Вісник Львівського університету. Серія філос.-політолог. студії. 2020. Випуск 33, с. 167–176
Visnuk of the Lviv University. Series Philos.-Political Studies. Issue 33, p. 167–176

УДК 327:[349:002.1-049.5](4-6ЄС)
DOI https://doi.org/10.30970/PPS.2020.33.22

МЕХАНІЗМИ ТА ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ЄС

Анастасія Хмель
Чорноморський національний університет імені Петра Могили,
факультет політичних наук,
кафедра міжнародних відносин та зовнішньої політики
вул. 68 Десантників, 10, 54003, м. Миколаїв, Україна

Микита Білоусов
Чорноморський національний університет імені Петра Могили,
факультет політичних наук,
кафедра міжнародних відносин та зовнішньої політики
вул. 68 Десантників, 10, 54003, м. Миколаїв, Україна

Європейський Союз є впливовим інтеграційним утворенням, економічну базу та політичний вплив якого не можна заперечувати. XXI ст. принесло нові виклики, зокрема і у сфері відносин, яка виникла тільки наприкінці XX ст. – інформаційній. ЄС, не зважаючи на свою міць, виявився не зовсім готовим до викликів у ній, тому на порядок денний і постало питання правового забезпечення та механізмів захисту інформації.

Правове забезпечення захисту інформації у ЄС є одним із компонентів безпекової політики ЄС, а вдале її планування та реалізація згодом може призвести до становлення інформаційного суспільства ЄС. Тому тема є актуальною, важливою і часом складною, оскільки інколи важко провести лінію між тією інформацією, яка має бути доступною для широкого загалу, і тією, що має бути конфіденційною. Навіть тоді, коли інформація визнана конфіденційною і підлягає утаємненню, вона може стати відомою більш широкому колу осіб, ніж це передбачалося.

Для того, щоб убезпечити сферу кіберпростору від шахрайства, крадіжки даних, незаконного поширення даних, Європейський Союз на рівні організації запровадив кілька регламентів і постанов, реалізація яких призвела до створення відповідних механізмів, які забезпечують безпеку інформації. Досліджуючи наявну документальну базу, автори дійшли висновку, що, не зважаючи на загальноєвропейські норми регламентації безпеки інформації, усі країни ЄС знаходяться в різних групах по забезпеченню безпеки і всі мають різний рівень захищеності.

ЄС продовжує тенденцію на зближення норм щодо захисту персональних даних, фактично перейшовши до уніфікації правового регулювання у цій сфері. Що ж до механізмів забезпечення безпеки інформації, зокрема і захисту персональних даних, то у 2016 році було прийнято «Загальний регламент щодо захисту даних», який має пряму дію і який замінив Директиву ЄС щодо захисту даних 95/46/ЄС. Він покликаний захистити права фізичних осіб щодо обробки персональних даних усіма компаніями, які пропонують свої послуги на європейському ринку. У 2017 році ЄК внесено також проект Регламенту про повагу до приватного життя та захист персональних даних в електронних комунікаціях. Ці документи складають основу правового регулювання захисту інформації у ЄС.

Ключові слова: ЄС, захист інформації та особистих даних, механізми захисту інформації, конфіденційність, DPO.

Вступ. Для України термін «інформаційна безпека», одним із елементів якої є захист інформації, є украй актуальним, адже однією з важливих причин подій на Сході України (створення терористичних організацій «ДНР» і «ЛНР» та російсько-українську війну) вва-

жають програш України в інформаційній війні, яку розпочала Російська Федерація ще на початку 2000-х років. Тому для більшості українців інформаційна безпека – це про суверенітет і незалежність України в тих кордонах, які ми мали на початок 2014 року. Але й для Європейського Союзу (далі – ЄС) у XXI ст. інформаційна безпека має важливе значення, оскільки вона зав'язана на безпеці держави, кожного окремого громадянина, безпеці ЄС як організації і дотриманні прав і свобод людини. Усі ці складники передбачає ЄС у принципах інформаційної безпеки та реалізує в зазначеному напрямі. Приклад ЄС для нашої країни може стати значущим, оскільки успішність ЄС у зазначеному напрямі доводить вдале подолання інформаційних небезпек.

ЄС є унікальним видом інтеграційного об'єднання держав. Вступ 1 грудня 2009 року у силу Лісабонського договору розширив повноваження ЄС. Вироблені в ЄС підходи до забезпечення інформаційної безпеки, які відображають узгоджену волю держав-членів та інституцій ЄС, можна розглядати як європейські рамкові стандарти у цій сфері, що можуть успішно застосовуватися різними країнами з урахуванням їх адаптації до особливостей національних правових систем і соціокультурної специфіки. Актуальність дослідження підтверджується і тим фактом, що системне вивчення основних принципів інформаційної безпеки в ЄС у вітчизняній історіографії майже відсутнє, тому рівень дослідження цієї проблеми нині залишається недостатнім.

Метою роботи є дослідження, аналіз та висвітлення основних механізмів і правового забезпечення захисту інформації у ЄС.

Методологія та методи дослідження. Для досягнення поставленої в роботі мети використані принцип об'єктивності, історизму, термінологічний принцип, системний підхід. Термінологічний принцип дав змогу з'ясувати сутність понять, якими ми оперували в дослідженні. Він є базовим для визначення понятійно-категоріального апарату роботи, зокрема для визначення поняття «інформаційна безпека». Комплексне дослідження було б не можливе без використання системного підходу, який дозволяє дослідити об'єкт роботи, враховуючи вплив як зовнішніх, так і внутрішніх факторів.

Результати дослідження. Зауважимо, що тема механізмів і правового забезпечення інформації у ЄС не надто досліджувана на теренах України. Більшість досліджень є загальними і стосуються здебільшого або просто інформаційної політики (А. Бангеманн, В. Брижко, В. Гафнер, Ю. Громов, В. Карпенко), або інформаційної безпеки ЄС (Є. Макаренко, Ю. Куришева, А. Хмель, Д. Біляєв, О. Юдін). Серед закордонних дослідників можна назвати М. Мінгеса, Шеріфа Хасема (Єгипет), Г. Почепцова (Росія), М. Сейсана, Х. Норлен (дослідники із ЄС, які готують звіт Європейської Комісії (далі – ЄК) щодо стану кібербезпеки в країнах ЄС) [15]. Як джерельну базу автори використовували нормативну базу ЄС (звіти й рішення ЄК).

З початку активних дискусій середини 1990-х років щодо розвитку інформаційного суспільства в ЄС часто порушувалося питання про сучасні ризики і загрози, які призводили до вироблення відповідних політико-правових інструментів протидії ним. Питання гарантування безпеки інформаційного суспільства піддавалися пильній увазі. Активна діяльність інститутів ЄС у цій сфері здійснювалася насамперед в рамках першої (Європейське Співтовариство) і третьої опори (співробітництво поліції і судів у кримінально-правовій сфері). У зв'язку зі вступом у дію 1 грудня 2009 року Лісабонської угоди була ліквідована система трьох опор і скасоване Європейське Співтовариство, повноправним наступником якого став ЄС. Подальший розвиток законодавства ЄС у сфері забезпечення інформаційної безпеки проводився в рамках єдиної системи правового регулювання ЄС (за винятком сфери загальної зовнішньої політики і політики безпеки) [5, с. 191–192].

Значення стабільної інформаційної політики та захисту інформації є важливим елементом для зниження конфліктності між суспільними групами сучасної держави. К. Шапранова зазначає, що країни, які повністю не розуміють значення реінтеграції та її механізмів, стимулювання ідентичності у суспільстві, поступово втрачають своє значення й на міжнародній арені. У таких країнах автоматично з'являються проблеми фрагментації, а історично зумовлені регіональні, етнічні чи релігійно-конфесійні відмінності починають переходити в режим конфронтації. Нині перед європейськими країнами постала необхідність переходу до нової суспільно-політичної моделі. Пріоритет у цьому належить інформаційній політиці держави та її підтримці з боку національних ЗМІ, оскільки формування вдалого інформаційного поля сприятиме зменшенню впливу з боку іноземних джерел [8, с. 256–257].

Український дослідник О. Юдін зазначає, що розвиток інформаційно-комунікаційних технологій та інформатизації суспільства у ЄС входить до його найважливіших пріоритетів і реалізується насамперед у рамках політик в сфері інформаційного суспільства "Information society policy" («Політика інформаційного суспільства»), аудіовізуальної продукції та ЗМІ "Audiovisual and Media policy" («Аудіовізуальна та медіа-політика») [9, с. 111].

У березні 2000 року під час роботи Європейської Ради в Лісабоні глави держав і урядів членів ЄС прийняли Лісабонську стратегію [18], в якій була визначена мета перетворення ЄС у найбільш конкурентно спроможну економіку в світі. Вона будувалася на трьох стовпах: економічному (перехід до конкурентної, динамічної, заснованої на знаннях економіки); соціальному (модернізація європейської соціальної моделі за рахунок інвестицій у людський капітал і боротьби із соціальним відчуженням) та екологічному (збереження навколишнього середовища при економічному зростанні). Вирішення зазначених завдань передбачало розвиток і використання потенціалу новітніх ІКТ.

Для досягнення заявлених цілей Лісабонської стратегії були прийняті два важливих документи ЄС: Плани дій «Електронна Європа 2002: Інформаційне суспільство для всіх» [11] і «Електронна Європа 2005: Інформаційне суспільство для всіх» [12]. У першому з них проголошувалися три найважливіші мети: більш дешевий, швидкий, безпечний інтернет; інвестування в людський капітал і розвиток навичок; стимулювання використання інтернету в різних сферах життя суспільства. Другий план дій ставив на чільне місце цілепокладання інтересів користувачів, заради яких і розвиваються ІКТ. Він базувався на двох групах дій: стимулювання послуг, програм і контенту, які охоплюють сфери онлайн послуг держави і електронного бізнесу; розвиток інфраструктури широкосмугового зв'язку та вирішення питань інформаційної безпеки.

У реалізації Лісабонської стратегії були досягнуті помітні успіхи. За даними підготовленого у 2005 році Порівняльного звіту про розвиток інформаційного суспільства, завдяки широкому розповсюдженню ІКТ, що зв'язують різні пристрої на основі цифрового формату обміну даними, інформаційне суспільство та мас-медіа отримали можливості для швидкого зростання, стала реальністю цифрова конвергенція інформаційного суспільства та ЗМІ.

У підготовленому документі було сформульовано три пріоритети політики ЄС у сфері інформаційного суспільства і мас-медіа: завершення формування єдиного європейського інформаційного простору; збільшення інновацій та інвестицій у дослідження ІКТ; формування всеосяжного європейського інформаційного суспільства. До завдань включався розвиток цифрового телебачення, широкосмугового та бездротового доступу в інтернет [15]. Тому розвиток цифрової економіки є очевидним пріоритетом для ЄС.

Для створення стабільно функціонуючого Єдиного цифрового ринку однією із ключових умов є забезпечення кібербезпеки. Найважливішими сферами регулювання, яким ЄС приділяє особливу увагу, є захист персональних даних і забезпечення безпеки об'єктів критичної інфраструктури. Забезпечити реалізацію фундаментального права на захист персональних даних покликана масштабна реформа, спрямована на уніфікацію правового регулювання цієї галузі. У рамках цієї реформи передбачено оновлення ключових законодавчих актів ЄС. Для зміцнення безпеки об'єктів критичної інфраструктури ЄС використовує тактику гармонізації, приймаючи директиви, що встановлюють мінімальні загальні стандарти [15].

Загальна концепція інформаційної безпеки ЄС полягає у: 1) плані реагування на широкомасштабні кібератаки; 2) зміцненні глобальної стабільності через міжнародне співробітництво; 3) усуненні загроз онлайн-платформам і наданні їм можливості здійснювати позитивний внесок у суспільство; 4) підтримці малих і середніх підприємств у конкурентній боротьбі в цифровій економіці; 5) інвестуванні у використання штучного інтелекту.

Щодо свободи преси, то в ЄС ЗМІ самостійно вирішують, яку інформацію надати суспільству. Згідно з доповідями Міжнародного інституту преси, ФРН значиться як держава, яка підтримує сильну позицію вільної преси. Найважливішим принципом виголошено повагу до правди і об'єктивне інформування громадськості. Варто зазначити, що у ФРН виключається монопольне право на інформацію, а також забороняється укладати договори на виняткове право на отримання інформації про ту чи іншу подію.

Проголошення свободи слова не означає, що у ФРН відсутні обмеження в цій сфері. Вони закріплені законом і носять обов'язковий характер. Згідно з п. 2 ст. 5 Основного закону, свобода думок, інформації та друку може бути обмежена нормами загальних законів згідно з правовими нормами про охорону молоді та правом, що гарантує охорону особистої честі. Рішення про те, чи діють ЗМІ в рамках закону, знаходиться в компетенції незалежного Конституційного Суду. Порушенням законодавства є розголошення державної таємниці, заклик до насильницького захоплення влади і повалення державного ладу, розпалювання нетерпимості або національної ворожнечі, пропаганда війни. У випадках доведення провини журналістам і органам ЗМІ загрожує кримінальна, адміністративна або інша відповідальність [4, с. 294].

Щодо впливу ЄС і міжнародного співтовариства на розвиток німецьких ЗМІ, то правові основи їх діяльності насамперед базуються на таких міжнародних актах: Загальна декларація прав людини, прийнята ГА ООН 10 грудня 1948 року [20], Конвенція про захист прав людини і основоположних свобод (1950 рік) [10], Міжнародний пакт про громадянські і політичні права (1966 рік) [17], який набрав чинності 23 березня 1976 року, Гельсінський заключний акт (1975 рік) [16] та інші.

У цій сфері є і певні проблеми. Так, Європарламент розробив директиви для телебачення, які часом не стикуються з правовими нормами ФРН. «Проблеми виникають у зв'язку з тим, що ЄК розглядає радіо і телебачення насамперед із позицій економіки і з точки зору створення умов для вільного ринку послуг, у той час як згідно з німецьким правовим розумінням на перший план повинні висуватися соціальна і культурна функції ЗМІ в державі і суспільстві» [1; 2, с. 15–17].

Для усунення прогалин у наднаціональному регулюванні протидії атакам на об'єкти критичної інфраструктури в 2016 року була прийнята Директива про мережеву та інформаційну безпеку "The Directive on security of network and information systems" («Директива про безпеку мережевих та інформаційних систем» (NIS Directive) (далі – Директива). Так, Директива передбачає створення «Групи співпраці» для сприяння стратегічній співпраці

та обміну інформацією між державами-членами, в тому числі шляхом підготовки керівних документів для полегшення імплементації та реалізації положень Директиви, що стосуються операторів послуг життєзабезпечення [6, с. 267–268].

Найважливішим координуючим становищем Директиви можна вважати створення Мережі груп реагування на інциденти комп'ютерної безпеки (далі – CSIRTs). У мережу повинні входити відповідні підрозділи в кожній із держав-членів ЄС. Головними завданнями Європейського агентства з мережевої та інформаційної безпеки (далі – ENISA) [19], яке було створено у 2004 році, є: 1) збір інформації з метою аналізу потенційних інформаційних ризиків і повідомлення про них держав-учасниць; 2) покращення співробітництва на усіх рівнях з метою ознайомлення з досвідом у сфері мережевої та інформаційної безпеки; 3) відстеження розвитку стандартів у сфері безпеки послуг і продуктів, ознайомлення з ними країн-учасниць [3, с. 37–42].

Директива NIS повинна стати основою для загальноєвропейської співпраці з протидії серйозним інцидентам у цифровому просторі і сприяти поліпшенню умов для розвитку взаємодій у цифровому середовищі. Проектом Директиви, зокрема, передбачається, що країни-члени ЄС повинні будуть розробляти і затверджувати національні стратегії мережевої та інформаційної безпеки, створювати національні органи в цій сфері з відповідними фінансовими ресурсами для забезпечення їх роботи. Крім того, документ передбачає створення механізму співпраці між країнами-членами ЄС і ЄК для раннього попередження можливих ризиків у сфері кібербезпеки та забезпечення надійності інфраструктури [15].

Більш доцільно аналізувати результати реалізації більшості ініціатив варто тільки після вступу в силу регламентів і повної імплементації директив. Багато положень директив були сформульовані максимально компромісно. Тому можна очікувати, що практичне примирення положень європейського законодавства в галузі мережевої та інформаційної безпеки виявиться в державах-членах ЄС дуже різним. Створена в ЄС мережа органів і агентств може дозволити мінімізувати негативні наслідки суперечок, які виникають в силу наявних відмінностей, у тому числі і в технічних можливостях.

Одним зі складників безпеки інформації є кібербезпека, яку також досліджують європейські служби. Так, у 2017 році в ЄС підготували доповідь, у якій визначається рівень захищеності кіберпростору країн Європи, і зазначається, що його правове та технічне регулювання знаходиться на дуже високому рівні. Але рівень захищеності в інформаційній сфері у всіх країн різний [15]. Наприклад, Італія та Іспанія є представниками південної частини ЄС і не потрапляють за звітами до найбільш захищених країн (в інформаційній сфері), але в той же час за різними критеріями захищеності вони знаходяться у різних групах [7, с. 76].

ЄС має на меті посилити рівень інформаційної безпеки в тих країнах, де він на більш низькому рівні, але документи для реалізації та посилення інформаційної безпеки, вдосконалення механізмів забезпечення безпеки приймаються на загальноєвропейському рівні. Так, у ЄС 25 травня 2018 року набув чинності Закон про захист персональних даних – "General Data Protection Regulation" (далі – GDPR). GDPR встановлює принципи і вимоги до захисту персональних даних. Мета прийнятого закону – зміцнити права суб'єктів персональних даних. GDPR має на меті більш серйозну відповідальність за недотримання правил зберігання і обробки персональної інформації, встановлює глобальні стандарти захисту даних і регламентує їх транскордонну передачу [15].

Під дію нового регламенту потрапили усі європейські й іноземні компанії, які надають послуги на території ЄС або займаються обробкою великої кількості персональних даних суб'єктів, які перебувають на території ЄС (наприклад, інтернет-магазини, авіаком-

панії, банки). Основна вимога GDPR – забезпечення прозорості процесу обробки персональних даних.

Відповідно до закону вводяться два терміни – організація-контролер і організація-обробник. Контролер – це організація, яка сама ініціює процес обробки персональних даних своїх співробітників або клієнтів, відповідає за його належне виконання, забезпечує права суб'єктів і звітує перед наглядовим органом. Оброблювач – організація, яка обробляє особисті дані від імені контролера. При цьому контролер буде нести відповідальність за безпеку обробки персональних даних, у тому числі і за дії обробника. Організації одночасно можуть виконувати роль і контролера, і обробника. Наприклад, організація може бути оброблювачем персональних даних клієнтів і бути контролером персональних даних власних співробітників.

Новий закон покликаний підвищити захищеність персональної інформації суб'єктів, які перебувають на території ЄС. Для юридичних осіб відповідність із новим регламентом означає можливість розширення бізнесу і роботи з європейськими клієнтами, оскільки до організацій, які виконують вимоги нового закону, підвищується рівень довіри з боку клієнтів і контрагентів. Крім того, нині на всій території ЄС діє один регламент, а не кілька регіональних, як це було раніше, що більш зручно для закордонних компаній, які мають філії на території ЄС, оскільки вони можуть привести усі філії у відповідність до вимог одного законодавства, а не щодо положень у кожній окремій країні. Це стосується і тих випадків, коли філій немає у ЄС, але все одно ведеться обробка персональних даних суб'єктів європейських країн (наприклад, продаж авіаквитків) [15].

Цей закон передбачає величезні штрафи для компаній-порушників. Так, за порушення базових принципів обробки даних, порушення правил передачі персональних даних, ігнорування заборони наглядового органу на обробку даних, порушення прав суб'єкта та інших на компанію буде накладено штраф у розмірі 4% від загального річного обороту підприємства або 20 млн євро (залежно від того, яка сума виявиться більшою). Нині процедура накладення штрафів на неєвропейські компанії не регламентована.

Для підвищення довіри до цифрового середовища необхідно забезпечити захист персональних даних і захист об'єктів критичної інфраструктури. Зрозуміло, що збій у роботі об'єктів критичної інфраструктури може відбитися на безпеці і добробуті не тільки окремих держав, а й самого Європейського Союзу. Серйозні наслідки може мати втрата контролю над персональними даними. Нині уже сформувалася «тіньова» цифрова економіка, у якій ключовим товаром є дані.

Набирає обертів і інша тенденція. Суспільство переходить від використання окремих підключених до загальної мережі пристроїв до Інтернету речей, у якому об'єкти і люди будуть пов'язані між собою через постійний обмін інформацією (даними) про статус кожного елемента і стан навколишнього середовища. В подальшому цінність даних буде збільшуватися, а їх вразливість підвищуватися. Відбувається помітне зближення інтересів кіберзлочинності і організованої злочинності, які спираються на можливості тіньової цифрової економіки, з чого випливає висновок про те, що атаки на персональні дані будуть ставати все більш витонченими.

GDPR захищає такі типи конфіденційних даних: основна інформація про особу (ім'я, адреса, ідентифікаційні номери); веб-дані (місцезнаходження, IP-адреса, дані cookie, теги); дані про стан здоров'я, генетичні дані; біометричні дані; расові чи етнічні дані; політичні думки; сексуальна орієнтація. Діяльність GDPR впливає на будь-які компанії, які зберігають або обробляють особисту інформацію про громадян ЄС у межах держав ЄС, навіть якщо вони не мають ділової присутності в межах ЄС. Конкретними критеріями для

компаній, яких потрібно дотримуватися, є присутність у країні ЄС або відсутність в ЄС, але обробка персональних даних жителів ЄС [14].

Одним з елементів реалізацій регламенту стало створення посади працівника служби захисту даних (далі – DPO) GDPR. Вирішальним для юридичного обов'язку призначення посадової особи з питань захисту даних є не розмір компанії, а основні заходи з обробки, які визначаються як такі, що є важливими для досягнення цілей компанії. Якщо ці основні види діяльності складаються з обробки чутливих персональних даних у великих масштабах або такої форми обробки даних, яка є особливо далекосяжною для прав суб'єктів даних, то компанія повинна призначити DPO. Державні органи завжди повинні призначати DPO, за винятком судів, які діють у своїй судовій якості.

Законодавча норма про призначення посадової особи з питань захисту даних передбачає гнучкість для держав-членів. Вони можуть вільно вирішувати, чи повинна компанія призначати DPO відповідно до більш жорстких вимог (наприклад, Розділ 38 Федерального закону про захист даних Німеччини). Якщо таке зобов'язання існує згідно із Загальним розпорядженням про захист даних або більш конкретним національним законодавством, то група підприємств може призначити одну посадову особу з питань захисту даних. У такому випадку така особа повинна бути легко доступною для контролюючих органів, працівників і зовнішніх суб'єктів даних. Якщо жодного юридичного зобов'язання не існує, компанії можуть призначити DPO на добровільних засадах для сприяння дотриманню вимог щодо захисту даних (що, наприклад, рекомендується французьким органом із захисту даних CNIL).

Групи та компанії мають дві можливості виконати свій обов'язок призначити особу, яка займається захистом даних. Або вони називають працівника внутрішнім працівником з питань захисту даних, або призначають зовнішнього співробітника з питань захисту даних. Вибираючи таку особу, вони повинні переконатися, що внутрішня посадова особа з питань захисту даних не зазнає конфлікту інтересів через свою роботу в IT-відділі, департаменті кадрів або вищому керівництві, де їй доведеться контролювати себе [13].

До обов'язків DPO належить робота над дотриманням усіх відповідних законів про захист даних, моніторинг конкретних процесів, таких як оцінка впливу на захист даних, підвищення обізнаності працівників щодо захисту даних та їх відповідне навчання, співпраця із наглядовими органами. Працівник, який виконує обов'язки з питань захисту даних, не повинен бути звільнений або покараний через виконання ним своїх завдань. Незважаючи на його функції моніторингу, компанія залишається відповідальною за дотримання законів про захист даних. Тому вона зобов'язана залучати DPO до усіх питань щодо захисту персональних даних «належним чином і своєчасно». Умисне або необережне невизначення DPO, незважаючи на юридичне зобов'язання, є порушенням, що підлягає штрафуванню.

Висновки. Отже, у найближчі кілька років буде продовжена дискусія щодо Регламенту про повагу до приватного життя та захист персональних даних. Нині можна зазначити, що ЄС продовжує тенденцію на зближення норм щодо захисту персональних даних, фактично перейшовши до уніфікації правового регулювання в цій сфері. Пряма дія Загального регламенту щодо захисту даних має забезпечити високий рівень координації усіх держав. Не деталізованою поки залишається відповідь на питання про зовнішню реакцію на нове європейське законодавство в сфері захисту персональних даних. Цілком можливо, що саме підхід ЄС послугує основою для загальносвітової практики.

Одним із ключових завдань у розвитку цифрових відносин є захист персональних даних. У 2016 році в рамках масштабної зміни правового регулювання цієї сфери був при-

йнятий «Загальний регламент щодо захисту даних» (“General Data Protection Regulation”, GDPR), який замінив Директиву ЄС щодо захисту даних 95/46/ЄС. Цей регламент покликаний захистити права фізичних осіб щодо обробки персональних даних усіма компаніями, які пропонують свої послуги на європейському ринку. У 2017 році ЄК внесено проект Регламенту про повагу до приватного життя та захист персональних даних в електронних комунікаціях. Ці документи повинні закласти основи для регулювання захисту персональних даних у ЄС. При цьому за загальним правилом регламенти матимуть пряму дію в державах-членах ЄС без необхідності імплементації їхніх положень на рівні національного законодавства.

Очевидним стає прагнення до уніфікації правового регулювання цієї сфери на всій території ЄС. Беручи до уваги транскордонний характер передачі даних, частина положень Загального регламенту поширюється на осіб, кампанії яких засновані за межами ЄС. Нині не зрозуміло, чи будуть провідні торгові партнери ЄС адаптувати своє законодавство з урахуванням цих змін, але можливо Загальний регламент вплине на загальносвітовий порядок обробки персональних даних.

Важливим складником захисту інформації є захист персональних даних, який за Регламентом 2016 року реалізується, зокрема, і шляхом створення посади працівника служби захисту даних, до функцій якого входить робота над дотриманням усіх відповідних законів про захист даних, моніторинг конкретних процесів, таких як оцінка впливу на захист даних, підвищення обізнаності працівників щодо захисту даних та їх відповідне навчання, співпраця із наглядовими органами.

Список використаної літератури

1. Андреева М.В. К вопросу о правовой основе информационной политики ФРГ. *«Студенческий научный форум – 2016»*. 2016. URL: http://www.scienceforum.ru/2016/1833/22938.
2. Бангеманн А. Европа и мировое информационное общество. Рост, конкуренція, занятость, цели и пути в XXI веке. *Бюллетень Европейской комиссии*. *Приложение*. 1993. № 6. С. 5–32.
3. Куренда Л.Д. Окремі аспекти забезпечення інформаційної безпеки Європейського Союзу. *«Правова інформатика»*. 2011. №№ 3-4(31). С. 37–42.
4. Лабенська М. Інформаційна політика Європейського Союзу. *Південна Україна в міжнародних відносинах: історія та сучасність* : збірка тез. Миколаїв, 2013. С. 294–296.
5. Макаренко Є.А. Європейська інформаційна політика. К. : Наша культура і наука, 2000. 368 с.
6. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI. СПб : Наукоемкие технологии, 2017. 546 с.
7. Хмель А., Біляєв Д. Порівняння кібербезпекових можливостей Іспанії та Італії на сучасному етапі. *European Political and Law Discourse*. Volume 5. Issue 2. 2018. P. 75–81.
8. Шапранова К. Інформаційна політика як фактор реінтеграції суспільства. *Глобалізаційні виклики і багатостороння дипломатія* : збірник тез доповідей (18 березня 2015 року). К. : ДАУ при МЗС України, 2015. С. 256–258.
9. Юдін О.К. Інформаційна безпека держави : навчальний посібник. Х. : Консум, 2005. 576 с.
10. Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols №№ 11, 14. URL: https://rm.coe.int/1680063765.
11. Europe 2005: an information society for all // EUR-Lex. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2002:0263:FIN:EN:PDF.

12. Europe 2020. A European strategy for smart, sustainable and inclusive growth // European Union official web-site. URL: https://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf.
13. GDPR. Data Protection Officer. URL: https://gdpr-info.eu/issues/data-protection-officer/.
14. General Data Protection Regulation GDPR (EU) 2016/679. The European Data Protection Regulationis applicable as of May 25th, 2018. URL: https://gdpr-info.eu/.
15. Global Cyber security Index, year 2017 (International Telecommunication Union). 2018, March, 29. The Official website of the International Telecommunication Union. URL: http://handle.itu.int/11.1002/pub/80f875fa-en.
16. Helsinki Final Act // Organization for Security and Cooperation in Europe. URL: https://www.osce.org/helsinki-final-act.
17. International Covenanton Civil and Political Rights. URL: http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.
18. Presidency Conclusions. Lisabon European Council // European Council. URL: https://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/00100-r1.en0.htm.
19. The European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu/.
20. Universal Declaration of Human Rights. URL: http://www.un.org/en/universal-declaration-human-rights/.

MECHANISMS AND LEGAL PROTECTION OF INFORMATION IN THE EU

Anastasiia Khmel
Petro Mohyla Black Sea National University,
Faculty of Political Science,
International Relations and of Foreign Policy Department
68 Desantnykiv str., 10, 54003, Mykolaiv, Ukraine

Mykyta Bilousov
Petro Mohyla Black Sea National University,
Faculty of Political Science,
International Relations and of Foreign Policy Department
68 Desantnykiv str., 10, 54003, Mykolaiv, Ukraine

The European Union is an influential integration entity whose economic base and political impact can not be challenged. At the same time, the 21st century brought with it new challenges, including in the sphere of relations that took place only at the end of the 20th century – information sphere. Despite its power, the EU was not quite ready for challenges in the information sphere, so the issue or legal support and mechanisms for protecting information arose on the agenda.

The legal protection of information in the EU is one of the components of EU security and its successful planning and implementation can subsequently lead to the formation of the EU information society. Therefore, the topic is relevant, important and difficult at times, as it is sometimes difficult to draw a line between the information that should be accessible to the general public and that which must be kept confidential. At the same time, even when information is recognized as confidential and classified, it may become known to a wider range of persons than it was intended.

In order to protect the cyber space from fraud, theft and illegal dissemination of data, the European Union, at the organization level, has introduced several rules and regulations, the implementation of which has led to the creation of appropriate mechanisms to ensure the security of information. Examining the existing documentary base, the authors concluded that despite the pan-European norms of governing the security of information, all EU countries are indifferent security groups and all have different levels of security. The

EU continues the trend towards convergence of personal data protection standards, effectively moving to the unification of legal regulation in this area.

With regard to mechanisms for ensuring the security of information, including the protection of personal data, the "General Regulationon Data Protection" was adopted in 2016, which is directly applicable and replaces the EU Directive on Data Protection 95/46/EU. It is designed to protect the rights of individuals in the processing of personal data by all companies offering their services in the European market. In 2017, the European Commission also introduced a draft Regulation on respect for privacy and the protection of personal data in electronic communications. These documents form the basis of the legal regulation of information protection in the EU.

Key words: EU, information and personal data protection, information protection mechanisms, confidentiality, DPO.