2. Розпорядження Кабінету Міністрів України «Про схвалення Концепції підготовки фахівців за дуальною формою здобуття освіти» від 19 вересня 2018 р. № 660-р. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/660-2018-р

3. Наказ від 26.01.2016 № 50 «Про затвердження Положення про організацію службової підготовки працівників Національної поліції України». [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua/laws/show/z0260-16#Text

Панченко Л.В.
Науковий співробітник відділу організації наукової роботи ДДУВС, викладач вищої категорії, викладач-методист

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВООХОРОННІЙ ТА ЮРИДИЧНІЙ ДІЯЛЬНОСТІ: МІЖНАРОДНИЙ ДОСВІД

В умовах розвитку сучасного суспільства на тлі загострення криміногенної ситуації в Україні надзвичайно актуальною є проблема правильного розроблення, впровадження та застосування нормативно–правових актів для забезпечення оптимального розвитку інформаційних технологій в Україні.

В Стратегії **національної безпеки України затвердженої** Указом Президента України від 14 вересня 2020 року № 392/2020. п.9 вказано, про стрімке зростання ролі інформаційних технологій у всіх сферах суспільного життя. В п.п. 51-52 розкрито основне завдання розвитку системи кібербезпеки, яке гарантується через кіберстійкість та кібербезпеку національної інформаційної інфраструктури, важливим завданням, окрім іншого є поширення цифрової грамотності серед населення України [10].

У Окінавській хартії глобального інформаційного суспільства, від 2000 року було закріплено, що «всі люди повсюдно, без винятку повинні мати можливість користуватися перевагами глобального інформаційного суспільства», на думку міжнародної спільноти країн Великої вісімки, які підписали хартію, «Права, закріплені у Загальній декларації прав людини, повинні бути реалізовані в інформаційну епоху, перебувати під захистом держави і суспільства незалежно від розвитку і впровадження нових технологічних досягнень»[6; с.74].

Наразі в Україні існує проблема недосконалості законодавчої бази, тому окрім удосконалення технічної сторони питання інформаційних технологій необхідно в першу чергу заповнити прогалини законодавчої бази в правоохоронній та юридичній діяльності.

Роль держави полягає в розробці законів та створенні компетентних правоохоронних та судових органів для забезпечення діяльності осіб, які надають

кваліфіковану юридичну допомогу. Для цього, необхідна якісна комплексна система правового забезпечення, що було вимогою викладеною в принципах та керівних положеннях ООН, 2012 року (резолюція 67/1872). [2; 9].

Одним з аргементів, який виступає на необхідність упорядочення та удосконалення правового забезпечення в інформаційній та юридичній діяльності є дані Лаабораторії Касперського, згідно яких, за останні 12 місяців, кожна друга промислова компанія пережила кіберінциденти в інформаційного характеру на усунення яких, було витрачено близько 497 тісяч доларів США[11].

Проблеми правового забезпечення інформаційних технологій розглядали в своїх працях Голубев В.А, Касперский Е., Вайман Г., Каплан Є., Коллін Б., та інші.

Бубницька О.П. в своїх працях дає таке визначення: «Правове забезпечення - сукупність правових норм, що визначають створення, юридичний статус і функціонування інформаційних систем, що регламентують порядок одержання, перетворення й використання відомостей».

Доступ до справедливого правосуддя на всіх рівнях має безапеляційне значення для всіх категорій населення в кожній країні.

Юридична допомога є важливим елементоми системи яка надає доступ до системи правосуддя кожної особи в державі.

Право на безоплатну юридичну допомогу викладено та вперише закріплено в Міжнародному пакті про громадянські та політичні права 8 , в с. 14(3)(d) [2; с.13].

Експертами Венеціанської комісії створено матеріали в яких відображено досвід судочинства країни Азії, що буде корисним в юридиній діяльності. [3; с.40-45].

Орієнтуючись на інтеграцію України до ЄС необхідно орієнтуватися на стратегію розвитку країн-учасниць ЄС та НАТО в інформаційній сфер, дотримуючись всіх вимог правового забезпечення в првоохоронній та юридичній діяльності [4;62].

Тому важливим є міжнародний досвід в становленні розвитку та адаптації законодавчої бази стосовно інформаційного забезпечення, оскільки події останніх років доводять, що Україна не готова до інформаційних війн, які ведуться на сьогодні в інтернет просторі.

На країни, які є членами Північноатлантичного Альянсу та Європейського Союзу. поширюються стандарти міжнародних організацій щодо інформаційної політики та забезпечення інформаційної безпеки.

Серед основних загроз в інформаційній сфері виділяють три складові: ведення інформаційної війни, інформаційний тероризм, інформаційні злочини.

Головними є стандарти НАТО щодо захисту інформації, викладені у Документі СМ (2002)49 “Безпека в організації Північноатлантичного договору (НАТО)”, офіційна політика НАТО у сфері кіберзахисту , стратегічна концепція кібербезпеки, сформульована за результатами Лісабонського саміту й уточнена за результатами Варшавського саміту. [4; с.63].

Для безпеки інформаційного простору Стратегії кібербезпеки розроблені на сьогодні в більшості є країн світу, таких як Австрія, Австралія, США, Ізраїль, Великобританія, Естонія, Іспанія, Італія, Канада, Латвія, Німеччина, Польща, Франція, Чехія таа інших [5;32-38].

Особа в інформаційному просторі наражається на небезпеку і загрози.

Інформаційне середовище не збігається зі звичною для суспільства тому необхідні норми, розроблені для регулювання інформаційно-просторових відносин, які б попереджували вчинення правопорушень та злочинів, що є особливо важливим в діяльності правоохоронних органів.

З 2018 року для Румунії та Болгарії, як і інших країн-членів ЄС, набули чинності нові правила захисту персональних даних (GDPR, важливим є введення більш суворого покарання за несвоєчасне повідомлення інформації про виток даних. Компаніям, які порушили положення та не доповіли про факт витоку або злому протягом 72 годин з моменту інциденту, загрожує штраф до 4 % річного доходу або до 20 млн. євро. [4; с.64].

У забезпеченні кібербезпеки Румунії відводиться її спеціальному контррозвідувальному органу – Румунській службі інформації, у структурі

якої створено національний центр кібербезпеки. Румунія забезпечує функціонування динамічного інформаційного середовища на основі функціональної сумісності й послуг, характерних для інформаційного суспільства, а також забезпечення відповідності основних прав і свобод громадян та інтересів національної безпеки у відповідних правових рамках. [4; с.64-65].

У квітні 2016 року в Болгарії розроблено проект Національної стратегії кібербезпеки під назвою "Стійка до кібератак Болгарія 2020", серед інших в якій ініціювання законодавчі зміни щодо забезпечення високого загального рівня мережної й інформаційної безпеки , а також для захисту політичних і виборчих прав громадян і в кіберпросторі; реалізації мережної моделі обміну інформацією й координації між організаціями, відповідальними за кібербезпеку у Болгарії.

В законодавстві Молдови в січні 2010 року прийнято Закон "Про попередження та боротьбу зі злочинністю у сфері комп'ютерної інформації". Згідно із яким генпрокуратура Молдови наділена повноваженнями координувати й здійснювати кримінальне переслідування осіб, що вчинили кіберзлочини. [4; с.67].

В Білорусії діє державна система спостереження (СОРМ), яка здійснює повний он-лайн-нагляд у всій країні, що регламентується значною кількістю нормативно-правових актів. Тут немає спеціальних законів, присвячених протидії кіберзлочинності, але деякі аспекти регулюються Кримінальним кодексом і законами, що стосуються регламентації діяльності глобальної інформаційної мережі Інтернет, що є достатньо ефективним, для інформаційної держави.[4; с.71].

У 2000 році в КНР створено «Проект С219» «електронної стіни» навколо національної зони мережі Інтернет. Китай є одніє з 20 країн , яка суворо регулює, доступ своїх громадян до інформаційної мережі. З 2011 року проголошено, про стоворення онлайн-армії «Блакитні мундири», для попередження кіберзагроз. Правилами регулюється діяльність блогерів, яких в країні понад 180 млн. Для доступу до мережі існує віковий ценз та триступенева система ідентифікації. Широко публікується інформація про арешти блогерів –дисидентів,тощо. Окрім того існує система матеріальних заохочень про повідомлення за інформаційні загрози. Так, приміром, за сигнал про поширення порно контенту винагорода від 60 - 241 дол. США. Та інші. .[12; с.96].

В Законі «Про кібербезпеку КНР», від 2016 року вказано на захист від випадкового чи навмисного витоку даних.[9; с.406].

В 2009 році в США затверджена «Комплексна національна ініціатива з кібербезпеки», яка спрямована на захист громадянських свобод особи . Кіберзагрози проти країни прирівнюються до інформаційної війни.

Для заборони поширення недостовірної інформації у Франції не потрібно дозвіл суду, лише рішення правоохоронних органів. [7; с.20].

Отже, для вирішення проблеми правового забезпечення інформаційної безпеки в правоохоронній та юридичній діяльності, суспільства, держави, Україна має співпрацювати з іншими країнами орієнтуючись на стандарти ЄС та НАТО. Для України є важливим досвід країн Східної Європи, щодо приведення національного законодавства у відповідність до вимог міжнародних організацій, щодо забезпечення балансу між свободою й безпекою в інформаційній сфері на законодавчому рівні.

Використані джерела:

1.Паспорт информационнной безопасности. Режим доступа: https://digital. gov.ru/uploaded/files/pasport-federalnogo-proekta-informatsionnaya-bezopasnost. pdf

2. Справочник по обеспечению качества юридической помощи в процессах уголовного правосудия: Практическое руководство и перспективная практика. Организация Объединенных Наций, февраль 2020 года.

3. Judicial systems of Central Asia a comparative overview Edited by G. Dikov Moscow Jurisprudence 2015,-328 c.

4. Ткачук Т.Ю., Забезпечення інформаційної безпеки: досвід окремих країн Східної Європи (ст. 62-72).//Журнал "Інформація і право" № 4(23)/2017.

5. Законодавство та стратегії у сфері кібербезпеки країн європейського союзу сша, канади та інших. Режим доступу: https://parlament.org.ua/wp-content/uploads/2016/11/INFODOVIDKA-ZAKONODAVSTVO-TA-STRATEGIYI-KIBERBEZPEKA.pdf

6. Ольга Золотар.Інформаційна безпека людини: теорія і практика. Монографія.-Київ 2018.

7. Сардарова Валерия Анатольевна. Вопросы кибербезопасности в американо-Китайском взаимодействии Cybersecurity in the US-China Interaction. Санкт-Петербург, 2018.

8. Кучмій О.П. Стратегія інформаційної безпеки в структурі внутрішньої й зовнішньої політики КНР.

9. Н.О. Піпченко. Здійснення політичної комунікації в китаї засобами мережі інтернет. Режим доступу: //http://vmv.kymu.edu.ua/v/p05/ar401414.pdf.

10. Указ Президента України , №392/2020 Про рішення Ради національної безпеки і оборони України від 14.09. 2020 року «Про Стратегію національної безпеки України».Режим доступу: https://www.president. gov.ua /documents /3922020-35037.

11. Офіційна інформація про дані Лабораторії Кассперського. Режим доступу: https://genproc.gov.ru

12. Дубцов Д. Політика Укитаю, щодо регулювання внутрішнього інфопростору.// Політичний менеджмент.№4, 2010.