УДК 343.3
DOI https://doi.org/10.32782/2524-0374/2023-7/82

КРИМІНАЛЬНО-ПРАВОВА ОХОРОНА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ЄВРОПЕЙСЬКІ СТАНДАРТИ

CRIMINAL LAW PROTECTION OF INFORMATION SECURITY: EUROPEAN STANDARDS

Демидова Л.М., д.ю.н., професор,
головний науковий співробітник відділу дослідження проблем кримінального права
Науково-дослідний інститут вивчення проблем злочинності імені академіка В.В. Сташиса Національної академії правових наук України

Стаття присвячена встановленню й дослідженню стандартів Європейського Союзу стосовно інформаційної безпеки, що охороняється за допомогою кримінального права як галузі права. Зазначається, що в сучасних умовах технологічних інновацій питання забезпечення інформаційної безпеки набувають особливого державного, соціального і правового значення, а поняття «інформаційна безпека» виходить на рівень міждисциплінарних і комплексних досліджень.

Авторка підкреслює, що інформаційна безпека є об'єктом кримінально-правової охорони з певною структурою відповідних суспільних відносин, елементами якої є предмет суспільних відносин, їх зміст, суб'єкти таких відносин. Залежно від суб'єктів суспільних відносин йдеться про інформаційну безпеку людини (фізичної особи), юридичної особи, суспільства, держави, світової спільноти. З одного боку, ці відносини можна оцінити як інформаційні, зокрема інформаційно-ціннісні, інформаційно-економічні, інформаційно-психологічні, інформаційно-технологічні, інформаційно-політичні. З іншого, – інформаційна безпека є складником особистої безпеки людини; безпеки юридичної особи; безпеки суспільств: національної безпеки України, зокрема основ національної безпеки України; міжнародної безпеки.

Звертається увага на значення стандартизації для забезпечення інформаційної безпеки, вивчаються і аналізуються підходи Міжнародної організації стандартизації, рішення та рекомендації Ради Європи й Європарламенту з цього питання. Дослідниця підтримує позицію науковців, які вважають, що Україна, обравши євроінтеграційних курс, має орієнтуватися на стратегію розвитку країн-учасниць ЄС в інформаційній сфері і здійснює порівняльно-правовий аналіз європейських підходів і стандартів та норм законодавства України про кримінальну відповідальність щодо кіберзлочинності й штучного інтелекту.

Пропонується авторське бачення шляхів і конкретних заходів впровадження низки визнаних європейських стандартів для удосконалення кримінально-правової охорони інформаційної безпеки в Україні, зокрема щодо комп'ютерних кримінальних правопорушень і обов'язковості контролю з боку людини за всіма процесами стосовно штучного інтелекту й результатами цих процесів.

Ключові слова: кримінальне право, кримінальна відповідальність інформаційна безпека, європейські стандарти, права людини, комп'ютерні кримінальні правопорушення, штучний інтелект.

The article is devoted to the establishment and study of the European Union standards on information security protected by criminal law as a branch of law. It is noted that in the current context of technological innovations, the issues of information security are of particular state, social and legal importance, and the concept of «information security» is reaching the level of interdisciplinary and comprehensive research.

The author emphasises that information security is the object of criminal law protection with a certain structure of relevant social relations, the elements of which are the subject matter of social relations, their content, and the subjects of such relations. Depending on the subjects of social relations, we are talking about the information security of a person (individual), legal entity, society, the State, and the world community. On the one hand, these relations can be assessed as information relations, in particular, information-value, information-economic, information-psychological, information-technological, information-political. On the other hand, information security is a component of personal security of a person; security of a legal entity; security of societies: national security of Ukraine, in particular, the foundations of national security of Ukraine; international security.

Attention is drawn to the importance of standardisation for ensuring information security, and the approaches of the International Organisation for Standardisation, decisions and recommendations of the Council of Europe and the European Parliament on this issue are studied and analysed. The researcher supports the position of scholars who believe that Ukraine, having chosen the European integration course, should be guided by the development strategy of the EU member states in the information sphere and conducts a comparative legal analysis of European approaches and standards and the norms of Ukrainian legislation on criminal liability for cybercrime and artificial intelligence.

The author offers his own vision of the ways and specific measures for implementing a number of recognised European standards to improve criminal law protection of information security in Ukraine, in particular, with regard to computer criminal offences and the mandatory human control over all processes related to artificial intelligence and the results of these processes.

Key words: criminal law, criminal liability, information security, European standards, human rights, computer criminal offences, artificial intelligence.

В умовах інформатизації суспільних процесів, глобалізації й інтеграції усіх видів людських, інституційних і міждержавних відносин інформаційна безпека (далі – ІБ) людини, юридичних осіб, суспільства, держави й світу набувала статусу найважливішої соціальної цінності. Особливо це проявляється у воєнний час та інших кризових ситуаціях. У воєнний і в мирний часи створюється, перетворюється, поширюється, використовуються, привласнюється, викрадається тощо інформація, яка є сучасним капіталом і/або така, що здатна руйнувати чи створювати загрозу руйнації правопорядку цивілізованої країни або міжнародного правопорядку; негативно впливати на психіку людини, особливо дітей; вводити в оману, шантажувати, знищувати моральні й культурні цінності конкретної особистості чи певних спільнот; здійснювати інший суспільно небезпечний вплив на соціальні цінності. Останні у зв'язку з їх важливим соціальним значенням знаходяться під охороною норм законодавства України про кримінальну відповідальність, або такі діяння потребують визнання кримінально-караними на законодавчому рівні. Орієнтиром для прийняття виважених рішень законодавця з питань кримінально-правової охорони інформаційної безпеки є європейські стандарти в цьому напрямку. З'ясування і впровадження цих важливих правил є актуальним питанням для правової системи України, яка визнана європейською спільнотою кандидаткою для вступу до Європейського Союзу (далі – ЄС).

При цьому питання ІБ є предметом наукового інтересу багатьох дослідників, зокрема і щодо європейських стандартів забезпечення такої безпеки. Проте кримінально-правовому аспекту введення європейських стандартів ІБ в національне кримінальне законодавство приділяється

науковцями недостатньо уваги. Хоча така проблематика потребує постійної уваги криміналістів-правників, враховуючи швидкий розвиток інформаційних технологій, ведення інформаційних війн, розробку і впровадження штучного інтелекту, модернізацію кримінально-караної поведінки в інформаційному просторі й появу нових, раніше невідомих суспільно небезпечних діянь в інформаційному просторі.

Метою статті є встановлення й дослідження низки стандартів ЄС і розвинутих європейських країн стосовно забезпечення інформаційної безпеки, що є необхідним для подальшого удосконалення кримінально-правової охорони такого виду безпеки.

Виклад основного матеріалу. Поняття «інформаційна безпека» є міждисциплінарним і багаторівневим. В умовах прориву інноваційних технологій воно стає предметом міждисциплінарних і комплексних досліджень.

Як справедливо зазначається в юридичній літературі, це поняття має багато визначень, наприклад, одне з них може бути таким: ІБ – це стан інформації, за якого забезпечується збереження визначених політикою безпеки властивостей інформації. Більш стандартизоване визначення: ІБ – це збереження конфіденційності, цілісності та доступності інформації. Крім того, можуть враховуватися інші властивості ІБ, наприклад, автентичність, відстежуваність, неспростовність і надійність [1, с. 53]. У наведених визначеннях критерієм встановлення змісту ІБ обрано безпеку інформації.

У кримінально-правовому значенні поняття ІБ презентується з більш широким значенням, тобто з виходом за межі її сприйняття як безпеки інформації. Інформаційна безпека є об'єктом кримінально-правової охорони з певною структурою відповідних суспільних відносин, елементами якої є предмет суспільних відносин, їх зміст, суб'єкти таких відносин. Залежно від суб'єктів суспільних відносин йдеться про ІБ людини (фізичної особи), ІБ юридичної особи, ІБ суспільства, ІБ держави, ІБ світової спільноти. З одного боку, ці відносини можна оцінити як інформаційні, зокрема інформаційно-ціннісні, інформаційно-економічні, інформаційно-психологічні, інформаційно-технологічні, інформаційно-політичні. З іншого, – ІБ є складником особистої безпеки людини; безпеки юридичної особи; безпеки суспільств: національної безпеки України, зокрема основ національної безпеки України; міжнародної безпеки. І кримінально-правова охорона найважливіших суспільних відносин ІБ здійснюється нормами переважної більшості розділів Особливої частини Кримінального кодексу (далі – КК) України.

Важливо, що на міжнародному рівні досягнуто консенсус стосовно певних термінів міждержавного вживання. Так, Організацією Об'єднаних Націй поняття «міжнародна інформаційна безпека» презентується як взаємодія акторів міжнародних відносин з операцій підтримання сталого миру на основі захисту міжнародної інфосфери, глобальної інфраструктури та суспільної свідомості світової спільноти від реальних і потенційних інформаційних загроз. Причому «інфосфера» сприймається як міжнародний інформаційний простір, що складається з інформаційних потоків, інформаційних ресурсів та всіх сфер життєдіяльності цивілізації [2].

Беручи до уваги вказану дефініцію, науковці визначають, що забезпечення міжнародної ІБ охоплює три аспекти: а) інформаційно-технічний («захист глобальної інфраструктури»); б) інформаційно-психологічний («захист суспільної свідомості світової спільноти»); в) інформаційну безпеку у сфері прав та свобод («захист міжнародної інфосфери») [3, с. 38]. Такий підхід до розуміння міжнародної ІБ обумовлений специфікою міжнародних відносин і важливістю прав і свобод як визнаних світовою спільнотою визначальних соціально-забезпечувальних цінностей. Крім того, здійснено акцент на світовому значенні глобальної інфраструктури з інформаційно-технологічної позиції, а також на інформаційно-психологічному аспекті в площині суспільної свідомості світової спільноти. Таким чином підкреслюються особисті й загальні цінності, що є важливими елементами для захисту міжнародної ІБ.

Інформаційні відносини швидко розвиваються, що є однією з визначальних тенденцій розвитку суспільних процесів у 21 столітті. Цей процес супроводжується наполегливою працею в сфері стандартизації, що покликана забезпечити ІБ в різних сферах життєдіяльності людини.

За визначенням ISO (Міжнародної організації стандартизації) стандарти – «це вичерпна мудрість людей, які мають досвід у своїй галузі та знають потреби організацій, які вони представляють, таких як виробники, продавці, покупці, клієнти, торгові асоціації, користувачі чи регулятори» [4].

При цьому погоджуємось з дослідниками, які підкреслюють, що Україна, обравши євроінтеграційних курс, має орієнтуватися на стратегію розвитку країн-учасниць ЄС в інформаційній сфері [5, с. 18; 6, с. 104].

До керівних стратегічних документів ЄС з питань ІБ, в яких закладені основи стандартів безпеки в інформаційному просторі, відносяться: «Європейські критерії безпеки інформаційних технологій» (1991); «Єдині критерії безпеки інформаційних технологій» (1996), в яких закладена модель тріади CIA з трьома визначальними рисами ІБ: конфіденційність, цілісність і доступність; документ Європейської комісії «Мережена і інформаційна безпека: європейський політичний підхід (2001), яким серед основних напрямків інформаційної безпеки визначено правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та боротьба з кіберзлочинністю [6, с. 105].

Цінні напрацювання з питань ІБ здійснені Радою Європи (далі – РЄ) та органами цієї поважної європейської інституції. До них відносимо Конвенцію про комп'ютерні злочини, що прийнята РЄ 23 листопада 2001 р. [7]. У Преамбулі цього документу акцентується увага на впевненості РЄ в необхідності проведення в пріоритетному порядку загальної політики в сфері кримінального права, спрямованої на захист суспільства від комп'ютерних злочинів, зокрема шляхом прийняття відповідних законодавчих актів та укріплення міжнародної співпраці. А також, серед іншого, наголошується про необхідність забезпечення балансу між інтересами підтримання правопорядку та поваги основоположних прав людини, як це передбачено Конвенцією РЄ про захист прав людини та основоположних свобод від 1950 р., міжнародним пактом Організації Об'єднаних Націй про громадянські та політичні права від 1966 р. та також іншими міжнародними договорами про права людини, що застосовуються, в яких підтверджується право кожного безперешкодно підтримуватися своїх думок, а також право на вільне вираження своїх думок, включаючи свободу пошуку, отримання та розповсюдження будь-якого роду інформацію й ідеї, незалежно від державних кордонів та права, що стосується невтручання в особисте життя.

Здійснений порівняльно-правовий аналіз положень згаданої Конвенції РЄ від 23 листопада 2001 р. і чинного Кримінального кодексу (далі – КК) України є підґрунтям для твердження про врахування Україною багатьох рекомендацій РЄ стосовно криміналізації комп'ютерних діянь, визначених у статтях 2-10 Конвенції. Вагомим внеском України в боротьбу з комп'ютерними кримінальними правопорушеннями є прийняття Закону України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» від 24 березня 2022 р., яким викладені в новій редакції статтях 361 і 361-1 КК, що нами підтримується з констатуванням впровадження низки про-

позицій автора цієї статті [8, с. 457–461] та результатів досліджень інших дослідників. Разом з тим, ще, на наш погляд, залишаються певні резерви для синхронізації національного і європейського правового забезпечення боротьби з кіберзлочинністю. Приміром щодо перспективного кроку є введення кримінальної відповідальності за несанкціоноване заволодіння в будь-який спосіб паролем, кодом доступу або іншою подібною інформацією, призначеною для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Про таке діяння (з відмінною термінологією опису) йдеться в ст. 6 Конвенції РЄ.

Особливої уваги потребують європейські підходи й стандарти щодо штучного інтелекту (далі – ШІ), який, з одного боку, є прогресивним проявом розробки й втілення інноваційних технологій, а, з другого, – його безконтрольованість людиною може привести до катастрофічних для цивілізації наслідків.

У 2017 році Європейська Рада закликала до «відчуття терміновості вирішення нових тенденцій», включаючи «такі питання, як штучний інтелект, водночас забезпечуючи високий рівень захисту даних, цифрових прав і етичних стандартів». У своїх Висновках 2019 року щодо скоординованого плану з розробки та використання ШІ Рада також підкреслила важливість забезпечення повної поваги прав європейських громадян і закликала до перегляду існуючого відповідного законодавства, щоб воно відповідало новим можливостям і викликам, пов'язаним із ШІ. Європейська Рада також закликала чітко визначити додатки ШІ, які слід вважати високоризиковими.

Останні Висновки від 21 жовтня 2020 року також закликали до вирішення проблеми непрозорості, складності, упередженості, певного ступеня непередбачуваності та частково автономної поведінки певних систем штучного інтелекту, щоб забезпечити їх сумісність з основними правами та полегшити виконання правових норм (Пояснювальна записка до Пропозиції до Регламенту Європейського парламенту та Ради встановлення гармонізованих правил щодо штучного інтелекту (Акт про штучний інтелект) та внесення змін до деяких законодавчих актів Союзу) [9].

Список заборонених практик стосовно ШІ (Розділ II зазначеної Пропозиції до Регламенту) включає всі ті системи ШІ:

– використання яких вважається неприйнятним через порушення цінностей Союзу, наприклад, через порушення основних прав;

– які мають значний потенціал для маніпулювання людьми за допомогою підсвідомих методів за межами їхньої свідомості або використання вразливостей конкретних уразливих груп, таких як діти чи люди з обмеженими можливостями, з метою суттєвого спотворення їх поведінки таким чином, що може завдати їм або іншій особі психологічної чи фізичної шкоди;

– інші маніпулятивні чи експлуатаційні практики, що впливають на дорослих, яким можуть сприяти системи штучного інтелекту, можуть бути охоплені чинним законодавством про захист даних, захист споживачів і цифрові послуги, яке гарантує, що фізичні особи належним чином поінформовані та мають вільний вибір не піддаватися профілюванню чи іншим практикам, які можуть вплинути на їхню поведінку;

– соціальні оцінки на основі ШІ для загальних цілей, які проводять державні органи.

Також визнається забороненим використання систем дистанційної біометричної ідентифікації «в реальному часі» в загальнодоступних місцях з метою правоохоронних органів, якщо не застосовуються певні обмежені винятки. законодавство про захист прав споживачів і цифрові послуги, які гарантують належне інформування фізичних осіб і вільний вибір не піддаватися профілюванню чи іншим практикам, які можуть вплинути на їхню поведінку.

У наведеному та інших документі ЄС є багато цінних для нашої країни рекомендацій, які доцільно вивчити і впровадити, зокрема в площині кримінально-правової охорони інформаційної безпеки (досягнення гнучкої до новітніх технологій термінології з достатнім рівнем юридичної визначеності; стандартизація й контрольованість усіх процесів людиною; юридичної визначеності заборонених практик стосовно ШІ). До цього доповнимо доцільність введення кримінальної відповідальності за створення, розробку, виробництво, використання, збут штучного інтелекту, забороненого для розробок і використання або якщо таке діяння призвело до неконтрольованого розробником немалозначного суспільно небезпечного наслідку діяльності штучного інтелекту. Доцільне всесвітнє визнання і впровадження принципу «Всебічна контрольованість людиною штучного інтелекту на усіх стадіях його розробки й використання» [10, с. 19].

У межах обсягу цієї статті відсутня можливість розглянути й інші документи ЄС щодо інформаційної безпеки.

Висновки. Проведене ознайомлення і аналіз документів ЄС з питань ІБ дозволяють висловити такі судження:

1. Удосконалення кримінально-правової охорони ІБ в Україні, яка визнана кандидаткою для вступу до ЕС, слід здійснювати з дотриманням і забезпеченням основоположних прав і свобод людини та інших соціальних цінностей, визнаних Конституцією України й нормативно-правовими актами ЄС.

2. У вирішенні питань правового забезпечення боротьби з кіберзлочинністю Україна досягла значних позитивних результатів і забезпечила, в основному, рекомендації Конвенції РЄ щодо комп'ютерних злочинів і створює правову основу щодо ШІ.

3. Одним із напрямків підвищення ефективності охорони інформаційної безпеки за допомогою засобів кримінального права може бути реалізація тих пропозицій, що висвітлюються в цій публікації.

4. Ураховуючи наукове й соціальне значення європейських стандартів для кримінального права як галузі права, а також швидкий розвиток інформаційних технологій і засобів, дослідження цього питання буде продовжено в інших публікаціях.

ЛІТЕРАТУРА

1. Гладун А.Я., Хала К. О. Таксономія стандартів інформаційної безпеки. *Інформаційні технології*. № 2. 2917. С. 53–64.

2. Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки : Резолюція ООН від 1 грудня 1999 року. URL: https //www.un.org (дата звернення: 10.07.2023).

3. Куренда Л. Д. Окремі аспекти забезпечення інформаційної безпеки Європейського Союзу. *Правова інформатика*. № 3–4 (31). 2011. С. 36–42.

4. ISO. URL: https://www.iso.org/standards.html (дата звернення: 17.07.2023).

5. Політанський В. С. Інформаційне суспільство в Україні: від зародження до сьогодення. *Науковий вісник Ужгородського національного університету*: серія «Право». Вип. 42. 2017. С. 16–22.

6. Ткачук Т. Ю. Забезпечення інформаційної безпеки в країнах Центральної Європи. *Електронний юридичний журнал*. № 5. 2017. С. 104–110.

7. CETS 185 – Convention on Cybercrime. URL: https://rm.coe.int/1680081580

8. Демидова Л. М. Проблеми кримінально-правової відповідальності за заподіяння майнової шкоди в Україні (майнова шкода як злочинний наслідок): теорія, закон, практика: монографія. Харків: Право, 2013. 752 с.

9. EUR – Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (дата звернення: 17.07.2023).
10. Демидова Л. М. Концептуальні засади кримінально-правової охорони національної безпеки в Україні в умовах інформатизації суспільних процесів і кризових ситуацій. *Національна безпека України в умовах інформатизації та глобалізації суспільних процесів: сучасні загрози та кримінально-правове регулювання* : матеріали VII Міжнар. наук.-практ. конф., м. Харків, 11 трав. 2023 р. / [редкол.: Л. М. Демидова (голов. ред.), Н. В. Шульженко та ін.]. Харків : Право, 2023. С. 16–21.