УДК 32:001.102]+007-049.5](4-6ЄС)
DOI: 10.34132/PARD2020.08.08

ДОСВІД КРАЇН ЄС ВІДНОСНО РОЗРОБЛЕННЯ ТА РЕАЛІЗАЦІЇ МОДЕЛЕЙ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ

Багмет М.О., д-р іст. наук, професор, керівник Інформаційного центру ЄС, Чорноморський національний університет імені Петра Могили, м. Миколаїв, Україна.

Гаркуша А.М., магістр публічного управління та адміністрування, документаліст Інформаційного центру ЄС, Чорноморський національний університет імені Петра Могили, м. Миколаїв, Україна.

Стаття присвячена висвітленню досвіду Німеччини, Франції, Італії, Іспанії, Польщі, Нідерландів та інших країн, які входять до складу ЄС по впровадженню в практику інформаційно-комп'ютерних технологій в ході сучасного всесвітнього глобалізаційного процесу. Окремо зазначається і роль Великобританії, яка хоча і заявила про вихід із складу ЄС, але має значний доробок в розроблення головних політико-правових аспектів в ході реалізації державної інформаційної політики та інформаційної стратегії, створення громадсько-мережевих інформаційних центрів та освоєння інформаційно-комунікаційних технологій.

Взагалі розроблення основних понять та категорій, всебічному обґрунтуванню європейської моделі реалізації державами ЄС інформаційної політики присвятили цілий ряд оригінальних праць як зарубіжних, так і вітчизняних вчених та практиків.

Наразі в Україні тривають реформи, які впливають на формування та розвиток інформаційного простору країни, інформаційного суспільства. Нагального вирішення потребує

проблема щодо створення оптимального законодавчого акту, який забезпечить ефективну роботу як державних, так і недержавних суб'єктів інформаційного сектору, а також полегшення доступу громадян до отримання послуг в режимі «онлайн», шляхом створення необхідної платформи і забезпечення захисту кіберпростору у мережі Інтернет. Усе це свідчить про великий перелік викликів та завдань, які необхідно вирішити задля досягнення важливої мети – створення конкурентоспроможної, інформаційно-розвиненої держави, яка реалізує ефективну державну інформаційну політику як всередині країни так і на міжнародній арені.

При здійсненні державно-управлінських реформ, постало питання про застарілість та невідповідність сучасному стану технологічного розвитку законодавства щодо інформації та діяльності засобів масової інформації, з урахуванням безпекового фактору та національних інтересів держави. Допомогти у формуванні векторів та пріоритетів державної інформаційної політики здатне й врахування здобутків інформаційної політики країн Європи, Азії та Америки.

Ключові слова: *державна інформаційна політика, електронна світова інформаційна політика, Європейський Союз, кібербезпека, моделі державної інформаційної політики, центри інформаційної політики.*

Постановка проблеми у загальному вигляді. Визначальний вплив на сучасні інформаційні процеси в Європі здійснює інтеграція. Інтеграційний процес почався з розробки загальної політики в сфері вугільно-металургійної промисловості та закінчився створенням глобального європейського наднаціонального і мультикультурного суспільства. На шляху регулювання діяльності Європейського Союзу європейським інститутам доводиться враховувати все різноманіття культур, традицій та інтересів країн-членів. Євросоюз будує свою політику на основі духу єдності і цілісності при збереженні національних відмінностей. Створення та підтримка цього духу неможлива без загальноєвропейської інформаційної

Isue DOI: 10.34132/pard

політики, що сприяє взаєморозумінню, взаємоповазі, формуванню єдиних соціальних і політичних цінностей, цілей та ідеалів.

Аналіз останніх досліджень і публікацій. Актуальність зазначеної проблеми підтверджується значною кількістю як зарубіжних, так і українських дослідників. Вагомий внесок у розроблення базових складових нормативно-правових аспектів державної інформаційної політики внесли такі зарубіжні вчені С. Браман, Д. Белл, М. Брюггеманн, Ф. Вайнгартен, М. Вершинін, П. Джегер, І. Дзялошинський, Є. Дьякова, М. Ковальова, А. Кондратенко С. Коновченко, Ч. МакКлюр, А. Манойло, Д. Мезенцев, А. Нестеров, В. Ніцевич, Ю. Нісневич, В. Попов, Х. Реліа, П. Симуш, А. Стрельцов, Ю. Тихомиров та багато інших.

Формулювання цілей статті (постановка завдання). Метою статті є обґрунтування та нагромадження зарубіжного досвіду реалізації державної інформаційної політики, який може сприяти перспективам та моделюванню оптимізації української інформаційної політики.

Важливо відзначити, що прискорений процес побудови інформаційного суспільства можна очікувати лише тоді, коли завдання щодо розвитку інформаційного суспільства, як свідчить досвід країн ЄС, стануть першочерговими державними пріоритетами.

Виклад основного матеріалу дослідження. Розвиток інформаційно-комунікаційних технологій та інформатизації суспільства в ЄС входить до числа його найважливіших пріоритетів і реалізується перш за все в рамках політики в галузі «інформаційного суспільства» (Information society policy) та «аудіовізуальної продукції і ЗМІ» (Audiovisual and Media policy).

Так як Європейський Союз не є державою у традиційному сенсі, то його інформаційна політика має наддержавний характер. Інформаційна політика ЄС відповідає інтересам, як самого суспільства, так і не обмежує інтереси країн-членів та європейців. Таке можливо лише при забезпеченні діалогу, спрямованого на спільне прийняття рішень в різних сферах життя. Ця особливість визначає двосторонній характер інформаційної політики ЄС.

У 1987 році Європейська комісія сформулювала внутрішню та зовнішню мету інформаційної політики, яка відповідала «створенню єдиного медіапростору ЄС» і «захисту внутрішнього комунікаційного простору Європейського Союзу від зовнішнього впливу» [2].

Базові принципи інформаційної політики ЄС умовно можна поділити на три групи прийнявши за основний критерій інтереси та цінності трьох ключових сторін: суспільства загалом, національних держав і Європейського Союзу. Ці принципи визначаються:

- «соціально-політичними цінностями, прийнятими в об'єднаній Європі (закріплені загальноєвропейськими законами, прийнятими ЄС);
- інтересами Європейського Союзу (сформульовані законами та директивами ЄС, заснованими на нормах міжнародного права);
- національними інтересами країн-членів ЄС (сформульовані законодавчою базою країн-членів, що відповідають нормам міжнародного права та законодавству Європейського Союзу)» [2].

2000 рік був визначальним для ЄС, оскільки відбулося дві важливі події. Першою з них було підписання у березні, главами держав та урядів членів Євросоюзу Лісабонської стратегії (Lisbon Strategy) [17], яка визначила мету перетворення Європейського Союзу в найбільш конкурентоспроможну економіку в світі. Вирішення завдань, які були окреслені цією Стратегією передбачало використання потенціалу новітніх ІКТ. Для досягнення заявлених цілей Лісабонської стратегії були прийняті два важливих документи ЄС [14]:

- «Електронна Європа - 2002» (більш дешевий, швидкий, безпечний Інтернет; інвестування в людський капітал і розвиток навичок; стимулювання використання мережі Інтернет в різних сферах життя суспільства);
- «Електронна Європа - 2005» (стимулювання послуг, програм, контенту, що охоплюють сфери онлайн-послуг держави і електронного бізнесу; розвиток інфраструктури широкосмугового зв'язку і вирішення питань інформаційної безпеки).

В реалізації Лісабонської стратегії були досягнуті значні успіхи. За даними підготованого в 2005 році Порівняльного звіту про розвиток інформаційного суспільства, кількість осіб, що мають

Isue DOI: 10.34132/pard

доступ до мереж Інтернет, збільшилася у період з 2002-2004 рр. з 39 % до 47 %; широкосмуговим доступом до Інтернету до 2005 року було охоплено 10,6 % користувачів. Однак, незважаючи на певний прогрес в застосуванні ІКТ в діяльності уряду та бізнесу, в цій сфері відзначалася недостатня ефективність (наприклад, тільки 46 % урядових послуг в ЄС були повністю доступні в онлайн режимі) [12].

Другою подією був саміт «Великої вісімки» в Окінаві у липні 2000 року. Там вперше офіційно було проголошено перехід світової спільноти до глобального інформаційного суспільства. Окінавська Хартія (Okinawa Charter on the Global Information Society) встановлює загальні принципи входження держав у глобальне інформаційне суспільство і є найважливішим документом, покликаним «організувати та активізувати діяльність міжнародного співтовариства в галузі формування глобального інформаційного суспільства» [19].

У Окінавській Хартії були встановлені основні принципи входження держав і країн в глобальне інформаційне суспільство:

1. «інформаційно-комунікаційні технології – одні з найбільш важливих факторів, що впливають на формування суспільства XXI ст.; їх революційний вплив стосується способу життя людей, їх освіти і роботи, а також взаємодії уряду та громадянського суспільства;

2. сенс стимулюючих ІКТ економічної та соціальної трансформації полягає в їх здатності сприяти у використанні знань та ідей суспільством;

3. всі люди, без винятку, повинні мати можливість користуватися перевагами глобального інформаційного розвитку;

4. керівники країн «вісімки» повинні здійснювати керівництво, у просуванні зусиль урядів, щодо укріплення відповідної політики та нормативної бази;

5. Хартія є, перш за все, закликом до всіх як в державному, так і приватному секторах ліквідувати міжнародний розрив в галузі інформації та знань» [19].

Не менш важливою подією став Всесвітній саміт на найвищому рівні з питань інформаційного суспільства, що проводився у два

етапи: Женева (2003 р.) і Туніс (2005 р.). За підсумками цієї зустрічі були прийняті чотири документи, а саме «Женевська Декларація принципів» [6], «Женевський План дій» [28], «Туніське зобов'язання» [24], «Туніська програма для інформаційного суспільства» [23], які закликали світову спільноту будувати інформаційне суспільство «орієнтоване на інтереси людей, відкрите для всіх, в якому кожен може створювати інформацію і знання, мати до них доступ, користуватися і обмінюватися ними» [10].

Саме з цього періоду розпочалася справжня трансформація та розвиток інформаційного суспільства в ЄС. Оскільки всі наступні дії були зроблені на основі Лісабонської стратегії та інших важливих документів, серед яких: ініціатива Європейської Комісії «2010 – Європейське інформаційне суспільство для зростання і зайнятості» [26]. В якій було сформовано три пріоритети політики Євросоюзу в галузі інформаційного суспільства та мас-медіа:

- завершення єдиного європейського інформаційного простору;
- збільшення інвестицій в дослідження ІКТ;
- формування всеосяжного інформаційного суспільства.

З початку другого десятиліття продовжився новий етап розвитку інформаційного суспільства в Європейському Союзі, пов›язаний з прийняттям документу під назвою Стратегія «Європа 2020» (Europe 2020 Strategy) [26] – нова політична Стратегія розвитку ЄС до 2020 року, яка також була спрямована на підтримку зайнятості населення, підвищення продуктивності та соціальної згуртованості в Європі. Важливим напрямком у цій Стратегії був «Цифровий порядок денний для Європи» (Digital Agenda for Europe) [7], який пов'язаний безпосередньо з використанням потенціалу інформаційно-комунікаційних технологій для стимулювання інновацій, економічного зростання і прогресу.

Включення цього напрямку у зміст основного стратегічного документу ЄС на найближче десятиліття показує, що розвиток ІКТ та інформаційного суспільства залишається одним з найважливіших стратегічних пріоритетів Європейського Союзу і розглядається як необхідна умова подальшого прогресу європейський країн. Виділивши 7 основних проблемних зон у розвитку ІКТ «Цифровий

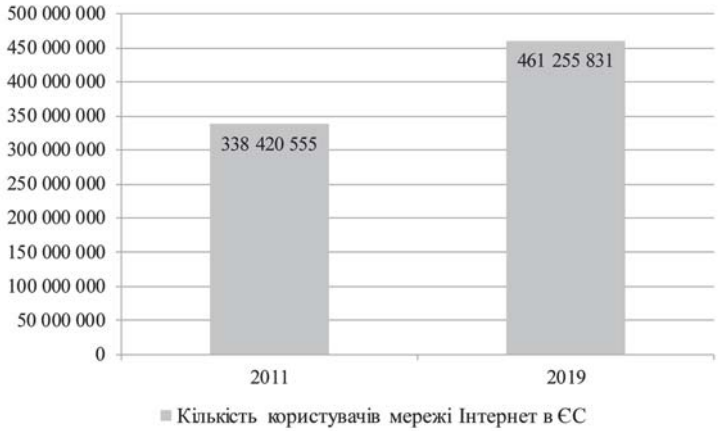
Isue DOI: 10.34132/pard

порядок денний для Європи» затвердив 7 пріоритетних напрямків діяльності [7]:

1. формування єдиного цифрового ринку;
2. забезпечення довіри і безпеки в Інтернеті;
3. забезпечення сумісності ІКТ-продуктів і послуг;
4. розвиток високошвидкісного Інтернету;
5. розвиток цифрових навичок і цифрової грамотності;
6. стимулювання досліджень та інновацій;
7. використання можливостей ІКТ у вирішенні соціальних проблем.

В результаті прийняття такої кількості важливих Стратегій та обрання пріоритетних шляхів, щодо створення єдиного ефективного інформаційного середовища можна побачити певні позитивні зміни за даними Internet World Stats - порівнявши дані станом на 2011 та 2019 роки (діаграма 1) [15].

Діаграма 1

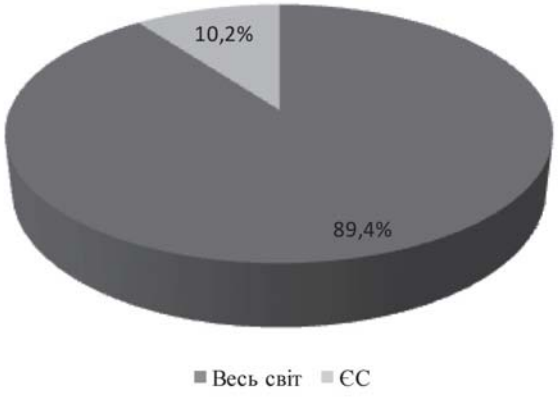


Кількість користувачів мережі Інтернет в ЄС

Станом на 31 березня 2011 року загальна кількість користувачів мережі Інтернет в Євросоюзі складала 338 420 555 осіб, у відсотковому еквіваленті рівень проникнення складав 67,3 %. Тоді, як станом на 30 червня 2019 року загальна кількість користувачів

підвищилась до 461 255 831, у відсотках – 90,4 %. При цьому доля користувачів мережі Інтернет від загальної кількості у світі, у 2019 році складає 10,2 % (діаграма 2) [15].

Діаграма 2



Доля Інтернет користувачів ЄС від загальної кількості у світі

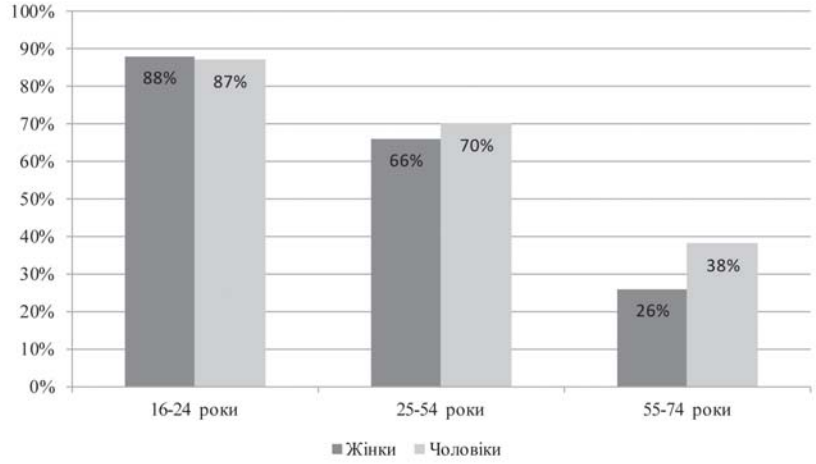
Ще одним важливим фактором є розподілення кількості постійних користувачів мережі Інтернет за віковими та гендерними групами: 16-24 роки; 25-54 роки; 55-74 роки (діаграма 3) [15].

Такі статистичні дані допомагають зрозуміти як краще розробляти наступні кроки, на кого орієнтуватися, а для кого навпаки почати розробляти певні програми, аби в майбутньому підвищити показники. Популярність мережі

Інтернет серед молоді пояснюється тим, що вона створює унікальні можливості для спілкування, для пошуку та обміну інформацією. Для більш зрілого віку – в колективному обговоренні соціально значущих проблем та вироблення спільних рішень. Особливо важливу роль вони відіграють в житті людей з обмеженими фізичними можливостями, дозволяючи їм також стати більш активними членами суспільства і отримати можливість впливати на певні політичні рішення шляхом висловлення своїх думок за допомогою мережі Інтернет.

Isue DOI: 10.34132/pard

Діаграма 3



Вікові та гендерні показники постійних користувачів мережі Інтернет в ЄС

На сьогодні «Єдиний цифровий ринок» один з напрямків ЄС, щодо продовження розвитку та створення цифрових можливостей для суспільства шляхом «підтримки медіа та цифрової культури», охоплюючи законодавство про аудіовізуальні медіа-послуги та збереження культурної спадщини. І включення інформаційного суспільства, яке отримує користь від «Єдиного цифрового ринку»: побудова розумніших міст, покращення доступу до електронного уряду, електронних служб охорони здоров'я та цифрових навичок – те, що дійсно дасть можливість утворити цифрове європейське суспільство [8].

Оскільки, як відомо, інформація та інформаційна політика має і негативні сторони – Євросоюз розробив певні запобіжні заходи. Так, 18 березня 2019 року була запущена в роботу «Система швидкого сповіщення про дезінформацію», в якій бере участь як Єврокомісія, так і країни Європейського Союзу. Виявленням дезінформації на рівні ЄС займаються робочі групи зі стратегічних комунікацій (StratCom) [20]. Сама система сповіщення про дезінформацію –

це «цифрова платформа для обміну інформацією про фейки та для координації реакції на них». За задумом Єврокомісії, система буде виконувати три основні функції: коли хто-небудь з учасників системи виявляє кампанію з дезінформації, система дозволить всім іншим швидко дізнатися про це; розкриття тенденцій та способів поширення дезінформації; формування координованої реакції на кампанії з поширення фейків і обмін досвідом, які заходи з протидії дезінформації є найбільш ефективними [21].

Інформаційно-правові системи та бази даних ЄС відносяться до числа найбільш досконалих у світі як по їх утриманню, так і з технічної оснащеності. Також представляють інтерес установи і служби, що забезпечують реалізацію інформаційної діяльності Європейського Союзу.

Серед основних друкованих органів ЄС: «Офіційний журнал Європейських співтовариств»; «Повідомлення Європейського Суду»; повну інформацію про всі дії, рішення, пропозиції Комісії можна отримати в бюлетені «COM» (COM Documents); інформація про діяльність Європарламенту отримує відображення в «Повідомленнях Європейського парламенту», а також в додатку до Офіційного журналу «Дебати в Європейському парламенті» та багато інших.

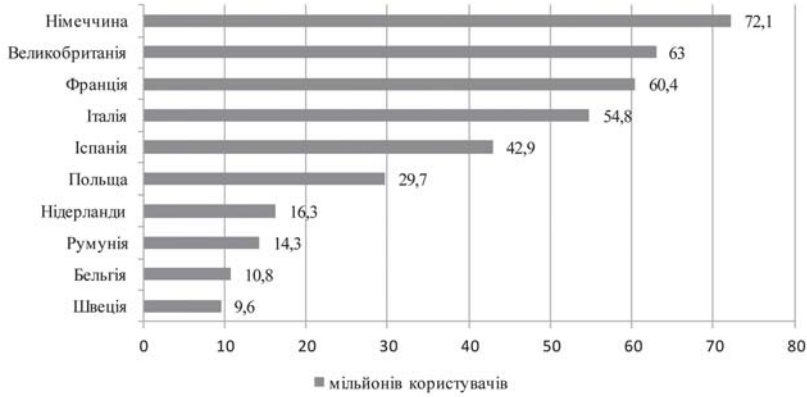
До інформаційних служб належать: «Європейське агентство офіційних публікацій»; Інформаційні центри в Європі (Information Centres on Europe); Інформаційні пункти Євро (Euro Info Points); Європейські депозитарні бібліотеки (European Depository Libraries); Система «Європраво» (EURO-Jus); Система Європейських центрів документації (European Documentation Centres).

До баз даних регулюючих міжнародний інформаційний обмін можна віднести «EUROBASE». Окрім різноманітних інформаційних систем, організованих та керованих безпосередньо ЄС, існують і неофіційні системи документації та поширення інформації Євросоюзу, які створюються державами-членами, комерційними організаціями і науковими інститутами [3, с. 34-41].

Звертаючись до Internet World Stats можна побачити рейтинг «Топ 10 країн Європейського Союзу з розвиненим використанням мережі Інтернет» (діаграма 4) [15].

Isue DOI: 10.34132/pard

Діаграма 4



Викладення основного матеріалу дослідження. Аналізуючи висвітлені дані можна побачити, що лідируючі позиції займають Німеччина – 72,1 %, Великобританія – 63 % і Франція – 60,4 %. Варто відзначити, що досягнення мети Євросоюзу з приводу побудови єдиного Європейського інформаційного простору лежить також в конкретних локальних розробках країн-членів ЄС.

Німеччина.

Модель інформаційної політики Німеччини полягає у «вільному транскордонному обміні інформацією; розвитку ІКТ та телекомунікаційних мереж; свободу конкуренції в інформаційній сфері; створення відповідно до змін певних норм і принципів регулювання інформаційної діяльності у країні» [13].

Уряд Німеччини поступово розробляв інформаційні програми, які в свою чергу мали відповідні цілі для політичного та економічного розвитку країни:

1. перша програма (1974 – 1977 рр.) полягала у забезпеченні широкої громадськості доступ до інформаційних систем, накопичення знань та розвиток навичок з інформаційних процесів, проведення політичних дискусій пов'язаних з активним інформаційним розвитком суспільства;

2. друга програма (1985 р.) переорієнтовувала федеральну інформаційну політику і ставила нові цілі, серед яких: «розвиток ринку інформаційних ресурсів; лібералізація інформаційної політики; посилення міжнародної позиції країни у світі; забезпечення доступу до міжнародних інформаційних систем» - основна ідея полягала у зменшенні регуляції урядом та розвитку ініціативи громади;

3. третя програма «Федеральна підтримка нових комунікаційних та інформаційних технологій» (1994 р.) – запровадження контролю міністерствами за здійсненням фінансування напрямів діяльності інформаційних центрів, державних установ та приватних підприємств;

4. четверта програма «Info-2000: німецький шлях до інформаційного суспільства», яка також полягала у «формуванні інформаційного суспільства Німеччини шляхом розвитку нових інформаційних магістралей; підтримці національного виробника електронних продуктів; активізації інформаційної політики з розширенням прав урядів і посилення відповідальності та контроль за змістом інформації» [13].

Починаючи з 2011 року уряд Німеччини активно сприяло розвитку так званої «Четвертої промислової революції» (Industrie 4.0). Цей проект був частиною «Плану дій стратегій високих технологій – 2020» (High-Tech Strategy 2020 Action Plan) – ця ініціатива стимулювала приватні компанії використовувати у своїй діяльності ІКТ.

Будучи лідером у розвитку та впровадженні інформаційно-комунікаційних технологій, держава також стакалася з високим рівнем кіберзлочинності, промислового шпигунства, умисного порушення критично важливих сервісів, а також інших шкідливих дій в кіберпросторі. І Німмечина заявила про намір захистити націю та зробити це на державному рівні обов'язком громадян. В 2008 році влада надала громадянам CD-диски, за допомогою яких вони могли провести чистку від шкідливих вірусів своїх комп'ютерів і інших пристроїв. Вже в 2011 році уряд здійснив більш систематичний та централізований підхід, опублікувавши першу версію документу

Isue DOI: 10.34132/pard

«Кібербезпека для Німеччини» (Cyber Security Strategy for Germany) [22]. Цей документ визначав взаємозв'язок між ІКТ і економічним та соціальним зростанням в країні.

Національна Стратегія кібербезпеки виділяє кілька стратегічних сфер і цілей для більш успішної боротьби з кіберзагрозами [9]:

- «захист критичних елементів інфраструктури та ІТ систем;
- захист ІТ-систем громадського управління за допомогою створення єдиної «федеральної мережі»;
- створення Національного центру кіберреагування (National Cyber Response Center) для реагування на інциденти та захисту даних і систем;
- створення Ради національної кібербезпеки (National Cyber Security Counsil) для активізації співпраці між організаціями державного і приватного сектору;
- розвиток активного міжнародного співробітнитва для координації діяльності з забезпечення кібербезпеки;
- розробка і створення надійних ІТ-продуктів з використанням інновацій;
- підготовка і тренінг працівників федеральних органів влади;
- ефективне використання інструментарію державних органів, а саме законодавство для боротьби з кіберзлочинністю» [9].

Крім того, данний документ визначив Федеральний офіс інформаційної безпеки Міністерства внутрішніх справ (Bundesamt für Sicherheit in der Informationstechnik, BSI) органом, відповідальним за кібербезпеку країни, а також відповідальним за реалізацію вказанної Стратегії [9]. Як вимагала Національна стратегія, BSI створив Національний центр кіберреагування (Nationales CyberAbwehrzentrum, NCAZ) – відповідальний за визначення, аналіз і розробку заходів, необхідних для нівелювання і усунення потенційних погроз. Також була створена Національна рада кібербезпеки, метою якої було дозволити секретаріатам всіх міністерств внести питання кібербезпеки в стратегії реалізації всіх політичних напрямків діяльності в країні та координувати застосування єдиних державних і приватних секторів превентивних заходів і міждисциплінарних підходів в сфері кібербезпеки [22].

В 2012 році BSI, для сприяння реалізації широких політичних завдань, спільно з Федеральною асоціацією інформаційних технологій і нових засобів комунікаціх (BITKOM) створили некомерційну організацію – «Альянс за кібербезпеку» (Alliance for Cyber Security). А в 2015 році було реалізовано «Акт про IT-безпеку» (IT Security Act) – який охарактеризував необхідність «постійної співпраці з операторами критично важливих елементів інфраструктури з метою визначення мінімальних стандартів рівня безпеки, а також з метою підвищення доступності, адекватності, конфіденційності та цілісності системи IT-безпеки по всій країні» [1].

Для забезпечення кращого розвитку інформаційного простору владою було розроблено і підтримано багато програм та ініціатив в різних галузях. Була створена «Ініціатива D21» (Intiatived D21) – створена задля забезпечення приватно-державного партнерства між бізнесом та державою шляхом підвищення довіри та безпеки в мережі Інтернет, покращення IT-обладнання у школах та електронного навчання.

Навіть був створенний Центр компетенцій «Kompetenzz», який сприяє рівним можливостям для жінок та чоловіків у цілому по країні, задля об'єднання досвіду досліджень та практик для визнання різноманітності як принципу успіху в бізнесі, суспільстві та технологічному розвитку.

«Інформаційне суспільство в Німеччині має стати інформаційним суспільством для всіх. Незалежно від рівня доходів та інших соціальних критеріїв, всі громадяни повинні мати можливість брати активну участь в інформаційному суспільстві» - таку мету ставить перед собою уряд країни. Одним з шляхів досягнення цієї мети було створення сайту «Bundesregierung» – задля популяції інформації.

Великобританія.

Ще одна країна з важливими показниками в даному відношенні є Великобританія – 63 %. Ціллю інформаційної стратегії країни є «удосконалення умов конкуренції на інформаційному ринку, підвищення ефективності інформаційних послуг і впровадження ІКТ у державне управління». До завдань британського уряду у сфері інформаційно-комунікаційних технологій належало:

 Isue DOI: 10.34132/pard

- «створення умов для інформаційного бізнесу і підприємництва;
- реалізація проекту британської інформаційної супермагістралі (Super Janet);
- розвиток телекомунікаційних мереж шляхом безпосереднього їх використання» [3, с. 127].

В данний час електронний уряд Великобританії розділений на три основних служби: служба DicertGov – відповідає за взаємодію з громадянами; служба BusinessLink – відповідає за взаємодію з юридичними особами; служба NHS Choices – відповідає за питання, пов'язані з охороною здоров'я. Подібна структура електронного уряду обумовлена тим, що ці три портали знаходяться у віданні різних відомств. DicertGov знаходиться під управлінням департаменту праці та пенсій, BusinessLink управляється Міністерством податкових і митних надходжень, а NHS Choices знаходиться під патронажем Міністерства охорони здоров'я [18].

Програма впровадження Е-врядування Великобританії обгрунтована основними положеннями документу «Біла Книга. Модернізація уряду Англії» (Modernising Government White Paper) [27]. Програма називается «Е-громадяни, Е-бізнес, Е-уряд. Стратегічна концепція обслуговування суспільства в інформаційну епоху» (E-citizen, E-business, E-government. A strategic framework for public service in the Information Age). Мета і завдання цієї Програми спрямовані на аналіз і конкретизацію процесу переходу до уряду інформаційної епохи. В рамках цього передбачається:

- «визначення структури та переліку послуг, які необхідно реалізувати для простих користувачів і неурядових організацій;
- розширення спектру послуг;
- забезпечення максимального охоплення населення урядовими послугами;
- радикальне поліпшення використання інформації;
- визначення конкретних заходів, щодо реалізації всіх необхідних змін» [3, с. 133-135].

Великобританія розробила свою національну Стратегію кібербезпеки в 2009 році і внесла зміни до неї в 2011 році. Ця Стратегія включала детальний опис кіберзагроз, які могли виник-

нути перед Сполученим Королівством та визначила кібератаки і кіберзлочини як один з п'яти важливих національних ризиків. До Стратегії додався план її реалізації, який був заснований на ключових цілях, серед яких – зміцнення кіберпотенціалу країни за допомогою створення Оборонної кібероперативної групи (Defence Cyber Operation Group), а також включення питань кібербезпеки в спільну оборону політику Великобританії [25]. Також був створенний Національний центр кібербезпеки (NCSC), розташований в Лондоні з регіональним підрозділом в Челтенхем. У Центра чотири основних обов'язки: дослідження і отримання знань про кіберсередовище і його безпеки, поширення цієї інформації і використання експертних знань для визначення і усунення системних вразливостей; зниження кіберризиків для громадян і державних органів Великобританії за допомогою надання консультацій і проведення навчань з кібербезпеки; реагування на кіберінциденти національного масштабу за допомогою підвищення координації зусиль уряду і правоохоронних органів; підвищення рівня можливостей щодо національної кібербезпеки [25].

В рамках реалізації Стратегії національної кібербезпеки на 2016-2021 роки уряд Великобританії сформував команду з 50 осіб, які пройшли ретельний відбір на здатність захистити країну від кібератак. Програма також передбачала створення Інституту досліджень в галузі кібербезпеки, який буде координувати роботу з розробки захисту для комп'ютерів і мобільних гаджетів. Крім того, надавалася фінансова допомога стартапам, які працюють над проблемою кібербезпеки [18].

В 2017 році країна представила Стратегію розвитку цифрових технологій (Digital Strategy) – документ включає сім напрямків за якими Великобританія має намір розвивати «провідну цифрову економіку» в світі. Одними з напрямків є: «цифровий сектор» – створення умов в країні як кращого місця, щоб почати і розвивати цифровий бізнес; «цифровий уряд» - підтримка Великобританії в якості світового лідера в обслуговуванні своїх громадян в мережі Інтернет; «кіберпростір» – створення в країні найбезпечнішого в світі місця, щоб жити і працювати онлайн. Для того, щоб громадяни не відчували не-

Isue DOI: 10.34132/pard

стачу в цифрових навичках, британський уряд надавав можливість безкоштовного навчання, до яких приєднався і приватний сектор, такі організації як Google, Lloyds Banking Group, Barclays [18].

31 січня 2020 року Великобританія вийшла зі складу Європейського Союзу – це викликало бурхливий сплеск в ЗМІ, оскільки до цього починаючи з референдуму 23 червня 2016 року, коли проголосували за вихід Сполученого Королівства з ЄС, в інформаційному середовищі почалося активне поширення інформації у вигляді «фейкових новин», «карикатур» та багатьох статей та інтерв'ю в друкованих та онлайн виданнях по всьому світу. Але, оскільки, Великобританія змогла побудувати гарне інформаційне середовище всередині країни, вихід з ЄС не повинен вплинути на цю складову [21].

Франція.

Країна, яка знаходиться на третьому місці серед лідируючих позицій – Франція з показником 60,4 %. Мета інформаційної політики цієї країни полягає у «реформуванні інформаційних магістралей, Е-ринку і банківської сфери, лібераізація комунікацій, реформування інформаційного законодавства, стимулювання наукових досліджень в області інформаційних продуктів, створення систем безпеки інформації і попередження комп'ютерних злочинів» [16].

В 2013 році та оновлений у 2015 році уряд Франції опублікував Національний план широкосмугового зв'язку (France Très Haut Débit). Відповідальними органами були: «на державному рівні – Міністерство економіки та фінансів, дій та державних рахунків (Ministère de l'Économie et des Finance, de l'Action et des Comptes publics); Цифрове агенство (L'Agence du numérique); французький регуляторний орган з питань електронної комунікації та пошти (Autorité de régulation des communication électroniques et des postes, arcep); Генеральна комісія з питань територіальної рівності (Commissariat Général à l'Egalité des Territoires) – яке діє як національне відомство з питань широкосмугової компетенції» [4].

Оприлюдненний 27 листопада 2018 року Закон ELAN про розвиток житла та цифрових технологій мав на меті сприяння цифровому переходу територій. Таким чином, уряд зробив цифрове покриття територій одним із своїх пріоритетів. Наступним кроком

був запуск системи 22 березня 2019 року «Цифрова згуртованість територій» (Cohésion Numérique des Territoires) [5].

Щодо забезпечення кібербезпеки у Франції, ще в 2015 році було прийнято Національну стратегію кібербезпеки, яка мала на меті супроводжувати цифровий перехід французького суспільства та вирішувати нові виклики зміни використання цифрових технологій та пов'язаних із цим загроз. Вона зосереджувалася на п'яти цілях: забезпечення національного суверенітету; забезпечення рішучої реакції на дії в кіберзлочинах; інформування громадськості; перетворення цифрової безпеки на конкурентну перевагу для представників французького бізнесу; підвищення голосу Франції на міжнародній арені [11]. З тих пір ця Стратегія була доповнена:

- «Міжнародна цифрова стратегія Франції» (2017 р.) – об'єднала всі стратегічні цілі, які країна просуває у цифровому полі, а саме управління, економіка та безпека;
- «Стратегічний огляд кіберзахисту» (2018 р.) – був доручений Генеральному секретаріату з питань оборони та національної безпеки (SGDSN), в цьому документі було викладено доктрину щодо управління кіберкризами;
- «Пакт про кібербезпеку» (2019 р.) – французький уряд підписав трирічний пакт про кібербезпеку з найбільшими в державі компаніями: «Airbus», «Dassault Aviation», «Thales», «Safran», «Ariane Group», «MBDA», «Naval Group» і «Nexter» [11].

Серед органів, що сприяють ефективному забезпеченню безпеки в інформаційному просторі можна віднести Французьку мережу та інформаційне агенство безпеки (The French Network and Information Security Agency), яка несе відповідальність за запобігання (у тому числі з нормативної точки зору) та реагування на IT-інциденти, що негативно впливають на певні організації, також організовує кризові навчання на національному рівні. Міністерство збройних сил Франції (The French Ministry for the Armed Forces) має місію забезпечувати захист мереж у випадку цифрової війни, в 2017 році було створено оперативну группу з кіберзахисту (COMCYBER) за наказом начальника штабу Збройних Сил. Роль Міністерства внутрішніх справ Франції (The France's Ministry of the Interior) полягає у боротьбі

Isue DOI: 10.34132/pard

бі з усіма формами кіберзлочинності проти національних інститутів та інтересів, економічно зацікавлених сторін та державних органів влади і окремих осіб [11].

Отже, проаналізувавши досвід країн, що є чи були країнами Європейського Союзу, можна прийти до висновку, що реалізація проекту щодо створення єдиного європейського інформаційного простору можлива лише за допомогою реалізації чіткого загальновизнаного алгоритму дій. А також завдяки реалізації стратегій та програм, які враховують гендерні та вікові аспекти для розвитку інформаційного середовища. Виокремивши три країни лідери за показниками розвитку використання мережі Інтернет серед яких: Німеччина, Великобританія та Франція, було проаналізовано на їх прикладі, як саме необхідно створювати модель інформаційної державної політики, які існують програми та стратегії для взаємодії держави та суспільства, а також рівень забезпечення країн нормативно-правовою базою, щодо кібербезпеки.

Висновки**.** Першочерговими завданнями України у сфері реалізації інформаційної політики є забезпечення конституційного права на одержання, поширення й зберігання інформації, на вільне вираження своїх поглядів на основі максимально ефективного використання для науково-технічного, культурного, соціального розвитку тих можливостей, які надають новітні засоби обміну інформацією, їх виробництво та просування на світовому рівні.

Час вимагає розроблення і вдосконалення таких нагальних питань, як розроблення проекту інформаційного кодексу, Стратегії державної (національної) політики України, формування, використання, зберігання й поширення національних інформаційних ресурсів, заходів спрямованих на підтримування вітчизняної індустрії програмного забезпечених, обміну інформацією в електронній формі, насамперед введення електронного документообігу, посилення стану інформаційної безпеки, захисту державних інформаційних ресурсів і персональних даних, створення єдиної системи стандартів, з Євросоюзом, узгодження нормативно-правової бази України з нормами і критеріями міжнародного права сертифікації.

Таким чином, ефективне імплементування в Україні досвіду ЄС можливий лише на основі комплексного підходу, що містить стратегічне бачення інформатизації суспільства й координується наявними соціально-економічними, політичними й культурними пріоритетами держави та міжнародною практикою.

Стаття надійшла до редакції: 03.04.20

THE EXPERIENCE OF EU COUNTRIES REGARDING THE DEVELOPMENT AND IMPLEMENTATION OF STATE INFORMATION POLICY MODELS

Mykhaylo Bagmet, Doctor of History, professor Black Sea National University of Petro Mohyla Mykolaiv, Ukraine

Anna Harkusha, Master of Public Administration, Documentator of the EU Information Center, Black Sea National University of Petro Mohyla Mykolaiv, Ukraine

The article is devoted to the experience of Germany, France, Italy, Spain, Poland, the Netherlands and other EU member states in the implementation of information and computer technologies in the modern globalization process. The role of Great Britain is also noted, although it has announced its withdrawal from the EU, but has made significant progress in developing the main political and legal aspects in the implementation of state information policy and information strategy, creation of public network information centers and development of information and communication technologies.

It is established that in the path of transformation and implementation of reforms, Ukraine should aim to create a competitive, information-developed state that implements effective state information policy both domestically and internationally. Because, information policy promotes contact between public authorities and the population, by involving them in socially important political decisions.

In general, a number of original works by both foreign and domestic scientists and practitioners have been devoted to the development of basic concepts and categories, to a comprehensive substantiation of the European model of EU information policy implementation by EU states.

Time requires the development and improvement of such urgent issues as the development of a draft information code, the Strategy of state (national) policy of Ukraine, the formation, use, storage and

dissemination of national information resources, measures to support the domestic software industry, information exchange in electronic form. introduction of electronic document management, strengthening the state of information security, protection of state information resources and personal data, creation of a single system of standards with the European Union, harmonization of the legal framework of Ukraine with the norms and criteria of international certification law.

Keywords: *state information policy, electronic world information policy, European Union, cybersecurity, models of state information policy, information policy centers.*

Received: 03.04.2020

References

1. Alliance for Cyber Security. – Retrieved from: https://www.tuvit.de/en/cyber-security/alliance-for-cyber-security-2352.htm [in English].

2. Audiovizualna polityka YeS. – Retrieved from: http://ec.europa.eu/comm/avpolicy/reg/index_en.htm [in Ukrainian].

3. Bryzhko, V. M., Tsybaliuk, V. S., Shvets, M. V., Koval, M. D. & Bazanov, Yu. K. (2006). E-maibutnie ta informatsiine pravo [E-future and information law]. (V. 2). K.: NDTsPI APrN [in Ukrainian].

4. Country information – France. – Retrieved from: https://ec.europa.eu/digital-single-market/en/country-information-france [in English].

5. Couverture numérique du territoire : les dispositions numériques de la loi elan décryptée. – Retrieved from: https://www.amenagement-numerique.gouv.fr/fr/actualite/20190605-loiELAN-voletnumerique [in French].

6. Deklaratsiia pryntsypiv «Pobudova informatsiinoho suspilstva – hlobalne zavdannia u novomu tysiacholitti» OON : Deklaratsiia, Mizhnarodnyi dokument vid 12.12.2003 r. № 995_s57. – Retrieved from: https://zakon.rada.gov.ua/laws/show/995_c57 [in Ukrainian].

7. Digital Agenda for Europe. – Retrieved from: http://europa.eu/legislation_summaries/information_society/si0016_en.htm [in English].

8. Digital Single Market. (2020). – Retrieved from: https://ec.europa.eu/digital-single-market/ [in English].

9. Federal Ministry of the Interior. Cyber Security Strategy for Germany. (2011). – Retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_ Germany.pdf?_blob=publicationFile [in English].

10. Flynn N. Modernising British Governent. – Retrieved from: https://academic.oup.com/pa/article-abstract/52/4/582/1589579?redirectedFrom=PDF [in English].

11. France and cyber security. – Retrieved from: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/ [in French].

12. Information Society Benchmarking Report. (2005). Retrieved from: http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/benchmarking_report_2005.pdf [in English].

13. Information Society Germany. Progress Report on the Federal Government's Action Programme. (2002). – Retrieved from: http://lincompany.kz/pdf/Germany/information_society_germany2002.pdf [in English].

14. Information Society Policy Formulation. – Retrieved from: https://studyres.com/doc/2029215/information-policy [in English].

15. Internet World Stats. – Retrieved from: https://www.internetworldstats.com/ [in English].

16. La France dévoile son plan de recherche en intelligence artificielle. (2018). – Retrieved from: http://www.lefigaro.fr/secteur/high-tech/2018/11/28/32001-20181128ARTFIG00163-la-france-devoile-son-plan-de-recherche-en-intelligence-artificielle.php [in French].

17. Lisbon European Council. Presidency Conclusions. (2000). – Retrieved from: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/-r1.en0.htm [in English].

18. Natsyonalnaia stratehyia kyberbezopasnosty 2016-2021. – Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643426/ National_Cyber_Security_Strategy_2016.pdf [in Russian].

19. Okinavska khartiia hlobalnoho informatsiinoho suspilstva Velykobrytaniia, Nimechchyna, Italiia [...] : Khartiia, Mizhnarodnyi dokument: vid 22.07.2000 r. № 998_163. – Retrieved from: https://zakon.rada.gov.ua/laws/show/998_163 [in Ukrainian].

20. Questions and Answers about the East StratCom Task Force. (2018). – Retrieved from: https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en [in English].

21. Shveiko Yu. V ES zapustyly systemu opoveshchenyia o dezynformatsy. – Retrieved from: https://www.dw.com/ru/ [in Russian].

22. Stackelberg F. Germany Prepares for Cyber War. New Security Learning. – Retrieved from: http://www.newsecuritylearning.com/index.php/feature/88-germanyprepares-for-a-cyber-war [in English].

23. Tuniska prohrama dlia informatsiinoho suspilstva. (2005). – Retrieved from: http://old.apitu.org.ua/wsis/tp [in Ukrainian].

24. Tuniske zoboviazannia. (2005). – Retrieved from: https://informationsociety.wordpress.com/basics/wsis_outcomes/tz/ [in Ukrainian].

25. UK Cyber Security Strategy: Statement on the Final Annual Report. (2016). – Retrieved from: https://www.gov.uk/government/speeches/uk-cyber-security-strategy-statementon-the-final-annual-report [in English].

26. Unsworth K. Information Policy: Global Issues and Opportunities for Engagement. – Retrieved from: https://asistdl.onlinelibrary.wiley.com/doi/pdf/10.1002/bult.2014.1720400512 [in English].

27. Vsesvitnii samit z pytan informatsiinoho suspilstva. – Retrieved from: https://nkrzi.gov.ua/index.php?r=site/index&pg=6&language=uk [in Ukrainian].

28. Zhenevskyi Plan dii. (2003). – Retrieved from: https://informationsociety.wordpress.com/basics/wsis_outcomes/pd/ [in Ukrainian].

Відомості про авторів / Information about the Authors

Багмет Михайло Олександрович: Чорноморський національний університет імені Петра Могили: вул. 68 Десантників 10, Миколаїв, 54003, Україна.

Mykhaylo Bagmet: Black Sea National University of Petro Mohyla: 68 Desantnykiv str. 10, Mykolaiv, 54003, Ukraine.

ORCID.ORG/ 000-0003-2386-4488

E-mail: mykhaylo.bagmet@gmail.com

Гаркуша Анна Михайлівна: Чорноморський національний університет імені Петра Могили: вул. 68 Десантників 10, Миколаїв, 54003, Україна.

Anna Harkusha: Black Sea National University of Petro Mohyla: 68 Desantnykiv str. 10, Mykolaiv, 54003, Ukraine.

E-mail: annagarckusha@outlook.com