№ 1556-р: станом на 29 груд. 2021 р. URL: https://zakon.rada.gov.ua /laws/show/1556– 2020-р#Text
4. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025-2026 роки: Розпорядж. Кабінету Міністрів України від 9 травня 2025 р. № 457-р: https://zakon.rada.gov.ua/laws/show/457-2025-%D1%80#Text
5. Кримінальний кодекс України: Закон України від 5 квіт. 2001 р. № 2341-III URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
6. CNPLaw. Generative AI and deepfakes. URL: https://www.cnplaw.com/generative-ai-and-deepfakes/?print-posts=pdf
7. DeNovo. Що принесе європейському ринку EU AI Act. URL: https://denovo.ua/blog/eu-ai-act-into-force
8. IMDA. 3 things Singapore is doing to take action against deepfakes. URL: https://www.imda.gov.sg/resources/blog/blog-articles/2024/07/3-things-sg-do-to-take-action-against-deepfakes
9. The Digital. Україна приєдналася до Європейської ради зі штучного інтелекту. URL: https://thedigital.gov.ua/news/progress/ ukrayina-pryyednalasia-do-yevropeyskoyi-rady-zi-shtuchnoho-intelektu
10. Шахраї за допомогою штучного інтелекту оформили кредити на українців – Нацполіція. URL: https://unn.ua/news/shakhrai-za-dopomohoiu-shtuchnoho-intelektu-oformliuvaly-kredyty-na-ukraintsiv-natspolitsiia

Манжус Богдан Олегович,
курсант Національної академії
внутрішніх справ
Науковий керівник:
Федорюк Людмила Василівна,
доцент кафедри оперативно-розшукової
діяльності та національної безпеки
Національної академії внутрішніх справ,
доктор філософії

ВПЛИВ МІЖНАРОДНОГО ДОСВІДУ НА ВДОСКОНАЛЕННЯ КРИМІНАЛЬНОГО ЗАКОНОДАВСТВА УКРАЇНИ ЩОДО ЗАХИСТУ ДАНИХ

Актуальність дослідження впливу міжнародного досвіду на вдосконалення кримінального законодавства України щодо захисту даних зумовлена стрімким розвитком цифрових технологій, зростанням кількості кіберзлочинів і необхідністю забезпечення ефективного правового механізму захисту персональної інформації. Вивчення міжнародного досвіду дозволяє удосконалити кримінально-правові норми, підвищити ефективність розслідування кримінальних правопорушень у сфері інформаційної безпеки й забезпечити баланс між правом на приватність і потребами національної безпеки, що є

надзвичайно важливим для формування сучасної цифрової правової держави.

Слід звернути увагу, що вже на наступний день після набрання чинності GDPR надійшли перші скарги щодо його порушення, які стосувалися порушень Facebook, Instagram, WhatsApp, Google, Android вільного надання згоди на обробку даних користувачами. Восени 2018 року португальський наглядовий орган (CNPD) оштрафував місцеву клініку на загальну суму 400 тис. євро за доступ працівників клініки до персональних даних пацієнтів через фальшиві облікові записи. У березні 2019 року в Польщі накладено штраф на загальну суму 220 тис. євро. на компанію, яка займалася збором даних із відкритих реєстрів та фактично здійснювала обробку даних понад 7 млн фізичних осіб без належного повідомлення всіх осіб про обробку їхніх персональних даних. У 2020 році через помилку співробітника лікарні, який випадково завантажив на Git Hub електронну таблицю з іменами користувачів, паролями і ключами доступу до конфіденційних державних систем, у відкритий доступ потрапили особисті та медичні дані 16 млн бразильців, які лікувалися від коронавірусу. У результаті інформацію було видалено з Git Hub, а урядовці змінили паролі й відкликали ключі доступу, щоб убезпечити свої системи. Не стала винятком і Україна. Так, у кінці 2020 року Національний координаційний центр кібербезпеки (НКЦК) при Раді безпеки і оборони України в ході моніторингу виявив витік персональних медичних даних з однієї з найбільших клінік Дніпра. «Серед інформації, яка опинилася у відкритому доступі, – персональні дані працівників і клієнтів цієї клініки, зокрема ПІБ, дати народження, адреси проживання, телефони, e-mail, діагнози, дані медичної карти (що становить медичну інформацію), включаючи результати аналізів, діагнози, інформацію про захворювання, результати проведення ПЛР-тестів, списки хворих на COVID-19». Витік стався в результаті помилок конфігурації в інформаційних системах і базах даних клініки, які мали доступ в мережу Інтернет. Варто звернути увагу на те, що вільний доступ до баз даних надавав можливість не лише викрадення персональної інформації, але й несанкціонованого внесення змін, включаючи модифікацію призначень ліків, результатів аналізів і обстежень, редагування записів у протоколах. Відповідно до п. 11 Плану заходів щодо імплементації Угоди про асоціацію між Україною та ЄС, затвердженого 25.10.2017 р., Україна має вдосконалити законодавство про захист персональних даних з метою приведення його у відповідність до GDPR. Однією з основних причин невідповідності інформаційного законодавства України вимогам сучасності є несформованість у суспільній і науково-правовій думці цілісного уявлення про інформаційну безпеку з позиції права та юридичної науки. Відповідно до інформації з Єдиного порталу судових рішень у 2020 р. налічувалося лише 15 реальних вироків за такими справами [1, с. 77].

Міжнародний союз електрозв'язку (МСЕ) як спеціалізована установа в системі Організації Об'єднаних Націй відіграє провідну роль в області стандартизації і розвитку електрозв'язку, а також в питаннях кібербезпеки. Серед іншої діяльності МСЕ є провідною організацією Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства (ВСІС). В Україні враховується міжнародний досвід щодо розбудови мережі ситуаційних центрів кіберзахисту на об'єктах критичної інформаційної інфраструктури та системи ситуаційних центрів кібербезпеки. Також необхідними змінами законодавства задля протидії протиправним посяганням на електронні інформаційні ресурси має бути закріплення механізму оперативного обмеження (блокування) певного інформаційного ресурсу (інформаційного сервісу) та впровадження особливих умов проведення обшуку і арешту електронних доказів, насамперед закріплення процесуально значимої можливості копіювання інформації, а також імплементація в національне законодавство положень про невідкладне фіксування і подальше зберігання даних операторами, провайдерами телекомунікацій, власниками ресурсу (веб-сайту) із забезпеченням їх цілісності. Прийняття низки правових актів спрямовані на підтримку інформаційної безпеки та боротьби і попередження кіберзлочинності [2, с. 390].

Стандартами безпеки НАТО та ЄС для побудови системи охорони інформації з обмеженим доступом запроваджено чотирьохрівневу систему обмеження доступу до вказаної інформації, ступені якої розподіляються за рівнем шкоди, що може бути заподіяна інтересам міжнародних організацій та країн-членів у разі розголошення таких відомостей: TOP SECRET – еквівалент «Особливої важливості»; SECRET – еквівалент «Цілком таємно»; CONFIDENTIAL – еквівалент «Таємно»; RESTRICTED – еквівалент «Для службового користування». Реформуючи систему охорони державної таємниці ми маємо визначитися з її новою моделлю. Відомо, що єдиного зразка системи охорони державної таємниці в зарубіжних країнах немає. Світова практика напрацювала певний комплекс заходів (організаційно-правових, технічних, криптографічних, оперативнорозшукових), спрямованих на охорону державної таємниці [3, с. 151].

Кіберзлочинам у кримінальних кодексах досліджуваних країн приділені окремі розділи, зокрема в: Польщі – Розділ XXXIII Кримінальні правопорушення проти охорони інформації; Чехії – Розділ V Кримінальні правопорушення проти власності; Болгарії – Главою 9 - Комп'ютерні кримінальні правопорушення; Литви – Розділ XXX Кримінальні правопорушення проти безпеки електронних даних та інформаційних систем. Варто зазначити, що в Польщі досліджувані діяння визначають як кримінальні правопорушення проти охорони інформації, а в Чехії кримінальні правопорушення проти власності. Своєю чергою у Кримінальних кодексах Литви та Болгарії ці кримінальні правопорушення є відокремленими. В досліджуваних

країнах, незважаючи на їх членство в Європейському Союзі, немає єдиного підходу до покарання за кіберзлочини, що можливо пояснити національними правовими традиціями та увагою політиків до інформаційної безпеки держави. При реформуванні кримінального права в Україні в умовах євроінтеграційних процесів є потреба у врахуванні досвіду зазначених країн лише часткового. Адже вже майже десятиліття точиться дискусія щодо необхідності прийняття нового кримінального кодексу, який має врахувати сучасні методи скоєння кримінальних правопорушень, їх класифікацію та групування [4, с. 143]. Викладене вище свідчить, що національне законодавство потребує суттєвих і негайних змін. Слід зазначити, що в листопаді 2019 року при Секретаріаті Уповноваженого Верховної Ради України з прав людини створено міжвідомчу робочу групу щодо розроблення законодавчих пропозицій у сфері захисту персональних даних, крім того, створено координаційну робочу групу з розроблення законопроєкту щодо внесення змін до Закону України «Про захист персональних даних» відповідно до положень GDPR [1, с. 77]. Отже, вплив міжнародного досвіду на розвиток кримінального законодавства України щодо захисту даних проявляється у формуванні сучасного підходу до визначення складів кримінальних правопорушень у сфері обробки, зберігання та поширення інформації. Використання міжнародних стандартів забезпечує більш чітке визначення меж кримінально караних діянь, підвищує ефективність досудового розслідування та судового розгляду, а також формує належну доказову базу у справах про порушення інформаційної безпеки.

Список використаних джерел

1. Легка О.В. Актуальні питання захисту персональних даних: вітчизняний та міжнародний досвід. Правова позиція. 2021. С. 74–79. URL: https://legalposition.umsf.in.ua/archive/2021/2/15.pdf

2. Саєнко М.І. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. 2021. С. 386–391. URL: http://visnyk-pravo.uzhnu.edu.ua/article/download/238897/237481.

3. Олійник В.І. Досвід кримінально-правового забезпечення охорони державної таємниці країн близького зарубіжжя. Юридична наука. 2020. С. 144–152. URL: https://journal-nam.com.ua/index.php/journal/article/view/609.

4. Грицишен Д.О. Удосконалення державної політики протидії кіберзлочинності на основі досвіду країн Європейського Союзу. Економіка, управління та адміністрування. 2024. С. 125–144. URL: https://ema.ztu.edu.ua/article/view/327188.