сама повідомляє всю інформацію шахраю.

Мальваре – створення та поширення шкідливого програмного забезпечення, зокрема, вірусів [177].

Протиправний контент – контент, що пропагує тероризм, екстремізм, порнографію, наркоманію, культ жорстокості і насильства. Підходи до обмежень описані в Рекомендаціях Ради Європи № R (89) 7 від 27.04.1989 р. [18], № R (97) 19 від 30.10.1997 р. [19], № R (97) 20 від 30.10.1997 р. [20] (див. також підрозділ 2.1 цієї дисертаційної роботи, а також статтю автора [159, с. 86-89]).

Рефайлінг – незаконна підміна телефонного трафіку [177].

На час пандемії COVID-19 експерти виділяють чотири основні причини таких правопорушень: збільшення кількості людей, працюючих віддалено, з використанням ІТ, але не маючих належних досвіду та знань);

збільшення кількості випадків фішингових атак; збільшення електронних платежів; збільшення можливостей для інформаційних й кібератак з метою дестабілізації ситуації [124].

Сталкінг (від англ. «stalking» – переслідування) – вид психологічного насильства, яке проявляється у тривалому та нав'язливому переслідувані [228]. Зловмисник слідкує за своєю жертвою, постійно шукає з нею зустрічі, може дарувати подарунки та ігнорувати прохання жертви зупинитися та дати їй спокій. Кіберсталкінг – здійснення таких дій онлайн: сталкер слідкує за своєю жертвою за допомогою соціальних мереж, пише їй у всі доступні месенджери, дзвонить без зупину тощо. Зловмисник також може одночасно вдаватися до двох таких видів сталкінгу – онлайн та офлайн. Кіберсталкінг – один з найнебезпечніших видів кібербулінгу. Переслідувач нагадує про себе щодня багато разів поспіль. Під час кампанії #StopStalking одна дівчина повідомила, що отримувала від сталкера по 300 дзвінків на день [228].

Деякі прояви сталкінгу потрапляють під дію статті 182 КК України «незаконне збирання, використання, зберігання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації». При цьому цей термін зустрічається у судовій практиці, наприклад, у рішенні від 06.02.2024 року у справі № 299/100/24 Виноградівського районного суду Закарпатської області [127, № 116844631]; Постанові про адміністративне правопорушення від 02.10.2023 року у справі № 756/10269/23 Оболонського районного суду міста Києва [127, № 113985196]; Постанові про адміністративне правопорушення від 06.03.2023 року у справі № 607/3270/23 Тернопільського міськрайонного суду Тернопільської області [127, № 109427567] та деяких інших.

Основним недоліком щодо запобігання негативним проявам наведених вище кіберзлочинів є відсутність системної роботи компетентних органів щодо їх виявлення та подолання, наявність лише декларативних положень у стратегіях (іншими вони і не можуть бути, що зрозуміло) та відсутність прийнятих законодавчих та підзаконних актів на їх конкретизацію та

розвиток, низьку поінформованість населення щодо можливих загроз, а також високу латентність злочинів у цій сфері, що унеможливлює або ускладнює виявлення та притягнення до відповідальності усіх винних осіб.

Наприклад, як резюмує В. Філінович щодо проявів сталкінгу [289], на жаль, в Україні питання правового захисту жертви сталкінга, а тим більше захисту жертви кіберсталкінга, не регулюється абсолютно. Можна говорити про те, що сьогодні користувачі Інтернет-мережі в основному стають жертвами онлайн-об'єднань (як одного зі складових кібербулінгу, куда входить і кіберсталкінг). Але як самі жертви, так і невільні свідки подібного зазвичай ігнорують подібне, феномен вважається занадто поширеним і, що головне, практично не карається. Також нерідкі випадки кіберсталкінга в чистому вигляді, з фізичними загрозами і сексуальними домаганнями (як в цифровому, так і в офлайн-середовищі). За даними статистики, саме жінки, в особливості молоді дівчата, частіше всього піддаються кіберсталкінгу. І відсутність достатнього нормативного регулювання проблеми, а також засобів захисту – все це допомагає сталкерам, тобто реальним злочинцям, залишатися безкарними. Ідеальним рішенням, на нашу думку, стало б інкорпорування деяких норм законодавства США, зокрема, штату Каліфорнія, які вже показали свою ефективність у відношенні суб'єктів, схильних до цифрового переслідування. Якщо сталкерів (кіберсталкерів) починають штрафувати і відправляти в тюрму, це точно призведе до підвищення їх рівня поінформованості, а, значить, до зниження рівня випадків кіберсталкінга [289, с. 139].

Кібершпигунство або комп'ютерний шпіонаж [148] (вживається також термін «кіберрозвідка» [270, с. 332]) – це несанкціоноване отримання інформації з метою досягнення особистої, політичної, економічної чи військової переваги. Кібершпигунство (комп'ютерний шпіонаж) здійснюється шляхом обходу (злому) систем комп'ютерної безпеки, із застосуванням шкідливого програмного забезпечення. Воно може здійснюватися як дистанційно, із застосуванням мережі Інтернету, так і шляхом проникнення в

комп'ютерні мережі і комп'ютери підприємств звичайними шпигунами («кротами»), а також хакерами.

З недавніх пір «кібершпигунство» включає також аналіз провідними спецслужбами (ЦРУ, Моссад, СБУ), «цифрового сліду» поведінки користувачів соціальних мереж (повідомлення, фотографії, відео, друзі тощо), таких як Facebook, Twitter, «ВКонтакте» тощо з метою виявлення терористичної, екстремістської чи антиурядової діяльності, закликів до мітинги проти влади.

Цифровий слід (або *цифровий відбиток*; англ. *digital footprint*) [296] – сукупність інформації про відвідування та внесок користувача під час перебування у мережі. Класифікується два види цифрових слідів: активні та пасивні. Активний цифровий слід з'являється, коли користувач сам публікує свої персональні дані в соцмережах і на сайтах. Пасивний цифровий слід – це дані, зібрані без відома власника, автоматично. Цифрові сліди відслідковуються переважно задля моніторингу, з метою шпигунства, в комерційних цілях.

Згідно пункту 14 ч. 1 ст. 1 Закону № 2163-VIII, кібершпигунство – шпигунство, що здійснюється у кіберпросторі або з його використанням.

З метою кримінально-правової кваліфікації кібершпигунства І.В. Діордіца [122] пропонує закласти у це визначення наступне: злочинна діяльність, яка здійснюється шляхом таємного вистежування, розшуку збирання, викрадення та передачі інформації, що становить державну таємницю, іноземній державі, іноземним організаціям, їх іноземним представникам, якщо ці дії вчинені іноземцем, або особою без громадянства із використанням методів кібернетики. Об’єктом цього кіберконфлікту є зовнішня безпека держави, її суверенітет, територіальна цілісність, державна економічна інформаційна безпека, кіберпростір загалом. Суб’єктами цього конфлікту є держава, іноземні громадяни та особи без громадянства які досягли 16 років [122, с. 53-54].

З урахуванням саме «кібер-»шпигунства пропонуються додаткові

ознаки. Якщо шпигунство вчинене шляхом незаконного втручання в роботу автоматизованих електронно-обчислювальних машин, їхніх систем чи комп’ютерних мереж, це потребує додаткової кваліфікації за ст. 361 КК України, а шляхом викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службової особи своїм службовим становищем – за ст. 362 КК. Якщо особою викрадено з метою передачі іноземній державі, іноземній організації чи їхнім представникам предмети, відомості про які становлять державну таємницю (зразки військової зброї, спеціальної техніки, криптографічного чи іншого обладнання, радіоактивні матеріали тощо), або офіційні документи, що є в державних підприємствах і містять державну таємницю, ці дії, залежно від їхнього конкретного способу, а також від особливостей предмета і суб’єкта, слід додатково кваліфікувати за ст. ст. 185-191. 262. 357, 410 КК України. Шпигунство, поєднане з незаконним використанням спеціальних технічних засобів негласного отримання інформації, повністю охоплюється ст. 114 КК і не потребує додаткової кваліфікації за ст. 359 КК [186, с. 53].

Кібервандалізм [186] – це вид ірраціональної деструктивної протиправної поведінки в мережі Інтернет, за якої предмету посягання завдається шкода. Серед видів кібервандалізму можна виділити такі: троянська програма, шкідливі та шпіонські програми; DoS-/DDoS-атаки (Distributed Denial of Service): атаки на IP-адреси; drive-by (попутне) завантаження; фішинг, який є видом соціальної інженерії з метою «виуджування» у користувачів Інтернету їх конфіденційних даних (див. вище), рекламні системи (adware), бот-нети (бот-сети) [186, с. 206]. Цей перелік не є вичерпним з огляду на постійну модернізацію інформаційних технологій [196, с. 206].

На думку автора статті [186], кібервандалізм є найбільш поширеною формою кіберконфлікту, що отримує суспільний резонанс. Зазвичай він містить зміни чи знищення змісту веб-сайту, відключення чи перезавантаження серверу, як це, наприклад, відбулося, коли «закрили»

відомий український файлообмінник, «впали» урядові сайти, зокрема й МВС. Однак, незважаючи на свій шкідливий характер, наслідки таких інцидентів обмежені в часі та відносно незначні [186, с. 206].

Кібервандалізм як підвид вандалізму набуває все більшого поширення на теренах України через необізнаність правоохоронних органів із можливостями використання інформаційних технологій під час розслідування цієї категорії злочинів. Важливим є розуміння поняття й ознак кібервандалізму задля ефективного пошуку та фіксації електронних слідів, а також для подальшого здійснення слідчих (розшукових) дій [186, с. 209].

Ще один вид кіберконфліктів – кібертероризм. Згідно пункту 13 ч. 1 ст. 1 Закону № 2163-VIII, кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням.

Створивши нові інформаційні технології, науково-технічний прогрес в короткі терміни трансформував процеси створення, збирання, одержання, використання, зберігання, поширення, захисту інформації. Сьогодні результати науково-технічного прогресу нерідко використовують і злочинці. Методи і засоби кібератак давно освоєні як міжнародними екстремістськими організаціями, так і національними сепаратистськими рухами. Внаслідок проникнення в інформаційну сферу та її використання кримінальними, в тому числі й терористичними елементами, виникли явища, які називаються кіберзлочинністю і кібертероризмом. Кібертероризм – проведення «атак» на комп’ютерні системи. Перші приклади «комп’ютерного тероризму» з’явилися наприкінці 1990-х рр., що пов’язано як із зростаючою роллю комп’ютерів у всіх сферах життя, так і з розвитком комп’ютерних мереж. В результаті до цих новацій зросла увага різних «кіберхуліганів» і «кібертерористів», які здійснюють напади за допомогою несанкціонованого доступу, щоб заважати нормальній роботі відповідних установ [271, с. 100].

Під кібертероризмом розуміють навмисну мотивовану атаку на інформацію, що обробляється комп’ютером, комп’ютерну систему або мережу, яка пов’язана з небезпекою для життя і здоров’я людей або

настанням інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування військового конфлікту [180].

Центр стратегічних і міжнародних досліджень визначає кібертероризм як використання комп`ютерних мережевих інструментів для припинення функціонування критичних об’єктів національної інфраструктури, або для примусу або залякування уряду або цивільного населення [345]. І.В. Діордіца вважає, що під кібертероризмом слід розуміти протиправне діяння, яке вчиняється з метою досягнення негативних наслідків, наприклад отримання матеріальних благ чи загроза інформаційній безпеці держави [121]. Кібертероризм має місце в кіберпросторі.

Таким чином, у даній дисертаційній роботі здійснені системні дослідження з питань кіберконфліктів. Проаналізована сутність поняття «кіберконфлікт». Розглянутий взаємозв’язок між поняттями «кіберконфлікт», з одного боку, та кіберінцидент і кіберзлочин, з іншого боку. Автор погоджується із пропозиціями деяких дослідників визначити конфлікт як оцінку характеру взаємодії. Таке визначення дає змогу зберегти назву конфлікт за ситуаціями протидії сторін одна одній, які ми традиційно називали конфліктом, і водночас поширити це поняття на ситуації несумісності певних елементів у складі цілого. Тобто несумісність певних елементів у складі цілого необов’язково пов’язано із злочинною поведінкою, але може підпадати під визначення «конфлікт».

Систематизовані види кіберконфліктів, які породжуються різноманітними зловживаннями у кіберпросторі. Доведено, що не усі поширені зловживання прямо криміналізовані (передбачені у КК України як злочини у кібернетичній сфері), що утруднює їх кваліфікацію як злочинів.

Висновки до Розділу 2

В умовах, коли мережеві та інформаційні системи та послуги відіграють важливу роль у суспільстві, їхня надійність та безпека суттєво визначають стабільність економічної та соціальної діяльності, а також безпеку окремих осіб. Отже, належне правове регулювання суспільних відносин, пов’язаних із запровадженням та використанням інформаційно-комунікаційних систем, є необхідним для їх ефективного використання.

У цьому розділі визначені особливості правового регулювання заходів забезпечення кібербезпеки правовими актами європейського рівня. Розглянуті ключові акти щодо правового регулювання заходів забезпечення кібербезпеки актами європейського рівня, а саме: Директива від 06.07.2016 Європейського парламенту і Ради ЄС 2016/1148 про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу (Директива була замінена Директивою 2022/2555 від 14.12.2022 року, яка набрала чинності 16.01.2023 року); Директива Ради 2008/114/ЄС від 08.12.2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту (Директива була замінена Директивою 2022/2557 від 14.12.2022 року, яка набрала чинності 16.01.2023 року); Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24.10.1995 року (Директива замінена Регламентом Європейського парламенту і Ради ЄС 2016/679 від 27.04.2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)), яка набрала чинності 24.05.2016 року; Директива Європейського Парламенту і Ради ЄС 2018/1972 від 11.12.2018 року; Регламент Європейського парламенту і Ради ЄС 2019/881 від 17.04.2019 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію

кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту ЄС № 526/2013 (Акт про кібербезпеку); Конвенція від 23.11.2001 року Ради Європи «Про кіберзлочинність»; Додатковий протокол від 28.01.2003 до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи; Рекомендація від 30.10.1997 р. № R (97) 19 Комітету міністрів Ради Європи «Про показ насильства електронними ЗМІ», ухвалена. Комітетом міністрів на 607-му засіданні заступників міністрів від 30.10.1997 р.; Рекомендація від 30.10.1997 р. № R (97) 20 Комітету міністрів Ради Європи «Про розпалювання ненависті», ухвалена. Комітетом міністрів на 607-му засіданні заступників міністрів від 30.10.1997 р.; Рекомендація від 27.04.1989 р. № R (89) 7 Комітету міністрів РЄ «Про принципи поширення відеозаписів насильницького, жорстокого чи порнографічного змісту», ухвалена. Комітетом міністрів на 425-му засіданні заступників міністрів від 27.04.1989 р. Сюди ж слід віднести розглянутий у розділі 1 Закон ЄС про кіберстійкість (The Cyber Resilience Act (CRA)). Наголошено, що перші 4 перелічені (чинні) документи (Директива 2022/2555 від 14.12.2022; Директива 2022/2557 від 14.12.2022; Регламент 2016/679 від 27.04.2016; Регламент 526/2013 від 17.04.2019) підлягають імплементації у законодавство України відповідно до Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, Розділ III «Юстиція, свобода та безпека». Прийняття Закону України від 16.12.2020 року № 1089-IX «Про електронні комунікації» є імплементацією Директиви Європейського Парламенту і Ради ЄС 2018/1972 від 11.12.2018 року про запровадження Європейського кодексу електронних комунікацій. Встановлені факти належної імплементації положень Директиви 2022/2555 в Закон України № 2163-VIII «Про основні засади забезпечення кібербезпеки України», зокрема, щодо норм про захист критичної інформаційної інфраструктури, щодо створення національної системи реагуваня на кіберзагрози, щодо

розробки національної стратегії кібербезпеки та її змісту.

Констатовано, що починаючи з 20-х років 21 століття путінська росія вдалася до гібридної та інформаційної війни й війни в кіберпросторі проти багатьох країн Європи, у тому числі членів НАТО: Естонії, Великої Британії, Німеччини, Норвегії, Нідерландів, Франції, Греції, Угорщини, Болгарії, Туреччини, а також Чорногорії, яка була кандидатом на вступ до НАТО. Зроблений огляд здійснених кібератак на критичну інфраструктуру європейських країн. Наголошується, що з огляду на зростаючий рівень загроз у кіберпросторі, створених людиною, ЄС визначив пріоритетом протидію гібридним загрозам та подальший розвиток системи кібербезпеки на найближчі роки, що і вирішує нова Директива 2022/2557.

Конвенція Ради Європи «Про кіберзлочинність» з Додатковим протоколом до неї вважається універсальним міжнародним документом, що спрямований на боротьбу з Інтернет-злочинністю та комп’ютерною злочинністю (кіберзлочинністю) й встановлює і класифікує злочини у сфері кіберзлочинності. Об’єктом таких кіберзлочинів може стати не тільки і навіть не стільки будь-який користувач Інтернету, але й особа, яка не є користувачем Інтернету. Наприклад об’єктом злочину у вигляді поширення контрафактної продукції через мережу Інтернет може стати суб’єкт авторського права, який не є користувачем Інтернету.

Метою Додаткового протоколу до Конвенції Ради Європи «Про кіберзлочинність» є внесення доповнень у відносинах між Державами – сторонами Протоколу до положень Конвенції про кіберзлочинність, які стосуються криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. Отже, цей Протокол повинен забезпечити кримінально-правовий захист когнітивної безпеки осіб та суспільства в частині запобігання проявам дій расистського та ксенофобного характеру.

Констатовано важливість Конвенції Ради Європи «Про кіберзлочинність» для України в умовах сучасної злочинної кібервійни рф

проти України, у тому числі масової антиукраїнської пропаганди та закликів до геноциду українського народу. Важливість цього напряму захисту когнітивної безпеки проілюстровано історією з радіо «Тисячі пагорбів».

Подальшими керівними документами щодо впровадженням заходів забезпечення когнітивної безпеки від інформаційно-психологічного впливу електронних засобів комунікації є Рекомендації Комітету міністрів РЄ № R (89) 7 від 27.04.1989 р. «Про принципи поширення відеозаписів насильницького, жорстокого чи порнографічного змісту» [18], № R (97) 19 від 30.10.1997 р. «Про показ насильства електронними ЗМІ» [19], № R (97) 20 від 30.10.1997 р. «Про розпалювання ненависті» [20]. Базовим принципом підходу до обмежень в даній сфері є правила, встановлені ст. 10 Конвенції Ради Європи про захист прав людини і основоположних свобод 1950 року.

Визначені особливості правового регулювання заходів забезпечення кібербезпеки актами національного права. Встановлена система законів і підзаконних нормативно-правових актів у сфері забезпечення кібербезпеки. Наголошено, що правозастосовна і прикладна діяльність у сфері кіберзахисту повинна здійснюватися, зокрема, з максимально можливим застосуванням національного та міжнародного права щодо повноважень і обов'язків державних органів, підприємств, установ, організацій, громадян у сфері кібербезпеки. Узагальнені наступні принципи правового регулювання у сфері кібербезпеки: верховенство права, захист національних інтересів, прозорість і стабільність кіберпростору, державно-приватну взаємодію, пропорційність заходів кіберзахисту, пріоритет запобігання загрозам і невідворотність покарання за кіберзлочини.

Встановлено, що хоча законодавство з кіберзахисту звернено, перш за все, до суб'єктів національної системи кібербезпеки, це законодавство покликано також забезпечення безпеки, прав, свобод та інтересів широкого кола користувачів об'єктами кібербезпеки та кіберзахисту, – через належне виконання уповноваженими суб'єктами національної системи кібербезпеки своїх обов'язків та повноважень у сфері кіберзахисту.

Доведено, що в контексті реалізації «відносини адміністративних зобов’язань», які притаманні засобам і способам адміністративного права, у Законі «Про основні засади забезпечення кібербезпеки України» послідовно реалізовані усі: а) відносини публічного управління – управлінські функції і повноваження Президента України, КМУ, міністерств, інших центральних органів виконавчої влади; місцевих державних адміністрацій; органів місцевого самоврядування; б) відносини адміністративних послуг – кібербезпека та адміністративні послуги пов'язані через цифровізацію державних сервісів, де захист даних стає ключовим завданням; в) відносини відповідальності публічної адміністрації за неправомірні дії або бездіяльність – суб’єкти національної системи реагування на кіберінциденти, кіберзагрози, кібератаки … несуть адміністративну, цивільно-правову, кримінальну відповідальність за неправомірне розголошення, неправомірне розкриття, неправомірне використання та інші неправомірні дії з інформацією про кіберінциденти відповідно до закону (ч. 3 ст. 9 Закону № 2163-VIII). Адміністративна відповідальність настає за порушення, передбачені КУпАП (див. також таблицю додатку Б1, стаття 212-6 КУпАП – за здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем та інше); г) відповідальності суб’єктів суспільства за порушення порядку і правил, встановлених публічною адміністрацією у межах її повноважень – посадові особи власників або розпорядників інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, де обробляються державні інформаційні ресурси та/або службова інформація та інформація, що становить державну таємницю, посадові особи операторів критичної інфраструктури, власників або розпорядників об’єктів критичної інформаційної інфраструктури несуть адміністративну відповідальність відповідно до закону за невиконання або невиконання у встановлені строки обов’язку щодо здійснення обов’язкових повідомлень про кіберінциденти,

кібератаки (ч. 6 ст. 9-1 Закону № 2163-VIII).

Запропонована логіка побудови структури описаних підзаконних нормативно-правових актів України у сфері кіберзахисту, яка наведена на схемі додатку Б7.

Встановлено, що сукупність нормативних приписів у сфері забезпечення кібербезпеки та протидії кіберзлочинності доповнена також таким специфічним актом, як Типологія легалізації (відмивання) доходів, одержаних злочинним шляхом, у 2013 році, затверджені Наказом від 25.12.2013 № 157 Державної служба фінансового моніторингу України. У Документі розглядаються наступні питання щодо кіберзлочинності: види кіберзлочинів, загрози та ризики кіберзлочинів, шахрайство з використанням інформаційно-комунікаційних систем та комп'ютерних технологій; кіберзлочинність нефінансового характеру, загальні напрямки протидії кіберзлочинам, виявлення підозрілих фінансових операцій. Наведені в Типології підходи використані в судовій практиці (Постанова від 21.06.2023 року у справі № 922/4091/19 Верховного Суду у складі колегії суддів Касаційного господарського суду).

Здійснені системні дослідження з питань кіберконфліктів. Проаналізована сутність поняття «кіберконфлікт». Розглянутий взаємозв’язок між поняттями «кіберконфлікт», з одного боку, та кіберінцидент і кіберзлочин, з іншого боку. Встановлено, що інцидент кібербезпеки (далі – кіберінцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора), спрямованих проти систем електронних комунікацій, систем управління технологічними процесами, а негативні прояви «кіберконфліктів» спрямовані проти інтересів осіб. Тобто, без врахування людського фактору як об’єкту негативного впливу розгляд проблематики кіберінцидентів є недостатнім та неповним.

Автор погоджується із пропозиціями деяких дослідників визначити конфлікт як оцінку характеру взаємодії. Таке визначення дає змогу зберегти

назву конфлікт за ситуаціями протидії сторін одна одній, які ми традиційно називали конфліктом, і водночас поширити це поняття на ситуації несумісності певних елементів у складі цілого. Тобто несумісність певних елементів у складі цілого необов'язково пов'язано із злочинною поведінкою, але може підпадати під визначення «конфлікт».

Систематизовані види кіберконфліктів, які породжуються різноманітними зловживаннями у кіберпросторі. Доведено, що не усі поширені зловживання прямо криміналізовані (передбачені у КК України як злочини у кібернетичній сфері), що утруднює їх кваліфікацію як злочинів. Основним недоліком у сфері запобігання негативним проявам наведених кіберзлочинів є відсутність системної роботи щодо їх виявлення та подолання, наявність лише декларативних положень у стратегіях (іншими вони і не можуть бути, що зрозуміло) та відсутність прийнятих законодавчих та підзаконних актів на їх конкретизацію та розвиток, низький рівень поінформованості населення щодо можливих загроз (варто відзначити позитивну роботу деяких банків у цій сфері), а також висока латентність злочинів у цій сфері, що унеможливлює виявлення та притягнення до відповідальності усіх винних осіб.

РОЗДІЛ 3. ЗАБЕЗПЕЧЕННЯ ВИМОГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СИСТЕМІ КІБЕРЗАХИСТУ І ЗАХИСТ ІНФОРМАЦІЙНИХ ПРАВ ГРОМАДЯН

3.1. Роль і значення забезпечення кібербезпеки в системі національної безпеки України

Розвиток інформаційного суспільства, що стало можливим завдяки інтеграції нових технологій у кожну сферу життєдіяльності та усі типи інфраструктур, підвищує залежність приватних осіб, організацій та країн від інформаційних систем та мереж. Безпека є головною складовою будь-якої діяльності. Її необхідно розглядати як послугу, яка сприяє формуванню можливості створення інших послуг та доданої вартості, зокрема, діджиталізація країни, електронне урядування, електронне навчання, електронні послуги з охорони здоров'я. Безпека є не лише питанням технологій. Поряд з цим, до теперішнього часу основні доступні інструменти зв'язку не мали ресурсів, необхідних та достатніх для забезпечення та гарантування мінімального рівня безпеки [95, с. 312].

Як зазначає проф. Ю.Д. Кунєв, 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 [179, с. 6].

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 [132,

с. 90].

Термін cybersecurity (кібербезпека) слід використовувати виключно щодо практичних методів забезпечення безпеки, які поєднують заходи наступального і оборонного характеру, які включають в себе сукупність або системи інформаційних та (або) операційних технологій або які ґрунтуються на них. Це всього лише одне визначення і одна рекомендація, але, зрозуміло, вони не єдині, на які спираються фахівці. На даний момент спостерігається, що деякі спеціалісти починають використовувати цей термін, або не надаючи технології для атак противника, або надаючи технології, які непридатні для таких атак [268, с. 65].

За науковою позицією, висловленою у монографії [269], небезпеки реалізуються тоді, коли небажаний (шкідливий) сигнал проникає до баз даних, долаючи системи захисту протилежної сторони. В результаті такого проникнення нелегально отримується інформація, яка не призначена для неконтрольованого поширення, виникає можливість перекручення, знищення або розкрадання інформаційних масивів. В деяких випадках, в залежності від мети проникнення, може блокуватися або обмежуватися доступ до інформаційних баз законних користувачів. Внаслідок кібервпливу можуть бути пошкоджені телекомунікаційні мережі, комп’ютерні системи, інші технічні засоби [269, с. 132-133].

Отже, вирішення багатоманітних проблем кібербезпеки, пов’язаних відкритими системами, наприклад Інтернет, та з інформаційними мережами може бути відносно складним, а потенційний вплив на діяльність суб’єкта та країни може бути руйнівним. Широка взаємодія систем, поглиблення взаємозв’язку між системами, а також підвищення рівня ризиків та небезпек змушує окремих осіб, організації, країни вживати заходів щодо покращання управління технологічними та комп’ютерними ризиками [95, с. 313].

Базовим правовим актом у сфері національної безпеки України є Закон від 21.06.2018 № 2469-VIII «Про національну безпеку України» [52]. Закон визначає основи та принципи державної політики у сфері національної

безпеки і оборони, а також структуру та повноваження органів, які відповідають за її забезпечення. При цьому питання кібербезпеки займає важливе місце в цьому Законі України, – адже вона є однією зі складових національної безпеки. У статті 1 та статті 3 Закону зазначено, що національна безпека України забезпечується в різних сферах, серед них – інформаційна та кібербезпека. Кібербезпека є частиною інформаційної безпеки та охоплює захист: інформаційного простору України; державних інформаційних ресурсів; критичної інформаційної інфраструктури (енергетика, транспорт, фінанси, урядові системи тощо); персональних даних і комунікацій громадян.

Відпоідно до статей 4, 6, 7, 8, 9 Закону № 2469-VIII, основні завдання держави у сфері кібербезпеки є:

– виявлення, запобігання та нейтралізація кіберзагроз, які можуть завдати шкоди державній безпеці;

– розвиток національної системи кіберзахисту державних інформаційних ресурсів;

– розвиток сил і засобів кібероборони у складі Збройних Сил України;

– міжнародна співпраця у сфері кібербезпеки, зокрема з НАТО, ЄС та іншими партнерами;

– підготовка кадрів і підвищення рівня обізнаності населення щодо кіберзагроз.

Кібербезпека у цьому Законі: визначена як невід’ємна складова національної безпеки; визнана ключовим напрямом державної політики у зв’язку з гібридною війною та кіберагресією рф; забезпечується спільними діями державних органів, приватного сектору й громадян.

Отже, Закон № 2469-VIII регулює правові основи кібербезпеки, визначив її як державний пріоритет, а також засади міжнародної співпраці у цій сфері.

Слід також зазначити, що у статті 3 Закону України від 06.12.1991 № 1932-XII «Про оборону України» [35] реалізацію заходів з кібероборони (активного кіберзахисту) визначено важлвиою складової для захисту

суверенітету держави, забезпечення її обороноздатності, відсічі збройній агресії.

Слід також зазначити, що Закон № 2469-VIII (частина 5 статті 3) передбачає, що загрози національній безпеці України, а також пріоритети у цій сфері визначаються у Стратегіях: національної безпеки України; воєнної безпеки України; кібербезпеки України; інтегрованого управління державним кордоном України, інших документах з питань національної безпеки і оборони, які схвалюються РНБО України та затверджуються указами Президента України. Одночсно цей Закон у частині 1 статті 1 надає нормативні характеристики безпекових стратегій України, які узагальнені у таблиці додатку Б8 (пункти 1-6), а нормативні характеристики, згідно із Законом, наведені у стовпчику 3. Разом із тим, як зазначено вище, з метою інституалізації положень, пов'язаних з національною безпекою України, в Україні протягом 2020-2021 рр. схвалена рішенням РНБО України та затверджена Указом Президента України низка безпекових стратегій, а саме: Стратегія національної безпеки України [22]; Стратегія воєнної безпеки України [23]; Стратегія кібербезпеки України [24]; Стратегія розвитку оборонно-промислового комплексу України [25]; Стратегія зовнішньополітичної діяльності України [26]; Стратегія інформаційної безпеки [28]; Стратегія забезпечення державної безпеки [29]. Сюди ж слід додати Стратегію енергетичної безпеки, схвалену, на відміну від попередніх Стретегій, розпорядженням КМУ [27], а не Указом Президента України.

Водночас слід зазначити, що попри прийняття Стратегій зовнішньополітичної діяльності України [26]; інформаційної безпеки [28]; забезпечення державної безпеки [29]; енергетичної безпеки, ці види Стратегій не згадуються у Законі № 2469-VIII, і їм не надається відповідний статус, хоча у частині 4 статті 3 Закону № 2469-VIII зовнішньополітична безпека, державна безпека, інформаційна безпека визначені складовою частиною національної безпеки. Отже, необхідно імплементувати вказані Стратегії, які не згадуються в Законі № 2469-VIII, у цей Закон – для надання

цілісності в системі стратегічного планування у сфері безпеки.

Огляд окремих «Стратегій» здійснений у публікації [131].

Стратегія національної безпеки України [22] є ключовою у системі безпекових Стратегій. Як зазначено в Огляді [131], цей документ є керівним для розробки галузевих стратегій. Саме на основі цього документа буде створюватися нова нормативно-правова база у сфері національної безпеки і оборони, формуватися відповідна державна політика. Стратегія національної безпеки вперше розроблена на основі нового Закону від 14.09.2020 [52], який заклав основу для реформ у цій надважливій сфері.

Пріоритети Стратегії (див. також [114]):

– відстоювання незалежності і державного суверенітету України;

– відновлення територіальної цілісності у межах міжнародно визнаних кордонів.

– розвиток людського капіталу, захист прав, свобод і законних інтересів громадян.

– європейська та євроатлантична інтеграція.

Засади Стратегії (див. також [131]):

– стримування – розвиток спроможностей для недопущення збройної агресії;

– стійкість – здатність держави і суспільства адаптуватися до змін безпекового середовища й функціонувати стабільно;

– взаємодія – розвиток стратегічних відносин з іноземними партнерами (ЄС, НАТО, США) та іншими державами.

Актуальні напрями діяльності:

– формування та розвиток спроможностей sectory безпеки і оборони, ***включаючи розвиток системи кібербезпеки***;

– протидія гібридним загрозам, ***інформаційній агресії, кіберзагрозам***;

– посилення правової держави, верховенства права, захист прав і свобод людини;

– абезпечення громадської безпеки, цивільного захисту, економічної,

екологічної та біологічної безпеки.

Стратегія національної безпеки України є стратегічною рамкою для формування державної політики у сфері національної безпеки.

Стратегія воєнної безпеки України [23] є ключовим документому сфері оборони. Він визначає цілі, пріоритети та завдання реалізації державної політики у сфері оборони та військового будівництва і є основою для розроблення інших оборонних документів. Головними пріоритетами є нарощування спроможностей ЗСУ та інших складових сил оборони, їх професіоналізація та перехід на стандарти НАТО. Основні цілі та пріоритети: розвиток ЗСУ, сил територіальної оборони та інших сил оборони для виконання покладених завдань; здійснення переходу на професійну армію в короткостроковій перспективі; трансформація професійної культури на основі стандартів НАТО у системах керівництва, управління, підготовки та військової освіти; забезпечення потреб оборони України шляхом стабільного та адекватного ресурсного задоволення. Стратегія воєнної безпеки України слугує основою для розробки Стратегічного оборонного бюлетеня, програмних документів з розвитку сил оборони.

Стратегія інформаційної безпеки [28] визначає досягнення інформаційної безпеки країни як одну з ключових функцій держави. В Стратегії здійснений аналіз викликів та загроз інформаційній безпеці, серед яких названі: збільшення кількості дезінформаційних кампаній, перш за все, з боку рф як держави-агресора, інформаційне домінування рф на тимчасово окупованих територіях України; вплив соціальних мереж в інформаційному просторі; недостатній рівень медіаграмотності населення в умовах швидкого розвитку цифрових технологій маніпуляції свідомістю громадян щодо євроінтеграції України тощо. Визначені механізми досягнення мети Стратегії. Ключовими результатами реалізації Стратегії визначено, зокрема, захищений інформаційний простір України; ефективна протидія поширенню ворожого контенту; ефективне функціонування системи стратегічних комунікацій; дотримання конституційних прав громадян, захист приватного

життя; формування української громадянської ідентичності.

Основні принципи, що лежать в основі інформаційної безпеки, – це конфіденційність, цілісність та доступність даних, які захищають інформацію від несанкціонованого доступу, спотворення чи видалення.

Ключові аспекти стратегії: протидія внутрішнім та зовнішнім загрозам в інформаційній сфері, включаючи дезінформацію та протиправну інформацію; забезпечення прав громадян на інформацію та захист персональних даних.

В Стратегії наголошується на оборонному контексті: інформаційна безпека є частиною національної безпеки і має на меті підтримку суверенітету, територіальної цілісності та обороноздатності держави.

Основні принципи інформаційної безпеки: конфіденційність – забезпечення доступу до даних лише авторизованим особам; цілісність – захист даних від випадкового або навмисного пошкодження чи викривлення; доступність – гарантування того, що інформація доступна у потрібний час авторизованим користувачам; автентичність – перевірка достовірності інформації та її джерела; відстежуваність – здатність відстежувати дії, пов'язані з інформацією.

Стратегія кібербезпеки України [24] визначає забезпечення кібербезпеки одним із ключових пріоритетів національної безпеки України. Цей пріоритету буде забезпечуватися за рахунок посилення можливостей національної системи кібербезпеки з метою протидії кіберзагрозам, що можливі у сучасному безпековому середовищі.

Стратегія кібербезпеки України спрямована на захист суверенітету, соціального та економічного розвитку через забезпечення безпечного кіберпростору. Вона передбачає підвищення стійкості до загроз, розвиток спроможностей для протидії агресії (включно з наступальними операціями), покращення кадрового потенціалу та стимулювання інновацій у сфері кібербезпеки. Основні суб'єкти такої системи включають державні органи, військові формування, правоохоронні органи, приватний сектор та громадян.

У Стратегії від 14.05.2021 р. [24] підбиваються підсумки виконання попередньої Стратегії від 15.03.2016 р. [21]. Констатовано, що затвердження цієї Стратегії стало важливим кроком щодо запровадженні заходів кібербезпеки в цій сфері. Було докладено зусиль для розвитку національної системи кібербезпеки. Важливий етап її інституалізації – прийняття Закону [51], який закріпив правові та організаційні засади забезпечення кібербезпеки. Удосконалено нормативне забезпечення кіберзахисту об'єктів критичної інфраструктури. Утворено підрозділи забезпечення кібербезпеки (кіберзахисту) в Держспецзв'язку, СБУ, Міністерстві оборони України, ЗСУ, Міністерстві інфраструктури України. У низці аналітичних матеріалів зазначено, що документ відіграв позитивну роль у формуванні державної політики в цій сфері [114]. Таким чином, Стратегія 2016 р. стала важливим кроком для України в напрямку системної політики кібербезпеки. Отриманий цінний досвід у подальшій розбудові кібербезпеки з точки зору формування її цілей та завдань. Однак, через стрімкі зміни у сфері загроз, зокрема воєнного характеру, документ пережив швидку трансформацію, й певні недоліки стали помітні, що створило необхідність розробки нового стратегічного документа, який уже містить оновлені підходи й індикатори успіху.

Основні цілі та завдання Стратегії від 14.05.2021 р. [24]:

– розвиток національного кіберпростору – створення глобального, відкритого, вільного, стабільного та безпечного кіберпростору для захисту національних інтересів;

– підвищення стійкості – збільшення здатності державних органів, бізнесу та громадян ефективно захищатися від кіберзагроз та реагувати на них;

– протидія недружнім діям – розвиток спроможності для швидкого виявлення, розслідування та протидії ворожим діям у кіберпросторі, а також можливість проведення превентивних наступальних операцій;

– розвиток кадрового потенціалу – підготовка висококваліфікованих

фахівців з кібербезпеки, що сприятиме створенню національних розробок.

– створення безпечного інформаційного суспільства – залучення до заходів кібербезпеки державних інституцій, приватних суб'єктів та громадян.

Одним з ключових виконавців Стратегії визнаний Держспецзв'язок, що розробляє та впроваджує політику у сфері кіберзахисту, включаючи реагування на інциденти та розробку базових заходів кіберзахисту. Наголошується на необхідності співпраці з приватним сектором та міжнародними партнерами.

Стратегія розглядає кіберпростір як новий театр воєнних дій поряд з іншими фізичними просторами. У системі Міністерства оборони України передбачається утворення кібервійськ як складової частини систему дієвої кібероборони, завдання яких включають як захист критичної інфраструктури, так і проведення наступальних операцій.

Як зазначається у статті [301], всі інструменти влади, розглянуті вище, не можуть розвиватись і застосовуватись ізольовано, а навпаки, є взаємопов’язаними [301, с. 8] У зв’язку із цим доцільно розглянути взаємозв’язок безпекових стратегій з інформаційною та кібер- бзпекою. Зазначене питання досліджувалося автором цієї дисертації у його роботах [151, 162, 164, 165, 171].

Оскільки, як зазначено вище, Стратегія 14.09.2020 національної безпеки України розроблена на основі нового (від 21.06.2018) Закону (№ 2469-VIII) «Про національну безпеку України» [52], вимоги Стратегії національної безпеки України слід розглядати у безпосередньому зв’язку із Законом «Про національну безпеку України».

Згідно ч. 1 ст. 4 Закону № 2469-VIII, державна політика у сферах національної безпеки і оборони спрямовується на забезпечення, зокрема, ***інформаційної*** та ***кібер- безпеки***.

Отже, інформаційна безпека і кібербезпека – це складові національної безпеки, зокрема її без пекової (або силової) політики.

У п. 45 Стратегії національної безпеки України вказано, що

пріоритетними завданнями правоохоронних, … та інших державних органів відповідно до їх компетенції [у сфері національної безпеки] є: активна та ефективна протидія … спеціальним ***інформаційним операціям та кібератакам***, російській та іншій підривній пропаганді. У пункті 52 Стратегії визначене основне завдання розвитку системи ***кібербезпеки*** – гарантування ***кіберстійкості та кібербезпеки національної інформаційної інфраструктури,*** …

Отже, у цих положеннях також прослідковується залежність забезпечення національної безпеки від ***інформаційної*** та ***кібер- безпеки***, а також завдання заходів кібербезпеки – технічний і організаційний захист кіберпростору, захист критичної інфраструктури, цифрових систем, державних реєстрів, захист інформаційного середовища від потрапляння ворожого, підривного контенту, який негативно впливає на населення та суспільство.

Зазначені положення слід розглядати в системному зв’язку із положеннями Стратегії інформаційної безпеки України, яка, серед іншого, звертає увагу на деструктивний вплив соціальних мереж в інформаційному просторі; недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку цифрових технологій; інформаційні маніпуляції щодо європейської та євроатлантичної інтеграції України тощо. Зазначається, заходи кібербезпеки повинні гарантувати доступ до об'єктивної та достовірної інформації, а також протидіяти поширенню незаконного контенту. У Стратегії інформаційної безпеки спеціально робиться відсилання, що питання, пов'язані із кібербезпекою, визначаються Стратегією ***кібербезпеки*** України. Таким чином, Стратегія інформаційної безпеки конкретизує загрози у сфері інформації, ЗМІ, комунікацій, підкреслює протидію інформаційним операціям, пропаганді, дезінформації, у тому числі засобами кібербезпеки.

В Стратегії кібербезпеки України важлива роль приділяється кіберзагрозам саме в інформаційній сфері. Розробники Стратегії

кібербезпеки погоджуються, що засоби кібербезпеки захищають не тільки апаратні і програмні засоби, але й інформацію, що там обробляється. Кібербезпека – технічна і технологічна основа інформаційної безпеки.

В Стратегії воєнної безпеки України передбачено, що всеохоплююча оборона України – це комплекс заходів, основний зміст яких полягає, зокрема, … протидії в кіберпросторі та нав'язуванні своєї волі ***в інформаційному просторі***. Відзначається, що на національному рівні рф залишається воєнним противником України, який здійснює збройну агресію проти України … системно застосовує воєнні, політичні, економічні, ***інформаційно-психологічні***, космічні, ***кібер-*** та інші засоби, що загрожують незалежності, державному суверенітету і територіальній цілісності України. Отже, оборонна та воєнна доктрини включають кібер- і інформаційний компоненти як інструменти гібридної війни, тобто: інформаційна безпека = стратегічна стійкість, кібербезпека = цифровий захист від гібридних атак.

Слід зазначити, що розглядаючи шляхи зміцнення воєнної безпеки України в умовах повномасштабного вторгнення Росії в Україну, В.В. Школяренко [301] констатує, що, враховуючи загальнодоступність і миттєвість проходження інформації у сьогоднішньому світі та перетворення інформації на зброю, під час відсічі військовим загрозам постають питання захисту власної інформації та всієї інформаційної інфраструктури від атак противника, а також впливу на відповідні інформацію та інформаційну інфраструктуру ворога. Ця інфраструктура охоплює, насамперед, мережі зв'язку та електронних комунікацій, які дають можливість віддалено управляти іншими критичними інфраструктурними мережами, як-от: електричними, транспортними, ресурсними тощо. Нині ця складова інформаційної боротьби більше стосується кібернетичної сфери. Іншою важливою складовою є інформаційний вплив на свідомість людей, використовуючи всі наявні засоби масової інформації та соціальні мережі. Як видно з досвіду війни з рф, російський інформаційно-пропагандистський влив спроможний керувати настроями та діями широких мас на свою

користь, заштовхуючи їх у віртуальну реальність та забираючи можливість і необхідність критичного мислення. Отже, інформаційний та кібер-інструмент, як підкреслюється в доктринах більшості країн – членів НАТО, є одним з інструментів влади, який відіграє важливу роль у забезпеченні національної та ***воєнної*** безпеки [301, с. 8].

В пункті 3 Стратегії забезпечення державної безпеки вказано, що об'єктами забезпечення державної безпеки є конституційний лад, державний суверенітет, територіальна цілісність, оборонний, науково-технічний та економічний потенціал України, ***інформаційна та кібер- безпека***, критична інфраструктура, службова інформація та державна таємниця. Відзначається, для реалізації власних цілей рф … системно застосовує економічні, політичні, ***інформаційно-психологічні*** засоби, ***кібератаки***.

Останнє знаходить переконливе підтвердження кібератаками рф, описаними у підрозділі 1.3 цієї роботи, в період широкомасштабної агресії проти України. Зокрема, повідомляється, що потужні кібератаки на енергетичну систему України російські війська здійснюють в сукупності за масованими обстрілами енергетичної системи. Також рф активно використовує всі методи поширення дезінформації, спрямованої на формування паніки серед населення, застосовує інформаційно-психологічні маніпуляції та пропаганду щодо стану енергетики [98].

В пункті 15 Стратегії зовнішньополітичної діяльності України наголошується, що ця Стратегія буде реалізовуватися, зокрема, на принципах … протидії ***кібератакам, дезінформації***... В пункті 38 Стратегії зазначається, що інформаційну загрозу для України становить використання засобів комунікації для підриву довіри до державних інститутів, ***поширення дезінформації*** та ***ворожої пропаганди***... В пунктах 45, 47 Стратегії визначаються такі цілі зовнішньополітичної діяльності України, як ***протидія дезінформаційним атакам*** із зовнішніх джерел, … максимально широке донесення до міжнародної спільноти правдивої інформації про скоєні злочини та наслідки агресії рф проти України.

В Стратегії енергетичної безпеки наголошується на високих ризиках кіберзагрози/кіберінцидентів щодо об'єктів критичної інфраструктури енергетичного сектору.

Таким чином, безпекові Стратегії України, прийняті у 2020-2021 рр., є взаємопов'язаними документами, реалізація яких ґрунтується на вимогах Стратегії національної безпеки України, а також на застосуванні механізмів забезпечення інформаційної безпеки і кібербезпеки України. В цьому контексті слід зазначити, що українська система безпекових стратегій побудована за моделлю НАТО та ЄС – НАТО розглядає інформаційну безпеку (information security) і кіберзахист (cyber defence) як єдиний операційний домен. ЄС у «Стратегії кібербезпеки для цифрового десятиліття» («Cybersecurity Strategy for the Digital Decade») (2020) також наголошує на взаємозалежності інформаційної стійкості, цифрового суверенітету та кіберзахисту.

Ідея взаємозв'язку напрямків забезпечення безпеки втілена, зокрема, у Законі України від 16.12.2020 року № 1089-IX «Про електронні комунікації» [53] (далі – Закон № 1089-IX). Огляд основних положень цього Закону виконаний у статті [244].

По-перше, Закон № 1089-IX передбачає надання гарантій захисту електронним комунікаціям від ***кіберзагроз***. Так, у ст. 105 Закону передбачені гарантії користувачам комунікаціних мереж застосування заходів належного реагування на інциденти безпеки, ***кібербезпеки,*** на загрози чи вразливості електронних комунікаційних послуг (мереж).

По-друге, Закон № 1089-IX передбачає заходи забезпечення ***національної та інформаційної безпеки*** в електронних комунікаційних мережах. Так, у пункті 7 статті 2 Закону наведений термін «безпека мереж і послуг» – це здатність електронних комунікаційних мереж і послуг протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж і послуг, а також ***даних***, що зберігаються, передаються чи обробляються, та пов'язаних із ними послуг, що надаються

або доступ до яких здійснюється через електронні комунікаційні мережі чи послуги.

Згідно ч. 2 ст. 31 Закону № 1089-IX, постачальники електронних комунікаційних мереж та/або послуг зобов'язані вживати відповідних технічних та організаційних заходів для забезпечення безпеки цих мереж та послуг з метою гарантування цілісності власних електронних комунікаційних мереж, безперервності надання електронних комунікаційних послуг, ***недопущення несанкціонованого доступу*** до електронних комунікаційних мереж.

Прийняття Закону № 1089-IX [53] є імплементацією Директиви Європейського Парламенту і Ради ЄС 2018/1972 від 11.12.2018 року про запровадження Європейського кодексу електронних комунікацій [12].

Таким чином, взаємозв'язок безпекових стратегій з інформаційною та кібербезпекою є фундаментальним для сучасної системи національної безпеки України (і будь-якої держави). Кібербезпека – це технічний фундамент інформаційної безпеки, а обидві вони є функціональними складовими національної безпеки. Без інтеграції цих трьох рівнів неможливо забезпечити ані стійкість держави до гібридних загроз, ані стабільність інформаційного простору.

3.2. Досягнення цілей забезпечення інформаційної безпеки у системі кіберзахисту

Згідно ст. 3 Конституції України, людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Держава відповідає перед людиною за свою діяльність. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави.

Таким чином, державна політика у сфері кібербезпеки як частина

діяльності держави спрямована, перш за все, на забезпечення конституційних прав громадян.

Зокрема, професор Г.В. Форос (із співавтором) вважає [293], що хоча у Конституції України 1996 року, як і в конституційному законодавстві більшості зарубіжних країн, дефініції «кібербезпека», «кіберзлочинність» та похідні не вказано, але ключовим завданням у цій сфері діяльності держави, яке постає перед державами, є забезпечення основних прав людини, згідно з міжнародними угодами, які підтверджують право кожного на свободу слова, право на пошук, отримання і передачу будь-якої інформації та ідей, незважаючи на кордони, а також права на недоторканість приватного життя, зокрема і в кіберпросторі. Зокрема, автори наголошують, що наріжним каменем одного з перших нормативно-правових актів в даній сфері – Конвенції від 23.11.2001 Ради Європи про кіберзлочинність – визначена необхідність забезпечити належний баланс між правоохоронними інтересами та повагою до основних прав людини. Зауважено також на право на захист особистої інформації, як це передбачено Конвенцією РЄ про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 р.

У преамбулі Закону № 2163-VIII [51] наголошено, що Закон визначає правові та організаційні основи забезпечення … інтересів людини і громадянина...

У пункті 5 ст. 1 Закону № 2163-VIII [51] кібербезпека визначена як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору …

Отже, як зазначено вище, діяльність української держави у сфері кібербезпеки визначається Конституцією України та Конвенцією про кіберзлочинність та ЄКПЛ, зокрема, в контексті забезпечення конституційних прав громадян.

Кібербезпека – це не лише технічна або військова категорія, а передусім правова сфера, спрямована на захист конституційних прав і свобод людини в цифровому середовищі.

Звідси побудовані такі основні принципи Закону № 2163-VIII [51]:

– пріоритет прав і свобод людини і громадянина – будь-які заходи кіберзахисту мають здійснюватися лише в межах закону і з дотриманням прав людини;

– законність і пропорційність – забороняється надмірне втручання у приватне життя під приводом кіберзахисту;

– публічність та відкритість державної політики у сфері кібербезпеки;

– демократичний цивільний контроль – діяльність спецслужб і військових у кіберсфері підконтрольна суспільству та парламенту.

Потенційними загрозами для конституційних прав громадян може бути:

– надмірне втручання у приватність під час моніторингу кіберінцидентів;

– нелегітимний збір або обробка персональних даних у державних чи приватних ІТ-системах;

– цензура або блокування контенту під приводом інформаційної безпеки;

– цифрова нерівність – обмежений доступ окремих груп громадян до безпечних електронних послуг;

– відсутність ефективних механізмів оскарження рішень, що порушують права користувачів у кіберпросторі.

Українські стратегічні документи (зокрема Стратегія кібербезпеки України від 14.05.2021 р. [24]) визначають, що держава забезпечує баланс між потребою у безпеці кіберпростору та збереженням прав і свобод людини в інформаційному суспільстві. Тобто кібербезпека не може виправдовувати тотальний контроль, а має створювати умови, за яких кожен громадянин може реалізувати свої права – без страху, що його дані чи цифрова активність будуть використані проти нього.

Отже, забезпечення конституційних прав у сфері кібербезпеки – це баланс між захистом держави та захистом людини. Кібербезпека повинна не

обмежувати, а гарантувати: приватність (ст. 32 Конституції), свободу слова та інформації (ст. 34 Конституції), безпечне користування цифровими сервісами (ст. 40 Конституції), і водночас – захист від кіберзагроз, які можуть ці права знищити.

Таким чином, правове регулювання питань кібербезпеки в Україні ґрунтується на вимогах досягнення балансу між захистом інформації і свободою вираження поглядів, позицією ООН і практикою ЄСПЛ. Зокрема, В.Ф. Загурська-Антонюк наголошує, що ефективним механізмом протидії інформаційним загрозам є обмеження доступу до інформації. Але цей автор також вказує, що такі обмеження можуть «виявитися неприпустимими у цивілізованих демократичних суспільствах, …» [130].

В ліберальних системах держави і права принцип свободи має пріоритет над принципом обмежень, тому будь-які обмеження наражаються на певні заперечення. Зокрема, згідно принципу свободи творчості (свободи самовираження), автор має право вільно обирати напрям своєї творчості. Однак свобода творчості знаходиться в досить складних і неоднозначних стосунках з суспільною мораллю, релігією, зокрема, з принципом терпимості, що включає заборони на певні теми і засоби вираження. Тому при виникненні конфлікту між прибічниками свободи та обмежень вкрай рідко вдається знайти компроміс [249, 307].

Огляд і узагальнення підходів демократичних авторів до гарантій свободи слова (свободи творчості) виконаний у дисертаційному дослідженні [307, с. 286-329].

Свобода слова найбільш трепетно оберігається демократичним світом. Вона тісно пов’язується зі свободою поглядів. Цю взаємопов’язаність британський філософ Дж. С. Мілль оцінив наступним чином [307, с. 287] (1859 р.): «зі свободою думки… нерозривно пов'язана свобода говорити і писати; свобода висловлювати і опубліковувати свої думки… має для індивідуума майже зовсім таке ж значення, як і свобода думки, і нерозривно з нею пов'язана».

У монографії [300, с. 412-413] С. Шевчук наводить сучасне теоретичне розуміння щодо таких складових свободи вираження поглядів: забезпечення розвитку особистості (індивідуальна самореалізація); здобуття знань і встановлення істини; забезпечення участі усіх членів суспільства у процесі прийняття державних рішень; утворення суспільства, більш здатного до змін.

У таблиці додатку Б9 наводяться правові позиції Верховних Судів демократичних країн з приводу пріоритету свободи слова (вираження поглядів). Наголошується, що свобода вираження поглядів, преси та всіх інших форм вираження належить до вічних та непорушних прав, основних прав людини, і що абсолютна гарантія таких прав є одним з основоположних правил і характеристик демократичної форми урядування, які відрізняють демократію від тоталітаризму. Як індикатор громадської думки свобода слова допускається у певних межах навіть авторитарною владою.

Сучасне демократичне суспільство намагається створити перешкоди адміністративному тиску влади, яка б намагалася обмежити вказані права. У британському Біллі про права від 16/26 грудня 1689 р. [307, с. 290] вказувалося, що свобода слова і дебатів не повинні бути приводом до будь-якого переслідування. Гарантії свободи слова, друку, самовираження у сучасних Конституціях демократичних країн наведені у таблиці додатку Б10. Аналогічні норми містяться і у Конституції України, ст. 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.

Узагальнення цих положень міститься у ст. 19 Загальної декларації прав людини [307], відповідно до якої кожна людина має право на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватися своїх переконань та свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів.

Стаття 10 ЄКПЛ «Свобода вираження поглядів» включає дві частини:

1). Кожен має право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів. Ця стаття не перешкоджає державам вимагати ліцензування діяльності радіомовних, телевізійних або кінематографічних підприємств.

2). Здійснення цих свобод, оскільки воно пов'язане з обов'язками і відповідальністю, може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законом в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для охорони порядку або запобігання злочинам, для охорони здоров'я або моралі, для захисту репутації або прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду і є необхідними в демократичному суспільстві.

Ці формулювання ст. 10 ЄКПЛ відображають єдність прав та обов'язків у сфері свободи самовираження, відповідно до якого вказані права можуть підлягати певними обмеженнями, однак пріоритет залишається за гарантуванням прав. Як вказується у п. 41 рішення ЄСПЛ від 10.08.2006 р. у справі «Ляшко проти України» [264], «предмет пункту 2 статті 10 (щодо обґрунтованості обмежень) застосовується не тільки до «інформації» чи «ідей», які … розглядаються як необразливі чи як малозначущі, але й до тих, які можуть ображати, шокувати чи непокоїти... потреба в таких обмеженнях має бути переконливо встановлена». Аналогічний підхід було зафіксовано і у статті 11 Французької Декларації прав людини і громадянина, де не тільки визначений пріоритет «вільного повідомлення іншим думок», але й встановлюється, що така свобода тягне «відповідальність за зловживання цією свободою у випадках, встановлених законом» (рядок 2 таблиці додатку Б10).

М. Бліхар, досліджуючи суспільно-політичний аспект свободи вираження поглядів, виділяє 3 елемента цього права: 1) безпосередня

реалізація людиною права на свободу вираження політичних поглядів; 2) діяльність органів публічної адміністрації та … щодо забезпечення реалізації особами права на вираження політичних поглядів; 3) процеси взаємодії людини та органів публічної адміністрації для організації діалогу щодо продукування позитивних змін у політичних процесах чи явищах [82, 278].

П.Д. Гуйван ототожнює свободу думки і свободу вільного вираження поглядів і переконань, розкриваючи їх як можливість кожної особи самостійно визначити для себе систему моральних, духовних та інших цінностей, а також вільно без ідеологічного контролю виявляти їх назовні [111, с. 63; 278].

Як було згадано раніше, свобода вираження поглядів важлива для реалізації власної гідності, участі в соціально-політичному житті держави. Без чітких гарантій права на свободу вираження поглядів не існує демократія та свобода держави. З юридичної точки зору – це можливість самостійно обирати вид і міру власної поведінки, висловлювати ідеї, погляди, думки, розуміючи в повному обсязі значимість заявленого. Така можливість може бути як позитивом, так і негативом [277, 278].

Пасивним проявом свободи вираження поглядів є свобода дотримуватися поглядів, тобто свобода поділяти і підтримувати думки, погляди, ідеї, висловлені іншими особами. Новим проявом такої свободи є розміщення коментарів та інша комунікація в мережі Інтернет і соціальних мережах. Право на свободу дотримання поглядів без втручання – невід’ємна частина свободи вираження поглядів, яка гарантується статтею 10 Конвенції. Держава не має повноважень щодо встановлення зобов’язань дотримуватися певних поглядів чи забороняти індивіду дотримуватися своїх поглядів [72, с. 63; 278].

Свобода вираження поглядів стосується не лише окремих осіб, а й засобів масової інформації як інституту громадянського суспільства. Невмотивоване та незаконне втручання у діяльність засобів масової

інформації, які порушують їхню свободу, є поширеним явищем навіть у найбільш розвинених демократичних суспільствах. Юридичні гарантії забезпечення права на свободу вираження поглядів для засобів масової інформації за загальним правилом встановлюються кожною державою відповідно до міжнародних стандартів і правових звичаїв цієї держави [278].

Право на свободу вираження поглядів гарантується механізмом його державного забезпечення, тобто можливістю суб'єкта звернутися за захистом до державних органів у випадку незаконного зазіхання на свободу слова з боку будь-яких осіб. Особливе правове становище в контексті гарантування забезпечення свободи вираження поглядів мають журналісти – головні учасники інформаційних відносин. Умисне перешкоджання професійній діяльності журналістів, переслідування журналістів за професійну діяльність або критику тягне за собою відповідальність, передбачену законодавством України. Свобода преси – це свобода спілкування і висловлення думок через медіа. У такому контексті свобода полягає у забезпеченні неможливості необґрунтованого втручання держави [112, с. 84; 278].

Як відповідь на нові виклики часу, окремі аспекти сутності свободи вираження поглядів тлумачить у своїй практиці ЄСПЛ. У справі «Murat Vural v. Turkey» Суд наголосив, що стаття 10 Конвенції захищає не тільки зміст висловлених поглядів, ідей та інформації, а й форму їхнього вираження. Крім того, відповідно до вимог плюралізму і толерантності як основи демократичного суспільства свобода вираження поглядів поширюється не лише на інформацію, яка сприймається прихильно, вважається необразливою або викликає байдужність, а й також на інформацію, яка ображає, шокує, турбує державу або частину населення [278, 323]. Раніше у справі «Нільсен та Йонсен проти Норвегії» Суд зазначив, що право на свободу вираження поглядів захищає самовираження, яке також може «образити, шокувати або турбувати» [278, 324].

У справі «Cengiz and Others v. Turkey» Судом було визнано відеоплатформу YouTube важливим засобом реалізації права осіб отримувати

та поширювати інформацію й ідеї, тоді як наказ про блокування платформи є втручанням держави у право на свободу вираження поглядів. Окрім того, було встановлено відсутність будь-якого законодавчого положення, яке б наділяло суд такими повноваженнями [278, 325]. Вказана справа підтвердила, що стаття 10 ЄКПЛ гарантує не лише право на передачу інформації, але й право осіб на її отримання.

Таким чином, висновує К.С. Токарєва, слід відзначити, що свобода вираження поглядів – це право кожної особи вільно, без будь-якого невмотивованого стороннього втручання отримувати, зберігати, поширювати, висловлювати інформацію та ідеї про різноманітні явища, процеси, події, надавати оцінку таким подіям у будь-якій формі вираження, а також дотримуватися переконань на власний розсуд у межах, визначених національним законодавством [278].

Разом із тим, проблема забезпечення свободи самовираження ***НЕ ЗАВЖДИ*** вирішується однозначно на користь особи, яка намагається захистити своє право. Так, у згаданому в таблиці додатку Б9, рядок 1, рішенні у справі «Roth v. United States» Верховного Суду США зазначено, що «безумовне формулювання Першої поправки[7] не було призначене для захисту кожного вираження» [358]. У рішенні від 03.07.1978 р. у справі «FCC[8] v. Pacifica Foundation» Верховного Суду США останній не зміг однозначно стати на сторону скаржника. У рішенні констатовано, що «зміст мовлення радіостанції, який був «вульгарними», «образливим» і «шокуючим», не має права на абсолютний конституційний захист, тому необхідно оцінити дії FCC в контексті цієї передачі в ефір. Суд вирішив, що FCC не могла повністю заборонити такий контент, але могла обмежити трансляції певним часом доби. Це було пов'язано з тим, що Комісія мала повноваження захищати дітей від потенційно образливого матеріалу та гарантувати, що небажана мова не порушує приватності сімей.

[7] Мається на увазі згадана у таблиці додатку А6, рядок 1, поправка 1 до Конституції США
[8] Федеральна комісія зі зв'язку США

Отже, завжди виникає проблема, з одного боку, меж свободи самовираження, і, з іншого боку, допустимості її обмежень. А такі обмеження є можливими як з точки зору зазначеного вище дуалізму прав і обмежень свободи самовираження (стаття 10 ЄКПЛ), так і з точки зору практичних потреб обмеження ворожих інформаційно-психологічних впливів, на що неодноразово вказувалося у розділах 1, 2 цієї роботи, а також в роботі [130]. Це ж саме унормовано і у частині 3 згаданої вище статті 34 Конституції України, відповідно до якої «здійснення цих прав [на свободу думки і слова, на вільне вираження своїх поглядів і переконань, вільне поширення інформації] може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя». Отже, потрібно розглянути міжнародні демократичні стандарти застосування таких обмежень.

Ці підходи узагальнені у дисертаційному дослідженні [336, с. 329-368].

Як вказує російський автор В. Чиркін [298, с. 184-185], державні органи не втручаються в творчий процес, в творчу працю художника, артиста, письменника. Але, згідно до законів, державні органи мають право приймати заходи щодо заборони псевдокультурних, деструктивних напрямів, проти пропаганди, спрямованої на підривання загальнолюдських цінностей, яка руйнує духовний світ, здоров'я, моральність людей, проти пропаганди тероризму, розпалювання соціальної, расової, національної і релігійної ворожнечі.

Варто зазначити, що ця позиція, правильна по суті, висловлена занадто категорично. Так, у монографії [300, с. 468-557] наголошується, що ЄСПЛ послідовно дотримується позиції, згідно з якою обмеження свободи слова мають тлумачитися вузько, а необхідність будь-яких обмежень має бути переконливо доведена [300, с. 472]. Вказується, що європейський стандарт

визначення правомірності обмежень свободи вираження, встановлений судовими рішеннями ЄСПЛ, відповідає тому́ загальному підходу, що визначений у цілому для статей 8, 9, 10 та 11 ЄКПЛ. Для такої оцінки ЄСПЛ розглядає справу відповідно до такої послідовності [300, с. 468]: а) визначення того, чи було втручання «встановлене законом»; б) чи переслідувало втручання «правомірну мету»; в) чи було таке втручання «необхідним у демократичному суспільстві».

Основоположною ідеєю першої частини стандарту є, перш за все, унеможливлення незаконного та свавільного втручання у здійснення свободи вираження поглядів. Таке міркування, безумовно, випливає з принципу правової визначеності, який є невід'ємною частиною ефективного захисту прав людини, що встановлений у ЄКПЛ. Щодо країн прецедентного права поняття «встановлене законом» включає у себе також судовий прецедент [300, с. 469].

Застосування критерію «необхідності в демократичному суспільстві» означає, що втручання у свободу вираження поглядів … повинно обумовлюватися гострою суспільною потребою та бути пропорційним законній меті. При цьому навіть за умови дотримання цих вимог втручання порушуватиме ст. 10 ЄКПЛ, якщо воно призводить до встановлення непропорційного покарання [300, с. 473].

Допустимі підстави обмеження свободи вираження поглядів встановлені у ч. 2 ст. 10 ЄКПЛ, а саме: територіальна цілісність або громадська безпека; охорона здоров'я або моралі; національна безпека; охорона порядку або запобігання злочинам; захист репутації або прав інших осіб; запобігання розголошенню конфіденційної інформації або підтримання авторитету і безсторонності суду.

Актуальні питання гарантування культурних прав громадян у контексті імплементації угоди про асоціацію з ЄС розглянуті, зокрема, у статті [306].

Огляд характеру обмежень, які ЄСПЛ визна́є прийнятними, свідчить про те, що найчастіше серед них визнаю́ться прийнятними обмеження щодо

захисту суспільної моралі. Наприклад, С. Шевчук відзначає, що захист національної безпеки підлягає навіть більш жорсткому нагляду з боку ЄСПЛ, ніж захист суспільної моралі [300, с. 543].

Підходи ЄСПЛ, сформульовані у рішеннях Суду, щодо обмежень свободи творчості докдано ілюструються витягами із текстів рішень, наведеними у таблиці додатку Б11.

Іншим аспектом захисту суспільної моралі є обмеження розповсюдження творів, що пропагують культ насильства і жорстокості [97]. Зокрема, згідно пункту 2 ч. 1 ст. 36 Закону України «Про медіа» [56], на території України в медіа та на платформах спільного доступу до відео забороняється поширювати, зокрема, висловлювання, що розпалюють ненависть, ворожнечу чи жорстокість до окремих осіб чи груп осіб за ознакою етнічного чи соціального походження, громадянства, національності, раси, релігії та вірувань, віку, статі, сексуальної орієнтації, гендерної ідентичності, інвалідності.

Ця вимога відповідає заборонам, передбаченим Додатковим протоколом [7] до Конвенції Ради Європи «Про кіберзлочинність» [6], згідно з яким забороняється поширення через інформаційно-комунікаційні системи інформаційної продукції ксенофобного та расистського характеру, яка (продукція) захищає, сприяє або підбурює до ненависті, дискримінації чи насильства проти будь-якої особи або групи осіб за ознаками кольору шкіри, раси, національного або етнічного походження, а також віросповідання, якщо вони використовуються як привід для будь-якої з цих дій.

Зокрема, у Рекомендації № R (89) 7, враховуючи, зокрема, норми ст.ст. 8 і 10 ЄКПЛ щодо свободи вираження поглядів і безперешкодного поширення інформації та ідей, визна́ється, тим не менш, важливість консолідації дій, спрямованих ***проти поширення відеозаписів насильницького, жорстокого й порнографічного змісту***, а також проти вживання наркотиків, зокрема задля захисту неповнолітніх.

У Європейській конвенції про транскордонне телебачення [5] (1998 р.)

вимагається (ст. 7), що усі елементи програмних послуг, зокрема, не повинні: a) бути непристойними і, особливо, містити порнографію; b) неправомірно пропагувати насильство чи спонукати до расової ненависті. Усі елементи програмних послуг, які можуть завдати шкоди фізичному, психічному чи моральному розвиткові дітей та підлітків, не повинні транслюватись, якщо під час трансляції та прийому вони мають змогу їх дивитися.

Додатково зазначимо, що відповідно до Рекомендації ЮНЕСКО [17], необхідні заходи для огородження національних культур від творів, що пропагують… насильство.

Комплекс підходів, що дає уявлення про європейські стандарти обмеження поширення матеріалів, що містять показ насильства та жорстокості, надають Рекомендації Комітету міністрів РЄ № R (89) 7 від 27.04.1989 р. [279], № R (97) 19 від 30.10.1997 р. «Про показ насильства електронними ЗМІ» [172], № R (97) 20 від 30.10.1997 р. «Про розпалювання ненависті» [20]. Базовим принципом підходу до обмежень в даній сфері є правила, встановлені ст. 10 ЄКПЛ (див. також підрозділ 2.1 цієї роботи).

Агресія рф проти України, суттєвою складовою якої виявилася інформаційна війна [109], поставила в останні 11 років, якщо рахувати від окупації рф Криму, перед Україною нові виклики, до яких Україна виявилася неготовою [258, с. 76]. Як зазначає Ю.О. Горбань [109, с. 137], антиукраїнська пропагандистська кампанія виявила недостатню сформованість наукових і методологічних обґрунтувань та пояснень щодо дій у подібних ситуаціях, продемонструвала слабку координованість дій державних органів влади, громадянського суспільства, експертного та наукового середовищ, журналістів щодо протидії таким кампаніям. Мета інформаційної війни – послабити моральні і матеріальні сили супротивника або конкурента та зміцнити власні [109, с. 137]. Секретар РНБО України О.В. Турчинов наголошує, що парадигма гібридної війни спрямована на підрив і руйнування усього комплексу суспільних відносин у об'єкта агресії, знищення волі до опору, у тому числі і за рахунок інформаційних операцій

[284]. Ізраїльський військовий інструктор Цві Аріелі вказує, що інформація – невіддільна частина будь-якої військової кампанії. У зв'язку з тим, що багато сучасних війн часто не ведуться на тотальне знищення, а цілями їх є обмежені політичні досягнення, інформація може зіграти вирішальну роль як на оперативному або оперативно-тактичному рівні, так і для закріплення результатів військової компанії в юридичному і міжнародно-політичному плані [69].

Доктор юрид. наук В.А. Ліпкан вказує на так звану білу (формально – легальну) пропаганду – відверто нелояльну до суб’єкта-адресата, яка ведеться будь-якими ЗМІ офіційними каналами без приховування її спрямованості та джерела. Така пропаганда, наприклад, ведеться російськими ЗМІ проти України, Туреччини, США, ЄС, їх посадових осіб. На телеканалах та у інших державних ЗМІ постійно відбувається відкрита фальсифікація інформації, дискредитація вищих посадових осіб з метою формування негативного ставлення, зокрема, до України та Туреччини… Фактично пропаганда становить спосіб інформаційної боротьби, який передбачає активний наступальний інформаційний вплив на об’єкт з метою внесення наперед заданих змін до інформаційного простору, що спричинює відповідні зміни у просторі реальності [194].

Вказане однозначно свідчить про загрози національній безпеці України інформаційного впливу агресора, тому виникають обґрунтовані підстави обмежувати чи забороняти поширення відповідної ворожої інформації. Такі заборони чи обмеження мають відповідати критеріям ч. 2 ст. 10 ЄКПЛ. Тому доцільно перевірити обґрунтованість таких обмежень за цими критеріями.

З приводу першого критерію обмежень – встановлення законом – слід зазначити, що українське право і практика пішли шляхом застосування таких заборон (обмежень), як-от: ретрансляції передач російського телерадіомовника; трансляції (поширення) телерадіопродукту виробництва рф; використання певних тем, що шкодять національній безпеці України, у національному телерадіопродукті.

Як зазначає К.С. Токарєва [278], новітній період історії Української держави, який триває з 2014 року в зв'язку з початком збройної агресії рф проти України, ознаменувався початком інформаційної гострої війни, що вагомо вплинуло на дотримання права свободи вираження поглядів в Україні та актуалізувало питання щодо обмеження такого права [278]. Проф. Ю.Д. Кунєв наголошує, що проблема забезпечення інформаційної та кібер-безпеки стає особливо актуальною під час зовнішніх загроз, зокрема, гібридної війни [180]. На виконання державної політики у сфері забезпечення державної безпеки законодавець закріпив певні обмеження, які безпосередньо впливають на свободу вираження поглядів в Україні. Зокрема, у друкованих засобах масової інформації та під час діяльності телерадіоорганізацій заборонено: розповсюджувати заклики до захоплення влади, насильницької зміни територіальної цілісності України або конституційного ладу; поширювати інформацію, яка розпалює ворожнечу, у тому числі національну; пропагувати війну, жорстокість, насильство; популяризувати та пропагувати російську федерацію з метою створення її позитивного образу та виправдання або визнання правомірною окупацію українських територій; заперечувати збройну агресію держави-агресора проти України; здійснювати глорифікацію осіб, які реалізують збройну агресію російської федерації проти України, поширювати російський інформаційний контент тощо. Аналогічні межі свободи встановлені для телерадіоорганізацій [278].

При прийнятті Закону України «Про медіа» [56] ці вимоги та заборони були послідовно реалізовані у цьому Законі. Так, згідно ч. 1 ст. 123 Закону, на території України забороняється поширювати аудіовізуальні медіа-сервіси на замовлення та сервіси провайдерів аудіовізуальних сервісів держави-агресора. Згідно ч. 1 ст. 124 Закону, до європейського та національного продукту не може відноситися програма, щонайменше один виробник, продюсер якої є:

1) фізичною особою, яка є громадянином держави-агресора (держави-

окупанта), за виключенням осіб, що мають дозвіл на тимчасове або постійне проживання в Україні;

2) юридичною особою, зареєстрованою у державі-агресорі (державі-окупанті) чи з місцезнаходженням у такій державі; або

3) юридичною особою, в якій кінцевим бенефіціарним власником є особа, яка є громадянином або резидентом держави-агресора (держави-окупанта), чи юридична особа, зареєстрована в такій державі або з місцезнаходженням у такій державі.

Виходячи з ворожої діяльності пропагандистських ЗМІ країни-агресора, такі обмеження та заборони мають легітимну мету і є необхідними в демократичному суспільстві для його захисту від деструктивних впливів. Адже це ті самі ЗМІ, які масово випускали брехливі та пропагандистські «новини» антиукраїнської спрямованості (мовою оригіналів): «распятый мальчик» «мать упомянутого распятого мальчика, которую привязали к танку и таскали по площади» «два раба», «обглоданные снегири, в отличие от синичек патриотичной расцветки», «пьяные негры танцуют на украинских танках», «Яценюк воевал в Чечне и участвовал в пытках и расстрелах российских военнопленных» тощо. Немає жодних підстав дозволяти цим агентствам та ЗМІ легітимно поширювати цю інформацію в Україні. Так, Представник України при ООН, посол В. Єльченко у виступі в ООН 11.05.2016 р. звернув увагу, що «жорстока і порочна пропаганда, поширювана державними ЗМІ в Росії, є одним з основних елементів гібридної агресії РФ. Існує необхідність боротьби з такими явищами, як державна пропаганда нетерпимості і ненависті» [286].

Як зазначає згаданий вище Ю.О. Горбань [109, с. 140], в інформаційній війні проти України Росія застосовує практично весь арсенал впливу на свідомість людей. Зокрема, спостерігачі відзначають, що, наприклад, усі 23 роки незалежності України на кримському телебаченні велася антиукраїнська пропаганда [109]. Російський журналіст А. Бабченко пише: «Путінська пропаганда дістала з людей всю гидоту, вивернула все найгірше

на місце хорошого, дозволила вбивства, ксенофобію, мракобісся, переслідування, цькування, ненависть, агресію, расову нетерпимість… – і це виявилося неймовірно ефективно… Я практично впевнений – жоден «кримнаш» не був би можливий без всіх цих серіалів про ментів, слідчих, вбивства, викрадення, бригади, кілерів, трупаків, «розслідування» про маніяків, про дитячих гвалтівників, про чоловічину в трилітрових банках і чорнуху, чорнуху, чорнуху» [73].

Висловлена А. Бабченком думка кореспондується з позицією небажаності пропаганди насильства та жорстокості, можливо навіть більш небезпечної, ніж порнографія. Ця пропаганда, яка була, переважно, привнесена на українське телебачення російським теле-, відео- продуктом, на була своєчасно оцінена українською владою як загрозлива, – і не тільки в сенсі загрози для суспільної моралі, але й у сенсі загрози для національної безпеки.

Філолог А. Гребенюк, вважає [110], що антиукраїнською пропагандою є сукупність методів спеціальних інформаційних операцій, що полягає у деструктивному маніпулятивному та відкритому ідейно-політичному, соціальному, релігійному та іншому впливові (шляхом використання комунікативних технологій, поширення і постійного, глибокого та детального роз’яснення ідей, поглядів, знань, закликів) на суспільство, групу осіб або окрему особу, з метою їх ***переорієнтації на інші цінності та ідеали*** й провокування запрограмованих емоцій, підштовхування до вчинення дій з дестабілізації ситуації й послаблення державного та суспільно-політичного устрою, посягання на державний суверенітет, територіальну цілісність, демократичний конституційний лад та інші життєво важливі національні інтереси України [110, с. 135].

Характерними особливостями проникнення в систему соціальних інформаційних комунікацій пропаганди, ворожої національним інтересам України є: розповсюдження (поширення, роз’яснення, доведення до адресатів) політичних, філософських, наукових, художніх, інших мистецьких

ідей, по глядів, знань, закликів зі змістом, що фальсифікує реалії розвитку нашого суспільства, подає їх у викривленому, негативному світлі; їх реалізація через ідейно-політичний, соціальний, релігійний в плив на широкі маси або певні групи людей; спекуляція на наявних суспіль них протиріччях, розпалювання внутрішньо-суспільної ворожнечі, провокування конфліктів, підрив суспільної єдності; локалізація серед методів спеціальних інформаційних операцій та у спектрі невоєнних загроз; деструктивність; переорієнтація об'єктів впливу на цінності та ідеали, не властиві або ж шкідливі для нашого суспільства, підштовхування до вчинення протиправних дій , послаблення державного та суспільно-політичного устрою України [110, с. 128].

Отже, російська пропаганда завдала і завдає національній безпеці України величезної шкоди, реально призводить до загибелі людей, тому обмеження такої пропаганди відповідає легітимній меті – забезпеченню національної безпеки – та є необхідною в демократичному суспільстві.

Варто також зазначити, що рф та Україна формально є учасниками Європейської конвенції про транскордонне телебачення [5]. Однак рф не ратифікувала цю Конвенцію і не вважає себе зв'язаною її умовами. При цьому слід мати на увазі, що трансляція за «Європейською конвенцією про транскордонне телебачення» здійснюється на принципах взаємності. Це означає, що країни-учасниці погоджуються забезпечувати трансляцію телевізійних програм своїх сусідів, якщо ті, в свою чергу, надають відповідні права для трансляції їхніх програм на своїй території. Принцип взаємності – це ключова умова конвенції, яка передбачає, що держава-учасниця повинна надавати право на трансляцію телевізійних програм іншої держави-учасниці, якщо остання надає подібні права для трансляції програм першої. Конвенція спрямована на сприяння поширенню культурного та інформаційного контенту між державами-учасницями, а взаємність є гарантією того, що це поширення буде двостороннім та збалансованим. Отже, Україна не зв'язана умовами Конвенції по відношенню до рф.

Виходячи з цих принципів, Україна у період гібридної війни рф проти України здійснила низку дій, спрямованих на обмеження проникнення російського і проросійського контенту в українські інформаційно-комунікативні мережі і у ЗМІ. Зокрема, здійснено:

– *заборона російських соціальних мереж і сайтів.* Указом від 15.05.2017 року № 133/2017 Президента України «Про рішення Ради національної безпеки і оборони України від 28.04.2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» [30] було запроваджене блокування доступу до російських сервісу mail.ru, соціальних мереж «ВКонтакте», «Одноклассники» та інших [30]. В подальшому блокування було продовжено Указом Президента України від 14.05.2020 року № 184/2020 «Про рішення Ради національної безпеки і оборони України від 14.05.2020 року «Про застосування, скасування і внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» [31] було запроваджене блокування доступу до російських сервісу mail.ru, соціальних мереж «ВКонтакте», «Одноклассники» та інших [31];

– *запровадження санкцій проти засобів масової інформації.* Указом Президента України від 02.02.2021 року № 43/2021 введено в дію Рішення Ради національної безпеки і оборони України від 02.02.2021 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» [32]. Санкції було застосовано до юридичних осіб, серед яких телеканали «112 Україна», «NewsOne», «Zik» [32].

Ці рішення викликали неоднозначну реакцію. Зокрема, за даними опитування Київського міжнародного інституту соціології, лише 36 % українців вважають, що заборона російських соціальних мереж є необхідною для захисту держави; 50 % українців притримуються думки, що заборона російських соцмереж є помилкою і призводить лише до обмеження прав громадян [242]. Щодо заборони телеканалів, то за даними опитування групи

«Рейтинг» 53 % опитаних українців схвалюють санкції РНБО проти тодішнього народного депутату України Віктора Медведчука. У той же час підтримка санкцій проти телеканалів Медведчука трохи нижча – їх підтримують 44 % респондентів. 39 % не підтримують санкції проти каналів 112, NewsOne та Zik, а 17 % не відповіли [230]. Така різниця цілком зрозуміла – заборона телеканалів стосується особистих звичок та уподобань окремих осіб. Як зазначає проф. О.О. Тихомиров [274], обмеження людини у доступі до певних звичних і комфортних для неї каналів отримання і поширення інформації … створює в її інформаційному просторі елементи інформаційного вакууму. Це може викликати негативні реакції, пов’язані з несприйняттям встановлених обмежень, що зумовлює додаткові психологічні вразливості і поле для подальших інформаційних маніпуляцій [274, с. 59]. У той же час такі обмеження переважно спрямовані на захист суспільних інтересів. Тому підходи до забезпечення інформаційних прав громадян підлягають окремому розгляду.

3.3. Структура інформаційних прав громадян. Захист прав громадян у сфері кібербезпеки

Фактично, українське суспільство набуло рис інформаційного, а інформаційні права та свободи сформували окрему групу, які викликали науковий інтерес та професійну дискусію. Зокрема, щодо поняття та переліку тих прав, які можуть входити до категорії інформаційних. Раніше науковий акцент зосереджувався на досить вузькому підході, який передбачав ототожнення інформаційних прав людини з конституційним правом на інформацію [224, с. 70]. Так, М. Муратов [214, 224] стверджує, що право на інформацію означає право знати про створення і функціонування усіх інформаційних систем, що стосуються особистого життя громадянина, право надавати згоду на збирання особистої інформації, право перевіряти достовірність такої інформації і спростовувати недостовірну інформацію,

право на достовірну інформацію про стан навколишнього середовища тощо [214]. Б. Гоголь зауважував, що право на інформацію – нормативно забезпечена можливість особи вільно збирати, обробляти, зберігати і поширювати інформацію у будь-який не заборонений законодавством спосіб, складовими права на інформацію називає права збирати, обробляти, зберігати, поширювати інформацію [104, 224].

Однак, які б широкі обсяги поняття «права на інформацію» не розглядалися науковою спільнотою, очевидним залишається те, що розвиток науки, права та світу не дозволяє назвати право на інформацію та інформаційні права ідентичними категоріями [224, с. 70]. Як висновує проф. О.О. Тихомиров [274], в юридичному сенсі потреби забезпечення безпеки людини в інформаційному суспільстві, які сьогодні втілюються в її інформаційних правах як ключовій ідеї на аксіологічному рівні, так і в змісті окремих новітніх інформаційних прав, не можуть сприйматися суто в контексті пошуку і юридичного оформлення балансу суспільного і приватного інтересу щодо свободи інформації [274, с. 63]. Тому інформаційні права та право на інформацію співвідносяться як ціле та його складова [224, с. 70]. До поняття інформаційних прав людини відносять абсолютно усі права та свободи, які існують та мають інформаційний характер. Загалом, на думку М.В. Ольховік, Конституція України містить понад 20 правових норм, які безпосередньо чи опосередковано встановлюють інформаційні права та свободи людини і громадянина, або тією чи іншою мірою мають інформаційний характер, зокрема, право на:

– свободу від цензури (ст. 15 Конституції України);

– таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31 Конституції України);

– недоторканість особистого і сімейного життя (ст. 32 Конституції України);

– свободу думки і слова, на вільне вираження своїх поглядів і переконань (ст. 34 Конституції України);

– свободу віросповідання та світогляду (ст. 35 Конституції України);

– вільне володіння, користуватиння і розпорядження своєю власністю, результатами своєї інтелектуальної, творчої діяльності (ст. 41 Конституції України);

– вільний розвиток своєї особистості (ст. 23 Конституції України);

– повагу до гідності (ст. 28 Конституції України);

– свободу об'єднання (ст. 36 Конституції України);

– участь в управлінні державними справами (ст. 38 Конституції України);

– зібрання (ст. 39 Конституції України);

– звернення до органів державної влади та місцевого самоврядування (ст. 40 Конституції України);

– вільну літературну, наукову, художню, творчість (ст. 54 Конституції України);

– те, щоб знати свої права та обов'язки (ст. 57 Конституції України) та інші.

Отже, під інформаційними правами людини слід розуміти мати можливості, необхідні для задоволення інформаційних потреб її життєдіяльності та розвитку в конкретних умовах, що об'єктивно визначаються рівнем розвитку суспільства та інформаційно-комунікаційних технологій, забезпечуються соціально зумовленими обов'язками інших суб'єктів та охороняються публічною владою [89, с. 159].

Дослідження, проведені у попередніх підрозділах цієї роботи, дозволили сформувати наступний перелік інформаційних прав, які мають відношення і підлягають забезпеченню в системі кіберзахисту: свобода слова; право на доступ до інформації, у тому числі право на звернення; захист персональних даних; захист інформаційної безпеки; захист прав інтелектуальної власності; право на захист від кримінальних посягань у кіберпросторі.

Свобода слова – це право вільно виражати свої думки та погляди.

Загальні підходи до забезпечення свободи слова та її обмежень викладені у підрозділі 3.2 цієї дисертаційної роботи. Свобода слова в Інтернеті – це право людини вільно висловлювати, поширювати та отримувати інформацію та ідеї онлайн, без втручання тих чи інших суб'єктів, зокрема, держваи. Це право включає свободу дотримуватися власних поглядів, відсутність цензури в Інтернеті та мережевий нейтралітет. Однак це право не є абсолютним і може бути обмежене законом в інтересах національної безпеки, громадського порядку, здоров'я та захисту прав інших людей. Зокрема, у статті [91, с. 50-51] констатується, що свобода слова в Інтернеті регулюється, зокрема, статтею 10 ЄКПЛ, а також в України – статтею 34 Конституції України.

Так, у справі «Дельфі АС проти Естонії» ЄСПЛ наголосив на тому, що ризик шкоди, завданої повідомленнями в Інтернеті, для здійснення та користування правами і свободами людини, може бути вищим, ніж у пресі, оскільки «незаконні висловлювання», включаючи ворожі висловлювання та заклики до насильства, можуть розповсюджуватися у всьому світі за лічені секунди, а іноді залишаються постійно доступними в мережі [326].

У рішенні ЄСПЛ у справі «Савва Терентьєв проти Росії» Суд дійшов висновку про потребу в справах щодо порушення права на свободу вираження поглядів в Інтернеті оцінювати потенційний вплив Інтернет-видання, тобто сферу охоплення ним громадськості. Потенційний вплив інформації, опублікованої в Інтернеті на платформі чи у соціальній мережі з невеликою аудиторією, та інформації, опублікованої на часто відвідуваних і відомих веб-сторінках, відрізнятимуться [327].

У справі «Кілін проти Росії» Суд також наголосив на неабсолютності права на свободу вираження поглядів. У своїй позиції ЄСПЛ вказав, що Інтернет – один із основних засобів, за допомогою якого реалізується право на свободу вираження поглядів завдяки своїй доступності та здатності зберігати та передавати великі обсяги інформації. У 2009 році Р. Кілін завантажив відеоролик (нарізку кадрів) із фільму під назвою «Россия 88» та музичну композицію «Слава Руси» групи «Коловрат» у соціальній мережі

«Вконтакте». У матеріалах справи зазначено, що сюжет вказаного фільму висвітлює діяльність неонацистів (субкультура «скінхедів») у Російській Федерації. Музична композиція містила заклики до насильницьких дій, спрямованих на посилення національної ворожнечі. Вироком суду першої інстанції Р. Кіліна було засуджено до позбавлення волі за публічні заклики до екстремістської діяльності. Апеляційний суд змінив мотивацію рішення, вказавши, що дії засудженого було спрямовано на розпалювання міжетнічної ворожнечі, хоча на міру покарання це не вплинуло. Касаційний суд підтримав позицію апеляції.

На думку заявника, стаття 10 Конвенції не допускає кримінального переслідування за прояв симпатії до певної інформації чи ідей, висловлених у уривку з кінематографічного твору, зокрема, якщо така інформація чи ідеї не були заборонені на національному рівні. На думку ЄСПЛ, розпалювання розбрату між етнічними групами через заклики до насильства може завдати шкоди всім задіяним групам та іншим верствам населення. Суд погодився з висновками національних судів про те, що опубліковані відеоролик та пісня були не засобом власного художнього вираження чи сатиричного соціального коментаря заявника, а розпалюванням етнічної ворожнечі, проявом нетерпимості. ЄСПЛ також наголосив на тому, що поширення матеріалів подібного змісту в навіть нечисленній онлайн-групі однодумців зумовлює радикалізацію їхніх ідей. Отже, порушення права на свободу вираження поглядів не було [328].

Таким чином, обмеження свободи вираження поглядів в соціальних мережах є необхідним в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для охорони порядку або запобігання злочинам, для охорони здоров’я або моралі, зокрема, у разі протидії розповсюдженню закликів до насильства і національному протистоянню, що є прямими загрозами національній безпеці держави.

Тому обмеження, запроваджені в Україні, на російські Інтернет-канали, соціальні мережі та платформи, є виправданими в демократичному

суспільстві.

Варто зазначити, що у 2017 році було зібрано 25.359 підписів під петицією про скасування Указу про блокування російських соціальних мереж і сайтів [211]. У своїй відповіді тодішній Президент України П.О. Порошенко повідомив, що російський холдинг Mail.ru Group, до складу якого входять ВКонтакте, Мейл.ru, Одноклассники, а також група компаній Яндекс та деякі інші інтернет-компанії широко використовуються російськими спецслужбами для просування російської пропаганди і проведення спеціальних інформаційних операцій проти України та її громадян. Зокрема, вказані компанії сприяють спецслужбам росії у збиранні, зберіганні, використанні та поширенні інформації з обмеженим доступом – персональних даних та особистого листування громадян України. Навіть угоди про користування вказаними сервісами містять положення про згоду користувачів на автоматичну передачу до компанії (фактично – до країни-агресора та її спецслужб) будь-якої інформації про них, її узагальнення, обробку та передачу третім особам. Таким чином, українські користувачі російських мереж потрапляють під контроль спецслужб рф, які спочатку створюють необхідні умови для вербування, а потім використовують наших громадян у власних протиправних цілях. Значна кількість зареєстрованих у соціальних мережах осіб залучається російськими спецслужбами для вербування українців до агентурної мережі та організації каналів збору інформації про пересування техніки й особового складу ЗСУ, що беруть участь у проведенні антитерористичної операції на сході України. Контентне наповнення цих ресурсів мережі Інтернет також спрямоване на намагання маніпулювати суспільною свідомістю через поширення недостовірної, неповної та упередженої інформації, сприяння присутньому, на жаль, в Україні протестному антиукраїнському потенціалу, втягненню його в антинародні акції та масові заворушення, спрямовані на насильницьку зміну конституційного ладу й повалення державної влади, перешкоджання Україні на шляху до європейської спільноти, а тому загрожує інформаційній безпеці

держави.

У статті [344] автора цієї дисертаційної роботи розглянуті підходи до «м'якого» (добровільного) регулювання Інтернет-ресурсів, якщо вони хочуть отримати статус ЗМІ.

Зокрема, в абзаці четвертому п. 12 постанови Пленуму Верховного Суду України від 27.02.2009 № 1 «Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи» зазначено, що якщо недостовірна інформація, яка порочить честь, гідність чи ділову репутацію, розміщена в мережі Інтернет на інформаційному ресурсі, *зареєстрованому в установленому законом порядку як засіб масової інформації*, то при розгляді відповідних позовів судам слід керуватися нормами, що регулюють діяльність засобів масової інформації».

У рішенні від 05.05.2011 ЄСПЛ у справі «Редакція газети «Правоє дело» та Штекель проти України» розглянута ситуація, коли ця газета (головний редактор – Штекель Л.І.) передрукувала з Інтернету інформаційні матеріали, які згодом виявилися недостовірними. За це газета була притягнута до відповідальності. У зверненні до ЄСПЛ заявники посилалися на чинну у той час ст. 42 Закону України «Про друковані засоби масової інформації (пресу) в Україні», яка звільняла від відповідальності за поширення недостовірної інформації, отриманої від інших ЗМІ (презумпція достовірності інформації).

Розглянувши цю ситуацію, ЄСПЛ (по тексту рішення – Суд) прийшов до наступних висновків (виділено автором) [265]:

«*60. Суд зауважує, що зазначена публікація була дослівним відтворенням матеріалу, завантаженого із загальнодоступної Інтернет-газети...*

61. Українське законодавство, зокрема, Закон України «Про друковані засоби масової інформації (пресу) в Україні» надає журналістам імунітет від цивільної відповідальності за дослівне відтворення матеріалу,

опублікованого у пресі. Суд звертає увагу на те, що це положення у загальному плані відповідає його підходу до свободи журналістів поширювати висловлювання, зроблені іншими (наприклад, рішення від 23.09.1994 р. у справі «Йерзільд проти Данії»).

62. Проте відповідно до позиції національних судів такий імунітет журналістів не поширюється на відтворення матеріалу з Інтернет-джерел, які не зареєстровані згідно із Законом України «Про друковані засоби масової інформації (пресу) в Україні». У зв'язку з цим Суд зауважує, що на той час не існувало національних нормативних актів стосовно державної реєстрації Інтернет-видань...

64. Однак, беручи до уваги роль, яку відіграє Інтернет у контексті професійної діяльності засобів масової інформації, та його важливість для загального здійснення права на свободу вираження поглядів, Суд вважає, що відсутність на національному рівні достатньої законодавчої бази, яка б дозволяла журналістам використовувати отриману з Інтернету інформацію без остраху наразитися на санкції, серйозно перешкоджає пресі відігравати свою роль «сторожового пса суспільства». На думку Суду, повне виключення такої інформації зі сфери застосування законодавчих гарантій журналістських свобод може саме по собі спричинити неправомірне втручання у свободу преси, гарантовану статтею 10 Конвенції».

Отже, на думку ЄСПЛ, повинно бути запровадження правове регулювання Інтернет-ресурсів як ЗМІ, і це не тільки не обмежує свободи поширення інформації, а навпаки, підвищує рівень гарантій для користувачів цією інформацією. Натомість не можна не рахуватися із тим, що через електронні мережі поширення інформації може цілеспрямовано поширюватися недостовірна та/або прямо ворожа інформація («чорна») інформація, яка в наступному буде тиражуватися через легалізовані ЗМІ з метою її «відбілювання». Окремі випадки та механізми такого «відбілювання» наведені у публікації розробників даної теми [320].

Зокрема, Г. Почепцов [234] повідомляє, що Гліб Павловський,

представлений «Комсомольською правдою» (26.02.1999) як «ветеран інформаційних воєн», приділяє особливу увагу різним Інтернет-проектам, розглядаючи їх як ідеальний інструмент для запуску необхідних історій в масову свідомість. Він каже: «Традиційні ЗМІ відповідають за інформацію, яку вони поширюють. Чутки, що передаються через Інтернет, є анонімними. Але тоді газети та телебачення отримують можливість посилатися на Інтернет. Тобто відбувається справжнє відмивання так званої "чорної" інформації. Раніше цю "чорну" інформацію можна було зробити лише "сірою" – поширювати її в кулуарах, не більше. Тепер можна повністю відмити будь-яку "дезінформацію"».

О. Мітенко також наголошує, що відсутність механізмів державного контролю за розповсюдженням інформації через Інтернет-сайти спричинює швидке збільшення обсягу соціально-політичного контенту (анонімного, достовірність якого викликає сумніви, провокаційного та відверто незаконного), що дублюється традиційними вітчизняними ЗМІ із посиланням на Інтернет [212].

О. Голуб повідомляє, що багато експертів наголошують на небезпеці використання соціальних мереж як джерела інформації, оскільки так звані нові ЗМІ є одним із найпоширеніших способів розповсюдження неправдивої інформації та фейків. Зазначається, що в останні роки все більше класичних ЗМІ використовують соціальні мережі як першоджерела. Потім ця неперевірена інформація потрапляє на телебачення і поширюється на масову аудиторію. Немає сумнівів щодо небезпеки поширення неправдивої інформації в контексті інформаційної війни, яка є частиною гібридної війни, яку росія веде проти України. Це впливає не тільки на цивільне населення України, але й демобілізує військових, які захищають свою країну. Всі ці технології вже давно перевірені. Дослідження показують, що люди розглядають найважливіші теми та проблеми, які активно висвітлюються та обговорюються у ЗМІ. Таким чином, можна цілеспрямовано скорегувати сприйняття суспільства – фактично, сформувати нову реальність [105].

За даними веб-сайту StopFake, фальшиві новини поширюються в основному російськими ЗМІ. Тому журналістам слід бути особливо обережними, перевіряючи інформацію із соціальних мереж, щоб не стати носіями фейків. Журналіст несе відповідальність за перевірку та обробку отриманої інформації. Власне, цим традиційні ЗМІ повинні відрізнятися від соціальних мереж та сайтів агрегаторів [105].

Тому прирівнювання правового статусу електронних засобів поширення інформації до «звичайних» ЗМІ повинно супроводжуватися і підвищенням рівня відповідальності таких електронних засобів поширення інформації за порушення законодавства у сфері ЗМІ.

Згідно ч. 1 ст. 117 Закону України «Про медіа» [56], суб'єкти у сфері медіа та їх працівники не несуть відповідальності за поширення інформації, забороненої цим Законом, а також інформації, що не відповідає дійсності, порушує права і законні інтереси особи, якщо ця інформація, зокрема, є дослівним або у переказі без спотворення суті відтворенням матеріалів, опублікованих іншим *зареєстрованим* медіа, або точним за змістом відтворенням оригінальних матеріалів іноземного медіа з посиланням на них.

Отже, інформація з Інтернету, отриманого від ресурсу, який не зареєстрований як ЗМІ, не може апріорі вважатися достовірною, що відповідає позиції ЄСПЛ і Верховного Суду України.

Окремо слід розглянути питання так званого «мережевого нейтралітету», який мало досліджений в українській науковій літературі.

Мережевий нейтралітет (англ. *network neutrality*, NN) – це принцип, згідно з яким провайдери телекомунікаційних послуг не віддають переваги одному цільовому призначенню перед іншим, або одним класам додатків (наприклад World Wide Web) перед іншими (наприклад, онлайн-ігри або IP-телефонія). Це означає, що провайдер не може дискримінувати користувачів, надаючи одним вигідніші умови доступу до контенту, ніж іншим; не має права втручатися в зміст, походження або призначення даних. Всі дані повинні оброблятися однаково, незалежно від того, хто їх надсилає або хто їх

отримує. Провайдер не може, наприклад, навмисно уповільнювати роботу певного сервісу, щоб надати перевагу власному сервісу або сервісу, з яким він має договір. Скасування мережевого нейтралітету може дозволити провайдерам створювати платні «швидкісні коридори» для певних компаній, а також блокувати або обмежувати доступ до конкурентів чи небажаних для них сайтів. Це може вплинути на конкуренцію, свободу слова та доступ до інформації в мережі.

У жовтні 2015 Європарламент ухвалив закон, що набрав чинності 30.04.2016. Інтернет-провайдери у ЄС не повинні блокувати чи навмисно уповільнювати інтернет-трафік для певних сайтів і осіб, усі повнолітні користувачі мусять мати рівний доступ до вебсайтів. Обмеження можуть запровадити тільки у випадку, якщо це потрібно для виконання судового рішення, дотримання законів, протистояння кібер-атакам. Водночас операторам дозволено пропонувати спеціальні послуги, але це не повинно зашкодити якості Інтернету для інших користувачів. 30.08.2016 Орган європейських регуляторів електронних комунікацій опублікував рекомендації, що роз'яснюють принципи, якими повинні керуватися європейські телекомунікаційні компанії при обробці даних. Ця публікація є зводом принципів мережевого нейтралітету ЄС, який зайняв жорстку позицію в цьому питанні.

Право на доступ до інформації – це можливість отримувати інформацію, що перебуває у володінні суб'єктів владних повноважень, та інформацію, яка становить суспільний інтерес. Це також право кожної людини вільно збирати, зберігати, використовувати та поширювати інформацію, яке гарантується Конституцією України (стаття 34) та законами. Це право може бути реалізоване через отримання інформації за запитами або шляхом її систематичного оприлюднення розпорядниками інформації.

Міністерство юстиції України надало узагальнююче роз’яснення від 03.05.2012 про право на доступ до інформації як елемент правового статусу особи. В Роз’ясненні зазначається, що це право реалізується згідно Законам

України «Про звернення громадян» [40], «Про інформацію» [36], «Про доступ до публічної інформації» [48] та іншими нормативно-правовими актами.

Закон «Про інформацію» регулює відносини, пов'язані зі створенням, збиранням, одержанням, зберіганням, використанням та поширенням інформації. Він гарантує право на інформацію, але встановлює заборону на її використання для розпалювання ворожнечі, закликів до повалення конституційного ладу та інших протиправних дій. Основні положення Закону:

– гарантується право на інформацію – кожен має право на інформацію, що означає можливість вільного одержання, використання, поширення, зберігання та захисту інформації;

– забезпечується захист інформації – законодавство передбачає комплекс заходів (правових, адміністративних, організаційних, технічних) для забезпечення збереження, цілісності та належного доступу до інформації;

– неприпустимість зловживання – забороняється використовувати інформацію для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства та розпалювання міжетнічної, расової чи релігійної ворожнечі;

– обмеження доступу – інформація з обмеженим доступом поділяється на конфіденційну, таємну та службову. До конфіденційної, наприклад, належить інформація про фізичну особу, доступ до якої може бути обмежено за її згодою, крім випадків, передбачених законом.

– відповідальність – порушення законодавства про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність відповідно до законодавства України.

Закон України «Про звернення громадян» – це нормативно-правовий акт, який регулює порядок подання та розгляду звернень громадян до органів державної влади, місцевого самоврядування, установ та посадових осіб. Закон визначає види звернень (скарги, заяви, пропозиції), порядок їх подання

(письмово, усно, електронно), а також терміни розгляду. Згідно Закону, кожен громадянин має право звертатися до органів державної влади, місцевого самоврядування, підприємств, установ та організацій із зауваженнями, скаргами, пропозиціями, заявами або клопотаннями.

Закон «Про доступ до публічної інформації» передбачає права кожної особи звернутися із запитом на інформацію до розпорядника, незалежно від того, чи стосується ця інформація її особисто чи ні, та без пояснення причини запиту. Розпорядники інформації мають обов'язок оприлюднювати її на офіційних сайтах, у друкованих виданнях, на інформаційних стендах тощо.

Доступ до інформації може бути обмежений, якщо це необхідно для:

– національної безпеки, територіальної цілісності або громадського порядку;

– охорони здоров'я населення;

– захисту репутації або прав інших осіб;

– запобігання розголошенню конфіденційної інформації.

Зокрема, обмеження особи щодо доступу до інформації може бути реалізоване для забезпечення безпеки самої цієї особи, враховуючи необхідність забезпечення її когнітивної безпеки, огородження її від інформаційно-психологічних впливів, що можуть викликати зрушення в цінностях, життєвих позиціях, орієнтирах, світогляді особистості, налаштувати її проти суспільства і держави, ослаблення морального духу населення, схиляння її до відмови від захисту Батьківщини.

Таким чином, заборона на отримання інформації, зокрема, від телевізійних каналів 112, NewsOne та Zik шляхом припинення їх трансляції є цілком прийнятною в контексті пункту 2 статті 10 ЄКПЛ.

Так, на думку С. Фурси, українського інвестиційного банкіра, фінансового експерта, публіциста, «удар по 112, Newsone, Zik не має нічого спільного з атакою свободу слова. Російська пропаганда знову підмінятиме поняття. В принципі вона завжди це робить. Вони прикидаються журналістами і намагаються руйнувати демократичне суспільство,

користуючись досягненнями цього суспільства. При чому чітко знищуючи вдома цю саму свободу слова. Телеканали Медведчука були не про свободу слова. Чи не про стандарти журналістики. Це була чиста вода антиукраїнська пропаганда. Саме антиукраїнська [134].

Варто зазначити, що відносно телеканалів 112, NewsOne і ZiK серед експертів немає розбіжностей з приводу того, що дані канали є провідниками проросійського інформаційного впливу. Зокрема, за коментарями «Deutsche Welle» (DW), патріотично налаштована частина українського суспільства підтримує санкції проти проросійських каналів, прокремлівська опозиція в Раді називає їх війною зі свободою слова [248]. На думку патріотично налаштованої більшості політиків і громадських діячів, заблоковані телеканали стали рупором проросійської інформаційної політики проти України на тлі війни в Донбасі, яка триває вже сьомий рік[9].

Голова правління громадської організації «Інтерньюз-Україна» К. Квурт не згоден з тими, хто звинувачує українську владу в наступі на свободу слова. Він вважає, що введення в дію санкцій, що призвело до закриття телеканалів, – це «спроба держави захистити українську політичну націю від ворожої пропаганди». Демократичні суспільства усього світу все ще безсилі перед тим, що путінський авторитарний режим використовує свободу слова для поширення дезінформації в якості елемента гібридної війни, – говорить Квурт.

Тодішній Секретар РНБО О. Данілов, коментуючи критику з боку деяких журналістських організацій IFJ та EFJ, наголосив [118], що рф напала на Україну, і Україна не може терпіти у себе в тилу проросійську пропаганду. Важко уявити, що під час Другої світової війни у Франції, Великобританії чи США працювали б філій фашистських газет і радіостанцій [118].

Таким чином, «свобода слова» не може бути абсолютною.

Обґрунтування законності припинення діяльності телеканалів 112, NewsOne і ZiK в контексті норм ЄКПЛ і рішень ЄСПЛ наводиться також у

[9] Публікація 2021 року

статті [76].

Як зазначалося у підрозділі 2.3 цієї дисертації, одним із засобів маніпулятивного впливу на Інтернет-користувачів є створення фейкових сайтів (фішинг). Фішинг (англ. phishing) – один з методів шахрайства з використанням соціальної інженерії, який полягає в тому, що зловмисники створюють фішингові (підроблені) сторінки, що імітують офіційні сторінки банків, інтернет-магазинів, платіжних сервісів, тощо. Разом із тим, в умовах агресивної інформаційної війни рф проти України та політичного Заходу організатори російських/проросійських пропагандистських кампаній вдаються до створення фейкових сайтів, які маскуються під відомі та авторитетні новинні сайти, тобто типовий фішинг у сфері інформаційної політики. Наприклад, в ефірі Ізраїльського радіо 22.09.2023 року було повідомлено [204], що в ізраїльському інформаційному просторі «нав'язливо з'являються якісь фейкові сайти, які ***маскуються під ізраїльські сайти***, де публікуються на івриті фейкові статті, написані нібито відомими ізраїльськими журналістами. І там мова йде про те, що українці вбивали євреїв під час Голокосту, або про те, що ми, ізраїльтяни, не повинні взагалі говорити про Україну, це не наша справа, вони самі розберуться, навіщо туди лізemo, ми маємо займатися своїми проблемами і таке інше в тому ж дусі».

У публікації [225] повідомляється, що французька влада виявила цифрову кампанію з маніпулювання інформацією, яку ведуть проти Франції із залученням російських виконавців; у ній брали участь державні або пов'язані з російською державою структури шляхом поширення неправдивої інформації. Кампанія була націлена на сайти низки французьких загальнонаціональних видань, а також на сайт Міністерства закордонних справ та інші урядові портали шляхом створення дзеркальних сторінок. «Залучення російських посольств і культурних центрів, які брали активну участь у розширенні цієї кампанії, зокрема через свої інституційні акаунти в соціальних мережах, є новою ілюстрацією гібридної стратегії, яку росія реалізує, щоб підірвати умови для спокійних демократичних дебатів, а відтак

– для підриву наших демократичних інституцій», – йдеться в заяві МЗС Франції. У Франції жертвами російської операції стали щонайменше чотири щоденні газети: Le Parisien, Le Figaro, Le Monde і 20 minutes. Агентство France-Presse зазначає, що, крім згаданих французьких видань, російська кіберкампанія дезінформації зачепила німецькі Frankfurter Allgemeine Zeitung, Der Spiegel, Bild і Die Welt, а також низку ЗМІ Італії. Ця операція є частиною тривалої і задокументованої практики впливу на суспільну думку, що проводиться росією, йдеться у звіті французького МЗС. Після вторгнення в Україну рф робить ставку на фейкові новини, щоб підірвати суспільну підтримку українців на Заході.

За власними спостереженнями автора, російські/проросійські пропагандисти маскують фейкову інформацію під зовнішнє оформлення відомих та авторитетних українських інформаційних сайтів, наприклад, «Обозреватель», УНІАН (додаток Б12).

Так, на сайті, замаскованому під сайт «Обозреватель», розміщена фейкова публікація «Ховаємо самі себе». В ній йдеться про те, що наші західні союзники передають Україні касетні боєприпаси, щоб максимально забруднити українські землі. Це цілком корелює і з іншими діями та задумами союзників, а з ними – і нашої київської влади. «Не з'їсти – то понадкушувати», не відвоювати території, то хоча б їх загадити, разом із тими, що можуть теж відійти до противника». Зрозуміло, що за цим стоїть прагнення дискредитувати західних союзників і зірвати їх військову допомогу Україні.

На сайтах, замаскованих під сайт «Обозреватель», розміщені фейкові публікації «Призовуть і хворих і убогих» та «У стрій стануть усі» розміщені брехливі публікації про нібито тотальну мобілізацію в армію. Стверджується, що нібито 16-річні діти проходитимуть всю необхідну підготовку. Що, безумовно, свідчить про одне: рано чи пізно вони також відправляться гинути в черговому "м'ясному штурмі"... Дуже нагадує Гітлер'югенд: останніми місяцями фюрер від безнадії почав відправляти на фронт дітей.

Мабуть, у нас ситуація нічим не краща». При цьому, вочевидь, українській армії приписується російська тактика м’ясних штурмів.

На сайтах, замаскованих під сайт УНІАН, розміщені брехливі публікації про нібито конфлікти в середені української влади і української влади з адміністрацією Президента США Байдена, а також про величезні, нічим і ніким не підтверджені втрати української армії

Зрозуміло, що за цим стоїть прагнення дискредитувати західних союзників і зірвати їх військову допомогу Україні. Разом із тим, існує низка ознак, які дозволяють вирізняти фейкові сайти: повторювання дат та авторів, посилання на інші сайти и неактивні сайти тощо.

В монографії [268, с. 200] різновидом прав на кібербезпеку назване право на захист від негативного інформаційного впливу та від поширення протиправного контенту (зокрема, і в Інтернеті), що може забезпечуватися автоматизованою інформаційною системою ведення й використання бази даних про сайти.

Захист персональних даних – це право контролювати використання та поширення своєї особистої інформації.

Як зазначено вище, Стратегія інформаційної безпеки від 15.10.2021 р. [28] визначає, зокрема, цілі та завдання, спрямовані на *захист персональних даних*.

Згідно пункту 3 ч. 1 ст. 2 Закону № 2163-VIII [51], застосування законодавства у сфері кібербезпеки … здійснюються зокрема, з додержанням принципів: забезпечення захисту прав користувачів інформаційно-комунікаційних систем, …, споживачів електронних комунікаційних послуг, у тому числі прав на невтручання у приватне життя і *захисту персональних даних*.

Відносини із захисту персональних даних регулюються Законом від 01.06.2010 р. № 2297-VI «Про захист персональних даних» [47]. Закон регулює відносини, пов'язані з обробкою персональних даних, з метою захисту основоположних прав і свобод людини, зокрема – на

недоторканність приватного життя. Він поширюється як на автоматизовану, так і на неавтоматизовану обробку персональних даних. Контроль за додержанням законодавства покладено на Уповноваженого ВРУ з прав людини.

Ключовими аспектами закону є:

– об'єкт захисту – захист надається персональним даним, які обробляються в базах даних;

– обмеження доступу – персональні дані за режимом доступу є інформацією з обмеженим доступом;

– заборона обробки – закон забороняє обробку чутливих персональних даних, таких як інформація про расове/етнічне походження, політичні/релігійні переконання, членство в партіях/спілках та судимості, якщо немає законних підстав;

– кримінальна відповідальність – незаконне збирання, зберігання, використання або поширення конфіденційної інформації може призвести до кримінальної відповідальності згідно зі статтею 182 КК України;

– знищення даних – персональні дані підлягають знищенню у випадках, передбачених законом: закінчення строку зберігання, припинення правовідносин або за рішенням суду;

– сфера дії – закон застосовується до всіх видів діяльності з обробки персональних даних, які здійснюються повністю або частково автоматизовано.

В ЄС діє Регламент Європейського Парламенту і Ради ЄС 2016/679 від 27.04.2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних [10]. Європейський Загальний регламент захисту персональних даних (GDPR) – це закон ЄС, який встановлює правила щодо збору, зберігання та обробки персональних даних осіб у межах ЄС. Його мета – гармонізувати законодавство про захист даних по всьому Союзу, модернізувати закони з урахуванням технологічного прогресу, посилити права громадян та збільшити вимоги до відповідальності

організацій, які обробляють дані.

Регламент, зокрема, констатує, що право на захист фізичних осіб під час опрацювання персональних даних є фундаментальним правом, що також гарантовано Хартією фундаментальних прав ЄС (стаття 8(1)), а також у Договорі про функціонування ЄС (стаття 16(1)).

Як висновується у стітті [319], одним із співавторів якої є дисертант, Закон України від 01.06.2010 р. № 2297-VI «Про захист персональних даних» [47] прийнятий до прийняття регламенту GDPR, тому назріла необхідність удосконалити деякі положення Закону з метою приведення його у відповідність із регламентом GDPR. Так, на відміну від Закону України від 01.06.2010 р. № 2297-VI «Про захист персональних даних» [47], Європейський Регламент містить визначення «персональні дані» – це будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими відомостями як ім'я, дані про місцеперебування, ідентифікаційний номер, онлайн-ідентифікатор (за окремим ідентифікатором чи їх сукупністю), що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи.

Пропонується внести це визначення в Закон України «Про захист персональних даних».

Основні положення та цілі GDPR

– **з**ахист даних: забезпечення однакового рівня захисту персональних даних для всіх громадян та резидентів ЄС, а також для експорту персональних даних за межі ЄС;

– права громадян**:** надання громадянам більшого контролю над своєю особистою інформацією;

– гармонізація законодавства**:** уніфікація правил щодо захисту даних у всіх державах-членах ЄС та Європейської економічної зони (ЄЕЗ);

– відповідальність: встановлення чітких вимог та обов'язків для компаній та організацій щодо збору, зберігання та управління особистими даними, а також для контролерів та обробників даних;

– прозорість: вимагає більшої прозорості щодо того, як, ким і для чого використовуються дані;

– технологічна адаптація: модернізує законодавство для відповідності сучасним технологіям та захисту в цифрову епоху;

– сфера застосування: поширення як на компанії в ЄС, так і на ті, що знаходяться за межами ЄС, але пропонують товари чи послуги резидентам ЄС або відстежують їхню поведінку.

В монографії [268, с. 200] різновидом прав на кібербезпеку названий захист персональних даних на основі здійснення особою своєї цифрової ідентичності. Людина отримує свій унікальний ідентифікатор (код), котрий є одним із засобів захисту інформації від несанкціонованого доступу, що дає змогу безпечно звертатися до органів державної влади, віддалено здійснювати фінансові операції, надсилати користувачам авторизовані повідомлення, провадити інші різноманітні дії в кібернетичному середовищі.

Захист інформаційної безпеки – це право на захист від несанкціонованого доступу до особистої інформації та можливість регулювати цей доступ.

Захист інформаційної безпеки – це сукупність заходів та засобів для забезпечення цілісності, конфіденційності та доступності інформації від природних або штучних загроз. Він включає фізичний та кіберзахист, управління доступом, використання антивірусного програмного забезпечення, брандмауерів, регулярне оновлення систем, створення резервних копій та дотримання політики безпеки.

Основні принципи та цілі

– цілісність – забезпечення точності та повноти даних, а також захист від несанкціонованої зміни;

– конфіденційність – забезпечення доступу до інформації лише

авторизованим користувачам;

– доступність – гарантування безперешкодного доступу до інформації авторизованим користувачам, коли це необхідно;

– автентичність, відстежуваність, неспростовність та надійність – ці властивості також можуть враховуватися для посилення безпеки.

Згідно з Д. Шацом, Дж. Волл і Р. Башроушу, кібербезпека (вона ж комп’ютерна безпека і безпека інформаційних технологій) – це захист комп’ютерних систем і комп’ютерних мереж від розкриття даних, пошкодження та крадіжки їх обладнання, програмного забезпечення або електронної інформації, а також від порушення або неправильного спрямування наданих ними послуг [349, с. 56-57].

Також можна говорити і про те, що кібербезпека – це використання сучасних технологій, процесів і засобів контролю з метою захистити комп’ютерні системи та мережі, програми, пристрої і дані від кібернетичних атак, а також з метою зниження ризику здійснення кібератаки [350].

В монографії [304] розглянуті можливі варіанти шкоди, яка може бути завдана особі внаслідок порушення її інформаційної безпеки в інформаційно-комунікаційній системі [304, с. 34-35]: копіювання комп'ютерної інформації (повторювання та стійке збереження інформації на іншому носієві); знищення комп’ютерної інформації (стирання її у пам'яті електронно-обчислювальної машини); модифікація комп’ютерної інформації (несанкціоноване внесення будь-яких змін у електронні дані); блокування комп’ютерної інформації (штучне утруднення доступу аутентифікованих користувачів, у тому числі власникі інформації, до цієї інформації, не пов'язане з її знищенням); обман (навмисне спотворення або приховування істини з метою введення зацікавлених осіб в оману, зокрема нав'язування хибної інформації).

Пропонуються наступні рекомендації для підвищення ступеня інформаційної безпеки:

– використання надійних паролів. Пароль (фр. parole – слово) – умовне

слово або набір символів, призначений для підтвердження особи або повноважень. Для входу в різні комп'ютерні системи використовується комбінація з двох наборів символів – реєстраційного імені користувача (логіна) та пароля. Здатність паролю протистояти атакам характеризує захищеність паролю й визначається кількома параметрами: довжина паролю – сукупна кількість символів парольної фрази; чим довший пароль, тим тяжче його атакувати; використання прописних літер: з погляду криптографії велика й мала літери є різними символами; використання цифр: наявність у паролі чисел також зміцнює його, адже в такому випадку для атаки доведеться використовувати не лише абетку, але й цифри; використання інших знаків: йдеться, зокрема, про знак оклику, знак питання, нижнє підкреслення, равлик (@), дефіс, знак долара, амперсанд (&) тощо [227, с. 4]. Рекомендується створювати складні та унікальні паролі для кожного сервісу та змінювати їх регулярно;

– регулярне оновлення програмного забезпечення**:** операційної системи та всі програми;

– використання антивірусного програмного забезпечення та брандмауера;

– уникнення відкриття підозрілих електронних листів, завантаження неперевіреного вмісту та переходів за сумнівними посиланнями;

– активація двофакторної аутентифікації – це додатковий рівень безпеки для важливих облікових записів. Двофакторна аутентифікація (2FA) – це метод безпеки, який вимагає двох різних способів підтвердження особи для доступу до облікового запису, що робить його більш захищеним, ніж просто пароль. Цей додатковий рівень захисту ускладнює несанкціонований доступ, навіть якщо зловмисник заволодів паролем;

– створення резервних копії, щоб уникнути втрати даних;

– використання тільки ліцензійних та офіційних програм.

Захист прав інтелектуальної власності в мережі Інтернет – це система правових, технічних і організаційних заходів, спрямованих на

попередження, виявлення та припинення порушень авторських і суміжних прав, прав на торговельні марки, патенти, промислові зразки тощо в онлайн-просторі.

Форми порушень в Інтернеті: Інтернет-піратство (цифрове піратство) – незаконному розповсюдженні інтелектуальної власності в Інтернеті [137, 177] без дозволу автора або іншої особи, яка має авторське право та/або суміжні права, та/або без виплати винагороди за використання творів у встановленому законом порядку; плагіат – копіювання текстів, фото, статей без дозволу і їх поширення під чужим іменем, у тому числі – в перекладі еа іншу(і) мову(и) [57, ст. 53]; кіберсквотинг – реєстрація доменів, схожих на відомі бренди [266]; незаконне використання торговельних марок у рекламі чи доменах [229]; неліцензійне використання програмного забезпечення.

Право інтелектуальної власності в мережі Інтернет охоплює захист авторських прав на контент (тексти, фото, музика, відео, програми, сайти); прав на торгові марки, патенти на винаходи та промислові зразки, логотипи, брендові зображення, що використовуються онлайн; комп’ютерні програми та бази даних; доменні імена (часто розглядаються як об’єкт, пов’язаний із торговельними марками). Захист реалізується як неюрисдикційно (самостійні дії правовласника), так і юрисдикційно (звернення до державних органів або суду). Ключовими аспектами є наявність доказів авторства (навіть через неофіційні методи, як-от відправка на власну адресу поштою) та реєстрація прав, особливо для торгових марок та патентів.

Як зазначає В. Філінович [340], у цифрову епоху інтелектуальна власність стикається з новими вразливостями. Хоча матеріальна власність може бути фізично захищена, інтелектуальна власність вимагає складних правових та технологічних гарантій, особливо в кіберпросторі. Швидкісне зростання кількості цифрового контенту в поєднанні із глобалізованим доступом та розповсюдженням посилило проблему забезпечення ефективного захисту прав інтелектуальної власності. Існуючі моделі правозастосування часто не справляються з транскордонними порушеннями

та швидким поширенням несанкціонованого контенту в Інтернеті [340, с. 159].

У своїй дисертаційній роботі В. Філінович [319] висновує, що проблема забезпечення дотримання права інтелектуальної власності у кіберпросторі ускладнюється швидким зростанням кількості інтелектуальних напрацювань, у той час як правове регулювання відстає від нових викликів і ризиків. Тому законодавство потребує удосконалення з урахуванням міжнародного досвіду та необхідності дотримання балансу між інтересами споживачів цифрових активів і правовласниками. Транскордонний характер кіберпростору ускладнює визначення приналежності до певної юрисдикції та суб'єктів правопорушень, що негативно позначається на забезпеченні дотримання прав інтелектуальної власності. «Віртуальність» інтелектуальної власності не применшує (й не рідко підвищує) її комерційну цінність як актива, а тому захист даного актива має забезпечуватися також на основі основоположних засад – принципів, зокрема, принципів права власності на інтелектуальну власність, примусового ліцензування, справедливої поведінки, балансу прав правовласника та громадськості, а також гармонізації як взаємної узгодженості та підпорядкування єдиній взаємно відповідній системі нормативних інструментів та стандартів. Завдяки останньому принципу можна буде досягти правової одноманітності в усьому світі, що, відповідно, позитивно впливатиме на бажання творців активізувати свою творчоінноваційну діяльність [319, с. 24].

Рекомендуються наступні технічні способи захисту прав інтелектуальної власності в мережі Інтернет: використання цифрових водяних знаків (watermark) [365]; DRM (Digital Rights Management) – технології контролю копіювання контенту [365]; системи моніторингу порушень (наприклад, Content ID у YouTube [331]).

Право на захист від кримінальних посягань у кіберпросторі – це гарантоване державою право кожної особи на безпеку, недоторканність її цифрової інформації, персональних даних, майна й честі від злочинних дій,

що здійснюються з використанням інформаційно-комунікаційних технологій. Це право гарантується Конституцією України. Захист цього права регулюється Кримінальним кодексом України, низкою законів України, а також Конвенцією про кіберзлочинність.

Основні види кримінальних посягань у кіберпросторі: несанкціонований доступ до комп'ютерних систем, баз даних або мереж (хакерство); шкідливе програмне забезпечення (віруси, трояни, ботнети); кібершахрайство – крадіжка грошей через фішинг, підроблені сайти, електронні платформи; кібербулінг та кіберпереслідування; поширення незаконного контенту (дитяча порнографія, терористичні матеріали, мова ненависті); порушення авторських прав у мережі; маніпуляції з криптовалютами та фінансовими системами.

Як зазначає С.Я. Лихова, ефективне забезпечення інформаційної безпеки правоохоронними органами передбачає пошук нових способів та форм її забезпечення, горизонтальну та вертикальну взаємодію на міжнародному та внутрішньодержавному рівнях, розроблення відомчих нормативно-правових актів, що регулюють цю діяльність, та їх юридичний аналіз. Основне завдання правоохоронних органів у цій галузі полягає у забезпеченні захисту прав та інтересів громадян в інформаційному просторі та протидії посяганням на інформаційну безпеку [190, с. 105-106].

Ключові напрямки захисту прав: кіберзахист – захист комп'ютерних систем, мереж та даних від несанкціонованого доступу, атак або руйнування; кібероборона – комплекс заходів, спрямованих на захист суверенітету та обороноздатності держави в кіберпросторі, включаючи захист від збройних конфліктів.

Таким чином, право на захист від кримінальних посягань у кіберпросторі – це важлива складова права на безпеку особи в цифрову епоху. Воно передбачає як державний, так і приватний рівень захисту, вимагає постійної взаємодії між державою, суспільством і міжнародними структурами.

Висновки до Розділу 3

Вперше системно розглянута сукупність безпекових стратегій, прийнятих в Україні протягом 2020-2021 рр., зокрема: Стратегія національної безпеки України від 14.09.2020 р.; Стратегія інформаційної безпеки від 15.10.2021 р.; Стратегія кібербезпеки України від 14.05.2021 р. Ключовою у системі наведених безпекових Стратегій є Стратегія національної безпеки України. Цей документ є дороговказом для розробки галузевих стратегій розвитку. Прийняті Стратегії свідчать про серйозну безпекову роботу української влади напередодні розширення агресивних дій рф проти України, вони є логічно взаємопов'язаними документами, реалізація яких ґрунтується на вимогах Стратегії національної безпеки України, а також на застосуванні механізмів забезпечення інформаційної безпеки і кібербезпеки України. В цьому контексті слід зазначити, що українська система безпекових стратегій побудована за моделлю НАТО та ЄС – НАТО розглядає інформаційну безпеку (information security) і кіберзахист (cyber defence) як єдиний операційний домен. ЄС у «Стратегії кібербезпеки для цифрового десятиліття» («Cybersecurity Strategy for the Digital Decade») (2020) також наголошує на взаємозалежності інформаційної стійкості, цифрового суверенітету та кіберзахисту. Отже, наша держава має правові засоби протидії інформаційним атакам.

В Стратегії кібербезпеки України важлива роль приділяється кіберзагрозам саме в інформаційній сфері. Розробники Стратегії кібербезпеки погоджуються, що засоби кібербезпеки захищають не тільки апаратні і програмні засоби, але й інформацію, що там обробляється. Кібербезпека – технічна і технологічна основа інформаційної безпеки.

Встановлено, що законодавче правое регулювання сутності і змісту безпекових Стратегій визначається Законом Укрїни «Про національну безпеку України». Разом із тим також встановлено, що такі безпекові Стратегії, як Стратегія зовнішньополітичної діяльності України, Стратегія

інформаційної безпеки, Стратегія забезпечення державної безпеки, Стратегія енергетичної безпеки цим Законом не регулюються і в Законі не згадуються, хоча сам Закон розглядає ці види безпек складовою частиною національної безпеки. Запропновано імплементувати вказані Стратегії в Закон «Про національну безпеку України».

Прийняття Закону України від 16.12.2020 року «Про електронні комунікації» є імплементацією Директиви Європейського Парламенту і Ради ЄС 2018/1972 від 11.12.2018 року про запровадження Європейського кодексу електронних комунікацій.

З точки зору конституційного принципу гарантій свободи думки і слова, права на вільне вираження своїх поглядів і переконань обіг інформації в інформаційно-комунікаційних системах, зокрема, в Інтернеті, підкоряється принципу, відповідно до якого такі свободи не можуть бути безмежними. Проблема встановлення меж свободи самовираження, з одного боку, і допустимості її обмежень, з іншого боку особливо гостро виникає внаслідок практичних потреб обмеження ворожих інформаційно-психологічних впливів, що є особливо гострим саме в інформаційно-комунікаційних системах у зв’язку із особливостями їх можливостей з точки зору доступу до аудиторії (адресатів ворожих думок) – широта охоплення аудиторії, швидкість поширення інформації, відносно низька трудомісткість і вартість її виготовлення. Зазначене надає підстави для обмежень державою поширення телевізійного контенту і Інтернет-мереж. В умовах агресивної інформаційної війни рф проти України керівництво країни було вимушене вдатися до певних обмежень в інформаційно-комунікаційному середовищі: заборона російських соціальних мереж і сайтів (Указ Президента України від 15.05.2017 року № 133/2017 з подальшим продовженням заборони Указом Президента України від 14.05.2020 року № 184/2020; запровадження санкцій проти засобів масової інформації (Указ Президента України від 02.02.2021 року № 43/2021) із забороною їх трансляції. У розділі наведено обґрунтування правомірності цих рішень в контексті частини 2 статті 10

ЄКПЛ, а також частини 3 статті 34 Конституції України.

Досліджені дії російських/проросійських пропагандистів щодо маскування фейкової інформації під зовнішнє оформлення відомих та авторитетних українських інформаційних сайтів, наприклад, «Обозреватель», УНІАН. Наведені приклади фактичних фейкових повідомлень (сайтів).

Запропоноване поняття «презумпція достовірності інформації», під якою розуміється відсутність необхідності додатково перевіряти достовірність інформації, розміщеної в легалізованих (зареєстрованих) ЗМІ. ЄСПЛ не вважає прийняття національних нормативних актів щодо державної реєстрації Інтернет-видань порушенням свободи слова. Навпаки, Європейський Суд з прав людини висновував, що принцип презумпції достовірності інформації, яка розміщена в Інтернеті, може бути застосований тільки щодо інформації, розміщеної в легалізованих (зареєстрованих) ЗМІ. За умови належного правового регулювання (у відповідності із вимогами ЄКПЛ) навпаки, така реєстрація підсилює гарантії діяльності журналістів і розширює коло інформації, до якої можна застосовувати презумпцію достовірності, – при одночасному підвищенні відповідальності таких Інтернет-видань за поширення неналежної інформації.

Запропонована авторська структура інформаційних прав громадян. Виходячи з того, що «інформаційні права» не тотожні «праву на інформацію», запропонована і розглянута наступна структура інформаційних прав: свобода слова (право вільно виражати свої думки та погляди); право на доступ до інформації, у тому числі право на звернення (можливість отримувати інформацію, що перебуває у володінні суб'єктів владних повноважень, та інформацію, яка становить суспільний інтерес); захист персональних даних (право контролювати використання та поширення своєї особистої інформації); захист інформаційної безпеки (право на захист від несанкціонованого доступу до особистої інформації та можливість регулювати цей доступ), захист прав інтелектуальної власності (захист авторських прав на контент), право на захист від кримінальних посягань у

кіберпросторі (право вимагати від уповноваженої органів держави запобігання, виявлення, припинення та розкриття кіберзлочинів).

Свобода слова в Інтернеті – це право людини вільно висловлювати, поширювати та отримувати інформацію та ідеї онлайн, без втручання з боку держави чи інших суб'єктів. Це право включає свободу дотримуватися власних поглядів, відсутність цензури в Інтернеті та мережевий нейтралітет. Однак це право не є абсолютним і може бути обмежене законом в інтересах національної безпеки, громадського порядку, здоров'я та захисту прав інших людей. Так, у справі «Дельфі АС проти Естонії» Європейський Суд з прав людини наголосив на тому, що ризик шкоди, завданої повідомленнями в Інтернеті, для здійснення та користування правами і свободами людини, може бути вищим, ніж у пресі, оскільки «незаконні висловлювання», включаючи ворожі висловлювання та заклики до насильства, можуть розповсюджуватися у всьому світі за лічені секунди, а іноді залишаються постійно доступними в мережі.

Вперше введений у правовий науковий оборот поняття «мережевий нейтралітет» – це принцип, згідно з яким провайдери телекомунікаційних послуг не віддають переваги одному цільовому призначенню перед іншим, або одним класам додатків перед іншими. Це означає, що провайдер не може дискримінувати користувачів, надаючи одним вигідніші умови доступу до контенту, ніж іншим; не має права втручатися в зміст, походження або призначення даних. Всі дані повинні оброблятися однаково, незалежно від того, хто їх надсилає або хто їх отримує. Провайдер не може, наприклад, навмисно уповільнювати роботу певного сервісу, щоб надати перевагу власному сервісу або сервісу, з яким він має договір. Скасування мережевого нейтралітету може дозволити провайдерам створювати платні «швидкісні коридори» для певних компаній, а також блокувати або обмежувати доступ до конкурентів чи небажаних для них сайтів. ЄС займає жорстку позицію щодо дотримання цього принципу. Відмова від цього принципу може негативно вплинути на конкуренцію, свободу слова та доступ до інформації в

мережі.

Право на доступ до інформації – це право кожної людини вільно збирати, зберігати, використовувати та поширювати інформацію, яке гарантується Конституцією України (стаття 34) та законами. Це право може бути реалізоване через отримання інформації за запитами або шляхом її систематичного оприлюднення розпорядниками інформації. Міністерство юстиції України надало узагальнююче роз’яснення від 03.05.2012 про право на доступ до інформації як елемент правового статусу особи. Зазначається, що це право реалізується відповідно до Законів України «Про звернення громадян», «Про інформацію», «Про доступ до публічної інформації». Кожної особи звернутися із запитом на інформацію до розпорядника, незалежно від того, стосується ця інформація її особисто чи ні, та без пояснення причини запиту. Доступ до інформації може бути обмежений, якщо це необхідно для: національної безпеки, територіальної цілісності або громадського порядку; охорони здоров'я населення; захисту репутації або прав інших осіб; запобігання розголошенню конфіденційної інформації.

Досліджені дії російських/проросійських пропагандистів щодо маскування фейкової інформації під зовнішнє оформлення відомих та авторитетних українських інформаційних сайтів, наприклад, «Обозреватель», УНІАН. Наведені приклади фактичних фейкових повідомлень (сайтів).

Принципи реалізації гарантій захисту персональних даних регламентуються Законом України «Про захист персональних даних», а також Регламентом ЄС 2016/679 від 27.04.2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних. Зокрема, ключовими аспектами закону є: об'єкт захисту: захист надається персональним даним, які обробляються в базах даних; обмеження доступу: персональні дані за режимом доступу є інформацією з обмеженим доступом; заборона обробки: закон забороняє обробку чутливих персональних даних, таких як інформація про расове/етнічне походження, політичні/релігійні переконання, членство в партіях/спілках та судимості, якщо немає законних

підстав; кримінальна відповідальність: незаконне збирання, зберігання, використання або поширення конфіденційної інформації може призвести до кримінальної відповідальності згідно зі статтею 182 КК України; знищення даних: персональні дані підлягають знищенню у випадках, передбачених законом: закінчення строку зберігання, припинення правовідносин або за рішенням суду; сфера дії: закон застосовується до всіх видів діяльності з обробки персональних даних, які здійснюються повністю або частково автоматизовано. Європейський Регламент, на відміну від Закону України «Про захист персональних даних», містить визначення «персональні дані». Запропоновано внести це визначення і в український закон «Про захист персональних даних».

Захист інформаційної безпеки – це право на захист від несанкціонованого доступу до особистої інформації та можливість регулювати цей доступ. Захист інформаційної безпеки – це сукупність заходів та засобів для забезпечення цілісності, конфіденційності та доступності інформації від природних або штучних загроз. Він включає фізичний та кіберзахист, управління доступом, використання антивірусного програмного забезпечення, брандмауерів, регулярне оновлення систем, створення резервних копій та дотримання політики безпеки. Основні принципи та цілі цілісність, конфіденційність, доступність для авторизованих користувачів, автентичність, відстежуваність, неспростовність та надійність. Розглянуті можливі варіанти шкоди, яка може бути завдана особі: копіювання комп'ютерної інформації; знищення комп’ютерної інформації; модифікація комп’ютерної інформації; блокування комп’ютерної інформації; обман (спотворення або приховування інформації, нав'язування хибної інформації).

Пропонуються наступні рекомендації для підвищення ступеня інформаційної безпеки: використання надійних паролів, регулярне оновлення програмного забезпечення**:** операційної системи та всі програми; використання антивірусного програмного забезпечення та брандмауера;

уникнення відкриття підозрілих електронних листів, завантаження неперевіреного вмісту та переходів за сумнівними посиланнями; активація двофакторної аутентифікації; створення резервних копії, щоб уникнути втрати даних; використання тільки ліцензійних та офіційних програм.

Захист прав інтелектуальної власності в мережі Інтернет – це система правових, технічних і організаційних заходів, спрямованих на попередження, виявлення та припинення порушень авторських і суміжних прав, прав на торговельні марки, патенти, промислові зразки тощо в онлайн-просторі (авторське визначення). Форми порушень прав інтелектуальної власності в Інтернеті: Інтернет-піратство, плагіат, кіберсквотинг, незаконне використання торговельних марок у рекламі чи доменах, неліцензійне використання програмного забезпечення. Право інтелектуальної власності в мережі Інтернет охоплює захист авторських прав на контент (тексти, фото, музика, відео, програми, сайти); прав на торгові марки, патенти на винаходи та промислові зразки, логотипи, брендові зображення, що використовуються онлайн; комп'ютерні програми та бази даних; доменні імена. Сформулювані рекомендації щодо захисту прав інтелектуальної власності в мережі Інтернет.

Право на захист від кримінальних посягань у кіберпросторі – це гарантоване державою право кожної особи на безпеку, недоторканність її цифрової інформації, персональних даних, майна й честі від злочинних дій, що здійснюються з використанням інформаційно-комунікаційних технологій (авторське визначення). Основні види кримінальних посягань у кіберпросторі: несанкціонований доступ до комп'ютерних систем, баз даних або мереж (хакерство); шкідливе програмне забезпечення (віруси, трояни, ботнети); кібершахрайство – крадіжка грошей через фішинг, підроблені сайти, електронні платформи; кібербулінг та кіберпереслідування; поширення незаконного контенту (дитяча порнографія, терористичні матеріали, мова ненависті); порушення авторських прав у мережі; маніпуляції з криптовалютами та фінансовими системами.

Отже, право на захист від кримінальних посягань у кіберпросторі – це

важлива складова права на безпеку особи в цифрову епоху. Воно передбачає як державний, так і приватний рівень захисту, вимагає постійної взаємодії між державою, суспільством і міжнародними структурами.

ВИСНОВКИ

У дисертації здійснено теоретичне узагальнення і подано нове розв’язання важливих наукових завдань розвитку основ адміністративного і інформаційного права, розроблення теоретичних і практичних основ адміністративно-правового регулювання діяльності із забезпечення кібернетичної безпеки України.

Під час дослідження розв’язане наукове завдання щодо розкриття сутності і змісту адміністративно-правових засад спрямування методів і засобів забезпечення кібернетичної безпеки на вирішення проблем забезпечення інформаційної та кібер- безпеки, усвідомлення сучасних викликів у зв’язку із широкомасштабною агресією рф проти України, визначено та окреслено основні шляхи їх розв’язання. Практично застосовані відомі й запропоновані нові підходи до розробки категорій і принципів діяльності публічної адміністрації у цій сфері, а також засобів оптимізації процесної та системної складових такої діяльності та її правової організації.

Необхідність нових наукових розробок та інноваційних підходів до правової організації діяльності у сфері інформаційної і кібер- безпеки обумовили те, що у своєму дослідженні автор пропонує наукову інтерпретацію вирішення завдань теоретичного осмислення ролі публічної інформації в системі публічного адміністрування інформаційної і кібер-безпеки, отриману як результат проведеного аналізу існуючих проблем у цій сфері та застосування розроблених теоретичних і практичних основ для дослідження та створення моделей і шляхів розвитку правової організації. Існування таких основ дозволяє розробляти ефективні методи забезпечення прав осіб в системі кібербезпеки в системному зв’язку з обмеженнями поширення шкідливої інформації, прийнятними в демократичному суспільстві та їх нормативно-правові моделі; виявляти недоліки та розробляти пропозиції щодо удосконалення нормотворчої та правозастосовчої діяльності у сфері інформаційної безпеки, кібербезпеки і кіберзахисту.

Наведемо положення, які відображають та конкретизують основні результати проведеного дослідження.

1. Усвідомлення сучасних викликів у зв’язку із широкомасштабною агресією рф проти України полягає у тому, що у сучасних реаліях широкого впровадження нових інформаційно-комунікаційних технологій, з одного боку, і тенденцій їх використання у гібрідних війнах для завдання шкоди особам, підприємствам, суспільству, державі, з іншого боку, перед державою постає завдання надійного захисту кібернетичної безпеки суб’єктів та їх прав у кіберпросторі. Впровадження міжнародних стандартів може підвищити рівень загальної готовності України до інформаційних загроз. Крім того, міжнародна співпраця є ключем до протидії інформаційним загрозам.

2. В роботі запропонований, обґрунтовується і досліджується міждисциплінарний підхід до вивчення та реалізації ефективних засобів правового забезпечення інформаційної й кібер- безпеки, який полягає у поєднанні засобів, методів і правил адміністративного права (принципи діяльності публічної адміністрації і організації публічного управління в демократичному суспільстві), інформаційного права (поєднання свободи інформаційної діяльності із захистом національного інформаційного простору України від розповсюдження ворожої інформаційної продукції, створення та використання інформаційних технологій), пра́ва кібербезпеки (врахування конкретних ситуацій прийняття рішень публічною адміністрацією), теорії психології впливів (захист осіб від шкідливих інформаційних впливів, забезпечення когнітивної безпеки), деліктології (вивчення заходів державного примусу адміністративно-правового і кримінально-правового характеру для забезпечення встановлених правил у сфері інформаційної та кібр- безпеки). В умовах, коли мережеві та інформаційні системи та послуги відіграють важливу роль у суспільстві, їхня надійність та безпека суттєві для економічної та соціальної діяльності і, зокрема, для функціонування внутрішнього ринку. Отже, належне правове регулювання суспільних відносин, пов’язаних із запровадженням та

використанням інформаційно-комунікаційних систем, є необхідним для їх ефективного використання. Вперше узагальнені встановлені КУпАП делікти у сфері обігу інформації і використання інформаціонно-комунікаційних систем.

3. Наголошено, на необхідності системної нейтралізації вразливостей, на що вказується у Стратегії кібербезпеки України, міжнародному стандарті ISO 27005, рекомендаціях Держспецзв'язку, відомчих нормативних документах, наприклад, Нормативному документі НД ТЗІ 1.1-003-99 Служби безпеки України «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу». Разом із тим, у Законі України «Про основні засади забезпечення кібербезпеки України» не надається визначення цього терміну, що обмежує уніфікацію робіт у цій сфері. Пропонується доповнити цей Закон визначенням поняття «вразливості», згідно із міжнародним стандартом інформаційної безпеки ISO 27005.

Пропонується авторське розуміння адміністративно-правового забезпечення діяльності у сфері кібернетичної безпеки України, яке полягає у використанні засобів і методів адміністративного права (публічне адміністрування, нормативно-правове регулювання, встановлення відповідальності за порушення встановлених нормативних правил), з урахуванням технічних аспектів і технологічних небезпек в кіберпрострі, включаючи протидію вразливостям, кіберінцедентам, кіберконлфктам.

Розглянуті правові засади застосування методу пошуку вразливостей на засадах системи Bug Bounty – це тестування електронних сервісів із залученням зовнішніх фахівців, яке дає можливість виявити вразливі місця і недоліки в програмних продуктах. Виконана періодизація офіційного правового запровадження даної системи в Україні, виділено 2 етапи: 1-й етап – запровадження відповідних змін до КК України, 2-й етап – запровадження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, затвердженого

Постановою КМУ від 16.05.2023 № 497 «Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж». Розглянуті принципи взаємодії між замовником і виконавцем(цями) при пошуку вразливостей, зокрема, висунення публічній пропозиції, підготовка звітів, виплата винагороди тощо.

Сформульовано положення про те, що загальна логіка пошуку і виявлення вразливостей у системах на засадах системи Bug Bounty грунтується на аналізі архітектури систем, конфігурації та програмного забезпечення, а також за допомогою тестування, яке може включати сканування на наявність вразливостей, проникнення та інші методи, у тому числі імітацію дій зловмисників для перевірки стійкості системи, з метою виявлення вразливостей; виявлення слабких місць у програмному забезпеченні та конфігурації. Практичне значення нормативно-правових актів про Bug Bounty полягає у тому, що це правове регулювання служить для розробки та впровадження заходів безпеки, що допомагають запобігти несанкціонованому доступу та іншим видам атак.

4. Розглянуті правові засади забезпечення належного рівня кібербезпеки Інтернет-речей (IoT) як чинників вразливостей – електронно-цифрових пристроїв, приєднаних до інформаційно-комунікаційних систем: «розумні» годинники, «розумні» лічильники, системи «розумний будинок», «розумне авто», розумні роботи, Wi-Fi роутери, ноутбуки, смартфони, датчики та камери, смарт-карти, мобільні пристрої, розумні колонки, маршрутизатори, перемикачі, промислові системи управління, програмне забезпечення, прошивка, операційні системи, мобільні додатки, настільні програми, відеоігри; компоненти (як апаратні, так і програмні); блоки обробки комп’ютера; відеокарти; програмні бібліотеки тощо. Небезпека цих пристроїв, коли вони приєднані до інформаційно-комунікаційних систем, полягає у тому, що вони є потенційною точкою входу для кібератаки. У підключеному середовищі інцидент кібербезпеки в одному продукті може

вплинути на всю організацію або весь ланцюг постачання, часто поширюючись через кордони внутрішнього ринку за лічені хвилини. Вперше введено в український правовий науковий оборот Закон про кіберстійкість (The Cyber Resilience Act (CRA)) – це нормативний акт ЄС щодо покращення кібербезпеки та кіберстійкості в ЄС шляхом встановлення спільних стандартів кібербезпеки для продуктів з цифровими елементами в ЄС, таких як обов'язкові звіти про інциденти та автоматичні оновлення безпеки. Досліджені його основні положення, якими запропоновано доповнити Закон України від 05.10.2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України». Одночасно запропоновано поширити вимоги цього Закону на соціальні мережі та/або приватні електронні інформаційні ресурси в мережі Інтернет, навіть якщо вони не містять інформацію, необхідність захисту якої встановлена законом, оскільки ці системи за визначенням взаємодіють із публічними мережами електронних комунікацій, зокрема, Інтернет. Де-факто інтереси інформаційного захисту потребують такого регулювання.

5. Проаналізовані особливості концептів «інформаційна безпека», «безпека інформації», «кібербезпека», «когнітивна безпека» в контексті безпекових стратегій України 2020-2021 років. Наголошується, що в сучасному інформаційному просторі актуальною стає не тільки захист інформації, але й захист від інформації. Це поділяє поняття «інформаційна безпека» на підмножини «безпека інформації» та «когнітивна безпека», тобто «інформаційно-психологічна безпека особи». Крім того, у якості підмножини «безпека інформації» слід розглядати поняття «кібербезпека» як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору. У кібербезпеці захищають кіберресурси, у когнітивній безпеці – розум людини. Ворожі інформаційні впливи можуть нести небезпеки не тільки інформаційним (комп’ютерним) системам, але й безпосередньо особам, оскільки можуть бути задіяні для доставляння небажаної інформації в обхід запобіжників отримання (доставляння) цієї

інформації. Інформація формує у свідомості людини систему знань, поглядів, смислів, якими людина керується у своїх вчинках – не тільки лояльних по відношенню до оточення, суспільства, держави, але й ворожих по відношенню до них. Інформаційний вплив може змінювати поведінку людей, нав’язувати їм цілі, які об’єктивно не входять в число їх інтересів. Отже, необхідно враховувати зворотній вплив кібербезпеки на когнітивну безпеку. Кібератаки активно використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення.

Запропоновано напрями термінологічного узгодження у ч. 2 ст. 8 та абз. 2 ч. 4 ст. 8 ЗУ «Про захист інформації в інформаційно-комунікаційних системах» та у ч. 3 ст. 6 ЗУ «Про основні засади забезпечення кібербезпеки України» («слова «інформаційної безпеки» замінити словами «безпеки інформації»).

6. Визначені особливості правового регулювання заходів забезпечення кібербезпеки правовими актами європейського рівня, розглянуті ключові акти у цій сфері, в їх історичному розвитку, а саме: Директива 2016/1148 від 06.07.2016 (Директива була замінена Директивою 2022/2555 від 14.12.2022 року, яка набрала чинності 16.01.2023 року); Директива 2008/114/ЄС від 08.12.2008 року (Директива була замінена Директивою 2022/2557 від 14.12.2022 року, яка набрала чинності 16.01.2023 року); Директива 95/46/ЄС від 24.10.1995 року (Директива замінена Регламентом 2016/679 від 27.04.2016 року, який набрав чинності 24.05.2016 року; Директива 2018/1972 від 11.12.2018 року; Регламент 2019/881 від 17.04.2019 року (Акт про кібербезпеку); Конвенція від 23.11.2001 року Ради Європи «Про кіберзлочинність»; Додатковий протокол від 28.01.2003 до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи; Рекомендація від 30.10.1997 р. № R (97) 19 Комітету міністрів Ради Європи «Про показ насильства електронними ЗМІ», ухвалена Комітетом міністрів на 607-му

засіданні заступників міністрів від 30.10.1997 р.; Рекомендація від 30.10.1997 р. № R (97) 20 Комітету міністрів Ради Європи «Про розпалювання ненависті», ухвалена Комітетом міністрів на 607-му засіданні заступників міністрів від 30.10.1997 р.; Рекомендація від 27.04.1989 р. № R (89) 7 Комітету міністрів РЄ «Про принципи поширення відеозаписів насильницького, жорстокого чи порнографічного змісту», ухвалена Комітетом міністрів на 425-му засіданні заступників міністрів від 27.04.1989 р. Сюди ж слід віднести Закон ЄС про кіберстійкість (The Cyber Resilience Act (CRA)). Наголошено, що перші 4 перелічені (чинні) документи (Директива 2022/2555 від 14.12.2022; Директива 2022/2557 від 14.12.2022; Регламент 2016/679 від 27.04.2016; Регламент 526/2013 від 17.04.2019) підлягають імплементації у законодавство України відповідно до Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, Розділ III «Юстиція, свобода та безпека». Прийняття Закону України від 16.12.2020 року № 1089-IX «Про електронні комунікації» є імплементацією Директиви 2018/1972 від 11.12.2018 року про запровадження Європейського кодексу електронних комунікацій. Встановлені факти належної імплементації положень Директиви 2022/2555 в Закон України № 2163-VIII «Про основні засади забезпечення кібербезпеки України», зокрема, щодо норм про захист критичної інформаційної інфраструктури, щодо створення національної системи реагуваня на кіберзагрози, щодо розробки національної стратегії кібербезпеки та її змісту.

7. Встановлено, що Конвенція Ради Європи «Про кіберзлочинність» з Додатковим протоколом до неї є універсальним міжнародним документом, що спрямований на боротьбу з Інтернет-злочинністю та комп’ютерною злочинністю (кіберзлочинністю) й встановлює і класифікує злочини у сфері кіберзлочинності. Об’єктом таких кіберзлочинів може стати не тільки і навіть не стільки будь-який користувач Інтернету, але й особа, яка не є користувачем Інтернету. Наприклад об’єктом злочину у вигляді поширення

контрафактної продукції через мережу Інтернет може стати суб’єкт авторського права, який не є користувачем Інтернету. Метою Додаткового протоколу до Конвенції Ради Європи «Про кіберзлочинність» є внесення доповнень у відносинах між Державами – сторонами Протоколу до положень Конвенції про кіберзлочинність, які стосуються криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. Отже, цей Протокол повинен забезпечити кримінально-правовий захист когнітивної безпеки осіб та суспільства в частині запобігання проявам дій расистського та ксенофобного характеру. Констатовано важливість Конвенції Ради Європи «Про кіберзлочинність» для України в умовах сучасної злочинної кібервійни рф проти України, у тому числі масової антиукраїнської пропаганди та закликів до геноциду українського народу. Важливість цього напряму захисту когнітивної безпеки проілюстровано історією з радіо «Тисячі пагорбів».

8. Подальшими керівними документами щодо впровадженням заходів забезпечення когнітивної безпеки від інформаційно-психологічного впливу електронних засобів комунікації є Рекомендації Комітету міністрів РЄ № R (89) 7 від 27.04.1989 р. «Про принципи поширення відеозаписів насильницького, жорстокого чи порнографічного змісту», № R (97) 19 від 30.10.1997 р. «Про показ насильства електронними ЗМІ», № R (97) 20 від 30.10.1997 р. «Про розпалювання ненависті». Базовим принципом підходу до обмежень в даній сфері є правила, встановлені ст. 10 Конвенції Ради Європи про захист прав людини і основоположних свобод 1950 року.

9. Визначені особливості правового регулювання заходів забезпечення кібербезпеки актами національного права. Встановлена система законів і підзаконних нормативно-правових актів у сфері забезпечення кібербезпеки. Наголошено, що правозастосовна і прикладна діяльність у сфері кіберзахисту повинна здійснюватися, зокрема, з максимально можливим застосуванням національного та міжнародного права щодо повноважень і обов’язків державних органів, підприємств, установ, організацій, громадян у сфері

кібербезпеки. Узагальнені наступні принципи правового регулювання у сфері кібербезпеки: верховенство права, захист національних інтересів, прозорість і стабільність кіберпростору, державно-приватну взаємодію, пропорційність заходів кіберзахисту, пріоритет запобігання загрозам і невідворотність покарання за кіберзлочини. Встановлено, що хоча законодавство з кіберзахисту звернено, перш за все, до суб'єктів національної системи кібербезпеки, це законодавство покликано також до забезпечення безпеки, прав, свобод та інтересів широкого кола користувачів об'єктами кібербезпеки та кіберзахисту, – через належне виконання уповноваженими суб'єктами національної системи кібербезпеки своїх обов'язків та повноважень у сфері кіберзахисту.

Доведено, що в контексті реалізації «відносини адміністративних зобов'язань», які притаманні засобам і способам адміністративного права, у Законі «Про основні засади забезпечення кібербезпеки України» послідовно реалізовані усі: а) відносини публічного управління – управлінські функції і повноваження Президента України, КМУ, міністерств, інших центральних органів виконавчої влади; місцевих державних адміністрацій; органів місцевого самоврядування; б) відносини адміністративних послуг – кібербезпека та адміністративні послуги пов'язані через цифровізацію державних сервісів, де захист даних стає ключовим завданням; в) відносини відповідальності публічної адміністрації за неправомірні дії або бездіяльність – суб'єкти національної системи реагування на кіберінциденти, кіберзагрози, кібератаки … несуть адміністративну, цивільно-правову, кримінальну відповідальність за неправомірне розголошення, неправомірне розкриття, неправомірне використання та інші неправомірні дії з інформацією про кіберінциденти відповідно до закону (ч. 3 ст. 9 Закону № 2163-VIII). Адміністративна відповідальність настає за порушення, передбачені КУпАП (за здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем та інше);

г) відповідальності суб’єктів суспільства за порушення порядку і правил, встановлених публічною адміністрацією у межах її повноважень – посадові особи власників або розпорядників інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, де обробляються державні інформаційні ресурси та/або службова інформація та інформація, що становить державну таємницю, посадові особи операторів критичної інфраструктури, власників або розпорядників об’єктів критичної інформаційної інфраструктури несуть адміністративну відповідальність відповідно до закону за невиконання або невиконання у встановлені строки обов’язку щодо здійснення обов’язкових повідомлень про кіберінциденти, кібератаки (ч. 6 ст. 9-1 Закону № 2163-VIII).

Запропонована логіка побудови структури описаних підзаконних нормативно-правових актів України у сфері кіберзахисту, яка формалізована схематично.

10. Вперше в наукових дослідженнях встановлено, що сукупність нормативних приписів у сфері забезпечення кібербезпеки та протидії кіберзлочинності доповнена також таким специфічним актом, як Типологія легалізації (відмивання) доходів, одержаних злочинним шляхом, у 2013 році, затверджені Наказом від 25.12.2013 № 157 Державної служба фінансового моніторингу України. У Документі розглядаються наступні питання щодо кіберзлочинності: види кіберзлочинів, загрози та ризики кіберзлочинів, шахрайство з використанням інформаційно-комунікаційних систем та комп'ютерних технологій; кіберзлочинність нефінансового характеру, загальні напрямки протидії кіберзлочинам, виявлення підозрілих фінансових операцій. Наведені в Типології підходи використані в судовій практиці (Постанова від 21.06.2023 року у справі № 922/4091/19 Верховного Суду у складі колегії суддів Касаційного господарського суду).

11. Здійснені системні дослідження з питань кіберконфліктів. Проаналізована сутність поняття «кіберконфлікт». Вперше розглянутий взаємозв’язок між поняттями «кіберконфлікт», з одного боку, та

кіберінцидент і кіберзлочин, з іншого боку. Встановлено, що інцидент кібербезпеки (далі – кіберінцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора), спрямованих проти систем електронних комунікацій, систем управління технологічними процесами, а негативні прояви «кіберконфліктів» спрямовані проти інтересів осіб. Тобто, без врахування людського фактору як об'єкту негативного впливу розгляд проблематики кіберінцидентів є недостатнім та неповним. Систематизовані види кіберконфліктів, які породжуються різноманітними зловживаннями у кіберпросторі. Доведено, що не усі поширені зловживання прямо криміналізовані (передбачені у КК України як злочини у кібернетичній сфері), що утруднює їх кваліфікацію як злочинів.

12. Вперше системно розглянута сукупність безпекових стратегій, прийнятих в Україні протягом 2020-2021 рр., зокрема Стратегія національної безпеки України від 14.09.2020 р.; Стратегія воєнної безпеки України від 25.03.2021 р.; Стратегія кібербезпеки України від 14.05.2021 р.; Стратегія інформаційної безпеки від 15.10.2021 р. Ключовою в системі наведених безпекових Стратегій є Стратегія національної безпеки України, на підставі якого розроблені галузеві стратегії розвитку. Прийняті Стратегії свідчать про серйозну безпекову роботу української влади напередодні розширення агресивних дій рф проти України, вони є логічно взаємопов'язаними документами, реалізація яких ґрунтується на вимогах Стратегії національної безпеки України, а також на застосуванні механізмів забезпечення інформаційної безпеки і кібербезпеки України. В цьому контексті слід зазначити, що українська система безпекових стратегій побудована за моделлю НАТО та ЄС, відповідно до якої (моделі) НАТО розглядає інформаційну безпеку (information security) і кіберзахист (cyber defence) як єдиний операційний домен.

В Стратегії кібербезпеки України важлива роль приділяється кіберзагрозам саме в інформаційній сфері. Визнається, що засоби

кібербезпеки захищають не тільки апаратні і програмні засоби, але й інформацію, що там обробляється. Кібербезпека – технічна і технологічна основа інформаційної безпеки.

Встановлено, що законодавче регулювання сутності і змісту безпекових Стратегій визначається Законом України «Про національну безпеку України». Разом із тим, також встановлено, що такі безпекові Стратегії, як Стратегія зовнішньополітичної діяльності України, Стратегія інформаційної безпеки, Стратегія забезпечення державної безпеки, Стратегія енергетичної безпеки цим Законом не регулюються і в Законі не згадуються, хоча сам Закон розглядає ці види безпек складовою частиною національної безпеки. Запропоновано імплементувати вказані Стратегії в Закон «Про національну безпеку України».

13. Запропонована авторська структура інформаційних прав громадян. Виходячи з того, що «інформаційні права» не тотожні «праву на інформацію», запропонована і розглянута наступна структура інформаційних прав: свобода слова (право вільно виражати свої думки та погляди); право на доступ до інформації, у тому числі право на звернення (можливість отримувати інформацію, що перебуває у володінні суб'єктів владних повноважень, та інформацію, яка становить суспільний інтерес); захист персональних даних (право контролювати використання та поширення своєї особистої інформації); захист інформаційної безпеки (право на захист від несанкціонованого доступу до особистої інформації та можливість регулювати цей доступ), захист прав інтелектуальної власності (захист авторських прав на контент), право на захист від кримінальних посягань у кіберпросторі (право вимагати від уповноваженії органів держави запобігання, виявлення, припинення та розкриття кіберзлочинів). Розкритті особливості і механізми забезпечення вказаних прав осіб у кібермережі.

Запропоновані авторські визначення окремих компонентів прав: «захист прав інтелектуальної власності в мережі Інтернет» – це система правових, технічних і організаційних заходів, спрямованих на попередження,

виявлення та припинення порушень авторських і суміжних прав, прав на торговельні марки, патенти, промислові зразки тощо в онлайн-просторі (авторське визначення); «право на захист від кримінальних посягань у кіберпросторі» – це гарантоване державою право кожної особи на безпеку, недоторканність її цифрової інформації, персональних даних, майна й честі від злочинних дій, що здійснюються з використанням інформаційно-комунікаційних технологій.

Наголошено, що з точки зору конституційного принципу гарантій свободи думки і слова, права на вільне вираження своїх поглядів і переконань, обіг інформації в інформаційно-комунікаційних системах, зокрема, в Інтернеті, підкоряється принципу, відповідно до якого такі свободи не можуть бути безмежними. Проблема встановлення меж свободи самовираження, з одного боку, і допустимості її обмежень, з іншого боку особливо гостро виникає внаслідок практичних потреб обмеження ворожих інформаційно-психологічних впливів, що є особливо гострим саме в інформаційно-комунікаційних системах у зв’язку із особливостями їх можливостей з точки зору доступу до аудиторії (адресатів ворожих думок) – широта охоплення аудиторії, швидкість поширення інформації, відносно низька трудомісткість і вартість її виготовлення. Зазначене надає підстави для обмежень державою поширення телевізійного контенту і Інтернет-мереж. В умовах агресивної інформаційної війни рф проти України керівництво країни було вимушене вдатися до певних обмежень в інформаційно-комунікаційному середовищі: заборона російських соціальних мереж і сайтів (Указ Президента України від 15.05.2017 року № 133/2017 з подальшим продовженням заборони Указом Президента України від 14.05.2020 року № 184/2020; запровадження санкцій проти засобів масової інформації (Указ Президента України від 02.02.2021 року № 43/2021) із забороною їх трансляції. Обґрунтована правомірність цих рішень в контексті частини 2 статті 10 ЄКПЛ, а також частини 3 статті 34 Конституції України.

14. Досліджені дії російських/проросійських пропагандистів щодо

маскування фейкової інформації під зовнішнє оформлення відомих та авторитетних українських інформаційних сайтів, наприклад, «Обозреватель», УНІАН. Наведені приклади фактичних фейкових повідомлень (сайтів).

15. Запропоноване поняття «презумпція достовірності інформації», під якою розуміється відсутність необхідності додатково перевіряти достовірність інформації, розміщеної в легалізованих (зареєстрованих) ЗМІ. ЄСПЛ не вважає прийняття національних нормативних актів щодо державної реєстрації Інтернет-видань порушенням свободи слова. Навпаки, Європейський Суд з прав людини висновував, що принцип презумпції достовірності інформації, яка розміщена в Інтернеті, може бути застосований тільки щодо інформації, розміщеної в легалізованих (зареєстрованих) ЗМІ. За умови належного правового регулювання (у відповідності із вимогами ЄКПЛ) навпаки, така реєстрація підсилює гарантії діяльності журналістів і розширює коло інформації, до якої можна застосовувати презумпцію достовірності, – при одночасному підвищенні відповідальності таких Інтернет-видань за поширення неналежної інформації.

16. Вперше введений у правовий науковий оборот поняття «мережевий нейтралітет» – це принцип, згідно з яким провайдери телекомунікаційних послуг не віддають переваги одному цільовому призначенню перед іншим, або одним класам додатків перед іншими. Це означає, що провайдер не може дискримінувати користувачів, надаючи одним вигідніші умови доступу до контенту, ніж іншим; не має права втручатися в зміст, походження або призначення даних. Всі дані повинні оброблятися однаково, незалежно від того, хто їх надсилає або хто їх отримує. Провайдер не може, наприклад, навмисно уповільнювати роботу певного сервісу, щоб надати перевагу власному сервісу або сервісу, з яким він має договір. Скасування мережевого нейтралітету може дозволити провайдерам створювати платні «швидкісні коридори» для певних компаній, а також блокувати або обмежувати доступ до конкурентів чи небажаних для них сайтів. ЄС займає жорстку позицію щодо дотримання цього принципу. Відмова від цього принципу може

негативно вплинути на конкуренцію, свободу слова та доступ до інформації в мережі.

17. Пропонуються наступні рекомендації для підвищення ступеня інформаційної безпеки: використання надійних паролів, регулярне оновлення програмного забезпечення**:** операційної системи та всі програми; використання антивірусного програмного забезпечення та брандмауера; уникнення відкриття підозрілих електронних листів, завантаження неперевіреного вмісту та переходів за сумнівними посиланнями; активація двофакторної аутентифікації; створення резервних копії, щоб уникнути втрати даних; використання тільки ліцензійних та офіційних програм.

18. За наслідками виконаного дослідження запропоновано внести такі зміни і доповнення до законодавства у сфері інформаційної і кібер- безпеки:

– доповнити Закон України від 05.10.2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» положеннями нормативного акту ЄС – Закону про кіберстійкість (The Cyber Resilience Act (CRA)), серед яких (положень) – встановлення стандартів кібербезпеки для продуктів з цифровими елементами в ЄС, зокрема обов'язкові звіти про інциденти та автоматичні оновлення безпеки;

– поширити вимоги Закону України від 05.10.2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» на соціальні мережі та/або приватні електронні інформаційні ресурси в мережі Інтернет навіть якщо вони не містять інформацію, необхідність захисту якої встановлена законом, оскільки ці системи за визначенням взаємодіють із публічними мережами електронних комунікацій, зокрема, Інтернет, тому, вони є потенційною точкою входу для кібератаки;

– доповнити Закон України від 05.10.2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» визначенням поняття «вразливості», згідно із міжнародним стандартом інформаційної безпеки ISO 27005;

– доповнити Закон України від 05.10.2017 р. № 2163-VIII «Про основні

засади забезпечення кібербезпеки України» визначенням поняття «кіберконфлікт» як зіткнення різноманітних інтересів в кіберпросторі;

– реалізувати у текстах законів напрями термінологічного узгодження у ч. 2 ст. 8 та абз. 2 ч. 4 ст. 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах» та у ч. 3 ст. 6 Закону України «Про основні засади забезпечення кібербезпеки України» («слова «інформаційної безпеки» замінити словами «безпеки інформації»);

– доповнити Закон України від 01.06.2010 р. № 2297-VI «Про захист персональних даних», визначенням «персональні дані» з Регламенту Європейського парламенту і Ради ЄС 2016/679 від 27.04.2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних: це «будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи»;

– доповнити Закон України «Про національну безпеку України» нормами щодо правового регулювання сутності і змісту Стратегії зовнішньополітичної діяльності України, Стратегії інформаційної безпеки, Стратегії забезпечення державної безпеки, Стратегії енергетичної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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

2. Загальна декларація прав людини: Прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН, від 10.12.1948 р. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=995_015

3. Декларация прав ребенка. Резолюция 1386 (XIV) Генеральной Ассамблеи ООН от 20.11.1959 г. URL: http://zakon3.rada.gov.ua/laws/show/995_384

4. Конвенція ООН про права дитини від 20.11.1989 р., ратифік. постановою Верховної Ради Української РСР від 27.02.1991 р. № 789-XII URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=995_021.

5. Європейська конвенція про транскордонне телебачення (Страсбург, 05.05.1989 р.), ратифік. Законом [46]. URL: http://zakon3.rada.gov.ua/laws/show/994_444

6. Конвенція від 23.11.2001 року Ради Європи «Про кіберзлочинність». URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

7. Додатковий протокол від 28.01.2003 до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text

8. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24.10.1995 року. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text

9. Директива Ради 2008/114/ЄС від 08.12.2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту. URL: https://zakon.rada.gov.ua/laws/show/984_002-08#Text

10. Регламент Європейського парламенту і Ради ЄС 2016/679 від 27.04.2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

11. Директива Європейського парламенту і Ради ЄС 2016/1148 від 06.07.2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text

12. Директива Європейського Парламенту і Ради ЄС 2018/1972 від 11.12.2018 року про запровадження Європейського кодексу електронних комунікацій. URL: https://zakon.rada.gov.ua/laws/show/984_013-18#Text

13. Регламент Європейського парламенту і Ради ЄС 2019/881 від 17.04.2019 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту ЄС № 526/2013 (Акт про кібербезпеку). URL: https://zakon.rada.gov.ua/laws/show/984_024-19#n136

14. Директива Європейського Парламенту і Ради ЄС 2022/2555 від 14.12.2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту ЄС № 910/2014 та Директиви ЄС 2018/1972 та скасування Директиви ЄС 2016/1148 (Директива NIS 2). URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#n721

15. Директива Європейського парламенту і ради ЄС 2022/2557 від 14.12.2022 року про стійкість критично важливих суб’єктів та скасування Директиви Ради 2008/114/ЄС. URL: https://zakon.rada.gov.ua/laws/show/9a3_002-22#n305

16. Стратегічні комунікації Європейського Союзу як протидія пропаганді третіх сторін» (EU strategic communication to counteract propaganda against it by third parties (2016/2030 (INI). URL:

https://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_EN.pdf

17. Рекомендация об участии и вкладе народных масс в культурную жизнь. ЮНЕСКО, Найроби, 26.11.1976 г. URL: https://zakononline.ua/documents/show/169451___169451

18. Рекомендація від 27.04.1989 р. № R (89) 7 Комітету міністрів РЄ «Про принципи поширення відеозаписів насильницького, жорстокого чи порнографічного змісту», ухвалена. Комітетом міністрів на 425-му засіданні заступників міністрів від 27.04.1989. URL: http://zakon5.rada.gov.ua/laws/show/994_723

19. Рекомендація від 30.10.1997 р. № R (97) 19 Комітету міністрів РЄ «Про показ насильства електронними ЗМІ», ухвалена Комітетом міністрів на 607-му засіданні заступників міністрів від 30.10.1997. URL: http://zakon5.rada.gov.ua/laws/show/994_735

20. Recommendation No. R (97) 20 «Of the committee of ministers to member states on «hate speech» (Adopted by the Committee of Ministers on 30 October 1997 at the 607th meeting of the Ministers' Deputies) [Рекомендація від 30.10.1997 р. № R (97) 20 Комітету міністрів Ради Європи «Про розпалювання ненависті», ухвалена. Комітетом міністрів на 607-му засіданні заступників міністрів від 30.10.1997]. URL: https://rm.coe.int/1680505d5b

21. Стратегія кібербезпеки України від 27.01.2016 р. Схвалена рішенням РНБО України від 27.01.2016 р. Затверджена Указом Президента України від 15.03.2016 р. № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text

22. Стратегія національної безпеки України. Схвалена рішенням РНБО України від 14.09.2020 р. Затверджена Указом Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

23. Стратегія воєнної безпеки України від 25.03.2021 р. Схвалена рішенням РНБО України від 25.03.2021 р. Затверджена Указом Президента України від 25.03.2021 р. № 121/2021. URL:

https://zakon.rada.gov.ua/laws/show/121/2021#Text

24. Стратегія кібербезпеки України від 14.05.2021 р. Схвалена рішенням РНБО України від 14.05.2021 р. Затверджена Указом Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

25. Стратегія розвитку оборонно-промислового комплексу України від 18.06.2021 р. Схвалена рішенням РНБО України від 18.06.2021 р. Затверджена Указом Президента України від 20.08.2021 р. № 372/2021. URL: https://zakon.rada.gov.ua/laws/show/372/2021#Text

26. Стратегія зовнішньополітичної діяльності України від 30.07.2021 р. Схвалена рішенням РНБО України від 30.07.2021 р. Затверджена Указом Президента України від 26.08.2021 р. № 448/2021. URL: https://zakon.rada.gov.ua/laws/show/448/2021#Text

27. Стратегія енергетичної безпеки. Схвалена розпорядженням Кабінету Міністрів України від 04.08.2021 р. № 907-р. URL: https://zakon.rada.gov.ua/laws/show/907-2021-%D1%80#Text

28. Стратегія інформаційної безпеки від 15.10.2021 р. Схвалена рішенням РНБО України від 15.10.2021 р. Затверджена Указом Президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n5

29. Стратегія забезпечення державної безпеки від 30.12.2021 р. Схвалена рішенням РНБО України від 30.12.2021 р. Затверджена Указом Президента України від 16.02.2022 р. № 56/2022. URL: https://zakon.rada.gov.ua/laws/main/56/2022.#Text

30. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)». Указ Президента України від 15.05.2017 року № 133/2017. URL: https://zakon.rada.gov.ua/laws/show/133/2017#n2

31. Про рішення Ради національної безпеки і оборони України від 14

травня 2020 року «Про застосування, скасування і внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)». Указ Президента України від 14.05.2020 року № 184/2020. URL: https://zakon.rada.gov.ua/laws/show/184/2020#n2

32. Про рішення Ради національної безпеки і оборони України від 02 лютого 2021 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)». Указ Президента України від 02.02.2021 року № 43/2021. URL: https://zakon.rada.gov.ua/laws/show/43/2021#Text

33. Кодекс України про адміністративні правопорушення (статті 1 – 212-24). Від 07.12.1984 р. № 8073-X. Відомості Верховної Ради (ВВР), 1984, додаток до № 51, ст. 1122.

34. Кримінальний кодекс України. Від 05.04.2001 р. № 2341-III. Відомості Верховної Ради (ВВР), 2001, № 25-26, ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

35. Про оборону України. Закон України від 06.12.1991 № 1932-XII. Відомості Верховної Ради України (ВВР), 1992, № 9, ст. 106. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text

36. Про інформацію. Закон України від 02.10.1992 № 2657-XII. Відомості Верховної Ради (ВВР), 1992, № 48, ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

37. Про державну таємницю. Закон України від 21.01.1994 р. № 3855-XII. Відомості Верховної Ради (ВВР), 1994, № 16, ст. 93. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

38. Про захист інформації в інформаційно-комунікаційних системах. Закон України від 05.07.1994 № 80/94-ВР. Відомості Верховної Ради України (ВВР), 1994, № 31, ст. 286. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

39. Про наукову і науково-технічну експертизу. Закон України від 10.02.1995 р. № 51/95-ВР. Відомості Верховної Ради (ВВР), 1995, № 9, ст. 56.

URL: https://zakon.rada.gov.ua/laws/show/51/95-%D0%B2%D1%80#Text

40. Про звернення громадян. Закон України від 02.10.1996 № 393/96-ВР. Відомості Верховної Ради України (ВВР), 1996, № 47, ст. 256. URL: https://zakon.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80#Text

41. Про охорону дитинства. Закон України від 26.04.2001 р. № 2402-III. Відомості Верховної Ради України (ВВР), 2001, № 30, ст. 142. URL: https://zakon.rada.gov.ua/laws/show/2402-14#Text

42. Про основи національної безпеки України. Закон України від 19.06.2003 р. № 964-IV. Відомості Верховної Ради (ВВР), 2003, № 39, ст. 351. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text

43. Про ратифікацію Конвенції про кіберзлочинність. Закон України від 07.09.2005 № 2824-IV. Відомості Верховної Ради (ВВР), 2006, № 5-6, ст. 71. URL:_https://zakon.rada.gov.ua/laws/show/2824-15#Text

44. Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. Закон України від 21.07.2006 № 23-V. Відомості Верховної Ради України (ВВР), 2006, № 39, ст. 328. URL: https://zakon.rada.gov.ua/laws/show/23-16#Text

45. Про Державну службу спеціального зв’язку та захисту інформації України. Закон України від 23.02.2006 р. № 3475-IV. Відомості Верховної Ради (ВВР), 2006, № 30, ст. 258. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

46. Про ратифікацію Європейської конвенції про транскордонне телебачення. Закон України від 17.12.2008. *Відомості Верховної Ради України (ВВР), 2009,* № *15,* Ст. 203. URL: https://zakon.rada.gov.ua/laws/show/687-17#Text

47. Про захист персональних даних. Закон України від 01.06.2010 р. № 2297-VI. Відомості Верховної Ради (ВВР), 2010, № 34, ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

48. Про доступ до публічної інформації. Закон України від

13.01.2011 р. № 2939-VI. Відомості Верховної Ради (ВВР), 2011, № 32, ст. 314. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

49. Про технічні регламенти та оцінку відповідності. Закон України від 15.01.2015 р. № 124-VIII. Відомості Верховної Ради (ВВР), 2015, № 14, ст. 96. URL: https://zakon.rada.gov.ua/laws/show/124-19#Text

50. Про Національну поліцію. Закон України від 02.07.2015 р. № 580-VIII. Відомості Верховної Ради (ВВР), 2015, № 40-41, ст. 379. URL:

51. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 р. № 2163-VIII. Відомості Верховної Ради (ВВР), 2017, № 45, ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

52. Про національну безпеку України. Закон України від 21.06.2018 № 2469-VIII. Відомості Верховної Ради (ВВР). 2018. № 31, ст. 241. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

53. Про електронні комунікації. Закон України від 16.12.2020 року № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text

54. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану. Закон України, від 24.03.2022 р. № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#n2

55. Про критичну інфраструктуру. Закон України від 16.11.2021 № 1882-IX. Відомості Верховної Ради України (ВВР), 2023, № 5, ст. 13. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

56. Про медіа. Закон України від 13.12.2022 р. № 2849-IX. Відомості Верховної Ради (ВВР), 2023, № 47-50, ст. 120. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text

57. Про авторське право і суміжні права. Закон України від 01.12.2022 № 2811-IX. Відомості Верховної Ради (ВВР), 2023, № 57, ст. 166. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text

58. Про правотворчу діяльність. Закон України від 24.08.2023 № 3354-IX. Відомості Верховної Ради України (ВВР), 2023, № 93, ст. 364. URL:

https://zakon.rada.gov.ua/laws/show/3354-20#Text

59. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Постанова Кабінету міністрів України від 16.05.2023 р. № 497. URL: https://zakon.rada.gov.ua/laws/show/497-2023-%D0%BF#Text

60. Про затвердження Типології легалізації (відмивання) доходів, одержаних злочинним шляхом, у 2013 році. Наказ від 25.12.2013 № 157 Державної служба фінансового моніторингу України. URL: https://zakon.rada.gov.ua/rada/show/v0157827-13#n10

61. Про затвердження Примірної публічної пропозиції про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж і Методичних рекомендацій з розроблення публічної пропозиції про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Наказ Адміністрації Держспецзв'язку від 14.07.2023 № 599. URL: https://zakon.rada.gov.ua/rada/show/v0599519-23#Text

62. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Нормативний документ НД ТЗІ 1.1-003-99. Затверджено наказом від 28.04.1999 р. № 22 Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. 1999. 22 с. URL: https://tzi.ua/assets/files/1.1_003_99.pdf

63. Адміністративна (поліцейська) діяльність органів внутрішніх справ. Заг. част. Підручник / Ю.І. Римаренко, Є.М. Моісеєв, В.І. Олефір та ін. К. КНТ, 2008. 816 с.

64. Абакумов В.М. Інформаційна безпека підприємництва як об'єкт адміністративно-правової охорони. *Форум права*. 2012. № 4. С. 10-16.

65. Ананьїн В.О., Пучков О.О. Інформаційна безпека як складова національної безпеки України. *Гілея: науковий вісник*. 2014. Вип. 85. С. 194-197.

66. Антонова С.Є., Мартинюк Г.Ф. Інформаційна безпека. *Державне управління: удосконалення та розвиток*. 2019. № 11. URL: http://www.dy.nayka.com.ua/?op=1&z=1528

67. Антонюк В.В. Основні науково-методологічні підходи до дослідження державної політики інформаційної безпеки. *Інвестиції: практика та досвід*. 2013. № 20. С. 143-147.

68. Апетик А. Анатомія кіберзлочину: ключові тренди 2020 року. Експертний центр з прав людини. 30.04.2020. URL: https://ecpl.com.ua/news/anatomiia-kiber-zlochynu/

69. Ариэли Цви. Информационная война: как Украине победить путинскую Россию? *Обозреватель*. 11.07.2016. URL: http://obozrevatel.com/blogs/78045-informatsionnaya-vojna-kak-ukraine-pobedit-putinskuyu-rossiyu.htm

70. Архипова Є.О. Соціально-філософське осмислення поняття «інформаційна безпека». *Вісник Нац. технічного ун-ту України «Київський політехнічний інститут». Філософія. Психологія. Педагогіка*. 2011. № 3. С. 7-11.

71. Бабакін В.М. Особливості міжнародного співробітництва при розслідуванні кіберзлочинів. *Форум права*. 2011. № 4. С. 27-35. URL: http:/Avww.nbuv.gov.ua/e-journals/FP/2011-4/11bvmprk.pdf

72. Бабой А., Опольська Н. Свобода вираження поглядів в мережі інтернет в умовах розвитку інформаційного суспільства. *Economic and Law Paradigm of Modern Society*. 2020. Вип. 2. С. 60-73

73. Бабченко А. Никакой Крымнаш не был бы возможен без артподготовки в виде «Аншлага» и «Дома-2». Детектор медиа. 30.04.2016. URL: https://detector.media/withoutsection/article/114796/2016-04-30-nykakoy-krymnash-ne-byl-by-vozmozhen-bez-artpodgotovky-v-vyde-anshlaga-y-doma-2/

74. Баран М.В. Інформаційна безпека як предмет адміністративно-правового регулювання. *Соціально-правові студії*. 2021. Вип. 3 (13). С. 50-56.

75. Безпека мобільних пристроїв**:** наук.-практ. посіб. / упоряд.: М.Г. Вербенський, В.О. Криволапчук, Д.В. Смерницький та ін. Київ. «Видавництво Людмила», 2023. 100 с.

76. Бєлкін Л.М. Заборона мовлення антиукраїнських телевізійних каналів у контексті конвенційних зобов'язань України. *Юридичний науковий електронний журнал. Електронне наукове фахове видання*. 2021. № 2. С. 155-159.

77. Бєлкін М.Л., Криволап Є.В., Юринець Ю.Л. Адміністративно-правове регулювання нейтралізації вразливостей інформаційно-комунікаційних систем. *Збірник матеріалів «Актуальні питання забезпечення кібербезпеки» IX Міжнародної науково-практичної конференції* (м. Київ, 13 листопада 2024 року). Київ. МАУП. 13 листопада 2024 року. С. 38-42.

78. Бєлкін Л.М., Юринець Ю.Л., Бєлкін М.Л., Криволап Є.В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020-2021 років. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2022. № 3 (64). С. 78-86.

79. Бєлкін Л.М., Юринець Ю.Л., Сопілко І.М., Бєлкін М.Л. Контрпропаганда vs пропаганда в умовах широкомасштабного збройного вторгнення Російської Федерації в Україну. *Юридичний науковий електронний журнал. Електронне наукове фахове видання*. 2022. № 6. С. 224-230.

80. Бєлкін Л.М., Юринець Ю.Л., Сопілко І.М., Бєлкін М.Л. Спростування «геноциду» на Донбасі як напрям контрпропаганди під час агресії Російської Федерації проти України. *Юридичний науковий електронний журнал. Електронне наукове фахове видання*. 2022. № 3. С. 12-17.

81. Битяк Ю.П. Адміністративне право: Підручник / Ю.П. Битяк, В.М. Гаращук, В.В. Богуцький та ін. ; за ред. Ю.П. Битяка, В.М. Гаращука, В.В. Зуй. 2-ге вид., переробл. та допов. Харків. Право, 2013. 656 с.

82. Бліхар М. Свобода вираження політичних поглядів: суспільно-політичний та адміністративно-правовий виміри. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2022. № 69. С. 224-228. С. 226.

83. Бобришева О. Інформаційна безпека бібліотеки: проблеми та шляхи формування. *Вісник Книжкової палати*. 2010. № 12. С. 18-20.

84. Богданович В.Ю., Воровича Б.О., Марко Є.І. Інформаційна безпека як основа воєнної безпеки держави та суспільства. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2018. № 3. С. 44-48.

85. Богданович В.Ю., Грищук Р.В., Левченко О.В. Система критеріїв та показників оцінювання ефективності функціонування системи забезпечення інформаційної безпеки. *Збірник наукових праць Національної академії Державної прикордонної служби України. Сер.: Військові та технічні науки*. 2017. № 4. С. 21-37.

86. Богданович В.Ю., Дудар М.С. Узагальнена модель управління інформаційно-психологічною безпекою великих груп людей в умовах низького рівня соціально-політичної стабільності в країні. Сучасний захист інформації. 2014. № 4. С. 4-11.

87. Брижко В.Н., Гальченко О.М., Цимбалюк В.С., Орєхов О.А., Чорнобров А.М. Інформаційне суспільство. Дефініції: людина, її права, інформація. Інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція. К. 2002. 523 с.

88. В Італії відбивають нову хвилю кібератак проросійських хакерів. *Європейська правда*. 22.03.2023. URL: https://www.eurointegration.com.ua/news/2023/03/22/7158445/

89. Вакарюк Л. Основні підходи до розуміння поняття «інформаційні права людини». *Підприємництво, господарство і право*. 2018. № 2. С. 155-159.

90. Валюшко І.О. Інформаційна безпека України в контексті російсько-українського конфлікту. Дис. … канд. політичних наук; спец. 23.00.04 «Політичні проблеми міжнародних систем та глобального розвитку. Київ, 2018. 210 с.

91. Ващенко А.В. Свобода вираження поглядів в Інтернеті: pro et contra. *Право та інновації*. 2014. № 3 (7). С. 49-54.

92. Вектор атаки. *Википедия*. URL: https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%BA%D1%82%D0%BE%D1%80_%D0%B0%D1%82%D0%B0%D0%BA%D0%B8_(%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C)

93. *Верголяс О.О. Спеціальні інформаційні операції в системі засобів протидії загрозам національній безпеці України. Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки». 2019. № 4.*

94. Веселова Л.Ю. Адміністративно-правові основи кібербезпеки в умовах гібридної війни. Дис… д-ра юр. наук. Спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». Одеса. Одеський державний університет внутрішніх справ. 2021. 500 с.

95. Веселова Л.Ю. Кібербезпека в умовах гібридної війни: адміністративно-правові засади. Монографія. Одеса. Видавничий дім «Гельветика». 2020. 486 с.

96. Вірус WannaCry пошкодив комп'ютери у 99 країнах світу. *BBC. NEWS.Ukrainian*. 13.05.2017. URL: https://www.bbc.com/ukrainian/features-39907984

97. Вітвіцька В.В. Кримінологічні проблеми попередження злочинних посягань на моральний і фізичний розвиток неповнолітніх. Автореф. дис… канд юрид. наук; спец. 12.00.08 «Кримінальне право і кримінологія;

кримінально-виконавче право». К. 2002. 22 с.

98. Волокіта В. РФ вдається до кібератак на енергосистему напередодні масованих обстрілів – Міненерго. *Економічна правда*. 04.12.2024. URL: https://epravda.com.ua/power/rf-vdayetsya-do-kiberatak-na-energosistemu-naperedodni-masovanih-obstriliv-minenergo-800469/

99. Волошина Н.М. Поняття «безпека інформації» та «інформаційна безпека» в сучасному науковому просторі. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2010. № 2. С. 53-56.

100. Вонс Р. Хакери атакували Швейцарію через візит Зеленського в Давос. *Главком*. 17.01.2024. URL: https://glavcom.ua/techno/hitech/khakeri-atakuvali-shvejtsariju-cherez-vizit-zelenskoho-v-davos-980873.html

101. Гірник А.М. Резаненко В.Ф. Концепт «конфлікт» у західній культурі та в культурі традиційних суспільств Далекого Сходу. Наукові записки НаУКМА. Педагогічні, психологічні науки та соціальна робота. 2012. Т. 136. С. 37-42.

102. Глущенко О. Российские хакеры атаковали Германию после ее решения передать Украине танки. *Українська правда*. 28.01.2023. URL: https://www.pravda.com.ua/ukr/news/2023/01/28/7386899/

103. Глущенко О. Росія посилює розпалювання антиукраїнських настроїв у Польщі – Генштаб ЗС Польщі. *Українська правда*. 04.11.2025. URL: https://www.pravda.com.ua/news/2025/11/04/8005687/

104. Гоголь Б. Зміст права на інформацію. *Юридична Україна*. 2008. № 5. С. 64-67.

105. Голуб О. Сайти соцмереж як джерело інформації. *Детектор медіа*. 24.02.2016. URL: https://ms.detector.media/sotsmerezhi/post/16123/2016-02-24-saiti-sotsmerezh-yakdzherelo-informatsii/

106. Голубєв В.О. Інформаційна безпека: проблеми боротьби з кіберзлочинністю. Запоріжжя, 2003. 250 с.

107. Гончаренко Г.А. До проблеми визначення та розмежування дефініцій «інформаційна безпека» і «кібербезпека». Аналітично-порівняльне

правознавство. Електронне наукове видання. 2024/10, № 10. С. 466-471.

108. Гончарук С.Т. Адміністративна відповідальність: сутність та окремі проблеми трансформації на сучасному етапі. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2007. Том 3, № 4. С. 57–60.

109. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення. *Вісник НАДУ*. 2015. № 1. С. 136-141.

110. Гребенюк А. Антиукраїнська пропаганда: характерні риси та поняття. *Наукові праці Національної бібліотеки України ім. В.І. Вернадського*. 2021. Вип.61. С. 128-139.

111. Гуйван П.Д. Вільне вираження поглядів у демократичному суспільстві. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки*. 2020. Т. 31 (70). № 3. С. 63-68.

112. Гуйван П.Д. Свобода вираження думки у ЗМІ: критерії правомірності реалізації права. *Правова позиція*. 2020. № 2 (27). С.83-87.

113. Гуренко-Вайцман М.М. Рецензія на монографію О.В. Бойченка «Інформаційна безпека в органах внутрішніх справ України (організаційно-правові засади)». *Форум права*. 2009. № 3. С. 738-740.

114. Гуцалюк М.В. Посилення кібербезпеки: європейський досвід. *Актуальні питання криміналістики та судової експертизи*. Матеріали міжвідом. наук.-практ. конф. (Київ, 25 листоп. 2022 р.) / [редкол.: В. В. Чернєй, С.Д. Гусарєв, С.С. Чернявський та ін.]. Київ : Нац. акад. внутр. справ, 2022. С. 64-66.

115. Гуцу С.Ф. Правове регулювання мережі Інтернет: міжнародний і вітчизняний досвід. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. 2018. Вип. 2 (38). С. 114-118.

116. Гришина Н.В. Адміністративна і кримінальна відповідальність: порівняльна характеристика. *Наукова періодика Каразінського університету. Часопис з юридичних наук*. 14.04.2015. URL: https://periodicals.karazin.ua/jls/issue/view/187

117. Грубінко А.В. Інформаційна безпека України: правове гарантування та реалії забезпечення. *Актуальні проблеми правознавства*. 2019. Вип. 1. С. 5-10.

118. Данилов А. На нашу страну напали, и мы будем действовать так, как нужно, чтобы сохранить Государство и Независимость. Обозреватель. 04.02.2021. URL: https://news.obozrevatel.com/politics/na-nashu-stranu-napali-i-myi-budem-dejstvovat-tak-kak-nuzhno-chtobyi-sohranit-gosudarstvo-i-nezavisimost.htm

119. Данильян О.Г., Дзьобань О.П. Інформаційна безпека України: загрози, зумовлені цивілізаційним вибором європейських цінностей. *Politology bulletin*. 2018. Iss. 81. С. 60-67.

120. Діордіца І.В. Адміністративно-правове регулювання кібербезпеки України. Дис... канд. юрид. наук: спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». Запоріжжя, 2018. 521 с.

121. Діордіца І.В. Поняття та зміст кібертероризму. *Глобальна організація союзницького лідерства*. 2016. URL: https://goal-int.org/ponyattya-ta-zmist-kiberterorizmu/

122. Діордіца І.В. Поняття та зміст кібершпигунства. Наукові праці Національного університету «Одеська юридична академія». 2020. Том 26. С. 49-55. URL: http://npnuola.onua.edu.ua/index.php/1234/article/view/660/695

123. Дія підтвердила безпечність застосунку за допомогою програми Bug Bounty. Дія. 30.12.2020. URL: https://diia.gov.ua/news/diya-projshla-perevirku-bagbaunti-ta-pidtverdila-bezpechnist-zastosunku

124. Дубов Д.В. COVID-19: ключові кібербезпекові тренди. Національний інститут стратегічних досліджень. URL: https://niss.gov.ua/sites/default/files/2020-03/cyber-security-covid-19.pdf

125. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва. Монографія. К. НІСД, 2014. 328 с.

126. Европейские принципы государственного управления. Публикация СИГМА. Париж, 1999. № 27. 28 с. URL: http://www.sigmaweb.org/

publications/Sergei_Rus_SP27_99Rev1.pdf

127. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/

128. Жабинець О.Й. Захист інформації та інформаційна безпека страхових компаній. *Економічний часопис-XXI*. 2014. № 7-8(2). С. 32-35.

129. Завгородня Ю.В. Роль НАТО у боротьбі з кіберконфліктами: політико-правовий аспект. Регіональні студії. 2022. № 30. С. 62-65.

130. Загурська-Антонюк В.Ф. Політично-інформаційні безпекові механізми в українській державній системі у контексті геополітичних змін. *Державне управління: удосконалення та розвиток*. 2020. № 2. URL: http://www.dy.nayka.com.ua/?op=1&z=1567

131. Задубінний А. Рік діяльності Уряду: розробка стратегічних документів у сфері безпеки та оборони. *АРМІЯinform*. URL: https://armyinform.com.ua/2021/03/02/rik-diyalnosti-uryadu-rozrobka-strategichnyh-dokumentiv-u-sferi-bezpeky-ta-oborony/

132. Заплатинський В.М. Логіко-детермінантні підходи до розуміння поняття «Безпека». *Вісник Кам'янець-Подільського національного університету імені Івана Огієнка*. Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2012. Вип. 5. 336 с.

133. Зацікавлені сторони. Вікіпедія. URL: https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D1%86%D1%96%D0%BA%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D1%96_%D1%81%D1%82%D0%BE%D1%80%D0%BE%D0%BD%D0%B8

134. «Зеленского после прихода к власти Байдена как будто подменили»: Фурса про три события. *Антикор*. 03.02.2021. URL: https://antikor.info/articles/436052-zelenskogo_posle_prihoda_k_vlasti_bajdena_kak_budto_podmenili_fursa_pro_tri_sobytija

135. Іленков А. Термінологія та її роль у представленні знань. *Вісник*

Нац. ун-ту «Львівська політехніка». Серія «Проблеми української термінології». 2009. № 648. С. 24–29.

136. Ілюк К. Інформаційна війна – це не тільки фейки. Детектор медіа. 31.03.2022. URL: https://ms.detector.media/propaganda-ta-vplivi/post/29264/2022-03-31-informatsiyna-viyna-tse-ne-tilky-feyky/

137. Інтернет-піратство – що це таке і як з ним боротися? Цікаво про IP в картках. Український національний офіс інтелектуальної власності та інновацій (IP офіс) 14.06.2024. URL: https://nipo.gov.ua/ipictures5-piratstvo/

138. Інформаційна безпека у контексті сучасних технологій інформаційно-психологічного протиборства: навчальний посібник / Петрик В.М., Назаренко О.А., Присяжнюк М.М., Курганевич В.І Василіу Є.В., Рябуха О.М., Голев Д.В., Гнатюк С.О., Фесенко А.О.; за заг. ред. О.А. Назаренка, В.М. Петрика. Київ: «ЦУЛ», 2025. 258 с.

139. Казанчук І.Д., Яценко В.П. Особливості правового регулювання діяльності національної поліції України у сфері забезпечення інформаційної безпеки в Україні. *Право і безпека*. 2020. № 4 (79). С. 32-38

140. Калюжний Р.А. Держава. Політика. Інформація *Юридичний вісник. Повітряне і космічне право*. 2014. № 2. С. 159-160.

141. Калюжний Р., Андросюк І. Проблеми захисту прав людини в інформаційній сфері. *Правова інформатика*. 2004. № 3. С. 17-20.

142. Калюжний Р.А. Теоретико-методологічні підходи до розуміння інформаційної безпеки людини. *Юридичний вісник. Повітряне і космічне право*. 2018. № 2. С. 197-198.

143. Калюжний Р., Баєв О. Систематизація нормативно-правового забезпечення України в інформаційній сфері. *Правова інформатика.* 2009. № 3. С. 5-10.

144. Карвацька С., Іванюк Р. Будапештська конвенція про кіберзлочинність як основний міжнародно-правовий стандарт щодо кіберзлочинності. *Сайт Юридичного факультету Чернівецького національного університету імені Юрія Федьковича*. 27.02.2025. URL:

https://law.chnu.edu.ua/budapeshtska-konventsiia-pro-kiberzlochynnist/#

145. Кард-шарінг. URL: https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D1%80%D0%B4%D1%88%D0%B0%D1%80%D0%B8%D0%BD%D0%B3

146. Кибератака, через которую в сеть попали секретные документы НАТО, была осуществлена на Португалию – СМИ. *Європейська правда.* 08.09.2022. URL: https://www.eurointegration.com.ua/rus/news/2022/09/8/7146443/

147. Кібербулінг. URL: https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D1%83%D0%BB%D1%96%D0%BD%D0%B3

148. Кібершпигунство. URL: https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D1%88%D0%BF%D0%B8%D0%B3%D1%83%D0%BD%D1%81%D1%82%D0%B2%D0%BE

149. Ключевая информация об атаке вирусом-вымогателем REviL на компанию Kaseya. *Хабр*. 12.07.2021. URL: https://habr.com/ru/companies/varonis/articles/567196/

150. Колот А. Міждисциплінарний підхід як передумова розвитку економічної науки та освіти. *Вісник Київського національного університету імені Тараса Шевченк*а. 2014. С.18-22.

151. Колпаков В.К. Адміністративно-деліктний правовий феномен. Монографія. Київ. Юрінком Інтер 2004. 528 с.

152. Колпаков В. Предмет адміністративного права: сучасний вимір. *Юридична Україна*. 2008. № 3. С. 33-38.

153. Конституции зарубежных государств. Учебное пособие. М. Издательство БЕК, 1996. 432 с.

154. Корченко А.О., Гребенюк В.М. Технологія виявлення та попередження кібератак. Київ. Нац. авіац. ун-т. 2021. 108 с.

155. Косенко В.В. Методологія ризик-адаптивного управління

потоками даних інфокомунікаційних мереж систем критичної інфраструктури. Дис. на здобуття наукового ступеня д-ра техн. наук; спец. 05.13.06 «Інформаційні технології». Харків, 2018. 356 с.

156. Костючков С.К. Нейрокогнітивний хакінг як інструмент активізації кіберконфліктного простору в умовах глобалізованого світу. Актуальні проблеми філософії та соціології. 2022. Вип. 38. С. 51-57.

157. Котляров В. Особливості категорії «інформаційна безпека» у міжнародному контексті. Наукові праці Міжрегіональної академії управління персоналом. Політичні науки та публічне управління. 2023. Вип. 4 (70). С. 21-26.

158. Красовська О.О. Міждисциплінарний підхід до професійної підготовки майбутніх учителів початкової школи у галузі мистецької освіти засобами інноваційних технологій. *Педагогічні науки: теорія, історія, інноваційні технології*. 2015, № 9 (53), с. 24-31.

159. Криволап Є.В. Адміністративно-правове регулювання заходів протидії кіберзагрозам актами європейського рівня. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право*». 2024. № 3 (72). С. 84-92.

160. Криволап Є.В. Адміністративно-правові засади виявлення та протидії вразливостям інформаційно-комунікаційних систем на підставі методів Bug Bounty (білий хакінг) в Україні. *VII Міжнародний молодіжний науковий юридичний форум*: [Матеріали форуму, м. Київ, Національний авіаційний університет, 16-17 травня 2024 р.] С. 145-147.

161. Криволап Є.В. Використання фейкових сайтів в російській пропаганді. *АЕРО-2024. Повітряне і космічне право*: [Матеріали Всеукраїнської конференції, м. Київ, Державне некомерційне підприємство «Державний університет «Київський авіаційний інститут», 20 листопада 2024 р.]. Тернопіль. «Вектор». С. 113-115.

162. Криволап Є.В. Вплив стратегій інформаційної та кібербзпеки на інші безпекові стратегії України. *VI Міжнародний молодіжний науковий*

юридичний форум: [Матеріали форуму, м. Київ, Національний авіаційний університет, 18 травня 2023 р.]. С. 119-121.

163. Криволап Є.В. Засади правового регулювання заходів забезпечення кібербезпеки актами європейського рівня. *Глобальні проблеми та рішення*: Матеріали 2-го Міжнародного науково-практичного Інтернет-конгресу, 10-11 квітня 2023 р. ФОП Марениченко В.В., Дніпро, Україна, С. 42-45.

164. Криволап Є.В. Засади правового регулювання заходів забезпечення кібербезпеки в контексті гарантій інформаційних прав громадян. Розділ 2.1 колективної монографії «Гарантії прав людини і громадянина в контексті європейської інтеграції України». Колективна монографія. Чернівці. Технодрук. 2023. С. 72-100.

165. Криволап Є.В. Питання застосування механізмів забезпечення інформаційної безпеки і кібербезпеки в реалізації безпекових стратегій України. *Наукові дослідження та інновації*: Матеріали 2-ї Міжнар. науково-практичної інтернет-конференції 3-4 квітня 2023 р. ФОП Марениченко В.В., Дніпро, Україна, С. 216-218.

166. Криволап Є.В. Підвищення рівня контролю і протидії вразливостям інформаційно-комунікаційних систем в аспекті відновлення України. *Правова парадигма відновлення України: проблеми та перспективи*: [Матеріали XIV Міжнародної науково-практичної конференції, м. Київ, Національний авіаційний університет, 23 лютого 2024 р.]. Тернопіль: Вектор, 2024. с. 220-223.

167. Криволап Є.В. Правові підходи до підвищення рівня кібербезпеки в Європейському Союзі (the Cyber Resilience Act, CRA). *Правова система України: європейський вектор розвитку в умовах воєнного стану*: [Матеріали XV Міжнародної науково-практичної конференції, м. Київ, Державний університет «Київський авіаційний інститут», 21 лютого 2025 р.]. Тернопіль: Вектор, 2025. С. 201-204.

168. Криволап Є.В. Публічно-правове регулювання підвищення рівня

кібербезпеки в Європейському Союзі на підставі акту про кіберстійкість (The Cyber resilience Act). *Наукові інновації та передові технології (Серія «Управління та адміністрування», Серія «Право», Серія «Економіка», Серія «Психологія», Серія «Педагогіка»)*: журнал. 2025. № 3 (43). С. 516-526.

169. Криволап Є.В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека». «Когнітивна безпека» як стійкість проти інформаційно-психологічних впливів на людину і суспільство. *Свобода, безпека та незалежність: правовий вимір*: [Матеріали XIII Міжнародної науково-практичної конференції, м. Київ, Національний авіаційний університет, 24 лютого 2023 р.]. С. 195-197.

170. Криволап Є.В., Юринець Ю.Л. До питання вразливості інформаційно-комунікаційних систем цивільної авіації: правовий аспект. *АЕРО-2023. Повітряне і космічне право*: [Матеріали Всеукраїнської конференції здобувачів вищої освіти і молодих учених, м. Київ, Національний авіаційний університет, 23 листопада 2023 р.]. Тернопіль: Вектор. С. 118-120.

171. Криволап Є.В., Юринець Ю.Л. Взаємозв'язок безпекових стратегій України з інформаційною безпекою та кібербзпекою. *Актуальні питання у сучасній науці*. 2023. № 8 (14). С. 477-487.

172. Криволап Є.В., Бєлкін Л.М., Юринець Ю.Л. Правові засади виявлення та протидії вразливостям інформаційно-комунікаційних систем на підставі методів Bug Bounty (білий хакінг) в Україні. *Впровадження інноваційних технологій та модернізація технічної складової сектору безпеки і оборони як вагомий чинник у боротьбі з агресором*: зб. матеріалів міжвідомчої науково-практичної конференції, 27 березня 2024 р., Київ / [відп. ред. Парфило О.А.]; Укр. наук.-дослід. ін.-т спец. техніки та судових експертиз Служби безпеки України. Київ : ІСТЕ СБУ, 2024. С. 99-103.

173. Криволап Є.В., Юринець Ю.Л., Бєлкін Л.М. Питання нейтралізації вразливостей інформаційно-комунікаційних систем цивільної авіації: правовий аспект. *Наукові праці Національного авіаційного університету:*

Серія «Юридичний вісник. Повітряне і космічне право». 2023. № 3 (68). С. 16-23.

174. Криволап Є.В., Юринець Ю.Л., Бєлкін Л.М. Правове регулювання заходів забезпечення кібербезпеки актами європейського рівня. *Moderní aspekty vědy: XL. Díl mezinárodní kolektivní monografie*. Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024. str. 103-114.

175. Криволап Є., Юринець Ю., Бєлкін Л., Бєлкін М. Поняття «кіберконфлікти» в системі термінології з кібербезпеки. *Innovations and New Directions in Scientific Research*. Proceedings of the 2nd International Scientific Conference (Manchester, United Kingdom, 20September2025). Lulu Press, Inc., 2025. P. 191-195.

176. Крижний А. Держслужбовцям і військовим заборонили використання Telegram на службі. *Економічна правда*. 20.09.2024. URL: https://epravda.com.ua/news/2024/09/20/719593/

177. Кримінальна відповідальність за кіберзлочини. URL: https://wiki.legalaid.gov.ua/index.php/%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%B2%D1%96%D0%B4%D0%BF%D0%BE%D0%B2%D1%96%D0%B4%D0%B0%D0%BB%D1%8C%D0%BD%D1%96%D1%81%D1%82%D1%8C_%D0%B7%D0%B0_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%BB%D0%BE%D1%87%D0%B8%D0%BD%D0%B8

178. Кузьо Тарас. Війна Путіна проти України. Революція, націоналізм і криміналітет / Пер. з англ. Андрія Павлишина. К. Дух і Літера. 2018. 560 с.

179. Кунєв Ю.Д. Забезпечення інформаційної безпеки: проблеми і перспективи розвитку. Розділ 1 колективної монографії «Забезпечення конституційних прав громадян в контексті конвенційних зобов’язань України». Колективна монографія. Київ: «Видавництво Людмила», 2022. С. 6-36.

180. Кунєв Ю.Д. Правове забезпечення інформаційної безпеки як

предмет правового дослідження. *Юридичний вісник. Повітряне і космічне право*. 2021. № 1 (58). С. 95-102.

181. Кунєв Ю.Д., Легеза Є.О. Правове забезпечення інформаційної безпеки як предмет адміністративно-правового дослідження. *Сучасне право в епоху соціальних змін*: матеріали XI Міжнар. наук.-практ. конф. 26 лютого 2021 р. Київ Т.1. С.185-187. С. 183-185.

182. Кунєв Ю.Д., Легенький М.І. Адміністративно-правова охорона регулятивних норм засобами адміністративної відповідальності. *Юридичний вісник. Повітряне і космічне право*. 2021. № 3 (60). С. 90-96.

183. Курбан О.В. Основи сучасної національної інформаційної безпеки України. *Вісник Харківської державної академії культури. Серія: Соціальні комунікації*. 2017. Вип. 50. С. 55-66.

184. Курс адміністративного права України. Підручник / В.К. Колпаков, О.В. Кузьменко, І.Д. Пастух та ін. / за ред. В.В. Коваленка. – К. : Юрінком Інтер, 2012. 808 с.

185. Кутєлєва І., Кацімон О. У Польщі фіксують зростання російських кібератак на критичну інфраструктуру. *Українська правда.* 11.10.2025. URL: https://www.pravda.com.ua/news/2025/10/11/8002329/

186. Латиш К.В. Кібервандалізм: окремі способи вчинення. Право і суспільство. 2018. № 6. С. 205-210.

187. Легенький М.І. До проблеми удосконалення системи правового забезпечення протидії булінгу. Науковий вісник Херсонського державного університету. 2025. Вип. 2. С. 11-18.

188. Леонов Б.Д., Лихова С.Я. Інформаційний тероризм як загроза національній безпеці України. *Юридичний вісник. Повітряне і космічне право*. 2021. № 2 (59). С. 170-176.

189. Лихова С.Я., Біленчук П.Д. Космічні і наземні кіберзагрози третього тисячоліття: засоби пізнання, доказування, розслідування. *Юридичний вісник. Повітряне і космічне право*. 2021. № 2 (59). С. 9-17.

190. Лихова С.Я., Сисоєва В.П. Діяльність правоохоронних органів

України у сфері забезпечення інформаційної безпеки. *Юридичний вісник. Повітряне і космічне право*. 2022. № 3 (64). С. 102-107.

191. Ліпкан В.А. Адміністративно-правові основи забезпечення національної безпеки України: автореф. дис... д-ра юрид. наук; спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». К. 2008. 34 с.

192. Ліпкан В.А. Доктрина національної безпеки: проблеми формування. *Науковий вісник Юридичної академії Міністерства внутрішніх справ*: зб. наук. праць. 2003. № 3. С. 195-198.

193. Ліпкан В.А. Доктрина недержавного забезпечення національної безпеки України. *Недержавна система безпеки підприємництва як складова національної безпеки України*. К. Вид-во Європ. ун-ту, 2004. С. 131-167.

194. Ліпкан В. Зміст пропаганди на сучасному етапі. *GOAL*. 2016. URL: http://goal-int.org/zmist-propagandi-na-suchasnomu-etapi/

194. Ліпкан В.А. Національна безпека України: навч. посіб. [2-е вид.]. К. КНТ, 2009. 576 с.

196. Ліпкан В.А. Основы права национальной безопасности. *Публичное и частное право*. 2009. № 2. С. 34-46.

197. Ліпкан В.А., Баскаков В.Ю. Адміністративно-правовий режим інформації з обмеженим доступом: монографія / за заг. ред. В.А. Ліпкана. К. ФОП О.С. Ліпкан, 2013. 344 с.

198. Ліпкан В.А., Дімчогло М.І. Консолідація інформаційного законодавства України: монографія / за заг. ред. В.А. Ліпкана. К. ФОП О.С. Ліпкан, 2014. 444 с.

199. Ліпкан В.А., Залізняк В.А. Систематизація інформаційного законодавства України: монографія / за заг. ред. В.А. Ліпкана. К. ФОП О.С. Ліпкан, 2012. 304 с.

200. Ліпкан В.А., Ліпкан О.В. Національна і міжнародна безпека у визначеннях та поняттях. 2-ге вид., доп. і перероб. К. Текст, 2008. 400 с.

201. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна

безпека України в умовах євроінтеграції. Навчальний посібник. К. КНТ. 2006. 280 с.

202. Ліпкевич С.Я., Щерба О.В. Інформаційна безпека у контексті побудови інформаційного суспільства в Україні. *Історичні записки*. 2012. Вип. 34. С. 139-146.

203. Мазник Л.В., Двуліт З.П. Управління діяльністю фахівців з кібербезпеки в умовах повномасштабного вторгнення. *Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку*. 2023. № 2 (9). С. 54-65.

204. Марк Фейгин на Лучшем Радио. Спецэфир. URL: https://www.youtube.com/watch?v=KXG5xiIEJPg

205. Маркова М.В. Інформаційно-психологічна війна: медико-психологічні наслідки та стратегії протидії. *Проблеми безперервної медичної освіти та науки*. 2016. № 4. С. 6-10.

206. Марущак А.І., Панченко В.М. До визначення поняття «інформаційна безпека». *Правничий вісник Університету «КРОК»*. 2010. Вип. 5 (1). С. 125-130.

207. Марущак А.І., Петров С.Г. Зміст поняття «державні електронні інформаційні ресурси». *Інформація і право*. 2018. № 4 (27). С. 15-21.

208. Мережевий нейтралітет. Вікіпедія. URL: https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B8%D0%B9_%D0%BD%D0%B5%D0%B9%D1%82%D1%80%D0%B0%D0%BB%D1%96%D1%82%D0%B5%D1%82

209. Миколаєць В.А., Новицька Н.Б. Еволюція правового регулювання наукового відкриття як об'єкта інтелектуальної власності. Ірпінський юридичний часопис. 2024. № 3 (16). С. 207-218.

210. Миколайчук М. Забезпечення системного підходу до формування національної безпеки України. *Національна безпека України в умовах воєнного стану*. Матеріали І Науково-практичної конференції з міжнародною участю (м. Чернігів, 06-08 березня 2024р.) / Під загальною редакцією

д.н.держ. упр., проф. З.В. Гбур Чернігів, ІПТ, 2024. С. 183-186.

211. Мінченко О. Порошенко пояснив, чому не можливо відновити доступ до ВКонтакте в Україні. *Watcher*. 30.06.2017. http://watcher.com.ua/2017/06/30/poroshenko-poyasnyv-chomu-ne-mozhlyvo-vidnovyty-dostup-do-vkontakte-v-ukrayini/

212. Мітенко О.В.Інформаційна безпека як складова національної безпеки України. *Інформаційна безпека людини, суспільства, держави*. 2019. № 1. С. 27-36.

213. Муравський В. Облік та кібербезпека. Монографія. Тернопіль. ЗУНУ. 2023. 200 с.

214. Муратов М.Я. Право на свободу слова: история и современность. Дис. … канд. юр. наук; спец. 12.00.01. 2002. 177 С.

215. Мы вдруг поняли, что народ в Донецке начал сходить с ума, – дончанин. *COMMENTS.UA*. 11.05.2016. URL: https://comments.ua/life/544390-mi-vdrug-ponyali-narod-donetske.html

216. Негода С. Курс з інформатики «Безпека в Інтернеті та захист інформації». Збірник практичних робіт. URL: https://www.calameo.com/read/00503199136c8e2ab45ea

217. Нідерланди звинуватили Китай у кібершпигунстві: хакери залізли в мережу військових. *Європейська правда – Українська правда*. 06.02.2024. URL: https://www.pravda.com.ua/news/2024/02/6/7440665/

218. Нова директива ЄС щодо стійкості критичної інфраструктури (CER DIRECTIVE). *Національний інститут стратегічних досліджень*. 12.04.2023. URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/nova-dyrektyva-yes-shchodo-stiykosti-krytychnoyi-infrastruktury

219. Новицька Н.Б., Прокопчук К.В., Скрипець В.І. Міжнародний досвід та шляхи вдосконалення врегулювання конфліктів у сфері інтелектуальної власності за допомогою медіації в національному праві. *Успіхи і досягнення у науці*. 2024. № 4 (4). С. 163-171.

220. Новости Крымнаша. Бал сатаны. *Обозреватель*. 05.05.2016. URL:

https://www.obozrevatel.com/blogs/87465-novosti-kryimnasha--bal-satanyi.htm

221. Нечай Л.О. Інформаційна безпека суб'єктів господарювання та фактори її розвитку. *Управління розвитком*. 2013. № 17. С. 145-148.

222. Новицька Н.Б., Пунда О.О., Добрянська О.Д. Принципи інформаційної політики в умовах війни та їх нормативно-правове закріплення. *Соціологія права*. 2022. № 1-2 (40-41). 2022. С. 71-76.

223. Овсянніков В.В., Дехтяр С.В., Паламарчук С.А., Черниш Ю.О., Шемендюк О.В. Аналіз нормативно-правових та організаційно-технічних аспектів забезпечення інформаційної безпеки. *Modern Information Technologies in the Sphere of Security and Defence*. 2015. № 3 (24). С. 187-193.

224. Ольховік М.В. Інформаційні права людини як основоположна складова інформаційної (національної) безпеки держави. Розділ 3 колективної монографії «Забезпечення конституційних прав громадян в контексті конвенційних зобов'язань України». Колективна монографія. Київ: «Видавництво Людмила». 2022. С. 68-86.

225. Операція Doppelgänger: як росія підробляла новини провідних європейських ЗМІ. Європейська правда. 14.06.2023. URL: https://www.eurointegration.com.ua/articles/2023/06/14/7163639

226. Павлюк О. НАТО пропонує включити кібербезпеку в нову ціль оборонних витрат. *Європейська правд*а. 28.05.2025. URL: https://www.eurointegration.com.ua/news/2025/05/28/7212622/

227. Парольний захист комп'ютерного та телекомунікаційного обладнання. Наук.-практ. посіб. Авт. кол.: М.Г. Вербенський, В.О. Криволапчук, Д.В. Смерницький та ін. Київ: «Видавництво Людмила», 2022. 42 с. (Серія «Кібербезпека»).

228. Переслідування в реалі та онлайн: як протидіяти стакеру? URL: https://supportme.org.ua/needle-and-bullying/stalking

229. Пирцхалава К.З. Актуальні питання незаконного використанням торговельних марок у доменних іменах. *Право та державне управління*. 2023. № 2. С. 237-243.

230. Понад половина українців підтримують санкції проти Медведчука, рівень підтримки закриття каналів дещо нижчий. *Детектор медіа*. 17.05.2021. URL: https://detector.media/infospace/article/188107/2021-05-17-ponad-polovyna-ukraintsiv-pidtrymuyut-sanktsii-proty-medvedchuka-riven-pidtrymky-zakryttya-kanaliv-deshcho-nyzhchyy/

231. Порнография. Википедия. URL: http://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%80%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F

232. Портников В. Радіо тисячі пагорбів. *Збруч*. 16.10.2022. URL: https://zbruc.eu/node/113449

233. Посилюємо кіберзахист: Уряд ухвалив механізм проведення Bug Bounty. Прес-офіс Міністерства цифрової трансформації України. 19.05.2023. URL: https://thedigital.gov.ua/news/posilyuemo-kiberzakhist-uryad-ukhvaliv-mekhanizm-provedennya-bug-bounty

234. Почепцов Г.Г. Информационные войны. К., Ваклер, 2000. 576 с. URL: https://litlife.club/books/265064/read

235. Почепцов Г. Контр- не всегда плохо, особенно если это контрпропаганда. Детектор медіа. 02.06.2019. URL: https://ms.detector.media/mediaanalitika/post/22973/2019-06-02-kontr-ne-vsegda-plokho-osobenno-esly-jeto-kontrpropaganda/

236. Почепцов Г. Метапропаганда как доминирование пропаганды над идеологией, а не наоборот. Хвиля. 17.09.2018. URL: https://hvylya.net/analytics/society/metapropaganda-kak-dominirovanie-propagandyi-nad-ideologiey-a-ne-naoborot.html

237. Почепцов Г.Г. Теория коммуникации. К. «Ваклер». 2001. 656 с.

238. Почепцов Г.Г., Чукут С.А. Інформаційна політика : навч. посіб. 2-ге вид. К., Знання, 2008. 559 с.

239. Право на доступ до інформації як елемент правового статусу особи. Роз’яснення Міністерства юстиції України від 03.05.2012. URL: https://zakon.rada.gov.ua/laws/show/n0012323-12#Text

240. Проблеми інформаційного законодавства України в сфері створення, поширення та використання інформації та шляхи їх вирішення: аналітична записка. *Національний інститут стратегічних досліджень*. 07.06.2013. URL: http://www.niss.gov.ua/articles/1189/

241. Размєтаєва Ю.С. Система міжнародної безпеки у світлі кіберзагроз: правові проблеми та перспективи. Актуальні проблеми сучасного міжнародного права: зб. наук. ст. за матеріалами І Харк. міжнар.-прав. читань, присвячених пам'яті проф. М.В. Яновського і В.С. Семенова, Харків, 27 листоп. 2015 р.: у 2 ч. Харків. 2015. ч. 1. С. 17-177.

242. Рік президента Зеленського, боротьба з епідемією коронавірусу, травневі свята та політичні рейтинги. *Київський міжнародний інститут соціології*. 19.02.2020. URL: https://www.kiis.com.ua/?lang=ukr&cat=reports&id=945&page=1

243. Розвиток національної системи фінансового моніторингу / Т.І. Єфименко, С.С. Гасанов, О.Є. Користін та ін. Київ. ДННУ «Акад. фін. управління», 2013. 380 с

244. Романенко Є.О., Мотренко Т.В. Закон «Про електронні комунікації» набув чинності. *Наукові перспективи*: журнал. 2021. № 1 (7). С. 260-270.

245. Російські хакери з початку війни скоїли майже 240 кібератак проти України – Microsoft. *Слово і Діло*. 28.04.2022. URL: https://www.slovoidilo.ua/2022/04/28/novyna/bezpeka/rosijski-xakery-pochatku-vijny-skoyily-majzhe-240-kiberatak-proty-ukrayiny-microsoft

246. Русаков М.О. Методы борьбы с фишингом и баннерами-вымогателями. Кібербезпека в сучасному світі: матеріали всеукраїнської науково-практичної конференції (м. Одеса, 29 листопада 2019 р.) / за ред. О.В. Дикого; уклад.: Я.І. Кузьма, Т.Ф. Стоянова, Ю.Ю. Пастернак. Одеса. Видавничий дім «Гельветика», 2019. С. 159-162.

247. Самые масштабные кибератаки на Украину. *Слово і Діло*. 24.03.2025. URL:

https://ru.slovoidilo.ua/2025/03/24/infografika/bezopasnost/samye-masshtabnye-kiberataki-ukrainu

248. Савицкий А. Как оценивают в Украине закрытие пророссийских каналов. *DW*. 04.02.2021. URL: https://www.dw.com/ru/zakrytie-prorossijskih-kanalov-v-ukraine-borba-s-propagandoj-ili-cenzura/a-56454095

249. Свобода творчества. *Википедия*. URL: https://ru.wikipedia.org/wiki/%D0%A1%D0%B2%D0%BE%D0%B1%D0%BE%D0%B4%D0%B0_%D1%82%D0%B2%D0%BE%D1%80%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%B0

250. Северина С.В. Інформаційна безпека та методи захисту інформації. *Вісник Запорізького Нац. ун-ту. Економічні науки*. 2016. № 1. С. 155-161.

251. Сєдая Ю.С. Кібервійна: основні теоретичні положення. У зб.: *Українське суспільство в умовах війни: виклики сьогодення та перспективи миротворення*: матеріали Всеукраїнської науково-практичної конференції, м. Маріуполь, 9 червня 2017 р. Маріуполь. ДонДУУ, 2017. С. 250.

252. Снопок О. Telegram, YouTube чи TikTok: звідки українці дізнаються новини. *Українська правда*. 26.07.2024. URL: https://www.pravda.com.ua/columns/2024/07/26/7467557/

253. Соломін Є. Інформаційна безпека України: від анексії до концепції через війну на сході. *Теле- та радіожурналістика*. 2016. Вип. 15. С. 68-72.

254. Сопілко І.М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Юридичний вісник. Повітряне і космічне право*. 2021. № 2 (59). С. 110-115.

255. Сопілко І.М. Інформаційні загрози та безпека сучасного українського суспільства. *Юридичний вісник. Повітряне і космічне право*. 2015. № 1. С. 75-80.

256. Сопілко І.М. Особливості протидії кіберзагрозам правовими методами та засобами. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2021. № 4 (61). С. 105-110.

257. Сопілко І.М. Роль доктрини інформаційної безпеки України в реалізації державної інформаційної політики України. *Журнал східноєвропейського права*. 2014. № 2. С. 36-41.

258. Сопілко І.М. Роль Закону України «Про основи національної безпеки України» в реалізації державної інформаційної політики України. *Юридичний науковий електронний журнал. Електронне наукове фахове видання*. 2014. № 2. С. 75-78.

259. Сопілко І.М. Становлення інформаційного суспільства та інформаційні загрози в мережі Інтернет. *Юридичний вісник. Повітряне і космічне право*. 2017. № 3. С. 61-69.

260. Сопілко І.М. Становлення мережевого суспільства та питання кібербезпеки. *Юридичний вісник. Повітряне і космічне право*. 2016. № 1. С. 79-86.

261. Сопілко І.М. Тролі, боти та бот-мережі як загрози розвитку інформаційного суспільства. *Юридичний вісник. Повітряне і космічне право*. 2016. № 4. С. 86-91.

262. Сопілко І.М., Лихова С.Я., Біленчук П.Д. Космічний кіберзлочин як загроза національній безпеці України. *Матеріали XV міжнародної науково-технічної конференції «АВІА-2021»*. К. НАУ. 2021. URL: http://conference.nau.edu.ua/index.php/AVIA/AVIA2021/paper/view/8017/6667

263. Соснін О., Повидиш В. Інформаційно-комунікаційна безпека в суспільстві: витоки проблем. *LexInform*. 05.04.2018. URL: https://lexinform.com.ua/dumka-eksperta/informatsijno-komunikatsijna-bezpeka-v-suspilstvi-vytoky-problem/

264. Справа «Ляшко проти України». Рішення по Заяві № 21040/02. Європейський Суд з прав людини. URL: http://zakon5.rada.gov.ua/laws/show/974_275

265. Справа «Редакція газети «Правоє дело» та Штекель проти України». Рішення по Заяві № 33014/05. URL: https://zakon.rada.gov.ua/laws/show/974_807#Text

266. Стародуб І. Кіберсквотинг: як захистити «візитівку» бізнесу. *Юридична газета*. 18.02.2022. № 1 (755). URL: https://yur-gazeta.com/dumka-eksperta/kiberskvoting-yak-zahistiti-vizitivku-biznesu.html

267. Суслін С. Правові аспекти міжнародного співробітництва України у сфері протидії інформаційним загрозам в умовах воєнного стану. *Експерт: парадигми юридичних наук і державного управління*. 2025. № 1 (33), с. 67-73.

268. Тарасюк А.В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи. Монографія. Київ; Одеса. Фенікс, 2020. 404 с.

269. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір. Монографія. К.: ТОВ «Видавничий дім «АртЕк», 2018. 422 с.

270. Термінологічний словник з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та корупції / Чубенко А.Г., Лошицький М.В., Павлов Д.М., Бичкова С.С., Юнін О.С. К. Ваіте, 2018. 826 с.

271. Тероризм: теоретико-прикладні аспекти. Навчальний посібник; за заг. ред. проф. В.К. Грищука. Львів. ЛьвДУВС, 2011. 328 с.

272. Технології виявлення вразливостой інформаційних систем. Лабораторний практикум / уклад.: Ю.Є. Хохлачова, В.М Кінзерявий, В.В. Погорелов та ін. К.: НАУ, 2022. 68 с.

273. Типові вразливості систем та причини їх появи. Львівський державний університет безпеки життєдіяльності. URL: https://virt.ldubgd.edu.ua/pluginfile.php/39792/mod_resource/content/4/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%8F%201.3.pdf

274. Тихомиров О.О. Ідея інформаційної гігієни в контексті інформаційної безпеки і захисту інформаційних прав людини. *Правові новели*. 2023. № 20. С. 59-65.

275. Тихомиров О.О. Класифікація інформаційних прав людини:

розвиток підходів. *Інформація і право*. 2022. № 1 (40). С. 46-63.

276. Тихомиров О.О., Коваленко О.О. Право на приватність в умовах сучасних комунікацій. *Юридичний електронний науковий журнал. Електронне видання*. 2020. № 5. С. 133−136.

277. Тітко Е.В. Історико-структурний підхід до визначення поняття і змісту права на свободу вираження поглядів. *Теорія і практика правознавства*. *Електронне фахове видання*. 2011. Т. 1. № 1. С. 3-4. URL: http://tlaw.nlu.edu.ua/issue/view/3796

278. Токарєва К.С. Забезпечення права на свободу вираження поглядів в розрізі національної безпеки України. Розділ 5 колективної монографії «Забезпечення конституційних прав громадян в контексті конвенційних зобов'язань України». Колективна монографія. Київ: «Видавництво Людмила», 2022. С. 114-137.

279. ТОП-5 вразливостей інформаційно-комунікаційних систем за статистикою ДЦКЗ: як захистити системи від зловмисників? Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/faqs/top-5-vrazlivostei-informaciino-komunikaciinikh-sistem-za-statistikoyu-dckz-yak-zakhistiti-sistemi-vid-zlovmisnikiv

280. Топчій В.В. Кібертероризм в Україні: поняття та запобігання кримінально-правовими та кримінологічними засобами. Науковий вісник Херсонського державного університету. Серія: Юридичні науки. 2015. Вип. 6 (3). С. 65-68.

281. Торяник В.М. Інформаційна безпека як складова національної безпеки держави. Роль ЗМІ в забезпеченні інформаційного суверенітету України. *Право і суспільство*. 2016. № 2. С. 151-156.

282. Трінько М. Північна Корея створює новий хакерський підрозділ із фокусом на зломи за допомогою ШІ – ЗМІ. *Українська правда. Межа.* 21.03.2025. URL: https://mezha.media/news/pivnichna-koreya-hakerskiy-pidrozdil-ta-shi-300619/

283. Тунік-Фриз В. Шахраї почали надсилати фейкові листи з

податкової. *Економічна правда*. 28.10.2025. URL: https://epravda.com.ua/power/shahraji-nadsilayut-listi-vid-imeni-podatkovoji-813443/

284. Турчинов О. Національна безпека України: виклики та пріоритети. *ЦЕНЗОР.НЕТ*. 18.08.2016. URL: https://censor.net/ru/resonance/402074/natsonalna_bezpeka_ukrani_vikliki_ta_proriteti

285. У КНУ ім. Шевченка та НАУ викладачам заборонили користуватися Telegram. *Букви*. 05.11.2024. URL: https://bukvy.org/u-knu-im-shevchenka-ta-nau-vykladacham-zaboronyly-korystuvatysya-telegram/

286. Украина в ООН официально обвинила Россию в поддержке терроризма. *Укринформ – Хвиля*. 11.05.2016. URL: https://hvylya.net/news/digest/ukraina-v-oon-ofitsialno-obvinila-rossiyu-v-podderzhke-terrorizma.html

287. Фармінг. URL: https://uk.wikipedia.org/wiki/%D0%A4%D0%B0%D1%80%D0%BC%D1%96%D0%BD%D0%B3

288. Федоренко О. Науково-інтелектуальні аспекти інформаційної безпеки України в умовах інформаційної війни. *Наукові праці Національної бібліотеки України імені В. І. Вернадського*. 2017. Вип. 46. С. 155-162.

289. Філінович В.В. Кибersталкинг: проблемы правовой защиты. *Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право»*. 2021. № 1 (58). С. 135-141.

290. Філінович В.В. Кібербезпека та загрози авіаційній сфері: правовий аспект. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2021. № 3 (60). С. 38-43. DOI: 10.18372/2307-9061.60.15950.

291. Філінович В.В. Кібербезпека та Інтернет речей: правовий аспект. *Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право»*. 2020. № 4 (57). С. 122-127.

292. Філінович В. Проблеми порушення прав людини внаслідок кіберзлочинів та шляхи їх подолання. *Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право»*. 2020. №3 (56). С. 143-148.

293. Форос Г.В., Жогов В.С. Особливості трактування поняття «кібербезпека» в сучасній юридичній науці. *Правова держава*. 2019. № 33. С. 128-134.

294. Фурашев В.М. Сутність та визначення понять «інформаційна безпека» і «безпека інформації». *Правова інформатика*. 2012. № 2. С. 51-59

295. Харебава Т. II BUSINESS & LEGAL IT FORUM: Кіберконфлікт не завершиться разом із бойовими діями, він, скоріше, тільки посилиться. Інтерв'ю: В. Стиран. 05.10.2022. URL: https://pravo.ua/ii-business-legal-it-forum-kiberkonflikt-ne-zavershytsia-razom-z-boiovymy-diiamy-vin-skorishe-posylytsia-shche-bilshe-volodymyr-styran-ekspert-z-kiberpezpeky/

296. Цифровий слід. URL: https://uk.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D0%B9_%D1%81%D0%BB%D1%96%D0%B4

297. Череватюк В.Б., Сопілко І.М., Юринець Ю.Л., Бєлкін Л.М., Криволап Є.В. Питання кібербезпеки в контексті забезпечення конституційних прав громадян. Розділ 8 колективної монографії «Забезпечення конституційних прав громадян в контексті конвенційних зобов'язань України». Колективна монографія. Київ: «Видавництво Людмила», 2022. С. 282-323.

298. Чиркин В.Е. Публичное управление. Учебник. М. Юристъ, 2004. 475 с.

299. Шевченко С.М., Складанний П.М., Негоденко О.В., Негоденко В.П. Дослідження прикладних аспектів теорії конфліктів у системах безпеки. Кібербезпека: освіта, наука, техніка. 2022, № 2 (18), С. 150-162. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/411/339

300. Шевчук С. Судовий захист прав людини: Практика Європейського

суду з прав людини у контексті західної правової традиції. К. Реферат, 2006. 848 с.

301. Школяренко В.В. Шляхи зміцнення воєнної безпеки України в умовах повномасштабного вторгнення Росії в Україну. *Наука і оборона*. 2022. № 2, с. 3-9.

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

303. Шопін А.Ю. Інформаційна безпека як фактор забезпечення конкурентоспроможності підприємства. *Управління розвитком*. 2013. № 17. С. 155-157.

304. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. К. Вид-во ТОВ «НВП «ІНТЕРСЕРВІС» 2009. 716 с.

305. Юридична енциклопедія : в 6 т. / редкол.: Ю.С. Шемшученко (відп. ред.) та ін. К. «Українська енциклопедія» ім. М.П. Бажана, 2003. Т. 5 (П – С). 736 с.

306. Юринець Ю.Л. Актуальні питання гарантування культурних прав громадян у контексті імплементації угоди про асоціацію з ЄС. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2014. № 3 (32). С. 79-83.

307. Юринець Ю.Л. Європеїзація адміністративного права України у сфері охорони культурних прав громадян. Дис. … д-ра юрид. наук. Спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». Київ. 2016. 676 с.

308. *Юринець Ю.Л., Бєлкін Л.М., Бєлкін М.Л.* Проблеми легітимізації Інтернет-ресурсів як засобів масової інформації в контексті інформаційної безпеки держави. *Юридичний вісник. Повітряне і космічне право*. 2020. № 2 (55). С. 114-122.

309. Юринець Ю.Л., Криволап Є.В. Соціальні мережі як чинник впливу

на формування іміджу закладу вищої освіти. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2025. № 2 (75). С. 201-210.

310. Юринець Ю.Л., Криволап Є.В., Сопілко І.М., Бєлкін Л.М., Бєлкін М.Л. Проблеми формування державної політики у сфері кіберконфліктів. *Успіхи і досягнення у науці* (Серія «Право», Серія «Освіта», Серія «Управління та адміністрування», Серія «Соціальні та поведінкові науки»), 2025. № 6 (16). С. 249-270.

311. Юринець Ю.Л., Сопілко І.М., Бєлкін Л.М., Бєлкін М.Л. Дослідження проблем інформаційної безпеки України на засадах міждисциплінарного підходу: соціологія, психологія, право. *Юридичний науковий електронний журнал. Електронне наукове фахове видання*. 2020. № 7. С. 300-307.

312. Ющук О.В. Інформаційна безпека користувачів мережі Інтернет. *Наукові записки Нац. ун-ту «Острозька академія». Сер.: Культура і соціальні комунікації*. 2009. Вип. 1. С. 224-231.

313. Як вбивають медіа. Інститут *постінформаційного суспільства*. 07.04.2017. URL: https://postinfosociety.com/yak-vbyvayut-media/

314. Яфонкін А.О., Шевчук В.А. Інформаційна війна проти держави та інформаційна безпека України. *Форум права*. 2017. № 5. С. 466–472.

315. *Aaron Yi Ding, Gianluca Limon De Jesus; Marijn Janssen. Ethical hacking for boosting IoT vulnerability management: a first look into bug bounty programs and responsible disclosure. Proceedings of the Eighth International Conference on Telecommunications and Remote Sensing – ICTRS '19. Ictrs '19. 2019. Rhodes, Greece: ACM Press: 49-55.*

316. Abdol Hossein Joodaki. The Ubiquitous Effect of Television and Dominant Surveillance in Ray Bradbury’s Fahrenheit 451 [Повсюдний вплив телебачення та домінантного спостереження у творі Рея Бредбері «451 градус за Фаренгейтом»]. Rupkatha Journal on Interdisciplinary Studies in Humanities. Volume VII, Number 3, 2015 General Issue.

317. Abi Tyas Tunggal, Kaushik Sen. Cybersecurity Vs. Information Security. What's the Difference? 01.06.2022. UpGuard. URL: https://www.upguard.com/blog/cyber-security-information-security#:~:text=Cybersecurity%20Vs.-,Information%20Security,integrity%2C%20and%20availability%20of%20information

318. Alison Grace Johansen. What is cyber security? What you need to know? NORTON.LifeLock. 28.04.2022. URL: https://us.norton.com/blog/malware/what-is-cybersecurity-what-you-need-to-know#

319. Aristova I., Kapitanenko N., Lyseiuk A., Kryvolap Ie., Kharytonov O. Information Sovereignty under Fire: Legal Challenges for Ukraine [Інформаційний суверенітет під вогнем критики: правові виклики для України]. *Applied Cybersecurity & Internet Governance*. 2025. Vol. 4, № 1. URL: https://www.acigjournal.com/Information-Sovereignty-under-Fire-Legal-Challenges-for-Ukraine,209993,0,2.html

320. Belkin L., Iurinets J., Belkin M., Chernyk Y. Current issues of information security of the state: the Ukrainian measurement [Актуальні питання інформаційної безпеки держави: український вимір]. Scientific approaches in jurisprudence: collective monograph. International Science Group. Boston. Primedia eLaunch, 2020. P. 76-85. URL: https://isg-konf.com

321. Bieliakov K.I., Tykhomyrov O.O., Kostenko O.V., Radovetska L.V. Digital rights in the human rights system [Цифрові права в системі прав людини]. InterEULawEast. (Q3). 2023. Vol. X (1). P. 183-207.

322. Bug Bounty. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Bug_Bounty

323. Case of Murat Vural v. Turkey. Рішення по Заяві № 9540/07. URL: https://hudoc.echr.coe.int/eng?i=001-147284

324. Case of Nilsen v. Norway. Рішення по Заяві № 23118/93. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58364%22]}

325. Case of Cengiz and Others v. Turkey. Рішення по Заяві № 48226/10 and 14027/11). URL: https://hudoc.echr.coe.int/rus?i=001-159188

326. Case of Delfi AS v. Estonia. Рішення по Заяві № 64569/09. URL: https://hudoc.echr.coe.int/rus?i=001-126635

327. Case of Savva Terentyev v. Russia. Рішення по Заяві № 10692/09. URL: https://hudoc.echr.coe.int/rus?i=001-185307

328. Case of Kilin v. Russia. Рішення по Заяві № 10271/12. URL: https://hudoc.echr.coe.int/rus?i=001-209864

329. Clean IT Project. *Wikipedia*. URL: https://en.wikipedia.org/wiki/Clean_IT_Project

330. Computer security. The Free Encyclopedia. URL: https://en.wikipedia.org/wiki/Computer_security

331. Content ID. *Wikipedia*. URL: https://uk.wikipedia.org/wiki/Content_ID

332. Council Directive 2008/114/EC «On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection» [Директива Ради 2008/114/ЄС «Про ідентифікацію та позначення європейських критичних інфраструктур та оцінку необхідності покращення їхнього захисту»]. URL: https://eur-lex.europa.eu/eli/dir/2008/114/oj/eng

333. Cyber Resilience Act. From Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Cyber_Resilience_Act.

334. Digital Rights Management. *Wikipedia*. URL: https://en.wikipedia.org/wiki/Digital_rights_management

335. Dobberstein, Laura. EU puts manufacturers on hook for smart device security. *The Register*. 16.09.2022. URL: https://www.theregister.com/2022/09/16/eu_cyber_resilience_act/

336. Dovhan O.D., Doronin I.M. Escalation of Cyber Threats to the National Interests of Ukraine and legal aspects of cyber defense, Kyiv, 2017.

337. Dupont B. L'environnement de la cybersecurite a l'horizon tendances, moteurs et implications.Note de recherche 14 Centre International de Criminology Compare. Universite de Montreal, Montreal. 2012.

338. EU Cyber Resilience Act. Briefing. *Think Tank European Parliament*. 20.12.2024. URL: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)739259

339. Filinovych V. Conceptual Grounds for Development of Effective Legal Enforcement of Intellectual Property Rights in Cyberspace. Journal of International Legal Communication [Концептуальні засади розвитку ефективного правового захисту прав інтелектуальної власності в кіберпросторі]. 2024. Vol. 13, № 2. P. 74–84.

340. Filinovych V.V. Principles of effective in enforcement in cyberspace: lessons from Ukraine and international practice [Принципи ефективного захисту прав інтелектуальної власності у кіберпросторі: уроки України та міжнародна практика]. *Юридичний вісник. Повітряне і космічне право*. 2025. № 2 (75). С. 24-29.

341. Fruhlinger J. What is information security? Definition, principles, and jobs. *CSO United States. 17.01.2020.* URL: https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html

342. Guoqiang Fu, Криволап Є.В. Особливості термінології в англомовній літературі у сфері кібербезпеки. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2023. № 1 (66). С. 63-71.

343. Huz A., Radovetska L., Tykhomyrov O., Tugharova O., Shepeta O. Methodology of legal research in the security field [Методологія правових досліджень у сфері безпеки]. *Military Logistics Systems* (Q3). 2024. 60 (1), 117-134.

344. Iurynets Juliya, Belkin Leonid, Belkin Mark, Kryvolap Evgeny. Legal regulation of internet resources: the principles of a humanistic approach [Правове регулювання інтернет-ресурсів: принципи гуманістичного підходу]. Digital Transformation in Ukraine: AI, Metaverse, and Society 5.0. Scientific Approbation. Monographe. Dieted by: Oleksii Kostenko, Yuriy Yekhanurov.

SciFormat Publishing Inc.Canada, 2024. P. 52-63.

345. James A. Lewis. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. The Office of Justice Programs. An official website of the United States government, Department of Justice. December 2002. URL: https://www.ojp.gov/ncjrs/virtual-library/abstracts/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats

346. Kostenko O.M., Bieliakov K.I., Tykhomyrov O.O, Aristova I.V. Legal personality» of artificial intelligence: methodological problems of scientific reasoning by Ukrainian and EU experts [«Правосуб'єктність» штучного інтелекту: методологічні проблеми наукового обґрунтування експертами України та ЄС]. *AI & SOCIETY* (Q1). February 2023.

347. Legenkyi M., Piankivska L., Tolbatov A. Legal basis for cybersecurity in Ukraine under martial law [Правові основи кібербезпеки в Україні в умовах воєнного стану] / CH&CMiGIN'24: Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, January 24–27, 2024, Kyiv, Ukraine. С. 334-342.

348. Lewis A.J., Neuneck G. The Cyber Index. International security trends and realities, New York and Geneva, United Nations Institute for Disarmament Research, 2013.

349. Lubenets S., Harchenko I., Pavlenko Y. Current problems of international information security. *The Journal of V.N. Karazin Kharkiv National University*. 2023. Vol. 17, pp. 42–48.

350. Luidold C., Jungbauer C. Cybersecurity policy framework requirements for the establishment of highly interoperable and interconnected health data spaces. *Frontiers in Medicine*. 2024. Vol. 11.

351. Lykhova S.Ya. Computer safety of aviation [Комп'ютерна безпека авіації]. *Юридичний вісник. Повітряне і космічне право*. 2022. № 4 (65). С. 24-29.

352. Matt Rosenthal. 5 Types of Cyber Security. MINDCORE Services. 05.09.2018. URL: https://mind-core.com/blogs/cybersecurity/5-types-of-cyber-

security/

353. Maskun S.H. Cyber Security: Rule of Use Internet Safely. Journal of Law, Policy and Globalization. 2013. Vol.15. P. 22.

354. Montalbano E., Writer C. Pegasus Spyware Infections Proliferate Across iOS, Android Devices. *DARKREADING*. 04.12.2024. URL: https://www.darkreading.com/endpoint-security/pegasus-spyware-infections-ios-android-devices

355. New EU Regulation Requires Cybersecurity for Software and Smart Devices. URL: https://connectontech.bakermckenzie.com/new-eu-regulation-requires-cybersecurity-for-software-and-smart-devices/

354. NIS2 Explained: Demystifying Directive (EU) 2022/2555. *Infoblox*. February 6, 2024. URL: https://blogs.infoblox.com/security/nis2-explained-demystifying-directive-eu-2022-2555/

357. Ros Krasny. Russia Is Boosting Its Cyber Attacks on Ukraine, Allies, Microsoft Says. Bloomberg. December 3, 2022. URL: https://www.bloomberg.com/news/articles/2022-12-03/russian-cyber-attacks-against-ukraine-likely-microsoft-says?srnd=premium-europe

358. Roth v. United States. U.S. Supreme Court. Рішення Верховного Суду США від 24.06.1957 р. URL: https://supreme.justia.com/cases/federal/us/354/476/

359. Schatz D., Bashroush R., Wall J. Towards a Mor ds a More Representativ esentative Definition of Cyber Security e Definition of Cyber Security. *Journal of Digital Forensics, Security and Law. 2017. № 2. P. 54-74.*

360. The European Cyber Resilience Act (CRA). URL: https://www.european-cyber-resilience-act.com/

361. The NIS2 Directive. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

362. Tykhomyrov O.O., Tykhomyrov D.O., Radovetska L.V., Vatral A.V. Informational human obligations: state and prospects of doctrine interpretation

[Інформаційні обов'язки людини: стан та перспективи інтерпретації доктрини]. *The Age of Human Rights Journal* (Q4). 2023. № 21. e 7698.

363. UN General Assembly Resolution 57/329, adopted at the 78th plenary meeting of the 57th session, 2002. URL: https://research.un.org/en/docs/ga/quick/regular/57

364. Vulnerability (computing). The Free Encyclopedia. URL: https://en.wikipedia.org/wiki/Vulnerability_(computing)

365. Watermark. *Wikipedia*. URL: https://en.wikipedia.org/wiki/Watermark

366. Zetter Kim. Feds Say That Banned Researcher Commandeered a Plane. Wired. 2015. May 15. URL: https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/

ДОДАТКИ

ДОДАТОК А

СПИСОК ПРАЦЬ, ОПУБЛІКОВАНИХ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України:

1. Бєлкін Л.М., Юринець Ю.Л., Бєлкін М.Л., Криволап Є.В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020-2021 років. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2022. № 3 (64). С. 78-86. DOI: https://doi.org/10.18372/2307-9061.64.16893

2. Guoqiang Fu, Криволап Є.В. Особливості термінології в англомовній літературі у сфері кібербезпеки. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2023. № 1 (66). С. 63-71. DOI: https://doi.org/10.18372/2307-9061.66.17419

3. Криволап Є.В., Юринець Ю.Л., Бєлкін Л.М. Питання нейтралізації вразливостей інформаційно-комунікаційних систем цивільної авіації: правовий аспект. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2023. № 3 (68). С. 16-23. DOI: https://doi.org/10.18372/2307-9061.68.17969

4. Криволап Є.В., Юринець Ю.Л. Взаємозв'язок безпекових стратегій України з інформаційною безпекою та кібербзпекою. *Актуальні питання у сучасній науці*. 2023. № 8 (14). С. 477-487. DOI: https://doi.org/10.52058/2786-6300-2023-8(14)-477-487

5. Криволап Є.В. Адміністративно-правове регулювання заходів протидії кіберзагрозам актами європейського рівня. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2024. № 3 (72). С. 84-92. DOI: https://doi.org/10.18372/2307-9061.72.19064

6. Юринець Ю.Л., Криволап Є.В. Соціальні мережі як чинник впливу

на формування іміджу закладу вищої освіти. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право»*. 2025. № 2 (75). С. 201-210. DOI: https://doi.org/10.18372/2307-9061.75.20235

7. Криволап Є.В. Публічно-правове регулювання підвищення рівня кібербезпеки в Європейському Союзі на підставі акту про кіберстійкість (The Cyber resilience Act). *Наукові інновації та передові технології (Серія «Управління та адміністрування», Серія «Право», Серія «Економіка», Серія «Психологія», Серія «Педагогіка»)*: журнал. 2025. № 3 (43). С. 516-526. DOI: https://doi.org/10.52058/2786-5274-2025-3(43)-516-526

8. Юринець Ю.Л., Криволап Є.В., Сопілко І.М., Бєлкін Л.М., Бєлкін М.Л. Проблеми формування державної політики у сфері кіберконфліктів. *Успіхи і досягнення у науці* (Серія «Право», Серія «Освіта», Серія «Управління та адміністрування», Серія «Соціальні та поведінкові науки»), 2025. № 6 (16). С. 249-270. DOI: https://doi.org/10.52058/3041-1254-2025-6(16)-249-270

Наукові праці, які засвідчують апробацію дисертації:

9. Криволап Є.В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека». «Когнітивна безпека» як стійкість проти інформаційно-психологічних впливів на людину і суспільство. *Свобода, безпека та незалежність: правовий вимір*: [Матеріали XIII Міжнародної науково-практичної конференції, м. Київ, Національний авіаційний університет, 24 лютого 2023 р.]. С. 195-197.

10. Криволап Є.В. Питання застосування механізмів забезпечення інформаційної безпеки і кібербезпеки в реалізації безпекових стратегій України. *Наукові дослідження та інновації*: Матеріали 2-ї Міжнар. науково-практичної інтернет-конференції 3-4 квітня 2023 р. ФОП Марениченко В.В., Дніпро, Україна, С. 216-218.

11. Криволап Є.В. Засади правового регулювання заходів забезпечення

кібербезпеки актами європейського рівня. *Глобальні проблеми та рішення*: Матеріали 2-го Міжнародного науково-практичного Інтернет-конгресу, 10-11 квітня 2023 р. ФОП Марениченко В.В., Дніпро, Україна, С. 42-45.

12. Криволап Є.В. Вплив стратегій інформаційної та кібербзпеки на інші безпекові стратегії України. *VI Міжнародний молодіжний науковий юридичний форум*: [Матеріали форуму, м. Київ, Національний авіаційний університет, 18 травня 2023 р.]. С. 119-121.

13. Криволап Є.В., Юринець Ю.Л. До питання вразливості інформаційно-комунікаційних систем цивільної авіації: правовий аспект. *АЕРО-2023. Повітряне і космічне право*: [Матеріали Всеукраїнської конференції здобувачів вищої освіти і молодих учених, м. Київ, Національний авіаційний університет, 23 листопада 2023 р.]. Тернопіль: Вектор. С. 118-120.

14. Криволап Є.В. Підвищення рівня контролю і протидії вразливостям інформаційно-комунікаційних систем в аспекті відновлення України. *Правова парадигма відновлення України: проблеми та перспективи*: [Матеріали XIV Міжнародної науково-практичної конференції, м. Київ, Національний авіаційний університет, 23 лютого 2024 р.]. Тернопіль: Вектор, 2024. с. 220-223.

15. Криволап Є.В., Бєлкін Л.М., Юринець Ю.Л. Правові засади виявлення та протидії вразливостям інформаційно-комунікаційних систем на підставі методів bug bounty (білий хакінг) в Україні. *Впровадження інноваційних технологій та модернізація технічної складової сектору безпеки і оборони як вагомий чинник у боротьбі з агресором*: зб. матеріалів міжвідомчої науково-практичної конференції, 27 березня 2024 р., Київ / [відп. ред. Парфило О.А.] ; Укр. наук.-дослід. ін.-т спец. техніки та судових експертиз Служби безпеки України. Київ : ІСТЕ СБУ, 2024. С. 99-103.

16. Криволап Є.В. Адміністративно-правові засади виявлення та протидії вразливостям інформаційно-комунікаційних систем на підставі методів bug bounty (білий хакінг) в Україні. *VII Міжнародний молодіжний*

науковий юридичний форум: [Матеріали форуму, м. Київ, Національний авіаційний університет, 16-17 травня 2024 р.] С. 145-147.

17. Бєлкін М.Л., Криволап Є.В., Юринець Ю.Л. Адміністративно-правове регулювання нейтралізації вразливостей інформаційно-комунікаційних систем. *Збірник матеріалів «Актуальні питання забезпечення кібербезпеки» IX Міжнародної науково-практичної конференції* (м. Київ, 13 листопада 2024 року). Київ. МАУП. 13 листопада 2024 року. С 38-42.

18. Криволап Є.В. Правові підходи до підвищення рівня кібербезпеки в Європейському Союзі (the Cyber Resilience Act, CRA). *Правова система України: європейський вектор розвитку в умовах воєнного стану*: [Матеріали XV Міжнародної науково-практичної конференції, м. Київ, Державний університет «Київський авіаційний інститут», 21 лютого 2025 р.]. Тернопіль: Вектор, 2025. С. 201-204.

19. Криволап Є., Юринець Ю., Бєлкін Л., Бєлкін М. Поняття «кіберконфлікти» в системі термінології з кібербезпеки. *Innovations and New Directions in Scientific Research*: Proceedings of the 2nd International Scientific Conference (Manchester, United Kingdom, 20September2025). Lulu Press, Inc., 2025. P. 191-195.

20. Криволап Є.В. Використання фейкових сайтів в російській пропаганді. *АЕРО-2024. Повітряне і космічне право*: [Матеріали Всеукраїнської конференції, м. Київ, Державне некомерційне підприємство «Державний університет «Київський авіаційний інститут», 20 листопада 2024 р.]. Тернопіль. «Вектор». С. 113-115.

21. Юринець Ю.Л., Криволап Є.В., Бєлкін Л.М. Використання соціальних мереж для формування іміджу закладів вищої освіти. *Соціально-економічний розвиток у контексті викликів сьогодення*: матеріали III Міжнародної науково-практичної конференції / Східноєвропейський центр наукових досліджень (Одеса, 16 серпня 2025 р). Research Europe, 2025. С. 123-127.

Публікації, що додатково висвітлюють результати роботи:

Наукова стаття, опублікована в зарубіжному журналі (видання підлягає індексації у наукометричній базі «Scopus»)

22. Aristova I., Kapitanenko N., Lyseiuk A., Kryvolap Ie., Kharytonov O. Information Sovereignty under Fire: Legal Challenges for Ukraine [Інформаційний суверенітет під вогнем критики: правові виклики для України]. *Applied Cybersecurity & Internet Governance*. 2025. Vol. 4, № 1. URL: https://www.acigjournal.com/Information-Sovereignty-under-Fire-Legal-Challenges-for-Ukraine,209993,0,2.html

Розділи колективних монографій, що рекомендова до друку вченою радою факультету:

23. Череватюк В.Б., Сопілко І.М., Юринець Ю.Л., Бєлкін Л.М., Криволап Є.В. Питання кібербезпеки в контексті забезпечення конституційних прав громадян. Розділ 8 колективної монографії «Забезпечення конституційних прав громадян в контексті конвенційних зобов'язань України». Колективна монографія. Київ: «Видавництво Людмила», 2022. С. 282-323.

24. Криволап Є.В. Засади правового регулювання заходів забезпечення кібербезпеки в контексті гарантій інформаційних прав громадян. Розділ 2.1 колективної монографії «Гарантії прав людини і громадянина в контексті європейської інтеграції України». Колективна монографія. Чернівці. Технодрук. 2023. С. 72-100.

Розділи колективних монографій, виданих у зарубіжних країнах

25. Криволап Є.В., Юринець Ю.Л., Бєлкін Л.М. Правове регулювання заходів забезпечення кібербезпеки актами європейського рівня. Moderní aspekty vědy: XL. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024. str. 103-114.

26. Iurynets Juliya, Belkin Leonid, Belkin Mark, Kryvolap Evgeny. Legal regulation of internet resources: the principles of a humanistic approach [Правове

регулювання інтернет-ресурсів: принципи гуманістичного підходу]. Digital Transformation in Ukraine: AI, Metaverse, and Society 5.0. Scientific Approbation. Monographe. Dieted by: Oleksii Kostenko, Yuriy Yekhanurov. SciFormat Publishing Inc.Canada, 2024. P. 52-63.

ДОДАТОК Б

ДОДАТОК Б1

Норми деліктів за КУпАП

№ статті КУпАП	Назва статті	Зміст (гіпотеза)
95-1	Порушення вимог нормативно-правових актів та нормативних документів з питань технічної експлуатації електричних станцій і мереж, енергетичного обладнання	Порушення вимог нормативно-правових актів та нормативних документів з питань технічної експлуатації електричних станцій і мереж, енергетичного обладнання суб'єктів електроенергетики, суб'єктів відносин у сфері теплопостачання та споживачів електричної енергії
147	Порушення правил охорони телекомунікаційних мереж	Порушення правил охорони телекомунікаційних мереж або пошкодження телекомунікаційної мережі чи технічних засобів телекомунікації, чи споруд електрозв'язку, що входять до складу телекомунікаційної мережі
148-1	Порушення Правил надання та отримання телекомунікаційних послуг	Здійснення дій, що призвели до зниження якості функціонування телекомунікаційних мереж, або самовільне (без відома оператора телекомунікацій) отримання телекомунікаційних послуг
148-2	Порушення порядку та умов надання послуг зв'язку в мережах загального користування	Порушення порядку та умов надання послуг зв'язку в мережах загального користування; Відмова оператора зв'язку надати споживачу вичерпну інформацію щодо змісту, якості та порядку надання телекомунікаційних послуг, що ним надаються та/або отримані споживачем протягом останніх шести місяців, а також порушення встановленого законом строку оприлюднення тарифів, які встановлюються операторами телекомунікацій самостійно
148-3	Використання засобів зв'язку з метою, що суперечить інтересам держави, з метою порушення громадського порядку та посягання на честь і гідність громадян	Використання засобів зв'язку з метою, що суперечить інтересам держави, з метою порушення громадського порядку та посягання на честь і гідність громадян -
148-4	Використання технічних засобів та обладнання, що застосовуються в мережах зв'язку загального користування, без документа про підтвердження відповідності	Використання технічних засобів та обладнання, що застосовуються в мережах зв'язку загального користування операторами зв'язку без документа про підтвердження відповідності
148-5	Порушення правил про взаємоз'єднання	Відмова в наданні необхідної інформації для взаємоз'єднання телекомунікаційних мереж, доступу до

	телекомунікаційних мереж загального користування	цих мереж у всіх технічно можливих місцях, інформації щодо ідентифікації виклику і його тривалості між телекомунікаційними мережами, відмова оператора, телекомунікацій з істотною ринковою перевагою на ринку певних телекомунікаційних послуг, подати на затвердження до національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, пропозиції щодо взаємоз'єднання телекомунікаційних мереж, відмова у виконанні рішення, яке прийняте національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, і набрало чинності
164-17	Порушення умов і правил, що визначають порядок припинення порушень авторського права і (або) суміжних прав з використанням мережі Інтернет	Порушення умов і правил, що визначають порядок припинення порушень авторського права і (або) суміжних прав з використанням мережі Інтернет, у тому числі невчинення власником веб-сайту, постачальником послуг хостингу передбачених законодавством про авторське право і суміжні права дій щодо унеможливлення доступу користувачів мережі Інтернет до об'єктів авторського права і (або) суміжних прав, ненадання або несвоєчасне надання відповіді на заяву суб'єкта авторського права і (або) суміжних прав власником веб-сайту, постачальником послуг хостингу, наведення завідомо недостовірних відомостей у відповіді на заяву суб'єкта авторського права і (або) суміжних прав, власником веб-сайту, постачальником послуг хостингу, а також нерозміщення власниками веб-сайтів, постачальниками послуг хостингу на власних веб-сайтах, в публічних базах даних записів про доменні імена (WHOIS) достовірної інформації про себе
164-18	Наведення завідомо недостовірної інформації у заявах про припинення авторського права і (або) суміжних прав, вчинених з використанням мережі Інтернет	Наведення особою завідомо недостовірної інформації щодо наявності авторського права і (або) суміжного права у заяві про припинення порушень авторського права і (або) суміжних прав з використанням мережі Інтернет, направленій відповідно до законодавства про авторське право і суміжні права
164-19	Порушення порядку надання інформації, необхідної для здійснення оцінки фіскальних ризиків, та невжиття заходів у сфері управління фіскальними ризиками	Ненадання, несвоєчасне надання посадовими особами центральних і місцевих органів виконавчої влади, фондів загальнообов'язкового державного соціального і пенсійного страхування, фінансових установ, суб'єктів господарювання державного сектору економіки та господарських товариств, 50 і більше відсотків акцій (часток) яких належать господарським товариствам, частка держави в яких становить 100 відсотків, інформації, необхідної для здійснення оцінки фіскальних ризиків, або надання завідомо недостовірної інформації центральному органу виконавчої влади, що забезпечує формування та реалізує державну фінансову і бюджетну політику

		¶ Невжиття особами, зазначеними у частині першій цієї статті, передбачених законодавством заходів у сфері управління фіскальними ризикам¤
172-5¤	Незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових або інших визначених законом повноважень¤	Незаконне розголошення або використання в інший спосіб особою у своїх інтересах інформації, яка стала їй відома у зв'язку з виконанням службових або інших визначених законом повноважень, -¶ Незаконне розголошення або використання в інший спосіб особою у своїх інтересах чи в інтересах іншої фізичної або юридичної особи інформації про викривача, його близьких осіб чи інформації, що може ідентифікувати особу викривача, його близьких осіб, яка стала їй (їм) відома у зв'язку з виконанням службових або інших визначених законом повноважень, -¤
188-7¤	Невиконання законних вимог національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації¤	Невиконання законних вимог національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, щодо усунення порушень законодавства про телекомунікації, поштовий зв'язок та радіочастотний ресурс України, або ненадання їм документів та інформації, необхідних для здійснення державного нагляду¤
188-31¤	Невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України¤	Невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України щодо усунення порушень законодавства про криптографічний та технічний захист державних інформаційних ресурсів, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, і законодавства у сферах електронних довірчих послуг та електронної ідентифікації, а також створення інших перешкод для виконання покладених на них обов'язків¤
195-5¤	Незаконне зберігання спеціальних технічних засобів негласного отримання інформації¤	Незаконне зберігання спеціальних технічних засобів негласного отримання інформації¤
212-2¤	Порушення законодавства про державну таємницю¤	Порушення законодавства про державну таємницю, а саме:¶ 1)°недодержання встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації;¶ 2)°засекречування інформації:¶ про стан довкілля, про якість харчових продуктів і предметів побуту;¶ про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися та загрожують безпеці громадян;¶ про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку,

		освіти та культури населення;¶ про факти порушень прав і свобод людини і громадянина;¶ про незаконні дії органів державної влади, органів місцевого самоврядування та їх посадових осіб;¶ іншої інформації, яка відповідно до законів та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути засекречена;¶ 3)°безпідставне засекречування інформації;¶ 4)°надання грифа секретності матеріальним носіям конфіденційної або іншої таємної інформації, яка не становить державної таємниці, або ненадання грифа секретності матеріальним носіям інформації, що становить державну таємницю, а також безпідставне скасування чи зниження грифа секретності матеріальних носіїв секретної інформації;¶ 5)°порушення встановленого законодавством порядку надання допуску та доступу до державної таємниці;¶ 6)°невжиття заходів щодо забезпечення охорони державної таємниці та незабезпечення контролю за охороною державної таємниці;¶ 7)°провадження діяльності, пов'язаної з державною таємницею, без отримання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщення державних замовлень на виконання робіт, доведення мобілізаційних завдань, пов'язаних з державною таємницею, в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах, організаціях, яким не надано спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею;¶ 8)°недодержання вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства та проведення роботи з ними;¶ 9)°невиконання норм і вимог криптографічного та технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення її конфіденційності, цілісності і доступності,-¤
212-3¤	Порушення права на інформацію та права на звернення¶ ¤	Неоприлюднення інформації, обов'язкове оприлюднення якої передбачено законами України°"Про доступ до публічної інформації",°"Про оцінку впливу на довкілля",°"Про засади моніторингу, звітності та верифікації викидів парникових газів",°"Про особливості доступу до інформації у сферах постачання електричної енергії, природного газу, теплопостачання, централізованого постачання гарячої води, централізованого питного водопостачання та водовідведення",°"Про доступ до архівів репресивних органів комуністичного тоталітарного режиму 1917-1991

		років"°та·"Про·запобігання·корупції";¶ Порушення°Закону·України°"Про·доступ·до·публічної·інформації",·а·саме:·необґрунтоване·віднесення·інформації·до·інформації·з·обмеженим·доступом,·ненадання·відповіді·на·запит·на·інформацію,·ненадання·інформації,·неправомірна·відмова·в·наданні·інформації,·несвоєчасне·або·неповне·надання·інформації,·надання·недостовірної·інформації;¶ Порушення·вимог°Закону·України°"Про·доступ·до·архівів·репресивних·органів·комуністичного·тоталітарного·режиму·1917-1991·років",·а·саме·необґрунтоване·віднесення·інформації·до·інформації·з·обмеженим·доступом,·ненадання·відповіді·на·запит·на·інформацію,·ненадання·інформації,·неправомірна·відмова·в·наданні·інформації,·неповне·надання·інформації,·неповідомлення·про·подовження·строку·розгляду·запиту,·відстрочення·розгляду·запиту,·крім·випадків,·визначених·цим·Законом;¶ Обмеження·доступу·до·інформації·або·віднесення·інформації·до·інформації·з·обмеженим·доступом,·якщо·це·прямо·заборонено·законом;¶ Неправомірна·відмова·в·наданні·інформації,·несвоєчасне·або·неповне·надання·інформації,·надання·інформації,·що·не·відповідає·дійсності,·у·відповідь·на·адвокатський·запит,·запит·кваліфікаційно-дисциплінарної·комісії·адвокатури,·її·палати·або·члена·відповідно·до°Закону·України·"Про·адвокатуру·та·адвокатську·діяльність"°-¶ Ненадання·доступу·до·судового·рішення·або·матеріалів·справи·за·заявою·особи,·а·також·інше·порушення°Закону·України·"Про·доступ·до·судових·рішень";¶ Незаконна·відмова·у·прийнятті·та·розгляді·звернення,·інше·порушення°Закону·України·"Про·звернення·громадян";¶ Несвоєчасне·внесення·документів·до·Єдиного·реєстру·з·оцінки·впливу·на·довкілля·згідно·із°Законом·України·"Про·оцінку·впливу·на·довкілля",·обмеження·доступу·до·інформації,·внесеної·до·Єдиного·реєстру·з·оцінки·впливу·на·довкілля;¶ Неправомірна·відмова·в·наданні·інформації,·несвоєчасне·або·неповне·надання·інформації,·надання·недостовірної·інформації·на·звернення·Національної·комісії·з·реабілітації,·регіональної·комісії·з·реабілітації·відповідно·до°Закону·України°"Про·реабілітацію·жертв·репресій·комуністичного·тоталітарного·режиму·1917-1991·років";¶ Нерозкриття,·порушення·строків·або·порядку·розкриття·інформації·у·видобувних·галузях·відповідно·до·Закону·України°"Про·забезпечення·прозорості·у·видобувних·галузях";¶ Неоприлюднення,·несвоєчасне·оприлюднення·

		інформації, оприлюднення недостовірної, неточної або неповної інформації, обов'язкове оприлюднення якої передбачено Законом України "Про відкритість використання публічних коштів"; Повторне протягом року вчинення порушення, передбаченого частиною дванадцятою цієї статті, за яке особу вже було піддано адміністративному стягненню.
212-5	Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію	Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, що призвело до розголошення такої інформації
212-6	Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем	Здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах; Незаконне копіювання інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі; Безоплатне незаконне розповсюдження інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі; Незаконний збут інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі.

ДОДАТОК Б2¶

¶

Класифікація виявлених вразливостей відповідно до рівня винагороди дослідника (ів)¶

¶

Категорія вразливостей¤	Вразливості¤	Винагорода¤
P1¤	File Inclusion, RCE, SQL Injection, XXE, Authentication Bypass, Critically Sensitive Data, Command Injection, Hardcoded Password¤	¤
P2¤	XSS (P2 specific), SSRF, CSRF (ApplicationWide), Application-Level DOS (NOT DDOS), Hardcoded Password, Weak Password Reset Implementation¤	¤
P3¤	HTTP Response Manipulation, Content Spoofing, Session Fixation, XSS and SSRF (P3 specific)¤	¤

¶

ДОДАТОК Б3

Глобальні загрози та проблеми безпеки в Інтернеті речей (IoT)

№	Загрози та проблеми безпеки в Інтернеті речей	%
1	Атаки на пристрої IoT, які можуть вплинути на критичні операції	33
2	Відсутність персоналу для впровадження безпеки Ioi’	32
3	Захист конфіденційних даних, створених пристроєм IoT	31
4	Ідентифікація або виявлення конфіденційних даних, створених пристроєм IoT	27
5	Втрата або крадіжка пристроїв IoT	27
6	Відсутність систем безпеки та засобів контролю в середовищі IoT	26
7	Порушення конфіденційності, пов’язані з даними, створеними пристроєм IoT	26
8	Відсутність ефективного контролю доступу/автентифікації пристрою	26
9	Відсутність галузевих стандартів для захисту пристроїв IoT	25
10	Перевірка цілісності даних, зібраних пристроями IoT (ідентифікація пристрою, надання)	7
11	Привілейований доступ користувачів до пристроїв IoT	2

Джерело: Муравський В. Облік та кібербезпека. Монографія. Тернопіль. ЗУНУ. 2023. 200 с.

ДОДАТОК Б4¶

ТОП-5 вразливостей інформаційно-комунікаційних систем за статистикою Державного центру кіберзахисту Держспецзв'язку (ДЦКЗ Держспецзв'язку)¶

Джерело: https://cip.gov.ua/ua/faqs/top-5-vrazlivostei-informaciino-komunikaciinikh-sistem-za-statistikoyu-dckz-yak-zakhistiti-sistemi-vid-zlovmisnikiv¶

¶

№п/п	Зміст вразливості	Характеристика вразливості
1.	Використання застарілого (вразливого) програмного забезпечення та/або операційних систем	Фахівці радять регулярно оновлювати операційні системи та програмне забезпечення до останніх версій, оскільки це може значно покращити швидкість та ефективність роботи програм. При цьому оновлюється і система безпеки. Також варто відмовитися від використання програмного забезпечення, що не підтримується виробником, застосувати мікросегментацію (техніку, яка забезпечує детальний контроль над мережевим трафіком, розділяючи його на менші, ізольовані сегменти) та обмежити доступ до систем, регулярне оновлення яких є проблематичним
2.	Надмірна кількість відкритих сервісів	Для усунення цієї вразливості фахівці радять провести аудит відкритих портів для виявлення незахищених сервісів та закрити всі невикористовувані порти і служби. Також варто використовувати брандмауер (Firewall) для обмеження доступу лише для дозволених IP-адрес, впровадити список дозволених сервісів (whitelist) та заблокувати всі інші.
3.	Недоліки у налаштуваннях мережевого обладнання, зокрема порушення контролю доступу	Порушення контролю доступу – ситуації, коли користувачі отримують доступ до ресурсів або функцій, не маючи на це відповідних прав. Для виправлення цієї вразливості спеціалісти радять використовувати список контролю доступу (ACL) для обмеження міжмережевої взаємодії, відокремити критичні сервіси в окремі віртуальні локальні комп'ютерні мережі (VLAN) або захищені зони. Також радять впровадити DMZ (Demilitarized Zones) для сервісів, які доступні з мережі Інтернет, та моніторинг трафіка для виявлення підозрілої активності. А ще застосувати фільтрацію MAC-адрес (адрес керування доступом до середовища) або 802.1X аутентифікацію (протокол контролю доступу клієнт-сервер, що дозволяє встановлювати автентичність та забороняє підключатись до локальної мережі через загальнодоступні порти комутатора)
4.	Недотримання вимог кібергігієни	Дотримання базових правил кібергігієни допомагає захистити пристрій користувача від ураження шкідливим програмним забезпеченням та можливого викрадення конфіденційної інформації. У цьому випадку фахівці наголошують на необхідності впровадження політики складних паролів – пароль має складатися з мінімум 12 символів та змінюватися кожні 90 днів. Також радять використовувати спеціалізовані менеджери паролів і

		заборонити· зберігання· паролів· у· відкритому· вигляді,· регулярно· проводити· тренінги· з· кібербезпеки,· не· допускати· зберігання· файлів· уніфікованого· електронного· підпису· на· незахищених· носіях· інформації.¤
5.8	Особливості· використання· віддаленого· доступу¤	Віддалений· доступ· дозволяє· користувачу· отримувати· доступ· до· систем· і· даних· та· керувати· ними· завдяки· підключенню· до· комп'ютера· або· мережі· з· іншого· місця.· °При· цьому· треба· дотримуватися· порад· фахівців,· аби· не· стати· жертвою· зловмисників· під· час· використання· віддаленого· доступу.· Зокрема,· використовувати· VPN· (віртуальна· приватна· мережа)· виключно· зі· стійкими· алгоритмами· шифрування.· Впровадити· двофакторну· автентифікацію· для· доступу· до· критичних· ресурсів· та· встановити· обмеження· доступу· за· IP-адресами,· а· також· вимкнути· віддалений· доступ· для· облікових· записів· з· правами· адміністратора.¤

ДОДАТОК Б5

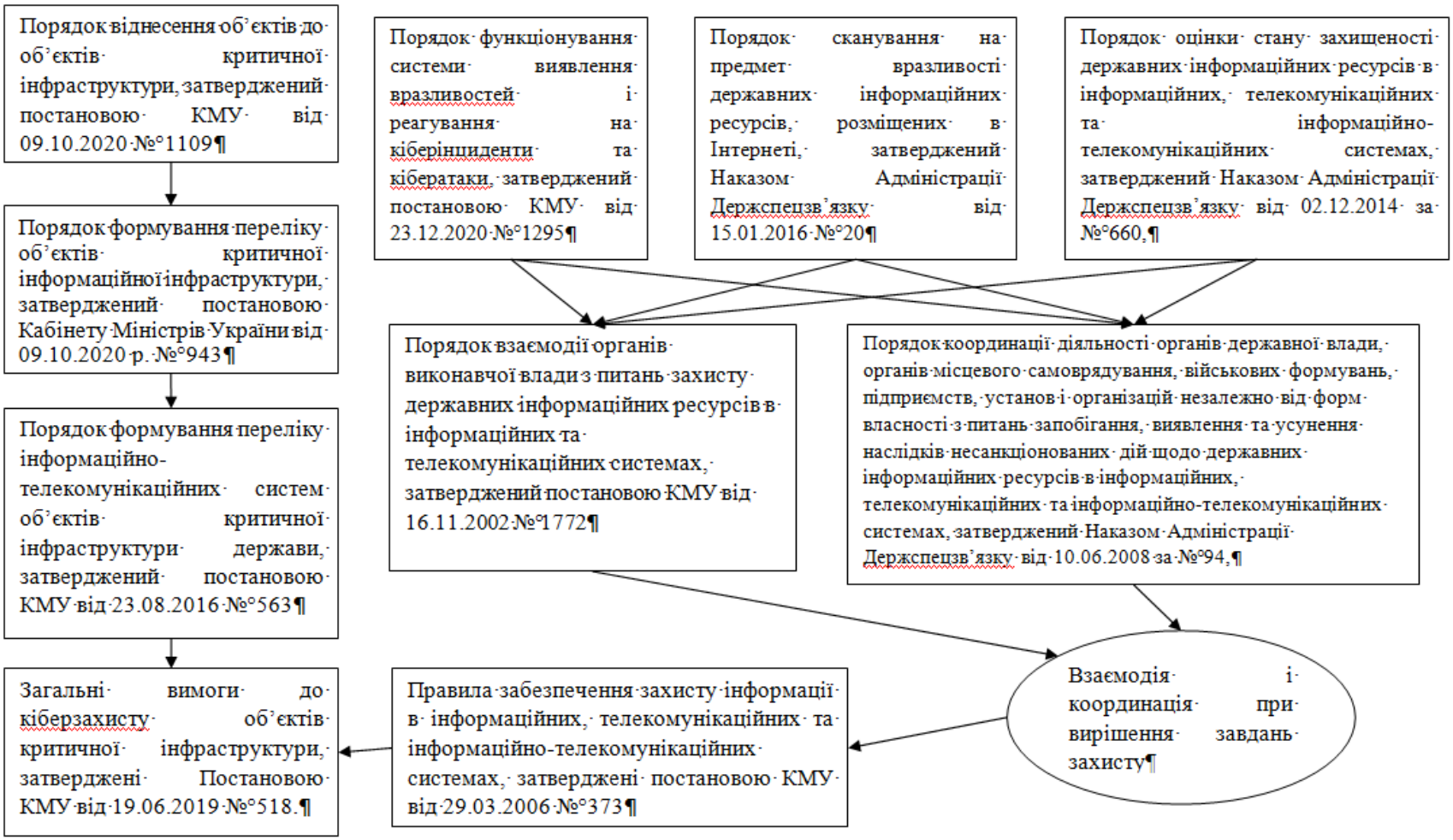
Наймасштабніші кібератаки в Україні

Джерело: https://ru.slovoidilo.ua/2025/03/24/infografika/bezopasnost/samye-masshtabnye-kiberataki-ukrainu

ДОДАТОК Б6

Схема запропонованої структури інформаційної безпеки

ДОДАТОК Б7. Логіка побудови структури описаних підзаконних нормативно-правових актів України у сфері кіберзахисту



ДОДАТОК Б8

Безпекові стратегії України, прийняті (затверджені) у 2020-2021 рр.

№ п/п	Найменування Стратегії,	Зміст документу, згідно Закону «Про національну безпеку України» (номер пункту ч. 1 ст. 1 Закону)	Номер Указу, дата	номер згідно Списку використаних джерел
1	2	3	4	5
1.	Стратегія національної безпеки України	Документ, що визначає актуальні загрози національній безпеці України та відповідні цілі, завдання, механізми захисту національних інтересів України та є основою для планування і реалізації державної політики у сфері національної безпеки (пункт 19);	№392/2020, 14.09.2020	[22]
2.	Стратегія воєнної безпеки України	Документ, у якому викладається система поглядів на причини виникнення, сутність і характер сучасних воєнних конфліктів, принципи і шляхи запобігання їх виникненню, підготовку держави до можливого воєнного конфлікту, а також на застосування воєнної сили для захисту державного суверенітету, територіальної цілісності, інших життєво важливих національних інтересів (пункт 20);	№121/2021, 25.03.2021	[23]
3.	Стратегія кібербезпеки України	Документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави (пункт 21)	№447/2021, 14.05.2021	[24]
4.	Стратегія громадської безпеки та цивільного захисту України	Документ довгострокового планування, що розробляється на основі Стратегії національної безпеки України за результатами огляду громадської безпеки та цивільного захисту і визначає напрями державної політики щодо гарантування захищеності життєво важливих для держави, суспільства та особи інтересів, прав і свобод людини і громадянина, цілі та очікувані результати їх досягнення з урахуванням актуальних загроз (пункт 23)	Станом на жовтень 2025 року не затверджена	
5.	Стратегія розвитку оборонно-промислового комплексу України	Документ, що розробляється за результатами огляду оборонно-промислового комплексу України та визначає пріоритетні напрями державної військово-промислової політики, цілі реформи оборонно-промислового комплексу та очікувані результати їх досягнення з урахуванням актуальних воєнно-політичних загроз і викликів (пункт 24);	№372/2021, 18.06.2021	[25]

6.○	Стратегія·інтегрованого·управління·державним·кордоном·України○	Документ·довгострокового·планування,·що·розробляється·на·основі°Стратегії·національної·безпеки·України·з·метою·визначення·пріоритетних·напрямів·державної·політики·у·сфері·охорони·та·захисту·державного·кордону·України,·стратегічних·цілей·розвитку·та·очікуваних·результатів·їх·досягнення·з·урахуванням·створення·і·підтримання·балансу·між·забезпеченням·належного·рівня·прикордонної·безпеки·і·збереженням·відкритості·державного·кордону·України·для·законного·транскордонного·співробітництва,·а·також·для·осіб,·які·подорожують·(пункт·25).○	Станом·на·жовтень·2025·року·не·затверджена○	○
7.○	Стратегія·зовнішньополітичної·діяльності·України○	○	№°448/2021,¶ 26.08.2021○	[26]○
8.○	Стратегія·інформаційної·безпеки○	○	№°685/2021,¶ 28.12.2021○	[28]○
9.○	Стратегія·забезпечення·державної·безпеки○	○	№°56/2022,¶ 16.02.2022○	[29]○
10.○	Стратегія·енергетичної·безпеки○	○	Розпорядження·КМУ¶ №°907-р·від¶ 04.08.2021○	[27]○

¶

ДОДАТОК Б9

Правові позиції Верховних Судів демократичних країн з приводу важливості свободи слова (свободи вираження поглядів)

№ п/п	Країна, суд	Зміст правової позиції	Джерело
1.	Верховний Суд США	Усі ідеї, які мають навіть найменшу соціальну значимість – неортодоксальні ідеї, суперечливі ідеї, навіть ідеї, які ненависні переважній більшості – мають повний захист гарантій Першої поправки (all ideas having even the slightest redeeming social importance – unorthodox ideas, controversial ideas, even ideas hateful to the prevailing climate of opinion – have the full protection of the [First Amendment] guaranties), крім окремих суворо регламентованих випадків (справа «Roth v. United States», рішення від 24.06.1957 р.)	[358]
2.	Верховний Суд Канади	Теорія свободи вираження… означає спосіб життя, який через заохочення терпимості, скептицизму, розумності та ініціативи дозволить людини повністю реалізувати її потенціал. Вона унеможливлює альтернативу цьому – тиранічне, конформістське, ірраціональне та застигле суспільство (справа «Attorney-General of Quebek v. Irwin Toy»)	[300, с. 414]
3.	Верховний Суд Австралії	Австралійська конституція, безперечно, визнає «свободу комунікації» (freedom of communication) щодо питань, які стосуються управління країною: «свобода комунікації з питань урядування та політики є невід'ємним елементом… представницького уряду… якщо ця свобода має ефективно слугувати цілям представницького урядування, вона не може бути обмежена лише періодом виборів… (справа «Lange v. Australian Broadcasting Corporation»)	[300, с. 418-419]
4.	Верховний Суд Японії	Немає необхідності докладно зупинятися на тому факті, що свобода зборів та асоціацій, а також свобода вираження поглядів, преси та всіх інших форм вираження… належить до вічних та непорушних прав, основних прав людини, і що абсолютна гарантія таких прав є одним з основоположних правил і характеристик демократичної форми урядування, які відрізняють демократію від тоталітаризму (справа «Metropolitan Ordinance»)	[300, с. 419]
5.	Верховний Суд Ізраїлю	свобода вираження поглядів тісно пов'язана з демократичним процесом. Вона виступає не тільки як засіб чи інструмент, але й як мета сама по собі. Свобода вираження є одним з найголовніших прав і разом з подібним правом на свободу совісті становить передумову для реалізації практично усіх інших свобод. Найвища цінність, що міститься у свободі вираження поглядів, залишається постійною та незмінною	[300, с. 423]

ДОДАТОК Б10

Положення Конституцій демократичних країн

щодо свободи слова та думок (свободи вираження поглядів)

№ п/п	Країна, акт	Зміст правової позиції	Джерело
1.	Білль про права 1789-1791 рр., Поправка 1 до Конституції США	Конгрес не має видавати закони, що встановлюють будь-яку релігію або забороняють вільне віросповідання, або обмежують свободу слова чи друку чи право народу мирно збиратися та звертатися до Уряду з петиціями про задоволення скарг	[153, с. 30]
2.	Французька Декларація прав людини і громадянина (ст. 11), складова Конституції Франції	Вільне повідомлення іншим думок є одне з дорогоцінних прав людини; тому кожен громадянин може вільно висловлюватися, писати, друкувати, несучи відповідальність за зловживання цією свободою у випадках, встановлених законом	[153, с. 103]
3.	Конституція ФРН (ст. 5)	1. Кожен має право вільно висловлювати і поширювати свою думку усно, письмово і за допомогою зображень і безперешкодно черпати знання із загальнодоступних джерел. Свобода друку і інформації через радіо і кіно гарантується. Цензури не існує. 2. Межі цих прав встановлюються приписами загальних законів про охорону молоді та правом на честь особистості. 3. Мистецтво та наука, дослідження та викладання вільні. Свобода викладання не звільняє від вірності Конституції	[153, с. 154]
4.	Конституція Італії (ст. 21)	Усі мають право висловлювати свої думки усно, письмово та будь-яким іншим способом їх поширення. ЗМІ не можуть підлягати дозволу чи цензурі Забороняються друковані твори, видовища та різноманітні маніфестації, що суперечать добрим звичаям. Закон установлює заходи, що забезпечують запобігання та припинення відповідних правопорушень	[153, с. 247-248]
4.	Конституція Японії (ст. 21)	Гарантується свобода зборів та об'єднань, а також свобода слова, друку і усіх інших форм висловлювання думок. Жодна цезура не допускається	[153, с. 295]
5.	Канадська Хартія прав і свобод (частина 1 Конституційного акту 1982 р.), (ст. 2)	Кожному належать наступні основні свободи: a) свобода совісті та віросповідання; b) свобода думки, переконань, думки і самовираження, включаючи свободу друку та інших засобів комунікації; c) свобода зібрань з мірними цілями$ d) свобода асоціацій.	[153, с. 318]

ДОДАТОК Б11

Позиція Європейського суду з прав людини щодо обмежень свободи творчості

№ п/п	Рішення, джерело	Сутність позиції
1.	від 24.05.1988°р. у справі «Мюллер та ін. проти Швейцарії», [300, с.°458-459]	Всі заявники, за винятком пана Йозефа Фелікса Мюллера, були у 1981°р. організаторами виставки сучасного мистецтва в колишній Великої семінарії м.°Фрейбурга. Виставка була організована з приводу 500-річчя входження кантону Фрейбург до складу Швейцарської конфедерації. Пан Мюллер, художник, був запрошений взяти в ній участь і представив три картини. 04.09.1981°р. уповноважений судовий слідчий розпорядився видалити картини пана Мюллера з виставки і піддати їх вилученню. Вони підпадали, в його уявленні, під дію ст.°204 Кримінального кодексу Швейцарії про непристойні публікації. 24.02.1982°р. кримінальний суд округу Сарин визначили міру покарання у вигляді стягнення з кожного заявника штрафу в розмірі 300 швейцарських франків за вчинення правопорушення по ст.°204. На додаток, він розпорядився формально конфіскувати згадані картини. Заявники подали апеляційну скаргу, але кантональний суд Фрейбурга як касаційна інстанція, відхилив її 26.04.1982°р. За заявою, поданою 29.06.1987°р. Йозефом Феліксом Мюллером, кримінальний суд округу Сарин розпорядився 20.016.1988°р. повернути йому картини: незабаром після цього він їх отримав. У судовому рішенні ЄСПЛ, перш за все, констатував, що ст.°10 ЄКПЛ включає в себе свободу артистичного вираження. Потім він повинен був визначити, чи було обмеження, якому піддався заявник у здійсненні свого права на свободу вираження і визнання винним і конфіскації, таким, що відповідає ч.°2 ст.°10 ЄКПЛ. ЄСПЛ прийшов до висновку, що рішення про визнання винним і визначення покарання були передбачені законом в сенсі ч.°2 ст.°10 ЄКПЛ… Суд також зазначив, що судове визнання винним і визначення покарання мало на меті захистити суспільну мораль і, відповідно до цього, мало законну мету в сенсі ч.°2 ст.°10 ЄКПЛ. Що стосується питання, чи було все це необхідним в демократичному суспільстві, ЄСПЛ заявив, що свобода вираження являє собою одну з найважливіших основ демократичного суспільства і ***застосовується до інформації***, навіть якщо вона шокує суспільство, ображає його або дратує його або якусь частину його населення. Такими є вимоги плюралізму, терпимості й відкритості погляду, без яких не може бути демократичного суспільства. З іншого боку, Суд підкреслив, що буде неможливо знайти однакову концепцію моралі в правовому і соціальному устрої різних держав-учасниць. В силу свого прямого і тривалого зв'язку з життєвими силами своїх країн, судові органи держави знаходяться, як правило, в кращому становищі, ніж суддя міжнародного суду, щоб висловити думку про точний зміст таких норм, як і щодо необхідності обмежень або покарань, що накладаються у зв'язку з цим. ЄСПЛ далі зазначив, що в даному випадку спірні полотна, які в грубій формі зображали, зокрема, статеві відносини між людьми і тваринами, були вільно доступні широкому загалу без обмежень з боку організаторів ані в формі плати за вхід, ані за віком. Зважаючи на це є

		поширюється не тільки на основні закони, а й на рішення, які застосували їх, навіть якщо вони були винесені незалежним судовим органом.¶ 52.°ЄСПЛ надає особливої важливості фактору, на який було звернуто увагу в рішенні місцевого суду від 29.10.1971°р., а саме, на передбачуване коло читачів Підручника. Воно було розраховано на дітей і підлітків у віці від дванадцяти до вісімнадцяти років. Будучи по стилю прямою, фактичною і зведеною до суті, за своїм стилем дана книга була легко доступна для розуміння ще більш юним читачам. Заявник відкрито стверджував, що планував широке поширення книги. Разом з пресрелізом він розіслав книгу в багато щоденних газет і періодичних видань для вивчення або в рекламних цілях. Більш того, він встановив більш ніж скромну ціну (тридцять пенсів), підготував до повторного друку 50.000 примірників книги незабаром після друку перших 20.000 штук, а також вибрав назву, яка передбачає, що даний твір носив характер довідкового посібника і міг бути використаний в школах.¶ По суті, в книзі містилася фактична інформація, яка в цілому була достовірна і часто корисна, як визнав місцевий суд. Однак, крім усього цього, в розділі про секс і в уривку під заголовком «Будь собою» глави про учнів, в ній містилися пропозиції і абзаци, які молоді люди в критичний етап свого розвитку могли витлумачити як спонукання до передчасних і шкідливих для них вчинків, і навіть до здійснення конкретних кримінальних злочинів. За таких обставин, незважаючи на різноманітність і постійну еволюцію поглядів на етику і освіту в Сполученому Королівстві, компетентні англійські судді, при здійсненні своєї свободи розсуду, мали право вважати, що вплив Підручника на багатьох дітей і підлітків, які прочитали її, буде згубним.¶ 59.°Порушення ст.°10 не було.¶ ¶ Джерело: https://europeancourt.org/wp-content/uploads/ECHR_Handyside_v_the_United_Kingdom_07_12_1976.pdf¤
3.¤	від 25.11.1996°р. у справі¶ «Уінгроув проти¶ Сполученого Королівства », п.п. 8, 11, 13, 32, 36, 52, 61, 64¤	8.°Пан Найджел Уінгроув, британський кінорежисер, написав сценарій і керував створенням відеофільму під назвою «Бачення екстазу». Його тривалість становить приблизно 18 хвилин. У фільмі повністю відсутні діалоги, а є тільки музика і відеоряд. Згідно заявнику, ідея створення фільму заснована на житті і писаннях святої Терези Авільської, кармелітської черниці і засновниці багатьох монастирів, що жила у XVI ст., яку відвідували сильні екстатичні бачення Ісуса Христа.¶ 11.°Фільм «Бачення екстазу» був представлений на розгляд Британського управління класифікації фільмів (Управління).¶ 13.°18.09.1989°р. Управління відхилило заявку на отримання сертифіката, резюмуючи такий висновок наступним підсумком: «…Справа не в тому, що образи сексуального характеру у фільмі «Бачення екстазу» виходять за рамки категорії «не молодше 18 років», а у тому, що протягом більшої частини відеотвору сексуальні образи концентруються на фігурі розп'ятого Христа. Якби чоловічий персонаж не був Христом, проблеми б не виникло...».¶ 32.°Пан Уінгроу подав скаргу до ЄСПЛ 18.06.1990°р. Посилаючись на ст.°10 ЄКПЛ, він стверджував, що відмова у видачі йому класифікаційного сертифіката на поширення відеофільму «Бачення екстазу» є порушенням його свободи слова.¶ 36.°Відмова Британського управління класифікації фільмів видати

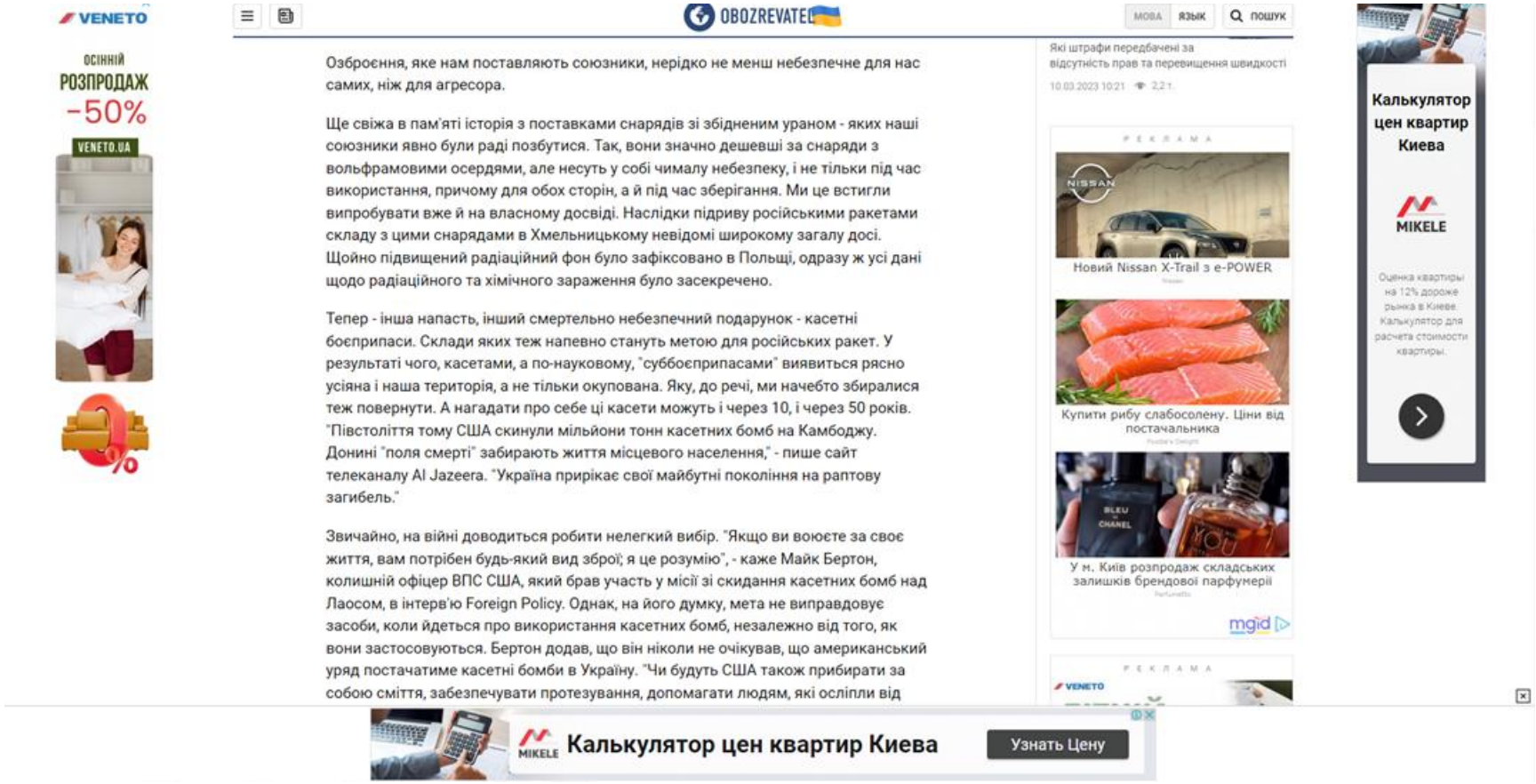
		сертифікат на відеотвір заявника «Бачення екстазу» в поєднанні із законодавчими нормами, згідно з якими поширення відеотворів без такого сертифіката вважається кримінальним злочином, рівносильна втручанню з боку державного органу у здійснення заявником свого права на поширення ідей.¶ 52.°Суд нагадує, що свобода слова є однією з основних підвалин демократичного суспільства. Однак, як спеціально вказується в ч.°2 ст.°10 ЄКПЛ, здійснення цієї свободи пов'язано з певними обов'язками і відповідальністю. В їх число в контексті релігійних переконань може бути легітимно включений і обов'язок уникати, наскільки це можливо, того, що інші особи можуть порахувати необґрунтовано образливим і навіть таким, що оскверняє релігійні цінності.¶ 61.°У відеофільмі «Бачення екстазу» зображений, серед іншого, жіночий персонаж, який сидить верхи на розпростертому тілі розп'ятого Христа і здійснює при цьому акт відверто сексуального характеру. Національні влади, використовуючи повноваження, які самі по собі не є несумісними з ЄКПЛ, порахували, що ця сцена подана так, що «не так підкреслює еротичні переживання персонажів, скільки прагне викликати такі у глядачів фільму, що і є основною функцією порнографії». Влада підкреслила, що в фільмі не зроблено ніяких спроб розкрити характер персонажів; його мета – «еротичне милування». Публічне поширення подібного відеофільму могло б поранити і образити почуття віруючих християн, що відповідає ознакам кримінального злочину богохульства.¶ 64.°Вірно, що вжиті владою заходи рівносильні повній забороні на розповсюдження фільму. Однак це було цілком зрозумілим наслідком позиції компетентних властей, згідно з якою поширення фільму призвело б до порушення кримінального права. До того ж, заявник відмовився змінити або вирізати кадри, що викликали заперечення. Прийшовши до висновку, що в такому вигляді зміст фільму був блюзнірським, влада не переступила меж свого розсуду.¶ Порушення ст.°10 не було.¶ ¶ Джерело: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-58080%22]}¤
4.¤	від 20.09.1994°р. у справі¶ «Інститут¶ Отто-Преміінгер¶ проти¶ Австрії»,¶ п.п. 51, 52, 55, 56¶ ¤	51.°Фільм, який був заарештований, а потім конфіскований на підставі ¤ судових рішень, винесених австрійськими судами, грунтувався на театральній п'єсі кількарічної давнини, але Суд займається тільки кінотвором, про який йде мова.¶ 52.°Уряд стверджував, що арешт фільму був необхідний тому, що у ньому містяться напад на християнську релігію, особливо римо-католицьку… Особливо різким і образливим випадом проти католицької моралі був фінал фільму… Відповідно, існувала гостра соціальна потреба в збереженні релігійного миру; потрібно було захистити громадський порядок, для якого фільм представляв небезпеку, і суди Інсбрука не переступили в цьому відношенні надану їм межу розсуду.¶ 55.°Перед Судом стоїть проблема, як врівноважити суперечливі інтереси при здійсненні двох основоположних свобод, гарантованих ЄКПЛ, а саме: права асоціації-заявника повідомляти громадськості спірні погляди, що має на увазі і право зацікавлених осіб знайомитися з такими поглядами, з одного боку, і права інших осіб на належну повагу їх свободи думки, совісті і релігії, з іншого боку. Вирішуючи цю проблему, слід взяти до уваги межі розсуду, залишені національним властям, чий

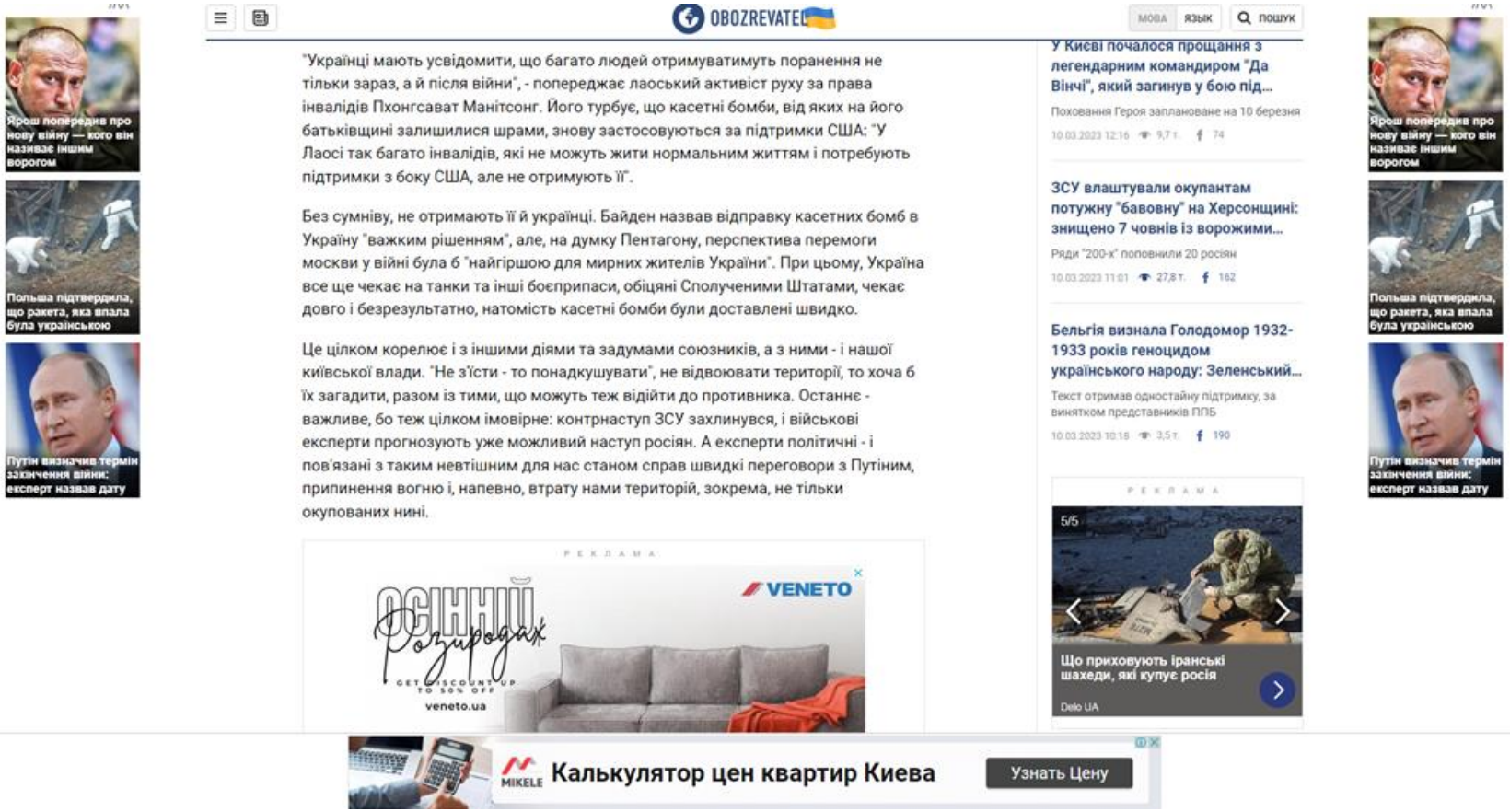
		обов'язок в демократичному суспільстві полягає також у тому, щоб враховувати в межах їх компетенції інтереси суспільства в цілому.¶ 56.°Австрійські суди, розпорядившись про арешт, а в подальшому і про конфіскацію фільму, розглядали його як образливий, в очах тірольської публіки, випад проти римсько-католицької церкви… Вони не вважали, що властивості фільму як твору мистецтва або як внеску в публічне обговорення проблем виправдовували такі його риси, які в значній мірі були б сприйняті широкою публікою як образа… ЄСПЛ не може ігнорувати той факт, що римсько-католицька віра є релігією переважної більшості тірольців. Наклавши арешт на фільм, австрійські власті діяли в інтересах забезпечення релігійного миру в цьому регіоні і для того, щоб у окремих людей не склалося відчуття, що їх релігійні переконання стали об'єктом необгрунтованих і образливих нападок. В першу чергу саме національним властям, які знаходяться в більш вигідному становищі, ніж міжнародний суд, доводиться давати оцінку потреби в подібній мірі в світлі тієї ситуації, яка складається в даному місці і в даний час. За всіх обставин цієї справи Суд жодного разу не визнав, що дії австрійської влади можуть розглядатися в цьому відношенні як такі, що виходять за межі їх розсуду.¶ Тому ЄСПЛ не вбачає порушення ст.°10.¶ ¶ Джерело: https://europeancourt.org/wp-content/uploads/ECHR_Ollinger_v_Austria_29_06_2006.pdf©

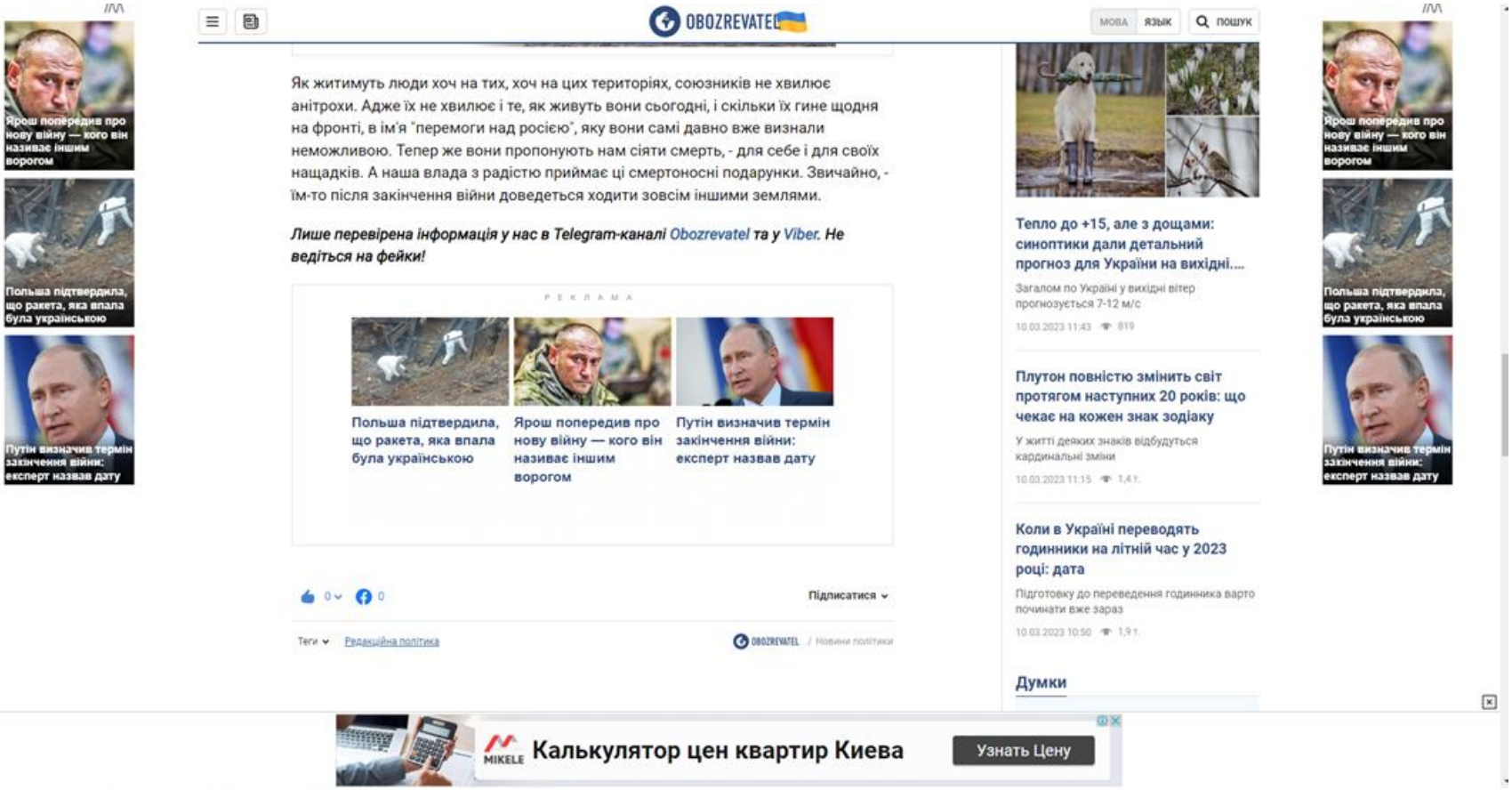
¶

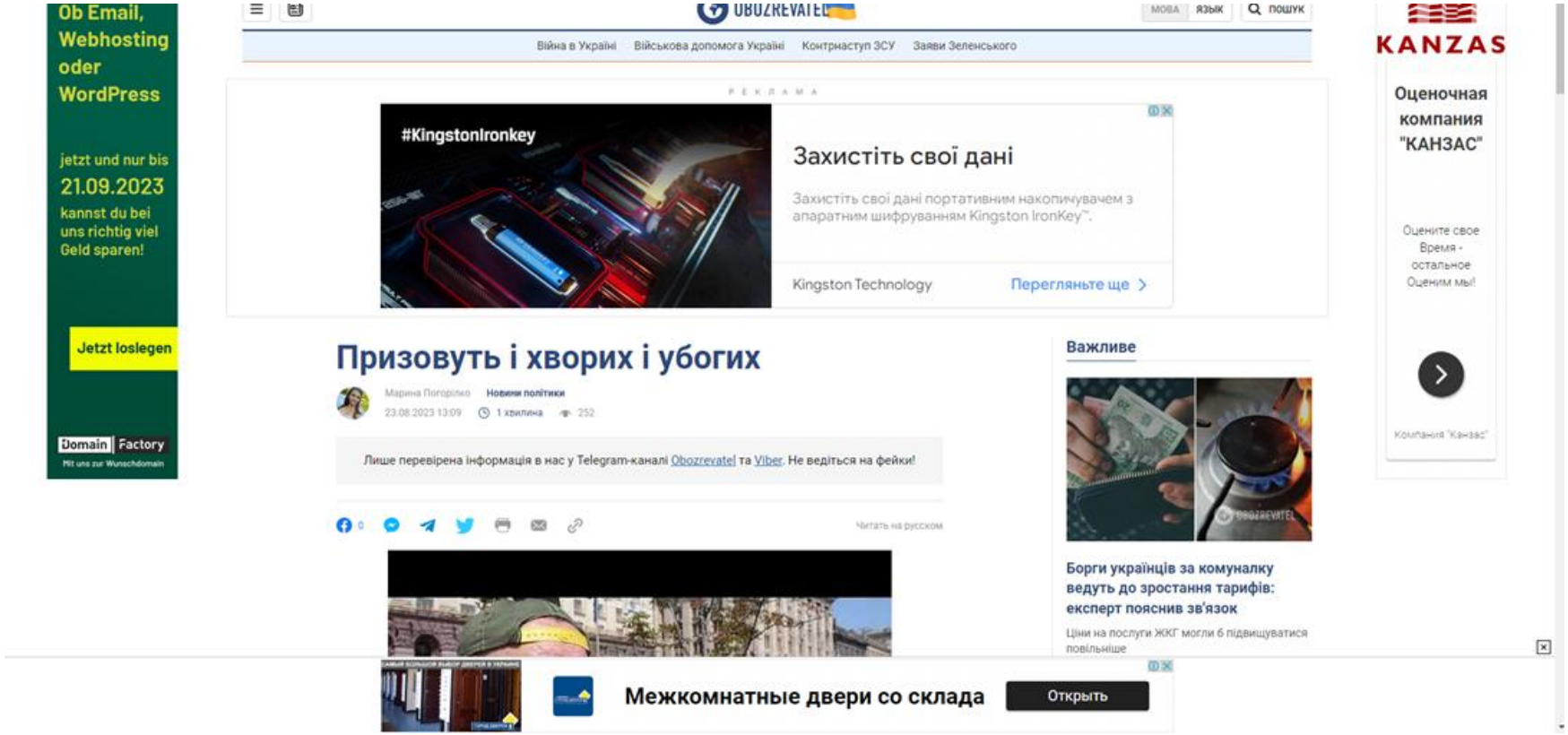
ДОДАТОК Б12

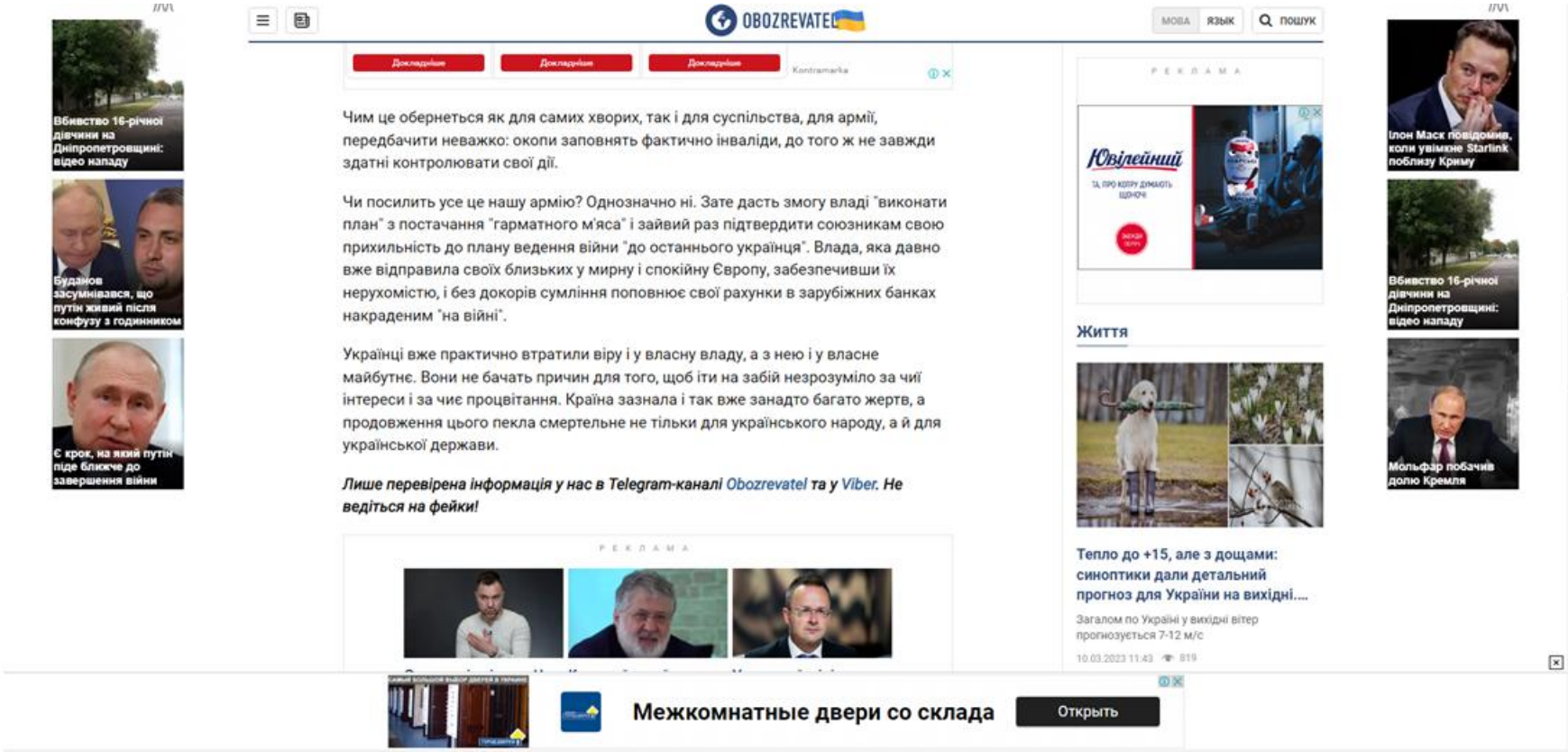

VENETO
ОСІННІЙ
РОЗПРОДАЖ
-50%
VENETO.UA
OBOZREVATEL
МОВА
ЯЗЫК
ПОШУК
MIKELE
Узнать Цену
Ховаємо самі себе
Марина Погорілко
Новини політики
23.08.2023 13:09
1 хвилина
252
Лише перевірена інформація в нас у Telegram-каналі Obozrevatel та Viber. Не ведіться на фейки!
Читать на русском
Важливе
Борги українців за комуналку ведуть до зростання тарифів: експерт пояснив зв'язок
Ціни на послуги ЖКГ могли б підвищуватися повільніше
10.03.2023 02:52
4,7 т.
35
Українці обрали нову назву для Південно-Західної залізниці, на...
Опитування триватиме до 17 березня
10.03.2023 10:55
4,2 т.
1
Десятки тисяч штрафу, позбавлення прав і конфіскація авто: як...
Які штрафи передбачені за
Калькулятор цен квартир Киева
MIKELE
Оценка квартиры на 12% дороже рынка в Киеве. Калькулятор для расчета стоимости квартиры.
MIKELE
Калькулятор цен квартир Киева
Узнать Цену


VENETO
ОСІННІЙ
РОЗПРОДАЖ
-50%
VENETO.UA
OBOZREVATEL
МОВА
ЯЗЫК
ПОШУК
Озброєння, яке нам поставляють союзники, нерідко не менш небезпечне для нас самих, ніж для агресора.
Ще свіжа в пам'яті історія з поставками снарядів зі збідненим ураном - яких наші союзники явно були раді позбутися. Так, вони значно дешевші за снаряди з вольфрамовими осердями, але несуть у собі чималу небезпеку, і не тільки під час використання, причому для обох сторін, а й під час зберігання. Ми це встигли випробувати вже й на власному досвіді. Наслідки підриву російськими ракетами складу з цими снарядами в Хмельницькому невідомі широкому загалу досі. Щойно підвищений радіаційний фон було зафіксовано в Польщі, одразу ж усі дані щодо радіаційного та хімічного зараження було засекречено.
Тепер - інша напасть, інший смертельно небезпечний подарунок - касетні боєприпаси. Склади яких теж напевно стануть метою для російських ракет. У результаті чого, касетами, а по-науковому, "суббоєприпасами" виявиться рясно усіяна і наша територія, а не тільки окупована. Яку, до речі, ми начебто збиралися теж повернути. А нагадати про себе ці касети можуть і через 10, і через 50 років. "Півстоліття тому США скинули мільйони тонн касетних бомб на Камбоджу. Донині "поля смерті" забирають життя місцевого населення," - пише сайт телеканалу Al Jazeera. "Україна прирікає свої майбутні покоління на раптову загибель."
Звичайно, на війні доводиться робити нелегкий вибір. "Якщо ви воюєте за своє життя, вам потрібен будь-який вид зброї; я це розумію", - каже Майк Бертон, колишній офіцер ВПС США, який брав участь у місії зі скидання касетних бомб над Лаосом, в інтерв'ю Foreign Policy. Однак, на його думку, мета не виправдовує засоби, коли йдеться про використання касетних бомб, незалежно від того, як вони застосовуються. Бертон додав, що він ніколи не очікував, що американський уряд постачатиме касетні бомби в Україну. "Чи будуть США також прибирати за собою сміття, забезпечувати протезування, допомагати людям, які осліпли від
Які штрафи передбачені за відсутність прав та перевищення швидкості
10.03.2023 10:21
РЕКЛАМА
NISSAN
Новий Nissan X-Trail з e-POWER
Купити рибу слабосолену. Ціни від постачальника
BLEU de CHANEL
У м. Київ розпродаж складських залишків брендової парфумерії
mgid
РЕКЛАМА
VENETO
Калькулятор цен квартир Киева
MIKELE
Оценка квартиры на 12% дороже рынка в Киеве. Калькулятор для расчета стоимости квартиры.
MIKELE
Калькулятор цен квартир Киева
Узнать Цену

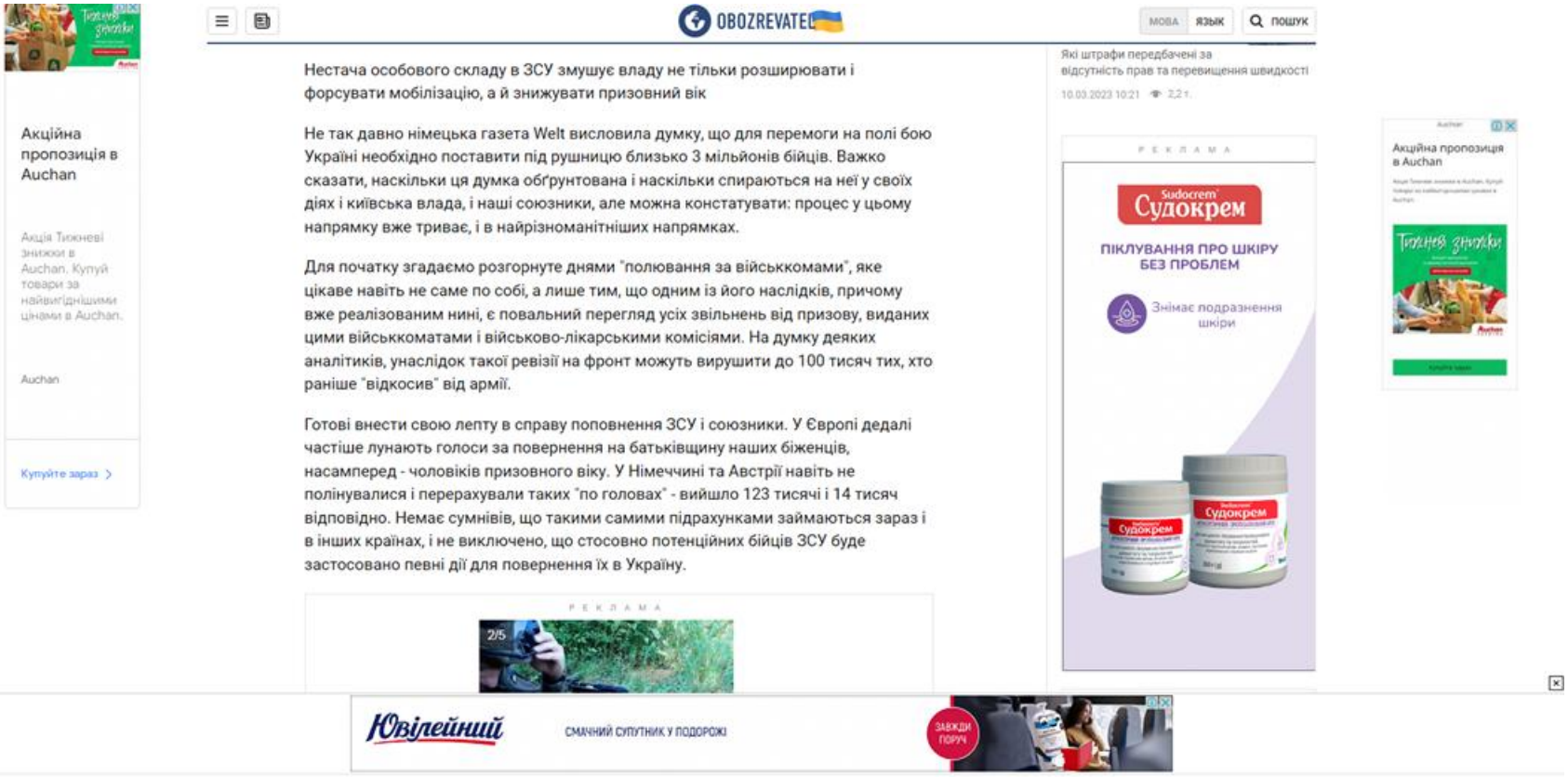

Ярош попередив про нову війну — кого він називає іншим ворогом
Польща підтвердила, що ракета, яка впала була українською
Путін визначив термін закінчення війни: експерт назвав дату
OBOZREVATEL
МОВА ЯЗЫК ПОШУК
"Українці мають усвідомити, що багато людей отримуватимуть поранення не тільки зараз, а й після війни", - попереджає лаоський активіст руху за права інвалідів Пхонгсават Манітсонг. Його турбує, що касетні бомби, від яких на його батьківщині залишилися шрами, знову застосовуються за підтримки США: "У Лаосі так багато інвалідів, які не можуть жити нормальним життям і потребують підтримки з боку США, але не отримують її".
Без сумніву, не отримають її й українці. Байден назвав відправку касетних бомб в Україну "важким рішенням", але, на думку Пентагону, перспектива перемоги москви у війні була б "найгіршою для мирних жителів України". При цьому, Україна все ще чекає на танки та інші боєприпаси, обіцяні Сполученими Штатами, чекає довго і безрезультатно, натомість касетні бомби були доставлені швидко.
Це цілком корелює і з іншими діями та задумами союзників, а з ними - і нашої київської влади. "Не з'їсти - то понадкушувати", не відвоювати території, то хоча б їх загадити, разом із тими, що можуть теж відійти до противника. Останнє - важливе, бо теж цілком імовірне: контрнаступ ЗСУ захлинувся, і військові експерти прогнозують уже можливий наступ росіян. А експерти політичні - і пов'язані з таким невтішним для нас станом справ швидкі переговори з Путіним, припинення вогню і, напевно, втрату нами територій, зокрема, не тільки окупованих нині.
РЕКЛАМА
ОСІННІ РОЗПРОДАЖІ
GET DISCOUNT UP TO 50% OFF
VENETO
veneto.ua
У Києві почалося прощання з легендарним командиром "Да Вінчі", який загинув у бою під...
Поховання Героя заплановане на 10 березня
10.03.2023 12:16 9,7 т. 74
ЗСУ влаштували окупантам потужну "бавовну" на Херсонщині: знищено 7 човнів із ворожими...
Ряди "200-х" поповнили 20 росіян
10.03.2023 11:01 27,8 т. 162
Бельгія визнала Голодомор 1932-1933 років геноцидом українського народу: Зеленський...
Текст отримав одностайну підтримку, за винятком представників ППБ
10.03.2023 10:18 3,5 т. 190
РЕКЛАМА
5/5
Що приховують іранські шахеди, які купує росія
Delo UA
MIKELE Калькулятор цен квартир Киева
Узнать Цену


Ярош попередив про нову війну — кого він називає іншим ворогом
Польща підтвердила, що ракета, яка впала була українською
Путін визначив термін закінчення війни: експерт назвав дату
OBOZREVATEL
МОВА
ЯЗЫК
ПОШУК
Як житимуть люди хоч на тих, хоч на цих територіях, союзників не хвилює анітрохи. Адже їх не хвилює і те, як живуть вони сьогодні, і скільки їх гине щодня на фронті, в ім'я "перемоги над росією", яку вони самі давно вже визнали неможливою. Тепер же вони пропонують нам сіяти смерть, - для себе і для своїх нащадків. А наша влада з радістю приймає ці смертоносні подарунки. Звичайно, - їм-то після закінчення війни доведеться ходити зовсім іншими землями.
Лише перевірена інформація у нас в Telegram-каналі Obozrevatel та у Viber. Не ведіться на фейки!
РЕКЛАМА
Польща підтвердила, що ракета, яка впала була українською
Ярош попередив про нову війну — кого він називає іншим ворогом
Путін визначив термін закінчення війни: експерт назвав дату
Підписатися
Теги
Редакційна політика
OBOZREVATEL / Новини політики
Тепло до +15, але з дощами: синоптики дали детальний прогноз для України на вихідні....
Загалом по Україні у вихідні вітер прогнозується 7-12 м/с
10.03.2023 11:43
819
Плутон повністю змінить світ протягом наступних 20 років: що чекає на кожен знак зодіаку
У житті деяких знаків відбудуться кардинальні зміни
10.03.2023 11:15
1,4 т.
Коли в Україні переводять годинники на літній час у 2023 році: дата
Підготовку до переведення годинника варто починати вже зараз
10.03.2023 10:50
1,9 т.
Думки
MIKELE
Калькулятор цен квартир Киева
Узнать Цену


Ob Email, Webhosting oder WordPress
jetzt und nur bis 21.09.2023
kannst du bei uns richtig viel Geld sparen!
Jetzt loslegen
Domain Factory
Mit uns zur Wunschdomain
OBOZREVATEL
МОВА ЯЗЫК ПОШУК
Війна в Україні Військова допомога Україні Контрнаступ ЗСУ Заяви Зеленського
РЕКЛАМА
#KingstonIronkey
Захистіть свої дані
Захистіть свої дані портативним накопичувачем з апаратним шифруванням Kingston IronKey™.
Kingston Technology
Перегляньте ще
KANZAS
Оценочная компания "КАНЗАС"
Оцените свое Время - остальное Оценим мы!
Компания "Канзас"
Призовуть і хворих і убогих
Марина Погорілко Новини політики
23.08.2023 13:09 1 хвилина 252
Лише перевірена інформація в нас у Telegram-каналі Obozrevatel та Viber. Не ведіться на фейки!
Читать на русском
Важливе
Борги українців за комуналку ведуть до зростання тарифів: експерт пояснив зв'язок
Ціни на послуги ЖКГ могли б підвищуватися повільніше
Межкомнатные двери со склада
Открыть

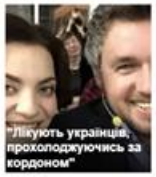

Вбивство 16-річної дівчини на Дніпропетровщині: відео нападу
Буданов засумнівався, що путін живий після конфузу з годинником
Є крок, на який путін піде ближче до завершення війни
OBOZREVATEL
МОВА
ЯЗЫК
ПОШУК
Докладніше
Докладніше
Докладніше
Kontramarka
Чим це обернеться як для самих хворих, так і для суспільства, для армії, передбачити неважко: окопи заповнять фактично інваліди, до того ж не завжди здатні контролювати свої дії.
Чи посилить усе це нашу армію? Однозначно ні. Зате дасть змогу владі "виконати план" з постачання "гарматного м'яса" і зайвий раз підтвердити союзникам свою прихильність до плану ведення війни "до останнього українця". Влада, яка давно вже відправила своїх близьких у мирну і спокійну Європу, забезпечивши їх нерухомістю, і без докорів сумління поповнює свої рахунки в зарубіжних банках накраденим "на війні".
Українці вже практично втратили віру і у власну владу, а з нею і у власне майбутнє. Вони не бачать причин для того, щоб іти на забій незрозуміло за чиї інтереси і за чиє процвітання. Країна зазнала і так вже занадто багато жертв, а продовження цього пекла смертельне не тільки для українського народу, а й для української держави.
Лише перевірена інформація у нас в Telegram-каналі Obozrevatel та у Viber. Не ведіться на фейки!
РЕКЛАМА
РЕКЛАМА
Ювілейний
Життя
Тепло до +15, але з дощами: синоптики дали детальний прогноз для України на вихідні....
Загалом по Україні у вихідні вітер прогнозується 7-12 м/с
10.03.2023 11:43
819
Ілон Маск повідомив, коли увімкне Starlink поблизу Криму
Вбивство 16-річної дівчини на Дніпропетровщині: відео нападу
Мольфар побачив долю Кремля
Межкомнатные двери со склада
Открыть

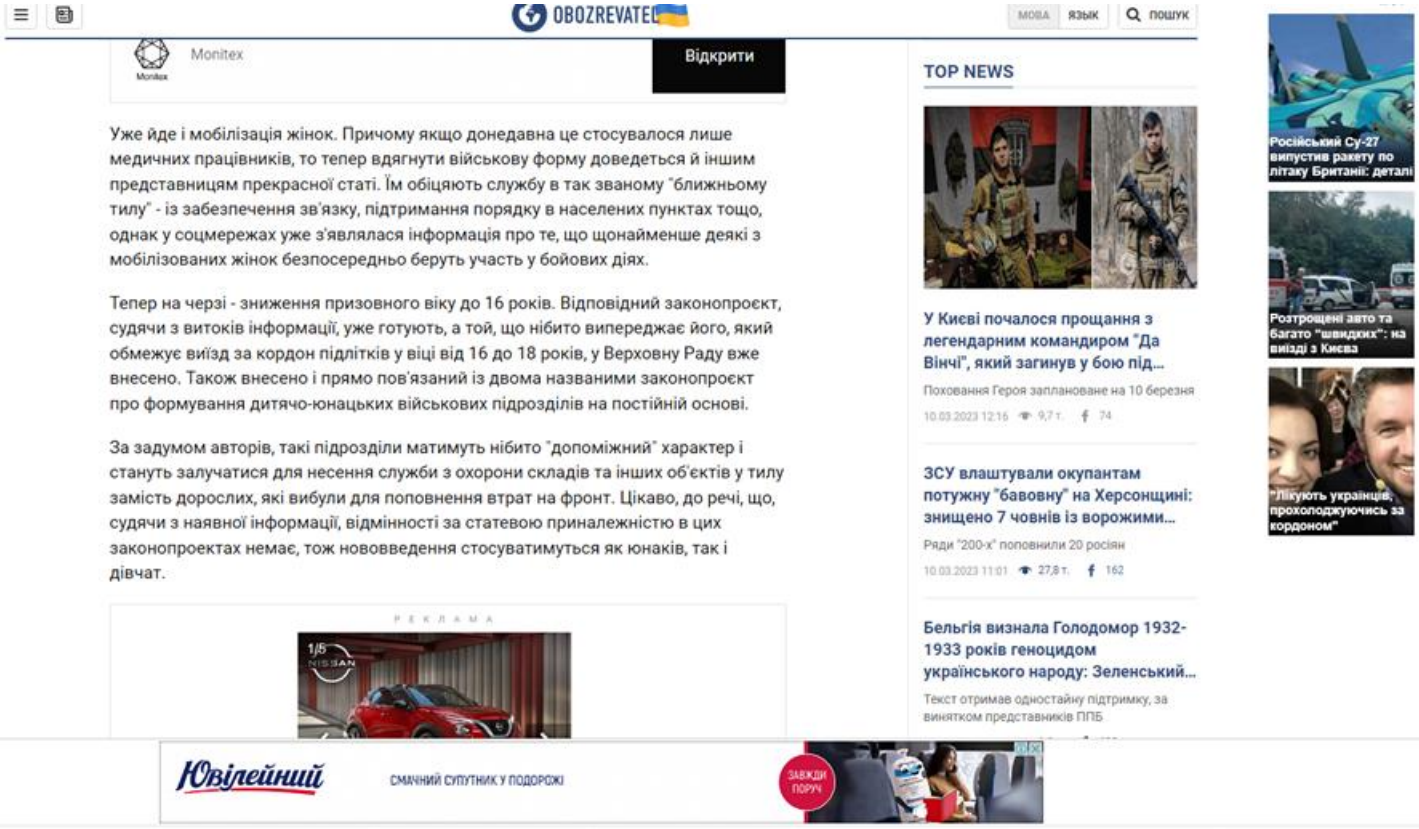

Акційна пропозиція в Auchan
Акція Тижневі знижки в Auchan. Купуй товари за найвигіднішими цінами в Auchan.
Auchan
Купуйте зараз
OBOZREVATEL
МОВА
ЯЗЫК
ПОШУК
ЖК Теремки
Докладніше
У стрій встануть усі
Марина Погорілко
Новини політики
23.08.2023 13:09
1 хвилина
252
Лише перевірена інформація в нас у Telegram-каналі Obozrevatel та Viber. Не ведіться на фейки!
Читать на русском
Важливе
Борги українців за комуналку ведуть до зростання тарифів: експерт пояснив зв'язок
Ціни на послуги ЖКГ могли б підвищуватися повільніше
10.03.2023 02:52
4,7 т.
35
Українці обрали нову назву для Південно-Західної залізниці, на...
Опитування триватиме до 17 березня
10.03.2023 10:55
4,2 т.
1
Десятки тисяч штрафу, позбавлення прав і
Акційна пропозиція в Auchan
Ювілейний
СМАЧНИЙ СУПУТНИК У ПОДОРОЖІ
ЗАВЖДИ ПОРУЧ


Акційна пропозиція в Auchan
Акція Тижневі знижки в Auchan. Купуй товари за найвигіднішими цінами в Auchan.
Auchan
Купуйте зараз
OBOZREVATEL
МОВА
ЯЗЫК
ПОШУК
Нестача особового складу в ЗСУ змушує владу не тільки розширювати і форсувати мобілізацію, а й знижувати призовний вік
Не так давно німецька газета Welt висловила думку, що для перемоги на полі бою Україні необхідно поставити під рушницю близько 3 мільйонів бійців. Важко сказати, наскільки ця думка обґрунтована і наскільки спираються на неї у своїх діях і київська влада, і наші союзники, але можна констатувати: процес у цьому напрямку вже триває, і в найрізноманітніших напрямках.
Для початку згадаємо розгорнуте днями "полювання за військкомами", яке цікаве навіть не саме по собі, а лише тим, що одним із його наслідків, причому вже реалізованим нині, є повальний перегляд усіх звільнень від призову, виданих цими військкоматами і військово-лікарськими комісіями. На думку деяких аналітиків, унаслідок такої ревізії на фронт можуть вирушити до 100 тисяч тих, хто раніше "відкосив" від армії.
Готові внести свою лепту в справу поповнення ЗСУ і союзники. У Європі дедалі частіше лунають голоси за повернення на батьківщину наших біженців, насамперед - чоловіків призовного віку. У Німеччині та Австрії навіть не полінувалися і перерахували таких "по головах" - вийшло 123 тисячі і 14 тисяч відповідно. Немає сумнівів, що такими самими підрахунками займаються зараз і в інших країнах, і не виключено, що стосовно потенційних бійців ЗСУ буде застосовано певні дії для повернення їх в Україну.
РЕКЛАМА
2/5
Які штрафи передбачені за відсутність прав та перевищення швидкості
10.03.2023 10:21
РЕКЛАМА
Sudocrem
Судокрем
ПІКЛУВАННЯ ПРО ШКІРУ БЕЗ ПРОБЛЕМ
Знімає подразнення шкіри
Акційна пропозиція в Auchan
Ювілейний
СМАЧНИЙ СУПУТНИК У ПОДОРОЖІ
ЗАВЖДИ ПОРУЧ


Російський Су-27 випустив ракету по літаку Британії: деталі


Розтрощені авто та багато "швидких": на виїзді з Києва

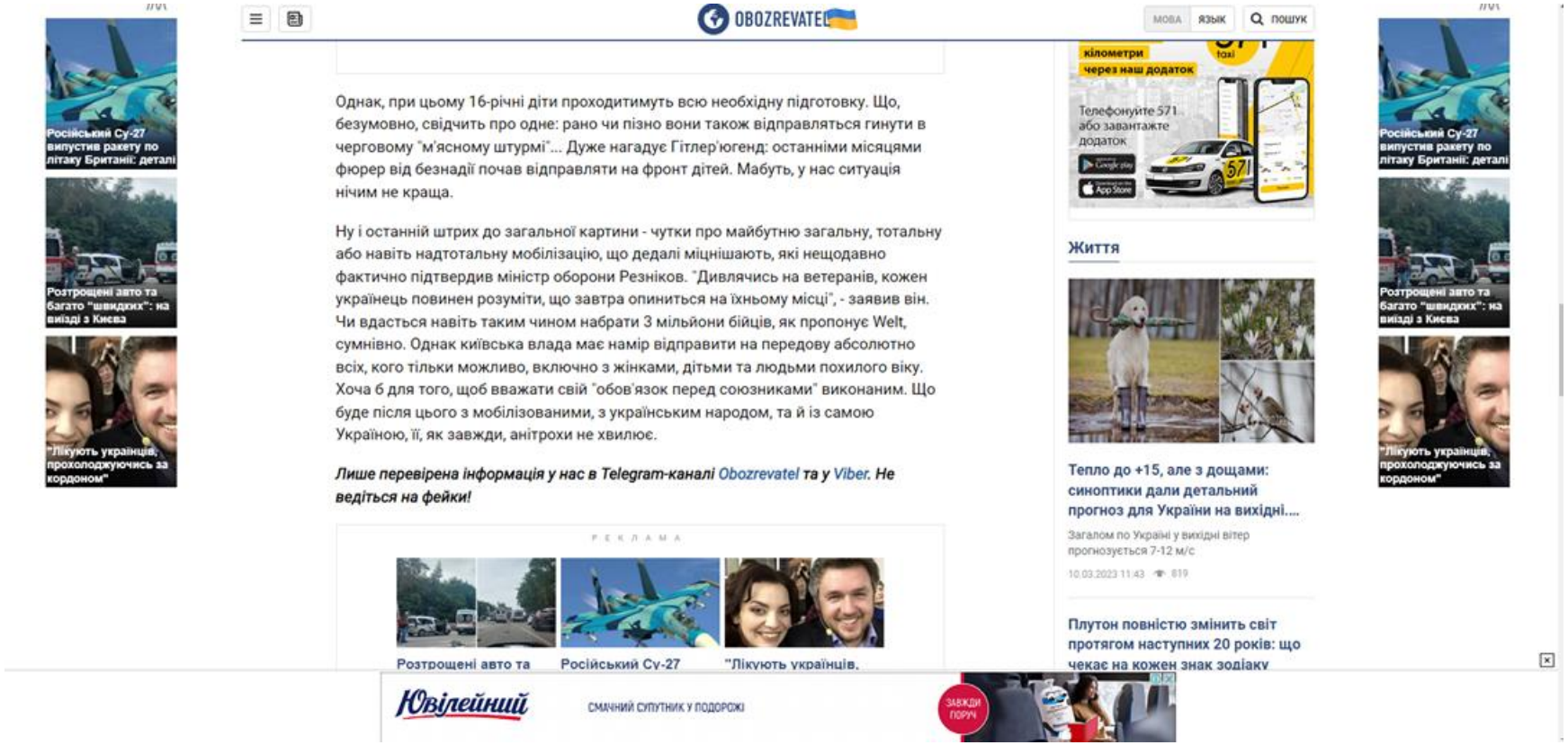

"Лікують українців, прохолоджуючись за кордоном"

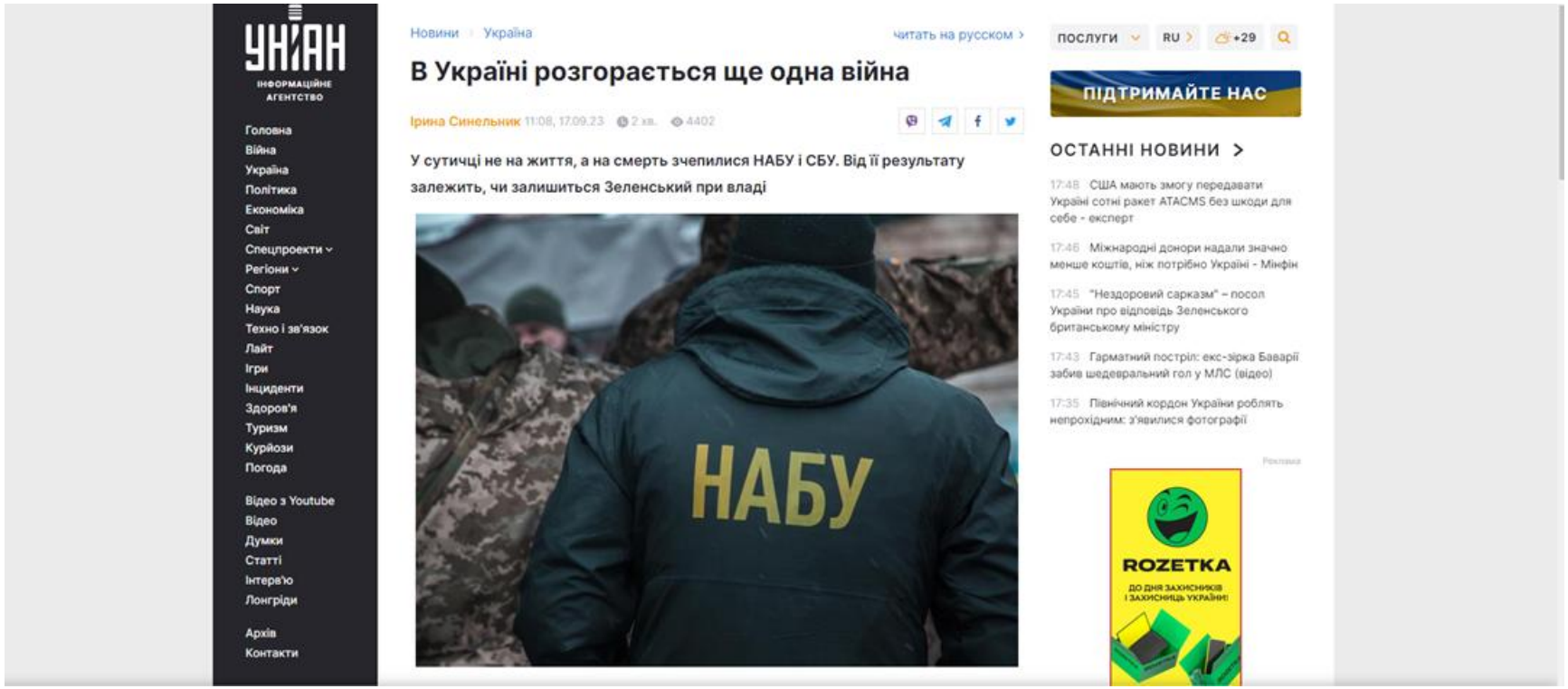

OBOZREVATEL
МОВА
ЯЗЫК
ПОШУК
Monitex
Відкрити
Уже йде і мобілізація жінок. Причому якщо донедавна це стосувалося лише медичних працівників, то тепер вдягнути військову форму доведеться й іншим представницям прекрасної статі. Їм обіцяють службу в так званому "ближньому тилу" - із забезпечення зв'язку, підтримання порядку в населених пунктах тощо, однак у соцмережах уже з'являлася інформація про те, що щонайменше деякі з мобілізованих жінок безпосередньо беруть участь у бойових діях.
Тепер на черзі - зниження призовного віку до 16 років. Відповідний законопроєкт, судячи з витоків інформації, уже готують, а той, що нібито випереджає його, який обмежує виїзд за кордон підлітків у віці від 16 до 18 років, у Верховну Раду вже внесено. Також внесено і прямо пов'язаний із двома названими законопроєкт про формування дитячо-юнацьких військових підрозділів на постійній основі.
За задумом авторів, такі підрозділи матимуть нібито "допоміжний" характер і стануть залучатися для несення служби з охорони складів та інших об'єктів у тилу замість дорослих, які вибули для поповнення втрат на фронт. Цікаво, до речі, що, судячи з наявної інформації, відмінності за статевою приналежністю в цих законопроектах немає, тож нововведення стосуватимуться як юнаків, так і дівчат.
РЕКЛАМА
1/5
NISSAN
TOP NEWS
У Києві почалося прощання з легендарним командиром "Да Вінчі", який загинув у бою під...
Поховання Героя заплановане на 10 березня
10.03.2023 12:16 9,7 т. 74
ЗСУ влаштували окупантам потужну "бавовну" на Херсонщині: знищено 7 човнів із ворожими...
Ряди "200-х" поповнили 20 росіян
10.03.2023 11:01 27,8 т. 162
Бельгія визнала Голодомор 1932-1933 років геноцидом українського народу: Зеленський...
Текст отримав одностайну підтримку, за винятком представників ППБ
Ювілейний
СМАЧНИЙ СУПУТНИК У ПОДОРОЖІ
ЗАВЖДИ ПОРУЧ

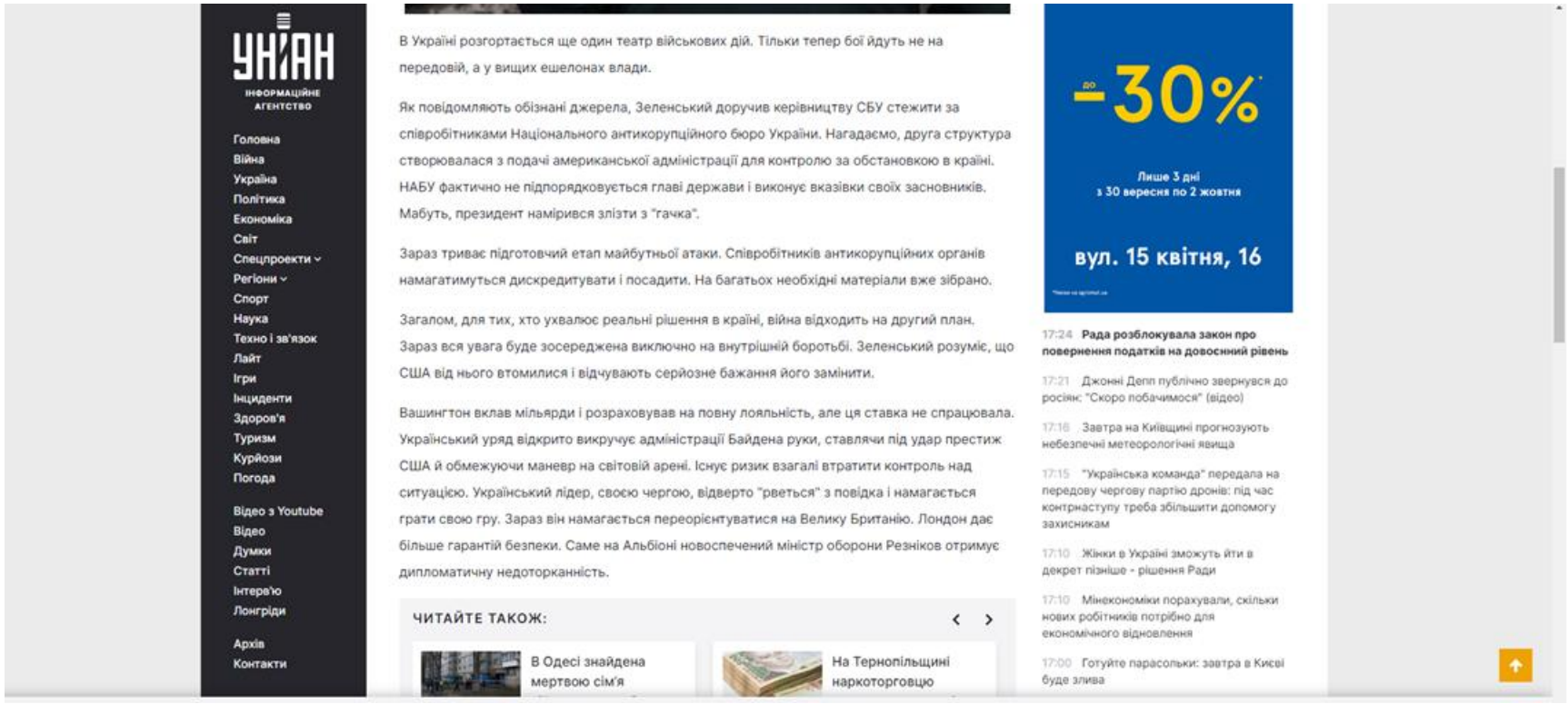
Російський Су-27 випустив ракету по літаку Британії: деталі

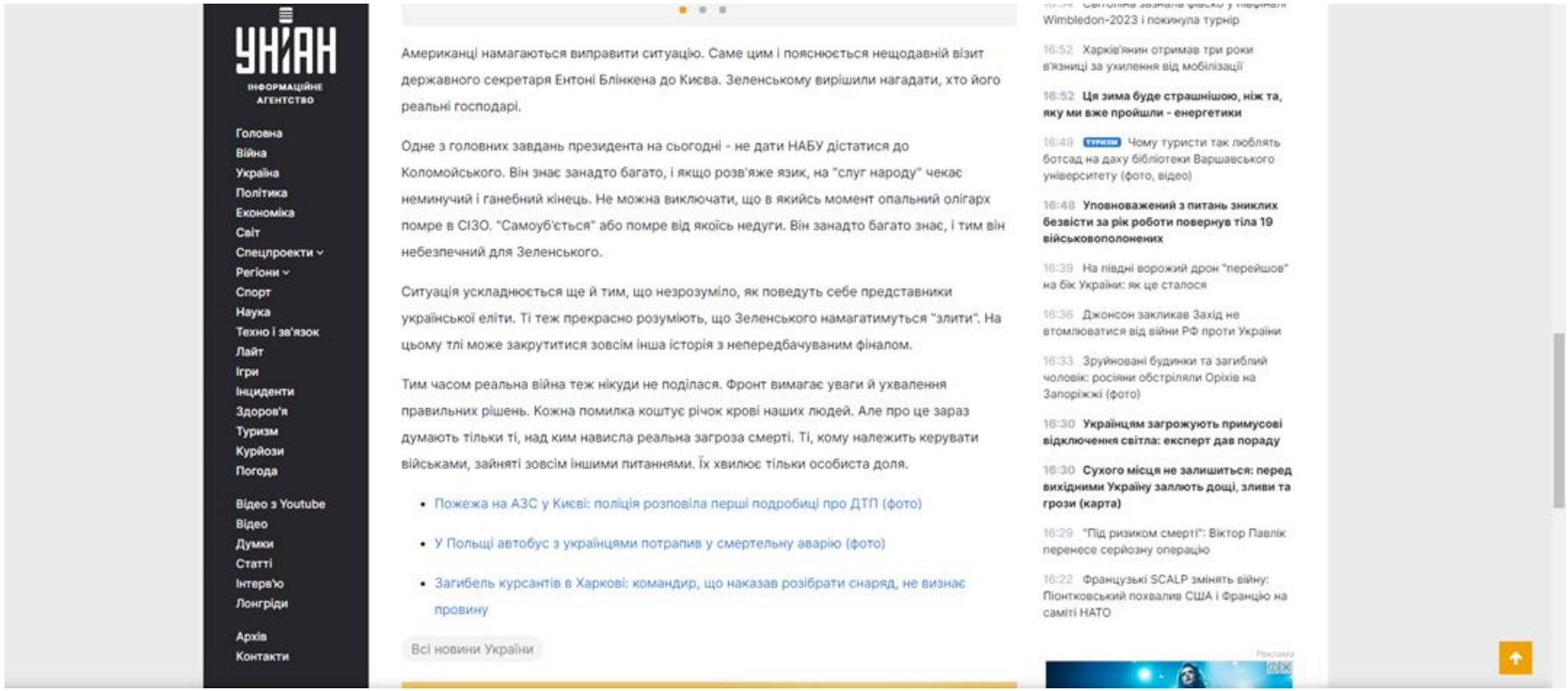
Розтрощені авто та багато "швидких": на виїзді з Києва

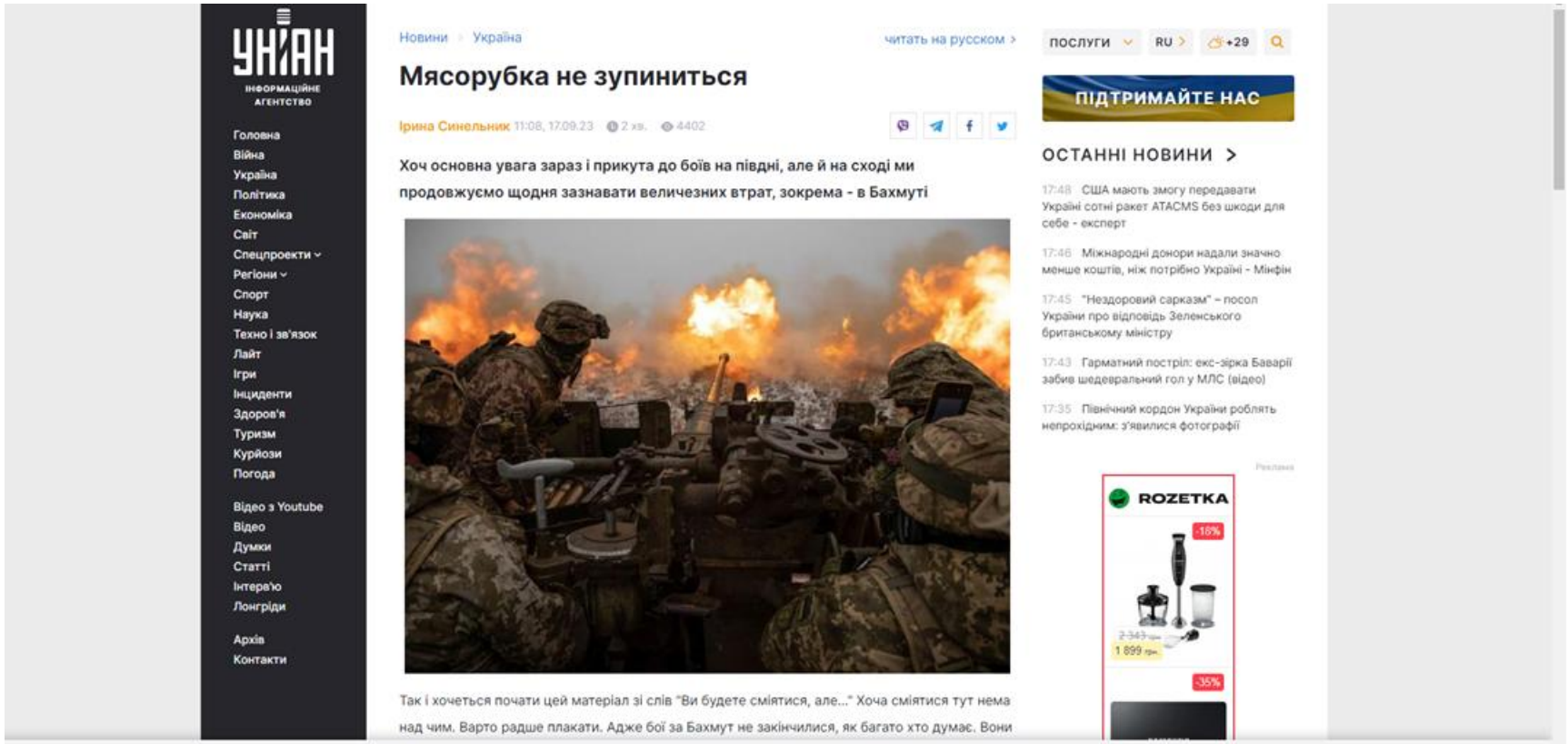
"Лікують українців, прохолоджуючись за кордоном"

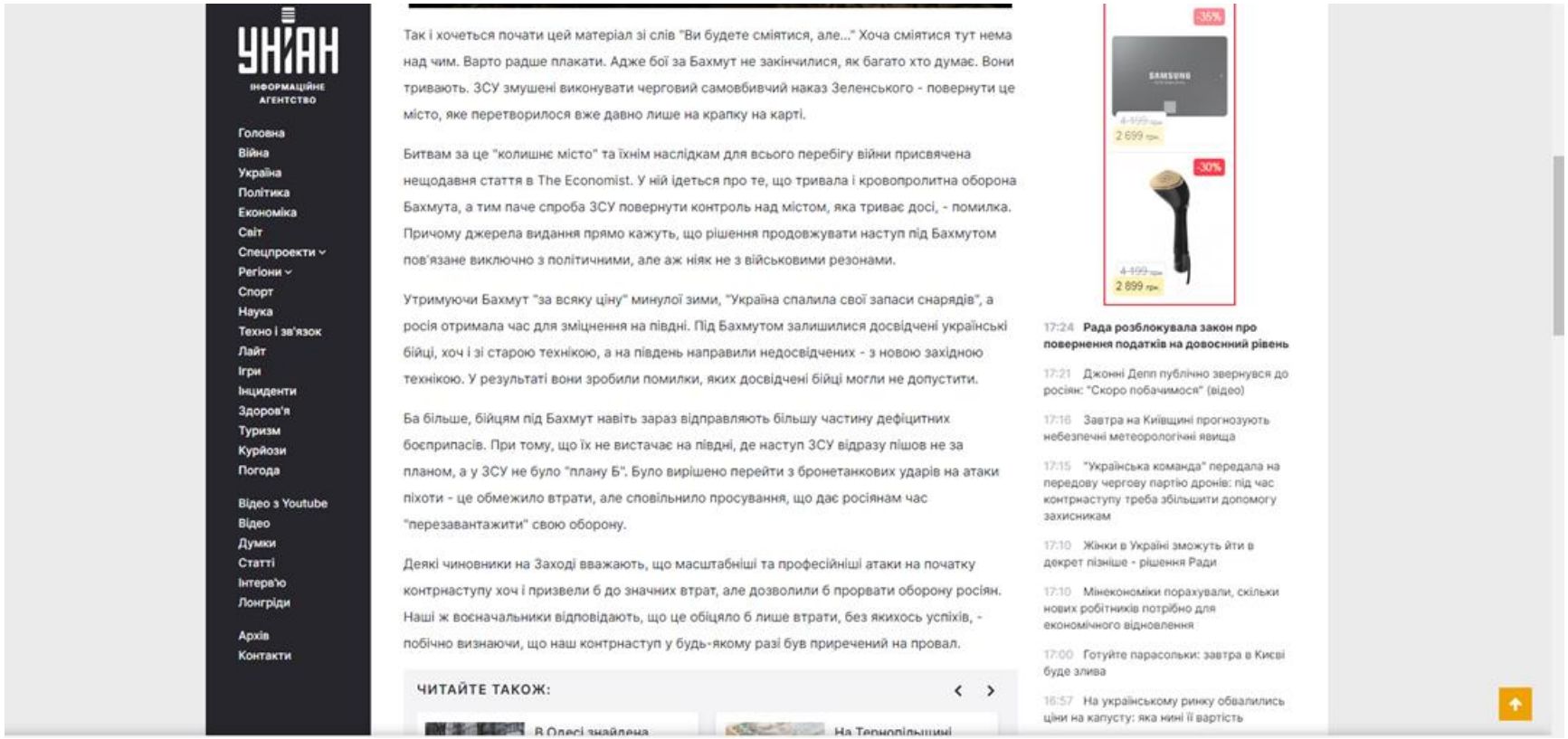

Російський Су-27 випустив ракету по літаку Британії: деталі
Розтрощені авто та багато "швидких": на виїзді з Києва
"Лікують українців, прохолоджуючись за кордоном"
OBOZREVATEL
МОВА
ЯЗЫК
ПОШУК
Однак, при цьому 16-річні діти проходитимуть всю необхідну підготовку. Що, безумовно, свідчить про одне: рано чи пізно вони також відправляться гинути в черговому "м'ясному штурмі"... Дуже нагадує Гітлер'югенд: останніми місяцями фюрер від безнадії почав відправляти на фронт дітей. Мабуть, у нас ситуація нічим не краща.
Ну і останній штрих до загальної картини - чутки про майбутню загальну, тотальну або навіть надтотальну мобілізацію, що дедалі міцнішають, які нещодавно фактично підтвердив міністр оборони Резніков. "Дивлячись на ветеранів, кожен українець повинен розуміти, що завтра опиниться на їхньому місці", - заявив він. Чи вдасться навіть таким чином набрати 3 мільйони бійців, як пропонує Welt, сумнівно. Однак київська влада має намір відправити на передову абсолютно всіх, кого тільки можливо, включно з жінками, дітьми та людьми похилого віку. Хоча б для того, щоб вважати свій "обов'язок перед союзниками" виконаним. Що буде після цього з мобілізованими, з українським народом, та й із самою Україною, її, як завжди, анітрохи не хвилює.
Лише перевірена інформація у нас в Telegram-каналі Obozrevatel та у Viber. Не ведіться на фейки!
РЕКЛАМА
Розтрощені авто та
Російський Су-27
"Лікують українців,
кілометри
через наш додаток
Телефонуйте 571
або завантажте
додаток
Життя
Тепло до +15, але з дощами: синоптики дали детальний прогноз для України на вихідні....
Загалом по Україні у вихідні вітер прогнозується 7-12 м/с
10.03.2023 11:43
619
Плутон повністю змінить світ протягом наступних 20 років: що чекає на кожен знак зодіаку
Ювілейний
СМАЧНИЙ СУПУТНИК У ПОДОРОЖІ
ЗАВЖДИ ПОРУЧ

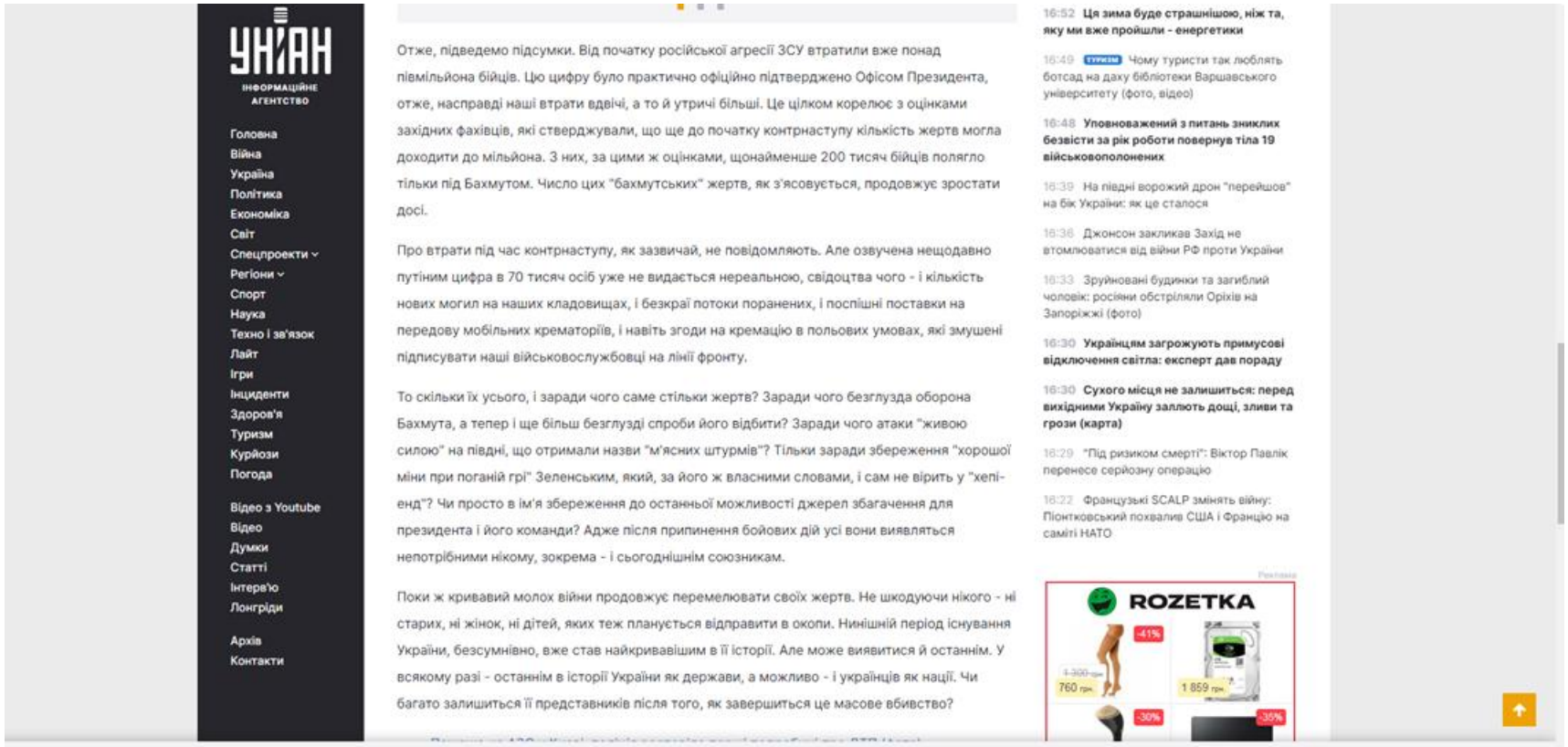

УНІАН
ІНФОРМАЦІЙНЕ АГЕНТСТВО
Головна
Війна
Україна
Політика
Економіка
Світ
Спецпроекти
Регіони
Спорт
Наука
Техно і зв'язок
Лайт
Ігри
Інциденти
Здоров'я
Туризм
Курйози
Погода
Відео з Youtube
Відео
Думки
Статті
Інтерв'ю
Лонгріди
Архів
Контакти
Новини › Україна
читать на русском ›
В Україні розгорається ще одна війна
Ірина Синельник 11:08, 17.09.23 2 хв. 4402
У сутичці не на життя, а на смерть зчепилися НАБУ і СБУ. Від її результату залежить, чи залишиться Зеленський при владі
НАБУ
ПОСЛУГИ
RU
+29
ПІДТРИМАЙТЕ НАС
ОСТАННІ НОВИНИ >
17:48 США мають змогу передавати Україні сотні ракет ATACMS без шкоди для себе - експерт
17:46 Міжнародні донори надали значно менше коштів, ніж потрібно Україні - Мінфін
17:45 "Нездоровий сарказм" – посол України про відповідь Зеленського британському міністру
17:43 Гарматний постріл: екс-зірка Баварії забив шедевральний гол у МЛС (відео)
17:35 Північний кордон України роблять непрохідним: з'явилися фотографії
ROZETKA
ДО ДНЯ ЗАХИСНИКІВ І ЗАХИСНИЦЬ УКРАЇНИ!


УНІАН
ІНФОРМАЦІЙНЕ АГЕНТСТВО
Головна
Війна
Україна
Політика
Економіка
Світ
Спецпроекти
Регіони
Спорт
Наука
Техно і зв'язок
Лайт
Ігри
Інциденти
Здоров'я
Туризм
Курйози
Погода
Відео з Youtube
Відео
Думки
Статті
Інтерв'ю
Лонгріди
Архів
Контакти
В Україні розгортається ще один театр військових дій. Тільки тепер бої йдуть не на передовій, а у вищих ешелонах влади.
Як повідомляють обізнані джерела, Зеленський доручив керівництву СБУ стежити за співробітниками Національного антикорупційного бюро України. Нагадаємо, друга структура створювалася з подачі американської адміністрації для контролю за обстановкою в країні. НАБУ фактично не підпорядковується главі держави і виконує вказівки своїх засновників. Мабуть, президент намірився злізти з "гачка".
Зараз триває підготовчий етап майбутньої атаки. Співробітників антикорупційних органів намагатимуться дискредитувати і посадити. На багатьох необхідні матеріали вже зібрано.
Загалом, для тих, хто ухвалює реальні рішення в країні, війна відходить на другий план. Зараз вся увага буде зосереджена виключно на внутрішній боротьбі. Зеленський розуміє, що США від нього втомилися і відчувають серйозне бажання його замінити.
Вашингтон вклав мільярди і розраховував на повну лояльність, але ця ставка не спрацювала. Український уряд відкрито викручує адміністрації Байдена руки, ставлячи під удар престиж США й обмежуючи маневр на світовій арені. Існує ризик взагалі втратити контроль над ситуацією. Український лідер, своєю чергою, відверто "рветься" з повідка і намагається грати свою гру. Зараз він намагається переорієнтуватися на Велику Британію. Лондон дає більше гарантій безпеки. Саме на Альбіоні новоспечений міністр оборони Резніков отримує дипломатичну недоторканність.
ЧИТАЙТЕ ТАКОЖ:
В Одесі знайдена мертвою сім'я
На Тернопільщині наркоторговцю
-30%
Лише 3 дні
з 30 вересня по 2 жовтня
вул. 15 квітня, 16
17:24 Рада розблокувала закон про повернення податків на довоєнний рівень
17:21 Джонні Депп публічно звернувся до росіян: "Скоро побачимося" (відео)
17:16 Завтра на Київщині прогнозують небезпечні метеорологічні явища
17:15 "Українська команда" передала на передову чергову партію дронів: під час контрнаступу треба збільшити допомогу захисникам
17:10 Жінки в Україні зможуть йти в декрет пізніше - рішення Ради
17:10 Мінекономіки порахували, скільки нових робітників потрібно для економічного відновлення
17:00 Готуйте парасольки: завтра в Києві буде злива


УНІАН
ІНФОРМАЦІЙНЕ АГЕНТСТВО
Головна
Війна
Україна
Політика
Економіка
Світ
Спецпроекти
Регіони
Спорт
Наука
Техно і зв'язок
Лайт
Ігри
Інциденти
Здоров'я
Туризм
Курйози
Погода
Відео з Youtube
Відео
Думки
Статті
Інтерв'ю
Лонгріди
Архів
Контакти
Американці намагаються виправити ситуацію. Саме цим і пояснюється нещодавній візит державного секретаря Ентоні Блінкена до Києва. Зеленському вирішили нагадати, хто його реальні господарі.
Одне з головних завдань президента на сьогодні - не дати НАБУ дістатися до Коломойського. Він знає занадто багато, і якщо розв'яже язик, на "слуг народу" чекає неминучий і ганебний кінець. Не можна виключати, що в якийсь момент опальний олігарх помре в СІЗО. "Самоуб'ється" або помре від якоїсь недуги. Він занадто багато знає, і тим він небезпечний для Зеленського.
Ситуація ускладнюється ще й тим, що незрозуміло, як поведуть себе представники української еліти. Ті теж прекрасно розуміють, що Зеленського намагатимуться "злити". На цьому тлі може закрутитися зовсім інша історія з непередбачуваним фіналом.
Тим часом реальна війна теж нікуди не поділася. Фронт вимагає уваги й ухвалення правильних рішень. Кожна помилка коштує річок крові наших людей. Але про це зараз думають тільки ті, над ким нависла реальна загроза смерті. Ті, кому належить керувати військами, зайняті зовсім іншими питаннями. Їх хвилює тільки особиста доля.
Пожежа на АЗС у Києві: поліція розповіла перші подробиці про ДТП (фото)
У Польщі автобус з українцями потрапив у смертельну аварію (фото)
Загибель курсантів в Харкові: командир, що наказав розібрати снаряд, не визнає провину
Всі новини України
Wimbledon-2023 і покинула турнір
16:52 Харків'янин отримав три роки в'язниці за ухилення від мобілізації
16:52 Ця зима буде страшнішою, ніж та, яку ми вже пройшли - енергетики
16:49 ТУРИЗМ Чому туристи так люблять ботсад на даху бібліотеки Варшавського університету (фото, відео)
16:48 Уповноважений з питань зниклих безвісти за рік роботи повернув тіла 19 військовополонених
16:39 На півдні ворожий дрон "перейшов" на бік України: як це сталося
16:36 Джонсон закликав Захід не втомлюватися від війни РФ проти України
16:33 Зруйновані будинки та загиблий чоловік: росіяни обстріляли Оріхів на Запоріжжі (фото)
16:30 Українцям загрожують примусові відключення світла: експерт дав пораду
16:30 Сухого місця не залишиться: перед вихідними Україну заллють дощі, зливи та грози (карта)
16:29 "Під ризиком смерті": Віктор Павлік перенесе серйозну операцію
16:22 Французькі SCALP змінять війну: Піонтковський похвалив США і Францію на саміті НАТО
Реклама


УНІАН
ІНФОРМАЦІЙНЕ АГЕНТСТВО
Головна
Війна
Україна
Політика
Економіка
Світ
Спецпроекти
Регіони
Спорт
Наука
Техно і зв'язок
Лайт
Ігри
Інциденти
Здоров'я
Туризм
Курйози
Погода
Відео з Youtube
Відео
Думки
Статті
Інтерв'ю
Лонгріди
Архів
Контакти
Новини › Україна
читать на русском >
Мясорубка не зупиниться
Ірина Синельник 11:08, 17.09.23 2 хв. 4402
Хоч основна увага зараз і прикута до боїв на півдні, але й на сході ми продовжуємо щодня зазнавати величезних втрат, зокрема - в Бахмуті
Так і хочеться почати цей матеріал зі слів "Ви будете сміятися, але..." Хоча сміятися тут нема над чим. Варто радше плакати. Адже бої за Бахмут не закінчилися, як багато хто думає. Вони
послуги
RU
+29
ПІДТРИМАЙТЕ НАС
ОСТАННІ НОВИНИ >
17:48 США мають змогу передавати Україні сотні ракет ATACMS без шкоди для себе - експерт
17:46 Міжнародні донори надали значно менше коштів, ніж потрібно Україні - Мінфін
17:45 "Нездоровий сарказм" – посол України про відповідь Зеленського британському міністру
17:43 Гарматний постріл: екс-зірка Баварії забив шедевральний гол у МЛС (відео)
17:35 Північний кордон України роблять непрохідним: з'явилися фотографії
Реклама
ROZETKA
-16%
1 899 грн
-35%


УНІАН
ІНФОРМАЦІЙНЕ АГЕНТСТВО
Головна
Війна
Україна
Політика
Економіка
Світ
Спецпроекти
Регіони
Спорт
Наука
Техно і зв'язок
Лайт
Ігри
Інциденти
Здоров'я
Туризм
Курйози
Погода
Відео з Youtube
Відео
Думки
Статті
Інтерв'ю
Лонгріди
Архів
Контакти
Так і хочеться почати цей матеріал зі слів "Ви будете сміятися, але..." Хоча сміятися тут нема над чим. Варто радше плакати. Адже бої за Бахмут не закінчилися, як багато хто думає. Вони тривають. ЗСУ змушені виконувати черговий самовбивчий наказ Зеленського - повернути це місто, яке перетворилося вже давно лише на крапку на карті.
Битвам за це "колишнє місто" та їхнім наслідкам для всього перебігу війни присвячена нещодавня стаття в The Economist. У ній ідеться про те, що тривала і кровопролитна оборона Бахмута, а тим паче спроба ЗСУ повернути контроль над містом, яка триває досі, - помилка. Причому джерела видання прямо кажуть, що рішення продовжувати наступ під Бахмутом пов'язане виключно з політичними, але аж ніяк не з військовими резонами.
Утримуючи Бахмут "за всяку ціну" минулої зими, "Україна спалила свої запаси снарядів", а росія отримала час для зміцнення на півдні. Під Бахмутом залишилися досвідчені українські бійці, хоч і зі старою технікою, а на південь направили недосвідчених - з новою західною технікою. У результаті вони зробили помилки, яких досвідчені бійці могли не допустити.
Ба більше, бійцям під Бахмут навіть зараз відправляють більшу частину дефіцитних боєприпасів. При тому, що їх не вистачає на півдні, де наступ ЗСУ відразу пішов не за планом, а у ЗСУ не було "плану Б". Було вирішено перейти з бронетанкових ударів на атаки піхоти - це обмежило втрати, але сповільнило просування, що дає росіянам час "перезавантажити" свою оборону.
Деякі чиновники на Заході вважають, що масштабніші та професійніші атаки на початку контрнаступу хоч і призвели б до значних втрат, але дозволили б прорвати оборону росіян. Наші ж воєначальники відповідають, що це обіцяло б лише втрати, без якихось успіхів, - побічно визнаючи, що наш контрнаступ у будь-якому разі був приречений на провал.
ЧИТАЙТЕ ТАКОЖ:
-35%
SAMSUNG
2 699
-30%
2 899
17:24 Рада розблокувала закон про повернення податків на довоєнний рівень
17:21 Джонні Депп публічно звернувся до росіян: "Скоро побачимося" (відео)
17:16 Завтра на Київщині прогнозують небезпечні метеорологічні явища
17:15 "Українська команда" передала на передову чергову партію дронів: під час контрнаступу треба збільшити допомогу захисникам
17:10 Жінки в Україні зможуть йти в декрет пізніше - рішення Ради
17:10 Мінекономіки порахували, скільки нових робітників потрібно для економічного відновлення
17:00 Готуйте парасольки: завтра в Києві буде злива
16:57 На українському ринку обвалились ціни на капусту: яка нині її вартість



УНІАН
ІНФОРМАЦІЙНЕ АГЕНТСТВО

Головна
Війна
Україна
Політика
Економіка
Світ
Спецпроекти
Регіони
Спорт
Наука
Техно і зв'язок
Лайт
Ігри
Інциденти
Здоров'я
Туризм
Курйози
Погода

Відео з Youtube
Відео
Думки
Статті
Інтерв'ю
Лонгріди

Архів
Контакти

Отже, підведемо підсумки. Від початку російської агресії ЗСУ втратили вже понад півмільйона бійців. Цю цифру було практично офіційно підтверджено Офісом Президента, отже, насправді наші втрати вдвічі, а то й утричі більші. Це цілком корелює з оцінками західних фахівців, які стверджували, що ще до початку контрнаступу кількість жертв могла доходити до мільйона. З них, за цими ж оцінками, щонайменше 200 тисяч бійців полягло тільки під Бахмутом. Число цих "бахмутських" жертв, як з'ясовується, продовжує зростати досі.

Про втрати під час контрнаступу, як зазвичай, не повідомляють. Але озвучена нещодавно путіним цифра в 70 тисяч осіб уже не видається нереальною, свідоцтва чого - і кількість нових могил на наших кладовищах, і безкраї потоки поранених, і поспішні поставки на передову мобільних крематоріїв, і навіть згоди на кремацію в польових умовах, які змушені підписувати наші військовослужбовці на лінії фронту.

То скільки їх усього, і заради чого саме стільки жертв? Заради чого безглузда оборона Бахмута, а тепер і ще більш безглузді спроби його відбити? Заради чого атаки "живою силою" на півдні, що отримали назви "м'ясних штурмів"? Тільки заради збереження "хорошої міни при поганій грі" Зеленським, який, за його ж власними словами, і сам не вірить у "хепі-енд"? Чи просто в ім'я збереження до останньої можливості джерел збагачення для президента і його команди? Адже після припинення бойових дій усі вони виявляться непотрібними нікому, зокрема - і сьогоднішнім союзникам.

Поки ж кривавий молох війни продовжує перемелювати своїх жертв. Не шкодуючи нікого - ні старих, ні жінок, ні дітей, яких теж планується відправити в окопи. Нинішній період існування України, безсумнівно, вже став найкривавішим в її історії. Але може виявитися й останнім. У всякому разі - останнім в історії України як держави, а можливо - і українців як нації. Чи багато залишиться її представників після того, як завершиться це масове вбивство?

16:52 **Ця зима буде страшнішою, ніж та, яку ми вже пройшли - енергетики**

16:49 ТУРИЗМ Чому туристи так люблять ботсад на даху бібліотеки Варшавського університету (фото, відео)

16:48 **Уповноважений з питань зниклих безвісти за рік роботи повернув тіла 19 військовополонених**

16:39 На півдні ворожий дрон "перейшов" на бік України: як це сталося

16:36 Джонсон закликав Захід не втомлюватися від війни РФ проти України

16:33 Зруйновані будинки та загиблий чоловік: росіяни обстріляли Оріхів на Запоріжжі (фото)

16:30 **Українцям загрожують примусові відключення світла: експерт дав пораду**

16:30 **Сухого місця не залишиться: перед вихідними Україну заллють дощі, зливи та грози (карта)**

16:29 "Під ризиком смерті": Віктор Павлік перенесе серйозну операцію

16:22 Французькі SCALP змінять війну: Піонтковський похвалив США і Францію на саміті НАТО

ДОДАТОК Б13

ОСНОВНІ ОСОБЛИВОСТІ

Постанови Кабінету Міністрів України від 03.12.2025 № 1580 «Деякі питання пошуку та виявлення потенційних вразливостей в інформаційно-комунікаційних системах» з огляду на зміни, які вона вносить у систему Bug Bounty та відповідний Порядок пошуку вразливостей (Постанова № 497 від 16.05.2023 р.).

1. Основна ідея постанови № 1580

Постанова затверджує новий Порядок пошуку та/або виявлення потенційних вразливостей в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, де обробляються державні інформаційні ресурси або інформація з обмеженим доступом, а також на об’єктах критичної інформаційної інфраструктури.

Цей Порядок встановлює організаційно-технічний механізм для здійснення пошуку вразливостей, включно з легальними програмами Bug Bounty, а також уніфікує підходи до сканування, оцінки захищеності та обміну інформацією про вразливості.

2. Новели, що вносяться в реалізацію механізму Bug Bounty

2.1. Юридична легалізація Bug Bounty для державних систем

Постанова прямо легалізує практику «Bug Bounty» – тобто пошук вразливостей за винагороду та узгоджене розкриття, що раніше не мало чіткої правової основи. Це дозволяє залучати зовнішніх фахівців (етичних «білих») хакерів) у правове полі. Це важливо для кібербезпеки державних ІТ-систем, оскільки:

надає правове підґрунтя для залучення дослідників без ризику притягнення до відповідальності;

встановлює чіткі правила участі, включно з обмеженнями щодо невтручання в роботу системи;

визначає обов’язок дослідника не пізніше 24 годин повідомити про знайдену вразливість власника системи та CERT-UA/CSIRT.

2.2. Публічна пропозиція умов Bug Bounty

Власник системи або організатор програми повинен оприлюднити публічну пропозицію із чіткими умовами:

зона тестування;

правила повідомлення;

джерела та порядок виплати винагороди.

Це забезпечує прозорість і зменшує ризики юридичних або етичних колізій.

3. Механізм узгодженого розкриття вразливостей

Постанова закріплює так званий coordinated disclosure (узгоджене розкриття): дослідник може повідомити про вразливість не лише власника, але й CERT-UA або відповідний CSIRT; це дозволяє координувати реагування та мінімізувати ризики несанкціонованого розголошення або експлуатації.

4. Зміни до Порядку № 497

Зміни до діючого порядку № 497 (2023 р.) унормовують:

участь «дослідника» у програмах пошуку вразливостей;

розширення термінів та визначень (наприклад, «експлуатація вразливості»);

можливість державно-приватної взаємодії у проведенні Bug Bounty.

Ці уточнення прибирають правові прогалини та стандартизують підходи до:

формування умов програм;

аналізу звітів;

перевірки результатів та оцінки ризиків.

5. Ключові положення нового порядку

5.1. Введення обов’язків для власників систем

Власники або розпорядники систем повинні на постійній основі забезпечувати пошук потенційних вразливостей, зокрема: збір інформації про них; оцінка захищеності; впровадження програм Bug Bounty за потреби.

5.2. Роль CERT-UA і CSIRT

Національна команда реагування CERT-UA і відповідні CSIRT:

координують обмін інформацією;

аналізують дані від дослідників;

поширюють рекомендації щодо усунення вразливостей.

Це створює координований національний канал для управління вразливостями, що значно посилює кіберзахист державних АІС.

6. Практичне значення для ІТ-спільноти

6.1. Переваги

Перехід Bug Bounty з «сірої зони» у правове поле.

Залучення зовнішніх фахівців до державної кібербезпеки без правових ризиків.

Чіткі правила та прозорість програм.

Координація через CERT-UA/CSIRT.

Стандартизація підходів до виявлення та обробки вразливостей.

6.2. Ризики/виклики

Необхідність узгодження умов винагороди з бюджетним і правовим контекстом.

Потреба побудови інфраструктури для обробки великої кількості звітів.

Забезпечення балансу між відкритістю участі та захистом критичних даних.

7. Джерела інформації:

7.1. Деякі питання пошуку та виявлення потенційних вразливостей в інформаційно-комунікаційних системах. Постанова Кабінет Міністрів України від 03.12.2025 р. № 1580. URL: https://zakon.rada.gov.ua/laws/show/1580-2025-%D0%BF#Text

7.2. Уряд легалізував Bug Bounty – «білих хакерів» – для державних систем. INSHE.TV. 09.12.2025. URL: https://inshe.tv/tehnologii-2/2025-12-09/966274/?utm_source=chatgpt.com

ДОДАТОК В

ВЕРХОВНИЙ СУД
КАСАЦІЙНИЙ ЦИВІЛЬНИЙ СУД
просп. Повітряних Сил, 28, м. Київ, 03063, Україна, тел. (044) 591 10 00
e-mail: kcs@supreme.court.gov.ua
Код ЄДРПОУ 41721784

ДОВІДКА ПРО ВПРОВАДЖЕННЯ

Результати дисертації аспіранта кафедри конституційного і адміністративного права Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут» Криволапа Євгенія Володимировича на тему «Адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України», підготовленої для захисту на здобуття ступеня доктора філософії за спеціальністю 081 «Право» впроваджено у діяльність секретаріату Касаційного цивільного суду у складі Верховного Суду.

Отримані результати автора використані в організації і плануванні роботи з протидії правопорушенням у кібермережі, зокрема: несанкціоноване втручання в роботу інформаційних (автоматизованих), інформаційно-комунікаційних, електронних комунікаційних систем, електронних комунікаційних мереж; створення шкідливих програмних чи технічних засобів з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут, які (засоби) призначені для несанкціонованого втручання в роботу інформаційних (автоматизованих), інформаційно-комунікаційних, електронних комунікаційних систем, електронних комунікаційних мереж; несанкціоновані збут або розповсюдження створеної та захищеної відповідно до чинного законодавства інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації; несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), комп'ютерних мережах, автоматизованих системах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї; порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), комп'ютерних мереж, автоматизованих систем чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється; перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), комп'ютерних мереж, автоматизованих систем чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку; шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки»; кібербулінг; кіберсталкінг.

Використання результатів дисертації забезпечило підвищення рівня організації і плануванні роботи секретаріату Касаційного цивільного суду у складі Верховного Суду з протидії правопорушенням у кібермережі.

Заступник керівника Апарату –
керівник секретаріату
Касаційного цивільного суду — Олена ГРИЦИК

Начальник управління
забезпечення роботи третьої судової
палати секретаріату
Касаційного цивільного суду,
кандидат історичних наук — Інна ВОЛКОВА

Начальник відділу технічної підтримки та
супроводу ІТ-інфраструктури
Касаційного цивільного суду — Олексій АЛЬОХІН

ЗАТВЕРДЖУЮ
Проректор з наукових досліджень та трансферу технологій
ДНП «Державний університет «Київський авіаційний інститут»
Сергій ГНАТЮК
“01” 12 2025 року
М.П.

АКТ

Комісія у складі:
голови – декана Факультету права та міжнародних відносин, к.ю.н., доцента Жукорської Ярини Михайлівни;

членів комісії: – завідувача кафедри теорії держави і права, конституційного та адміністративного права, к.ю.н., доцента Макеєвої Олени Миколаївни;
– професора кафедри теорії держави і права, конституційного та адміністративного права, д.ю.н., професора Кунєва Юрія Дем’яновича.

цим Актом засвідчує, що результати дисертаційного дослідження аспіранта кафедри конституційного і адміністративного права Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут» Криволапа Євгенія Володимировича на тему «Адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України», підготовленого для захисту на здобуття ступеня доктора філософії за спеціальністю 081 «Право», впроваджена у наукову діяльність Факультету права та міжнародних відносин Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут» (при виконанні робіт – Національний авіаційний університет), зокрема, кафедри конституційного та адміністративного права, при виконанні тем: «Забезпечення конституційних прав громадян в контексті конвенційних зобов’язань України» (державний реєстраційний номер 0119U103091); «Людиноцентричність публічного права України» (державний реєстраційний номер 0124U003363) та держбюджетної науково-дослідної роботи № 312-ДБ20 «Проблеми формування та реалізації державної політики у сфері інформаційної безпеки України: теорія і практика» (державний реєстраційний номер 0120U102136), зокрема, з урахуванням даних розробок підготовлені і передані Комітету Верховної Ради України з питань правоохоронної діяльності пропозиції щодо удосконалення законодавчого регулювання в галузі криміналізації правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (розділ XVI Кримінального кодексу України), з

урахуванням Конвенції про кіберзлочинність, ратифікованої Законом України від 07.09.2005 № 2824-IV «Про ратифікацію Конвенції про кіберзлочинність», які (пропозиції) підготовлені в рамках наукової теми 312-DB20 «Проблеми формування та реалізації державної політики у сфері інформаційної безпеки України: теорія та практика». Відповідно до листа Комітету, зазначені пропозиції надані народним депутатам України – членам Комітету для ознайомлення.

Голова комісії
Декан Факультету права та
міжнародних відносин,
к.ю.н., доцент — Ярина ЖУКОРСЬКА

Члени комісії:
Завідувач кафедри теорії держави і права,
конституційного та адміністративного права,
к.ю.н., доцент — Олена МАКЄЄВА

Професор кафедри теорії держави і права,
конституційного та адміністративного права,
д.ю.н., професор — Юрій КУНЄВ

Паперова копія електронного документа

ВЕРХОВНА РАДА УКРАЇНИ
Комітет з питань правоохоронної діяльності
01008, м.Київ-8, вул. М. Грушевського, 5, тел.: 255-35-06

Проректору
Національного
авіаційного університету
Романенку Є.О.

Шановний Євгенію Олександровичу!

Комітетом Верховної Ради України з питань правоохоронної діяльності отримано пропозиції щодо удосконалення законодавчого регулювання в галузі криміналізації правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (розділ XVI Кримінального кодексу України), з урахуванням Конвенції про кіберзлочинність, ратифікованої Законом України від 07.09.2005 № 2824-IV «Про ратифікацію Конвенції про кіберзлочинність», що підготовлені докторами юридичних наук Сопілко І.М. та Юринець Ю.Л. в рамках наукової теми 312-DB20 «Проблеми формування та реалізації державної політики у сфері інформаційної безпеки України: теорія та практика».

Повідомляємо, що зазначені пропозиції надані народним депутатам України – членам Комітету для ознайомлення.

З повагою

Голова Комітету **С. Іонушас**

ЗГІДНО З ОРИГІНАЛОМ
Керівник секретаріату Комітету
Верховної Ради України
з питань правоохоронної діяльності
(підпис) 14.12.2022 (дата)

ЄАС ВЕРХОВНОЇ РАДИ УКРАЇНИ
Підписувач: Іонушас Сергій Костянтинович
Сертифікат: 58E2D9E7F900307B04000000D0512F00D41E8F00
Дійсний до: 26.01.2023 0:00:00

Апарат Верховної Ради України
04-27/12-2022/214837 від 13.12.2022
1069093

ЗАТВЕРДЖУЮ
Ректор Київського національного
університету будівництва і архітектури
Олексій ДНІПРОВ
«24» 2025 року
М.П.

АКТ

Комісія у складі:
Голови – проректора з науково-педагогічної роботи та стратегічного розвитку, к.п.н., доцента Дудника Юрія Павловича;

членів комісії: – декана Факультету урбаністики та просторового планування, к.т.н. доцента Мамедова Алірзи Махмуда огли;
– завідувача кафедри права та публічного управління, д.ю.н. Нікітіна Володимира Вікторовича

цим Актом засвідчує, що результати дисертаційного дослідження аспіранта кафедри теорії держави і права, конституційного та адміністративного права Факультету права та міжнародних відносин державного некомерційного підприємства «Державний університет «Київський авіаційний інститут» Криволапа Євгенія Володимировича на тему: «Адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України» на здобуття ступеня доктора філософії за спеціальністю 08 - Право за спеціальністю 081 - Право впроваджені в діяльності Київського національного університету будівництва і архітектури.

Дослідження та результати дисертанта, зокрема, використані у процесі підготовки пропозицій щодо розробки навчальних програм та курсів кафедри права та публічного управління Факультету урбаністики та просторового планування, підготовки курсів лекцій з дисциплін «Цифрові трансформації у суспільстві та електронне урядування», «Захист персональних даних», «Адміністративне право і процес», «Конституційне право України», «Верховенство права через призму конституційного та адміністративного права та процесу» з використанням аналітичних матеріалів щодо сутності і змісту адміністративно-правових засад спрямування методів і засобів забезпечення кібернетичної безпеки, на вирішення завдань забезпечення інформаційної безпеки.

Голова комісії
Проректор з науково-педагогічної роботи
та стратегічного розвитку,
к.п.н., доцент Юрій ДУДНИК

Члени комісії
Декан факультету урбаністики
та просторового планування,
к.т.н., доцент Алірза Махмуд огли МАМЕДОВ

Завідувач кафедри права та
публічного управління, д.ю.н. Володимир НІКІТІН

УКРАЇНСЬКА АСОЦІАЦІЯ
ІНВЕСТИЦІЙНОГО БІЗНЕСУ
Саморегулівна організація

вул. Предславінська, 28
03150, м. Київ, Україна
Телефон/факс: (044) 528-72-66, 528-72-70
E-mail: office@uaib.com.ua

THE UKRAINIAN ASSOCIATION
OF INVESTMENT BUSINESS
Self-regulation organization

28 Predslavinska St.
03150 Kyiv, Ukraine
Phone/fax: 528-72 -66, 528-72-70
E-mail: office@uaib.com.ua

01.12.2025р.

Довідка

Результати дисертації аспіранта кафедри конституційного і адміністративного права Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут» Криволапа Євгенія Володимировича на тему «Адміністративно-правове забезпечення діяльності у сфері кібернетичної безпеки України», підготовленої для захисту на здобуття ступеня доктора філософії за спеціальністю 081 «Право» впроваджена у діяльність Української асоціації інвестиційного бізнесу.

Отримані результати автора використані в організації роботи з підвищення рівня захисту інформаційних баз даних, зокрема, використання надійних паролів, регулярне оновлення програмного забезпечення: операційної системи та всі програми; використання антивірусного програмного забезпечення та брандмауера; уникнення відкриття підозрілих електронних листів, завантаження неперевіреного вмісту та переходів за сумнівними посиланнями; активація двофакторної аутентифікації; створення резервних копії, щоб уникнути втрати даних; використання тільки ліцензійних та офіційних програм тощо.

Використання результатів дисертації забезпечило підвищення рівня захисту інформаційних баз даних в Українській асоціації інвестиційного бізнесу.

Генеральний директор **А.А. Рибальченко**