УДК 343.9 (411)
DOI https://doi.org/10.24144/2788-6018.2023.05.91

ІНФОРМАЦІЙНА БЕЗПЕКА У СИСТЕМІ ЗАХОДІВ ЗАПОБІГАННЯ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ: ДОСВІД КРАЇН ЄС ТА США

Юзікова Н.С.,
професор, доктор юридичних наук,
професор кафедри адміністративного і кримінального права
Дніпровського національного університету імені Олеся Гончара
ORCID ID: https://orcid.org/0000-0003-0879-2228
e-mail: Yzikovans@ua.fm

Юзікова Н.С. Інформаційна безпека у системі заходів запобігання кримінальним правопорушенням у сфері інформаційних технологій: досвід країн ЄС та США.

Статтю присвячено проблемам запобігання кримінальним правопорушенням у сфері інформаційних технологій. Для досягнення цієї мети, використовувалися загальнонаукові та спеціальні наукові методи дослідження, зокрема, формально-логічний, системний, порівняльно-правовий та ін. методи. Проведено стислий огляд наукових досліджень у сфері інформаційної безпеки. При цьому зауважено, що дослідження заходів запобігання кримінальним правопорушенням у сфері інформаційних технологій, в умовах воєнного стану та повоєнної розбудови, набуває більшої актуальності, потребує об'єктивного кримінологічного аналізу реальних та потенційних ризиків у цифровому середовищі. Здійснено аналіз сучасних загроз у сфері інформаційних технологій, серед яких особливе місце посідає негативний інформаційно-психологічний вплив на суспільну свідомість громадян України, що відбувається через систематичне поширення дезінформації, неповної або упередженої інформації про політичні, економічні, соціальні процеси, що відбуваються в Україні. Зазначено, що незадовільний стан інформаційної безпеки, детермінує викривлене уявлення про процеси, які відбуваються в Україні; деструктивні зміни у поведінці та комунікації особистості; сприяє формуванню деформованих моральних установок. Представлено аналіз сучасних зарубіжних програм, що спрямовані на запобігання злочинності у сфері інформаційних технологій, які ефективно діють у країнах ЄС та США. Характеристика програм здійснюється за алгоритмом: окреслення мети програми; головних напрямів її діяльності; розміру фінансування; залучення урядових та неурядових організації; кола фахівців тощо. Значна частина створених проектів функціонує як незалежні міжнародні установи, фактично за відсутності підтримки у вигляді державного фінансування. Кошти на реалізацію проектів надходять у вигляді недержавного фінансування, грантових внесків або пожертв членських і асоційованих організацій. Цільовою аудиторією впливу проектів є громадянське суспільство, а не населення в цілому, що пояснюється більш активною роллю громадянського суспільства в західних країнах та пасивністю більшої частини громадськості. Зроблено висновок про доцільність міжнародної співпраці та координації зусиль національної та міжнародної спільноти із запобігання кримінальним правопорушенням у сфері інформаційних технологій. Доведено важливість підняття рівня обізнаності та грамотності населення стосовно дезінформації та її методів, шляхом проведення інформаційної та роз'яснювальної роботи. Наголошено на важливості формування національних підходів збалансованого та відповідального використання цифрового середовища, головною ідеєю яких, є поєднання запобіжних заходів кримінально-правового, нормативного, технічного та організаційно-управлінського характеру.

Ключові слова: цифрове середовище, інформаційна грамотність, дезінформація, кіберзлочинність, гібридні загрози, національний підхід.

Yuzikova N.S. Information security in the system of measures to prevent criminal offences in the field of information technology: experience of EU and United States countries.

The article is devoted to the problems of prevention of crimes in the field of information technology. To achieve this goal, the author used general scientific and special scientific research methods: formal-logical, systemic, comparative legal, etc. A review of scientific research in the field of information security is carried out. It is noted that the study of measures to prevent criminal offences in the field of information technology is becoming increasingly relevant and requires an

objective criminological analysis in the context of martial law and post-war reconstruction. The author analyses modern threats in the field of information technology. Among the threats, the author singles out the negative information and psychological impact on the public consciousness of Ukrainian citizens. This impact is due to the systematic dissemination of disinformation, incomplete or biased information about political, economic and social processes taking place in Ukraine. The unsatisfactory state of information security causes a distorted view of the processes taking place in Ukraine; destructive changes in the behaviour and communication of individuals; and contributes to the formation of deformed moral attitudes. The author presents an analysis of modern foreign programmes aimed at preventing crimes in the field of information technology. These programmes are effective in the EU and the USA. The programmes are characterised according to the following algorithm: the purpose of the programme; the main areas of activity; the amount of funding; involvement of governmental and non-governmental organisations; the range of specialists, etc. A significant number of the established projects operate as independent international institutions, with virtually no support from government funding. Funds for project implementation come in the form of non-governmental funding, grant contributions or donations from member and associated organisations. The target audience of the projects is civil society rather than the general population, which is explained by the more active role of civil society in Western countries and the passivity of the majority of the public. The author concludes that international cooperation and coordination of efforts of the national and international community to prevent criminal offences in the field of information technology is expedient. The importance of raising public awareness and literacy about disinformation and its methods through information and explanatory work is proved. The importance of developing a national model for the balanced and responsible use of the digital environment is emphasised. The main idea of the model is a combination of criminal law, regulatory, technical, organisational and managerial measures.

Key words: digital environment, information literacy, disinformation, cybercrime, hybrid threats, national approach.

Постановка проблеми. У реаліях сьогодення, рівень захищеності інформаційного простору є показником рівня розвитку країни, фактором її сталого економічного, соціального, правового, політичного стану, спрямованого на забезпечення національних інтересів, захист і дотримання прав особи цифровому просторі. Інформаційна безпека України – це надійний щит, який має бути спрямований на безпечний розвиток потенціалу інформаційної сфери України, на підвищення ефективності захисту прав людини у цифровому просторі. Головною метою системи інформаційної безпеки – забезпечення механізму захисту від негативного впливу на фізичне, емоційне та психологічне благополуччя особи у цифровому середовищі. Ефективна практична реалізація такої мети має ґрунтуватись на залученні всіх суб'єктів інформаційних відносин. Комплексна та системна взаємодія держави з приватним сектором та громадою в інтересах ефективного розвитку інформаційної сфери є запорукою спільного захисту особи, держави, суспільства від загроз пов'язаних з інформаційними технологіями.

Для запобігання злочинності у сфері інформаційних технологій необхідно сформувати адресний цифровий кейс нормативно-правових, організаційно-управлінських та техніко-технологічних заходів спрямованих на захист різних сфер суспільної діяльності з урахуванням викликів, спричинених військовою агресією та іншими надзвичайними та кризовими станами.

Забезпечення інформаційної безпеки повинно мати відповідне правове підґрунтя, чіткий стратегічний вектор. При цьому, зростає значення форм, методів та засобів пізнання різних елементів інформаційної безпеки, особливо у кризових та надзвичайних ситуаціях. Вимагає адресного і відповідного удосконалення методологія пізнання питань інформаційної безпеки та протидії дезінформації, з огляду на характер, сферу, форми прояву та наслідки.

Відповідно до ст. 17 Конституції України «Забезпечення інформаційної безпеки України є однією з найважливіших функцій держави справою всього Українського народу» [1]. У Стратегії інформаційної безпеки на період до 2025 року визначено актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних та затверджено план заходів з її реалізації на період до 2025 року [2]. Тому пріоритетом сьогодення є захист національного інформаційного простору та забезпечення національної безпеки в інформаційній сфері, особливо в умовах воєнного стану та післявоєнної розбудови України.

Стан опрацювання проблематики. Важливий науковий внесок у дослідження питань інформаційної безпеки та запобігання кримінальним правопорушенням у сфері інформаційних технологій зробили такі вчені, як О. Бандурка, В. Батиргарєєва, Ю. Баулін, М. Гаврильців, В. Голіна, В. Горбулін, Д. Кондратов, О. Костенко, О. Литвинов, В. Новицький, М. Орел, У. Ільницька, Р. Черниш та багато інших. Зокрема, В.Я. Новицький виокремив актуальні загрози у сфері

інформаційної безпеки України. До них автор відніс: повноформатну експансивну інформаційну політику РФ; низький рівень медійної грамотності громадян; збільшення кількості глобальних дезінформаційних кампаній; інформаційне домінування РФ на тимчасово окупованих територіях; використання технологій маніпулювання свідомістю пересічних громадян щодо наслідків вступу України в НАТО та ЄС тощо [3, с. 112]. У. Ільницька надала авторське бачення щодо подолання загроз і викликів які становлять небезпеку функціонування держави, її політичного та економічного розвитку, інтеграції у європейські та євроатлантичні структури [4, с. 28-29]. М.Т. Гаврильців здійснила аналіз факторів, що зумовлюють загострення загроз інформаційній безпеці, які мають системний характер, а тому охоплюють усі сфери життєдіяльності людини, суспільства і держави [5, с. 200]. Заслуговує на увагу у контексті розгляду проблеми інформаційної безпеки, робота Р. Черниша де проаналізовано досвід країн ЄС у протидії поширенню дезінформації, що розповсюджується для підриву обороноздатності України шляхом поширення тенденційної інформації в ЗМІ та формування у громадян антидержавницьких поглядів [6, с. 125].

Однак, незважаючи на те, що тема дослідження є достатньо вивченою, постійна трансформація цифрової сфери, вдосконалення ІТ, потребує розробки нових, сучасних заходів запобігання злочинності у інформаційній сфері на основі ґрунтовного кримінологічного аналізу відповідних загроз та наслідків. Крім того, дослідження заходів запобігання кримінальним правопорушенням у сфері інформаційних технологій в умовах воєнного стану та повоєнної розбудови набуває більшої актуальності, потребує об'єктивного кримінологічного аналізу реальних та потенційних ризиків у цифровому середовищі, у тому числі, породжених кризовими та надзвичайними станами.

Метою статті є розгляд проблеми запобігання кримінальним правопорушенням у сфері інформаційних технологій шляхом всебічного аналізу зарубіжних програм та практик у відповідній сфері.

Виклад основного матеріалу. Цифрове середовище є важливим інструментом у житті людини для освіти, роботи, дозвілля, соціалізації, комунікації, водночас його безпрецедентне та масштабне використання породжує фактори здатні негативно вплинути на фізичне, емоційне та психологічне благополуччя особи. З моменту зародження Інтернету у жовтні 1969 року [7, 8], світ кардинально змінився. Нові цифрові технології, глобальне використання Інтернету під час пандемії та в умовах воєнного стану збільшили масштаби використання ІТ ресурсів. Незадовільний стан інформаційної безпеки, розміщення спотвореної, упередженої, провокаційної, забороненої інформації або дезінформації про політичні, економічні, соціальні процеси, що відбуваються в Україні, у цифровому середовищі, чинить негативний інформаційно-психологічний вплив на суспільну свідомість громадян України; детермінує зміни у поведінці та комунікації особистості; сприяє формуванню деформованих моральних установок, девіантної поведінки та асоціального способу життя; продукує віктимну, суїцидальну поведінку. Змінилась система поводження з інтернетом. Все більше людство поглинається інформаційним простором, від тимчасового відвідування окремих інтернет ресурсів до постійного перебування в режимі онлайн. Так, щохвилини на YouTub завантажується по 72 години відео, у Twitter публікується 100 000 нових твітів, у Facebook – 700 000 нових коментарів. Виникає запитання, який відсоток цього контенту є корисним для особи, суспільства, держави? Який відсоток корисної, деструктивної та дезінформації ?

Кількість користувачів Інтернету збільшилось з 414 794 957 (6,8%) у 2000 році до 3 424 971 237 (46,1%) у 2016 році [9]. Сьогодні у більшості цивілізованих країн кількість інтернет-користувачів становить понад 50% населення цих країн. Так у Великобританії кількість інтернет-користувачів, становить 92, 6%, Германії 88%, Данії 96,3%, Італії 65,6%, Ісландії 100%, Іспанії 82,2%, Латвії 76,3%, Литві 77,2%, Естонії 91,4%, Нідерландах 93,7%, Польщі 72,4%, Китаї 721434547 (52,2%), США 88,5%, Фінляндії 92,5%, Франції 86,4%, Чеській Республіці 88,4%, Україні 44,1%, Японії 91,1%, Швейцарії 87,2%, Швеції 93,1%[10].

Показник інтернет-активності пояснюється доступністю інтернету, інтенсифікацією використання інформаційних і телекомунікаційних технологій. Корисною складовою глобального інформаційного простору «без кордонів» є: інформація, зручність у спілкуванні, можливості для бізнесу, здійснення покупок, розваги тощо. Поряд з цим існує деструктивна, негативна сторона: це шкідливі програми, викрадення персональних даних, розвиток кіберзлочинності, шахрайство у мережі, дезінформація тощо.

Значну небезпеку в умовах боротьби з COVID у світі, а також в умовах воєнного стану, становить дезінформація, яка прямо загрожує безпеці, здоров'ю та життю особи. Тому, науково практичний інтерес представляє стислий аналіз окремих програмних заходів, що ефективно запроваджені у зарубіжну (країни ЄС та США) правозастосовну практику.

EUvsDisinfo – це основний («флагманський») проект Оперативної робочої групи зі стратегічних комунікацій (East Strat Com Task Force) Європейської Служби Зовнішніх комунікацій. Проект був створений у 2015 році для більш ефективного

реагування на поточні кампанії РФ з дезінформації, які стосуються Європейського Союзу, його держав-членів та сусідніх країн. Частково діяльність даної програми стосується країн Східного партнерства.

Використовуючи служби аналізу даних та моніторингу проектна група EUvsDisinfo у ЗМІ 15 мовами, виявляє та розкриває випадки дезінформації, створені російськими та афілійованими з ними ЗМІ, які поширюються у країнах ЄС та Східного партнерства. EUvsDisinfo — виступає єдиним у своєму роді сховищем з вільним доступом та підтримкою функцій пошуку даних, яка наразі містить понад 6500 прикладів прокремлівської дезінформації. База даних та коротке зведення інформаційних трендів оновлюються щотижня.

Першочергово проектом Оперативної робочої групи зі стратегічних комунікацій було заплановано діяльність проекту у 3-х напрямах:

1) цільова група мала трансформувати власне спілкування і мовлення в державах ЄС, при цьому приділяти особливу увагу країнам Східного партнерства;

2) цільова група також має надавати можливу допомогу в посиленні та зміцненні вільних та незалежних засобів масової інформації як національного і регіонального, так і місцевого рівнів;

3) цільова група також має піднімати рівень обізнаності та грамотності населення стосовно дезінформації та її методів, проводячи інформаційну та роз'яснювальну роботу. Отже, по суті EUvsDisinfo є кампанією по підвищенню інформаційної грамотності громадян. Команда EUvsDisinfo також бере активну участь у роботі з громадськістю та представниками урядів. Вони проводять інструктаж та навчання в установах ЄС, урядах держав-членів, серед журналістів та в організаціях громадянського суспільства, а також виступають на міжнародних конференціях. Дані матеріали є важливим ресурсом для політичних лідерів, державних установ, дослідників, аналітичних центрів та журналістів у всьому світі.

Ще однією програмою спрямованою на підвищення медійної грамотності на посилення стійкості громадян Європейського Союзу до дезінформації є проект Start 2 Think. Реалізація проекту відбувається Центром міжнародних відносин (Польща), а також за рахунок організацій-партнерів: Асоціація європейських проектів з Бельгії, Informo з Хорватії, Центру громадянської стійкості з Res Publica з Литви, а також за підтримки Європейського Союзу. Головною метою програми є запобігання та інформування користувачів Інтернету про можливу діяльність з дезінформації; головні інструменти ворожого впливу і методи; навчання громадян заходам захисту від небезпеки, яка виходить від ворожої дезінформації; укріплення критичного мислення кожного громадянина та громадянського суспільства в цілому.

Сьогодні діяльність програми здебільшого зосереджена на питаннях, які стосуються НАТО, міжнародної безпеки та кібербезпеки, складових частин європейської інтеграції, трансатлантичних відносин, інтеграції в рамках східного партнерства, однак є й відповідні молодіжні проекти, спрямовані на студентську аудиторію. Проект має власний глосарій термінів щодо інформації та дезінформації, а також аналізує засоби, методи та навіть поодинокі випадки потужних кампаній з дезінформації (наприклад, дезінформацію, яка проводилась у 2020 році у зв'язку з виходом Великобританії з Європейського Союзу).

Credibility Coalition (Коаліція довіри) є міжнародним недержавним проектом, заснованим журналістськими організаціями Hacks/Hackers та Meedan, що фактично є дослідницькою спільнотою журналістів, дослідників, вчених, студентів, політиків, технологів та добровольців. Коаліція довіри сприяє зміцненню співробітництва, спрямованого на всебічне дослідження та ідентифікацію дезінформації та пошуку рішень з різних точок зору. Підтримка Credibility Coalition загалом зводиться до методу інкубації, коли надається простір і платформа для зустрічей, суспільну інфраструктуру, мережі та певну фінансову підтримку для покриття ряду видатків. У подальшому, результат роботи передається технологам, дослідникам та політикам.

Важливим напрямом програми є намагання фактично обмежити монополію центральних та найбільших засобів масової інформації з метою надання можливості меншим засобам масової інформації впливати на цільову аудиторію. В рамках даного напряму діяльність платформи була спрямована на пошук намірів користувачів та виявлення їх найбільш поширених запитів при пошуку інформації. Враховується також та обставина, що подання однієї і тієї ж самої новини в національних, регіональних та місцевих засобах масової інформації може радикальним чином відрізнятися.

Європейський центр з протидії гібридним загрозам (Hybrid CoE) є міжнародною, автономною від державного впливу організацією, побудованою за принципами мережі, яка займається просуванням загальнодержавних та загально соціальних засобів протидії гібридним загрозам (включаючи інформаційну). Фактично виступає у ролі аналітичного центру або науково-дослідного інституту. Метою програми Hybrid CoE є посилення безпеки держав-учасників та організацій шляхом надання експертних висновків та навчання у боротьбі з гібридною загрозою. Програма прагне забезпечити стале функціонування відкритих і демократичних інститутів суспільства без деструктивного зовнішнього втручання. У

2017 році бюджет програми склав 1,5 млн. євро. На 2022 рік виконавцями програми Hybrid CoE є 36 осіб персоналу центру 12 різних національностей, з них 15 експертів.

Відповідно до звіту програми у 2022 році діяльність Hybrid CoE спрямовується на три основні напрямки:

1) зміцнення знань щодо особливих характеристик і складових гібридної загрози, аналіз їхньої діяльності та пошук пропозиції з протидії таким загрозам. Зокрема, здійснюється аналіз кожної складової такої гібридної загрози з метою відповідного реагування;

2) зміцнення знань щодо безпосереднього впливу гібридної загрози як частини стратегій або політик відповідних діячів та пошук варіантів по протидії такому впливу. В цій частині програми основна увага приділяється вже негативним наслідкам впливу гібридної загрози, проводиться оцінка наслідків такого впливу;

3) зміцнення знань щодо вразливостей Західного суспільства перед гібридними загрозами та пошук ідей по усуненню таких вразливостей. В цій частині основною є аналіз безпосередньо точок впливу гібридної загрози, протидія в яких є недостатньою.

Альянс із забезпечення демократії (ASD) є незалежною програмою, розташованою в Німецькому фонді Маршалла в Сполучених Штатах, яка розробляє комплексні стратегії для стримування, захисту та підвищення витрат на авторитарні зусилля з підриву та втручання в демократичні інститути. Метою програми ASD виступає підвищення стійкості інституцій громадянського суспільства до протидії гібридним загрозам та, в першу чергу, дезінформації. Як видно з суті програми, її завданням стоїть не лише протидії ворожій дезінформації, а і максимальне ускладнення просування такої дезінформації серед власних громадян, переведення дезінформації в становище невигідних політичних та економічних проектів. Програма фінансується групою з понад 175 приватних осіб та невеликих сімейних фондів з усього політичного спектру, не отримуючи фінансової підтримки від уряду чи компаній соціальних мереж.

Програма ASD має доволі розгалужену структуру. Трансатлантична консультативна рада використовує багаторічний досвід в галузі національної безпеки, розвідки, кібербезпеки та політики, щоб висвітлювати роботу ініціатив програми. Консультативна рада надає поради, вказівки та напрямки, а також організовує зустрічі та форуми, щоб вивчити результати зусиль, обговорити загальну доктрину і стратегію та визначити сфери для подальших досліджень. Консультативну раду підтримує технічний консультативний комітет, до якого входять експерти з протидії дезінформації, кібербезпеки, незаконного фінансування та інших відповідних сфер.

Підсумовуючи контент аналіз проектів, слід зазначити що, більшість проектів та організацій функціонує у якості незалежних міжнародних установ, фактично за відсутності підтримки у вигляді державного фінансування. Значна частина коштів надходить у вигляді недержавного фінансування, грантових внесків або пожертв членських і асоційованих організацій. При цьому, структура створених організацій є доволі складною, в ряді випадків спостерігається формування децентралізованих мереж організацій в різних країнах (досвід ЄС). Дана обставина, жодним чином, не впливає на результативність та функціональність таких проектів. Навіть у випадках, коли проект створено державними або військовими особами, участь громадянського суспільства все одно залишається доволі значною.

Цільовою аудиторією впливу заходів проектів є громадянське суспільство, а не широкі маси верстви населення. Це пов'язано з більш активною роллю громадянського суспільства у країнах ЄС та пасивністю більшої частини громадськості, у зв'язку з чим для зміни масової свідомості людей такі проекти не застосовуються. Тому, важливим у програмному форматі є запобігання впливу дезінформації саме на громадянське суспільство як найбільш активний прошарок суспільства, який виступає у якості рушійної сили змін у державі, що видно навіть у проектах, у яких беруть участь військові. З іншого боку, ряд проектів (Start2Think, Media Literacy) займається просвітою найменш захищених верств населення таких як студенти, безробітні, мігранти, особи з обмеженими можливостями.

Важливо наголосити, що жоден із проаналізованих проектів не відповідає на дезінформацію у «дзеркальний спосіб», тобто власною пропагандою або засобами контрпропаганди. В переважній більшості дані проекти протидії дезінформації являють собою аналітичні центри або майданчики для діалогу чи обміну думок, за результатами яких приймаються відповідні рішення. При цьому, безпосереднє блокування пропагандистських ресурсів або ефірів (наприклад, припинення мовлення пропагандистських каналів) розглядається як крайній захід. Переважно, програми спрямовані на підвищення інформування громадянського суспільства та посилення стійкості громадян до пропагандистського впливу. Як наслідок, у разі підвищення такої стійкості пропаганда чи дезінформація стають невигідними або взагалі безперспективними. Саме такий підхід має бути запроваджений в Україні при формуванні національних підходів до запобігання злочинності у сфері інформаційних технологій.

Висновки. Підсумовуючи, зазначу, що шлях до розуміння сутності й природи запобігання злочинності у сфері інформаційних технологій; визна-

чення реальних та потенційних ризиків і наслідків, лежить через оволодіння сучасним інноваційним комплексом захисту інформаційної сфери. А ефективність системи захисту передбачає можливість дослідження та запровадження ефективного досвіду зарубіжних країн у означеній сфері.

Цінність зарубіжного досвіду у формуванні системи заходів запобігання кримінальним правопорушенням у сфері інформаційних технологій полягає у можливості координації та ефективної міжнародної співпраці між національними та зарубіжними спеціалізованими правоохоронними органами, неурядовими організаціями які здійснюють моніторинг ризиків і загроз у цифровому середовищі, формують систему протидії їм та здійснюють навчання громадян заходам захисту від небезпеки, яка виходить від ворожої дезінформації; укріплення критичного мислення кожного громадянина та громадянського суспільства в цілому. Крім того, важливо отримувати послуги міжнародних консультантів з питань інформованої безпеки та захисту й дотримання прав людини у цифровому середовищі, з урахуванням воєнного стану та перспективи післявоєнної розбудови України.

Основні напрямки запобігання кримінальним правопорушенням у сфері інформаційних технологій мають базуватись на підвищенні рівня поінформованості громадян про форми, прояви, причини і наслідки деструктивного впливу, а також ефективні заходи захисту від небезпеки у цифровому середовищі. Забезпечення інформаційної безпеки у країні, своєчасного та ефективного захисту прав людини у кризових та надзвичайних ситуаціях, подібних до тієї, з якою стикається громада в Україні сьогодні, сприятиме успішній післявоєнній розбудові та підвищенню іміджу України на міжнародній арені.

Необхідно розробити національні підходи збалансованого та відповідального використання цифрового середовища при формуванні яких важливо поєднати запобіжні заходи кримінально-правового, нормативного, технічного та організаційно-управлінського характеру. У межах моделі запровадити проекти, в яких цільовою аудиторією впливу буде громадянське суспільство.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Конституція України URL: https://zakon. rada. gov.ua/ laws/show/ 254% D0%BA/96-%D0%B2%D1%80#Text.
2. Стратегія інформаційної безпеки на період до 2025 року. URL: https://zakon.rada.gov.ua/ laws/ show/685/2021#n7.
3. Новицький В.Я. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. Інформація і право. 2022. Вип. 1 (40). С. 111–118.
4. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози. Humanitarian vision. 2016. Vol. 2, Num. 1. С. 27–32.
5. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий електронний журнал. 2020. № 2. С. 200–203.
6. Черниш Р. Правовий досвід країн європейського союзу у сфері протидії поширенню фейкової інформації. Інформаційне право. 2019. № 10. С. 123–128.
7. Kromhout, W. W. 2009, Oct. 15. UCLA, birthplace of the Internet, celebrates 40th anniversary of network's creation. UCLA Newsroom. URL: http://newsroom. ucla. edu/releases/birthplace-of-the-internet-celebrates-111333.
8. Modesti, K. 2009, Oct. 29. How the Internet was born at UCLA. Los Angeles Daily News. URL: http://www.dailynews. com/article/ ZZ/ 20091029/ NEWS/ 910299877.
9. Internet Live Stats. (2017, February). URL*:* www.InternetLiveStats.com.
10. Internet users by country (2016). URL: http://www.internetlivestats.com/internet-users-by-country.