Вісник Львівського університету. Серія філос.-політолог. студії. 2024. Випуск 54, с. 162–172
Visnyk of the Lviv University. Series Philos.-Political Studies. Issue 54, p. 162–172

УДК 327+316.256]:316.77-049.5ЄС
DOI https://doi.org/10.30970/PPS.2024.54.19

ПОЛІТИЧНЕ ПІДҐРУНТЯ ТА ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЄС

Микита Білоусов
Чорноморський національний університет імені Петра Могили,
факультет політичних наук, кафедра міжнародних відносин та зовнішньої політики
вул. 68 Десантників, 10, 54000, м. Миколаїв, Україна

У науковій статті досліджено політичне підґрунтя та інституційне забезпечення інформаційної безпеки ЄС протягом 2014–2024 рр.

Автор зауважує, що починаючи з 2014 р. у сфері інформаційної безпеки перед ЄС постали нові виклики. Але реакція ЄС на дії РФ, що становили потенційну гібридну загрозу, проявилася трохи запізно, зокрема, в інституційному плані.

Автор звертає увагу на те, що після вторгнення РФ на територію України у 2014 р., зокрема, після повномасштабного – 2022 р., ЄС почав виділяти нові виклики чи загрози у сфері інформаційної безпеки, адже цілеспрямовані атаки з боку Росії створювали широкомасштабний ризик з огляду на взаємопов'язаність інституцій ЄС. Слід зазначити, що після 24 лютого 2022 р. ЄС почав йти шляхом адаптації свого законодавства з урахуванням всіх змін породжених російською гібридною війною.

У статті автором проаналізована система нормативно-правових актів, які регулюють питання інформаційної безпеки ЄС, а саме: Стратегія кібербезпеки ЄС: відкритий, безпечний і захищений кіберпростір від 2013 р.; Директива ЄС щодо мережевої та інформаційної безпеки (NIS-1) від 2016 р.; Закон про захист персональних даних «General Data Protection Regulation» (GDPR) від 2018 р; Стратегічний порядок денний ЄС на 2019–2024 рр.; Директива про мережеву та інформаційну безпеку (NIS-2) від 2022 р.; Закон про дані ЄС від 2023 р.; Регламент про кібербезпеку, що встановлює заходи для високого загального рівня кібербезпеки в установах, органах, офісах і агентствах ЄС від 2024 р.

Автор приходить до висновку, що якщо ЄС зможе забезпечити безпечне та стійке державне управління у сфері цифрової трансформації, то лише за таких умов цей процес може бути успішним. Нові правила допоможуть суб'єктам ЄС запобігати та протистояти інформаційним загрозам та викликам, зокрема, кібератакам, кількість яких стрімко збільшилась після 24 лютого 2022 р.

Ключові слова: інформаційна безпека, кібербезпека, ЄС, Україна, РФ.

Постановка проблеми. Слід зазначити, що у XXI ст. для Європейського Союзу (далі – ЄС) інформаційна безпека має важливе значення, оскільки зав'язана на безпеці держави, кожного окремого громадянина, безпеці ЄС як організації і дотриманні прав і свобод людини. Усі ці складові передбачає ЄС у принципах інформаційної безпеки та реалізує в зазначеному напрямку [5, с. 168]. Інформаційна безпека ЄС є одним із п'яти стратегічних принципів Спільної політики безпеки і оборони (далі – СПБО) [23, с. 295–296].

Починаючи з 2014 р. перед ЄС постали нові виклики у сфері інформаційної безпеки. Але реакція ЄС на дії РФ, що становили потенційну гібридну загрозу, проявилася трохи запізно, зокрема в інституційному плані.

Однак, повномасштабне вторгнення РФ на територію України 24 лютого 2022 р., значно вплинуло на прийняття законодавчих ініціатив у сфері інформаційної безпеки ЄС, що, відповідно, обумовило зміну в політичному підґрунті та інституційному забезпеченні безпеки ЄС в інформаційній сфері.

Якщо до повномасштабного вторгнення розвиток законодавства ЄС в сфері забезпечення інформаційної безпеки проводився в рамках єдиної системи правового регулювання ЄС (за винятком сфери СПБО), то після 24 лютого 2022 р. ЄС почав йти шляхом адаптації свого законодавства з урахуванням всіх змін породжених російською гібридною війною та, відповідно, вимог загальносвітового порядку обробки персональних даних. Формування зовнішньої політики ЄС, що характеризується співпрацею з країнами-партнерами, певним чином зосереджується на запобіганні та вирішенні конфліктів, включаючи інформаційну безпеку, завдяки широкому та збалансованому підходу, який звертає увагу на кібердипломатію.

Актуальність обраної проблематики підтверджує той факт, що в умовах російської гібридної війни стала очевидною суттєва недостатність потенціалу інформаційної безпеки та кіберстійкості ЄС, адже цілеспрямовані атаки створюють широкомасштабний ризик з огляду на взаємопов'язаність інституцій ЄС. Протистояти інформаційним загрозам та кіберризикам в інформаційній сфері на сучасному етапі здатна ефективно організована система забезпечення інформаційної безпеки, яка має ґрунтуватися на взаємодії керівних органів ЄС, громадян та недержаних організацій.

Мета наукової статті полягає в здійсненні аналізу політичного підґрунтя та інституційного забезпечення інформаційної безпеки ЄС.

Під час написання статті автор використовував напрацювання зарубіжних науковців, зокрема, роботи європейських та американських дослідників можна поділити на дві групи. До першої групи належать наукові публікації, які стосуються саме політичного підґрунтя інформаційної безпеки ЄС. Це роботи М.Д. Кавелті [7], Г. Крістоу [9], Д. Фіотт [16], А.А. Матле [21], С. Меркадо-К'єркегор [22]. Друга група дослідників звернула свою увагу на інституційне забезпечення інформаційної безпеки ЄС: А. Монар, Ф. Асдеракі, С. Пайле-Кало [23], Дж. Рерл [27], Дж. Рінгхоф [28], К.Ф. Слівінскі [30], В. Вебер [32].

Необхідно відмітити, що обрана проблематика мало висвітлена у працях українських дослідників, що ще більше підсилює актуальність обраного дослідження. Зокрема, серед українських дослідників, які звертали увагу на інституційне забезпечення інформаційної безпеки ЄС загалом слід згадати: А. Хмель, М. Білоусова [5], О. Фурсай [4], Т. Перун [2], С. Трояна [3].

Виклад основного матеріалу дослідження. Щоб гарантувати мінімальний рівень інформаційної безпеки, починаючи з 1990-х рр. на рівні ЄС, був прийнятий комплекс відповідних правових актів у складі системи правового регулювання телекомунікацій і захисту інформації. Слід зазначити, що право на захист персональних даних включено Хартією ЄС про основні права 2007 р. в каталог основних прав громадян ЄС (ст. 8) [8].

Загалом система нормативно-правових актів, які регулюють питання інформаційної безпеки ЄС включає: Стратегію кібербезпеки ЄС: відкритий, безпечний і захищений кіберпростір [19] від 2013 р.; Директиву ЄС щодо мережевої та інформаційної безпеки (NIS) від 2016 р. [31]; Закон про захист персональних даних «General Data Protection Regulation» (GDPR) від 2018 р. [17].

Слід зазначити, що мета «Стратегії кібербезпеки ЄС: відкритий, надійний та безпечний кіберпростір» від 2013 р. – підвищення стійкості і нарощування потенціалу в області кібербезпеки держав-членів ЄС (посилення боротьби з кіберзлочинністю, формування ефективної інфраструктури забезпечення безпеки, розробка принципів міжнародної політики в області кібербезпеки). Задля досягнення цієї мети ЄС вирішив розробити політику кіберзахисту ЄС для захисту мереж у місіях і операціях СПБО, включаючи динамічне управління ризиками, покращений аналіз загроз та обмін інформацією. Зокрема, розробка

такої політики передбачала удосконалення навчання із кіберзахисту для військових, як в європейському, так і у багатонаціональному контексті, включаючи інтеграцію елементів кіберзахисту в існуючі формати навчань [9, с. 177].

25 травня 2018 р. в ЄС набув чинності «Закон про захист персональних даних» («General Data Protection Regulation» (GDPR) [17]. GDPR є найсуворішим законом про конфіденційність і безпеку в світі. Незважаючи на те, що Закон був розроблений і прийнятий ЄС, цей нормативно-правовий акт накладає зобов'язання на всі організації, якщо вони займаються збором даних, пов'язаних з громадянами в ЄС [33].

Слід зазначити, що інституційне забезпечення інформаційної безпеки ЄС координується Європейським центром боротьби з кіберзлочинністю, який є окремим органом при Європолі та був офіційно створений у 2013 р. [22, с. 433]. Центр координує національні органи щодо боротьби з кіберзлочинністю та займається навчанням національних експертів з кібербезпеки, діє як європейський координаційний центр у боротьбі з кіберзлочинністю [30, с. 477]. Його головна мета полягає в тому, щоб забезпечити скоординовану відповідь на кіберзлочинність, сприяти обміну інформацією, проводити судово-медичний аналіз, надавати розвідувальні дані та правову допомогу, надавати підтримку державам-членам у розслідуванні кіберзлочинів та сприяти зустрічам з експертами з кіберзлочинності [7, с. 312].

У Стратегічному порядку денному ЄС на 2019–2024 рр. боротьба з гібридними загрозами була визначена як один з пріоритетів [6]. Країни, які підписали цей документ погодились розвивати та зміцнювати спільну боротьбу з тероризмом і транскордонною злочинністю, покращуючи співпрацю та обмін інформацією, а також захищати європейське суспільство від зловмисної кіберактивності, гібридних загроз і дезінформації, що походять від ворожих державних і недержавних суб'єктів. Подолання таких загроз потребує комплексного підходу з більшою співпрацею, більшою координацією, більшими ресурсами та більшими технологічними можливостями [6].

9 листопада 2023 р. Європейський парламент ухвалив Закон про дані ЄС. Європейська комісія пояснила, що Закон про дані «забезпечить справедливість у цифровому середовищі, стимулюватиме конкурентний ринок даних, відкриє можливості для інновації, керовані даними, і зможе зробити дані більш доступними для всіх». 16 листопада 2023 р. Європейська рада із захисту даних випустила проект Керівних принципів 2/2023 щодо технічної сфери застосування ст. 5(3) Директиви про електронну конфіденційність. Стаття 5(3) Директиви про електронну конфіденційність вимагає отримання згоди перед збереженням або доступом до інформації на пристрої кінцевого користувача за допомогою файлів cookie або подібних технологій [25]. Депутати Європарламенту домоглися чіткого визначення комерційної таємниці та власників комерційної таємниці, щоб запобігти незаконній передачі даних і витоку даних до країн із слабкішими правилами захисту даних. Вони запевнили, що Закон про дані означає, що клієнти хмарних послуг матимуть право укладати контракти та уникати «прив'язки» до певного постачальника. Закон про дані отримав офіційне схвалення Європейської ради 27 листопада 2023 р., але на момент весни 2024 р. він не діє [14].

Центр має цілісну перспективу протидії кіберзлочинності і складається з трьох різних підрозділів: операції, стратегія та судово-медична експертиза [27, с. 101]. У 2019 р. Центр опублікував нову оцінку загрози організованої злочинності в Інтернеті (IOCTA) [18], яка стосується викликів, пов'язаних з новими технологіями, законодавством і терористичною діяльністю в кіберпросторі. Цей формальний щорічний огляд подій щодо кіберзлочинності також опосередковано стосується кібертероризму. IOCTA обговорює

терористичну діяльність у кіберпросторі, таку як пропаганда, вербування, радикалізація, фінансування та використання шифрування.

Європейський поліцейський коледж (CEPOL) є ще одним ключовим агентством ЄС, яке прагне у співпраці з Європолом розвивати та координувати навчання щодо пріоритетів безпеки та розслідування, а також ефективної боротьби з кіберзлочинністю [27, p. 154].

Спільна робоча група щодо боротьби з кіберзлочинністю (J-CAT) була створена у вересні 2014 р. та підтримує роботу Європейського центру боротьби з кіберзлочинністю. Її метою є боротьба з кіберзлочинами та сприяння транскордонним розслідуванням [20].

Слід зазначити, що починаючи з 2014 р., коли РФ незаконно анексувала український півострів Крим і почала війну на Сході України, крім одностайного засудження дій Росії, дві організації відповіли Спільною декларацією в липні 2016 р., яку підписали тодішній президент Європейської ради Дональд Туск, тодішній президент Європейської комісії Жан-Клод Юнкер і генеральний секретар НАТО Єнс Столтенберг.

Декларація визначила сім напрямків політики, які мають бути пріоритетними в інституційних відносинах: 1) захист від гібридних загроз та відповідь на них; 2) операції, в тому числі в морській сфері; 3) кібербезпека та захист; 4) обороноздатність; 5) оборонна промисловість і дослідження; 6) навчання (включаючи гібридні сценарії); 7) підвищення стійкості партнерів. Кілька місяців по тому було складено список із 42 конкретних заходів для виконання зобов'язань щодо більш тісної співпраці. Додавання 32 проектів до цього списку в 2017 р. мало підкреслити важливість, яку обидва органи надають спільним діям і співпраці.

Друга Спільна декларація, опублікована у 2018 р., по суті підтвердила зміст попереднього документа та розширила масштаби і глибину стратегічного партнерства між ЄС та НАТО. Заходи проти поширення дезінформації напередодні виборів були додані до переліку спільних зусиль [21].

Також було вжито важливих кроків для посилення кіберстійкості через постійну структуровану співпрацю (PESCO) – структуру для поглиблення оборонної співпраці між державами-членами ЄС. Десять проектів PESCO зосереджені на кіберсфері. Проект груп швидкого кібернетичного реагування PESCO та взаємної допомоги в кібербезпеці (CRRTs) був першим, який було активовано в оперативному контексті, коли його учасники були розгорнуті для допомоги Україні в її кіберзахисті, демонструючи здатність країн ЄС співпрацювати у відповідь на кіберзагрози в умовах кризи. ЄС повинен прискорити впровадження спільних кіберпідрозділів і вжити заходів для розвитку активної позиції кіберзахисту, що є суперечливим, оскільки включає деякі наступальні елементи [32, с. 3].

Вплив російської гібридної війни не обмежився Україною, але був також поширений на ЄС. У той час Литва, Латвія, Естонія та Швеція повідомили про численні випадки російських кампаній дезінформації, починаючи від вбивств політичних лідерів і закінчуючи підривом державних інституцій. Крім кібератак, РФ грала в обережну гру «розділяй і володарюй»: наприклад, на тлі серйозної боргової кризи в ЄС РФ оголосила про готовність скасувати загальне ембарго у відповідь на імпорт продовольства для Греції, Угорщини та Кіпру, які зіштовхнулися з важкою економічною битвою.

На стратегічному рівні на перший план вийшли недостатні витрати Європи та зростаюча залежність від такої американської парасольки безпеки. Фінансування РФ та онлайн-підтримка ультраправих політичних партій по всій Європі – Австрії, Італії, Франції, Угорщини та Німеччини – становили виклик, який був не лише стратегічним, а й системним.

Органи ЄС ставали все більш привабливими об'єктами для кіберзловмисників, причому кількість серйозних інцидентів зросла більш ніж у 10 разів між 2018 і 2021 рр. Саме тому, 20 червня 2019 р. Європейська Рада запросила інституції ЄС разом із державами-членами працювати над заходами для підвищення стійкості та покращення культури безпеки ЄС проти кібер- та гібридних загроз поза межами ЄС, а також краще захищати інформаційні та комунікаційні мережі ЄС, зокрема процеси прийняття рішень від шкідливих дій усіх видів [12, с. 29].

Регламент, що встановлює загальну структуру кібербезпеки для інституцій, органів, офісів і агенцій ЄС, є одним із заходів, передбачених у Стратегії кібербезпеки ЄС для цифрового десятиліття, представленій Комісією та Верховним представником ЄС із закордонних справ та політики безпеки в грудні 2020 р. для посилення колективної стійкості ЄС проти кіберзагроз.

Європейська комісія прийняла нову переглянуту Стратегію безпеки на період 2020-2025 рр., щоб зміцнити безпеку всіх держав-членів шляхом боротьби з тероризмом (політика боротьби з радикалізацією має зосереджуватися на ранньому виявленні, зміцненні стійкості та розмежуванні, а також як реабілітація та реінтеграція в суспільство), запобігання гібридним загрозам, кіберзлочинам і посилення кібербезпеки [15].

У своїх висновках від 22 березня 2021 р. щодо цієї стратегії Рада підкреслила, що кібербезпека є життєво важливою для функціонування державного управління та інституцій як на національному рівні, так і на рівні ЄС, а також для європейського суспільства та економіки в цілому.

Після повномасштабного вторгнення РФ на територію України 24 лютого 2022 р., інституції ЄС у травні 2022 р. досягли політичної згоди щодо переглянутої Директиви про мережеву та інформаційну безпеку (NIS-2), яка, зокрема, посилила правила кібербезпеки та запровадила суворіші наглядові заходи та вимоги до виконання.

Голова Ради та учасники переговорів у Європейському парламенті у травні 2022 р. досягли попередньої згоди щодо регламенту, спрямованого на забезпечення високого спільного рівня кібербезпеки в установах, органах, офісах та агентствах ЄС. Ці заходи були запропоновані Комісією в березні 2022 р. на тлі значного сплеску кількості складних кібератак, які зачіпають органи державного управління ЄС протягом останніх років. Новий регламент створив загальну структуру для всіх суб'єктів ЄС у сфері кібербезпеки та покращив їх стійкість і здатність реагувати на інциденти:

1. Щоб забезпечити високі загальні стандарти в інституціях, органах, офісах і агенціях ЄС, нові правила вимагають від них створення системи управління, управління ризиками та контролю в сфері кібербезпеки.

2. Усі суб'єкти ЄС також повинні будуть впровадити заходи кібербезпеки, спрямовані на усунення виявлених ризиків, проводити регулярні оцінки зрілості кібербезпеки та запровадити план кібербезпеки.

3. Згідно з новим регламентом, повноваження Групи реагування на комп'ютерні надзвичайні ситуації ЄС (CERT-EU) також будуть посилені, і вона буде перейменована на «Службу кібербезпеки для установ, органів, офісів і агентств Союзу», зберігаючи поточну абревіатуру.

4. CERT-EU консультуватиме всі інституції, органи, офіси та агентства ЄС і допомагатиме їм запобігати, виявляти і реагувати на інциденти. Він також виступатиме центром обміну інформацією та координації кібербезпеки, а також реагування на інциденти. Усі установи ЄС повинні будуть надавати несекретну інформацію про інциденти CERT-EU без зайвих затримок [13].

Крім того, новий регламент створить міжінституційну раду з кібербезпеки, яка керуватиме та контролюватиме виконання регламенту інституціями, органами, офісами та агентствами ЄС. Нова рада також контролюватиме реалізацію загальних пріоритетів і цілей CERT-EU і забезпечуватиме стратегічне керівництво.

Рада складатиметься з представників усіх установ та дорадчих органів ЄС, Європейського інвестиційного банку, Європейського центру компетенції з кібербезпеки, Агентства ЄС з кібербезпеки (ENISA), Європейського інспектора із захисту даних, Агентства ЄС з космічної програми, а також представників Мережі агенцій ЄС. Секретаріат правління забезпечуватиме Європейська комісія [10].

Парламент офіційно прийняв директиву NIS-2 10 листопада 2022 р. Щодо суперечливого питання про присвоєння авторства, ЄС досяг успіху 10 травня 2022 р., коли Союз і кілька міжнародних партнерів засудили – і тим самим приписали – зловмисну кібератаку, здійснену РФ проти України, яка була спрямована на супутникову мережу [29]. 15 вересня 2022 р. Комісія запропонувала нові кіберзаходи щодо забезпечення стійкості з метою зміцнення правил кібербезпеки для забезпечення більш безпечних апаратних та програмних продуктів.

10 листопада 2022 р. Високий представник/віце-президент (HR/VP) та Комісія висунули Спільне повідомлення про політику ЄС у сфері кіберзахисту, яка «спрямована на посилення можливостей ЄС у сфері кіберзахисту та посилення координації та співпраці між військовими та цивільними кіберспільнотами». Спільне повідомлення також, зокрема, прагне посилити управління кіберкризами в ЄС і зменшити стратегічну залежність у сфері кібертехнологій і посилити співпрацю з партнерами в кіберзахисті [11].

Новий Регламент про кібербезпеку, що встановлює заходи для високого загального рівня кібербезпеки в установах, органах, офісах і агентствах ЄС, набув чинності 7 січня 2024 р. Цей Регламент узгоджується з цілями політики Комісії, визначеними Стратегією безпеки ЄС і Стратегією ЄС з кібербезпеки, і забезпечує узгодженість з іншими законодавчими ініціативами у сфері, а саме: 1) Директива про заходи для високого спільного рівня кібербезпеки в Союзі («NIS-2»); 2) Закон про кібербезпеку; 3) Рекомендація Комісії щодо скоординованої реакції на широкомасштабні інциденти та кризи кібербезпеки.

У Регламенті встановлюються заходи щодо створення внутрішньої системи управління ризиками кібербезпеки, управління та контролю для кожного суб'єкта ЄС, а також створюється нова Міжвідомча рада з кібербезпеки для моніторингу та підтримки його впровадження суб'єктами Союзу. Він надає розширені повноваження Групи реагування на комп'ютерні надзвичайні ситуації для інституцій, органів, офісів і агентств ЄС (CERT-EU) як центру аналізу загроз, обміну інформацією та координації реагування на інциденти, центрального консультативного органу та постачальника послуг. Відповідно до свого мандату CERT-EU перейменовано на Службу кібербезпеки для установ, органів, офісів і агенцій Союзу, але зберігає коротку назву «CERT-EU» [24].

ЄС постійно вдосконалює свій потенціал і стратегію задля стримування та протидії кіберзагрозам або атакам. Щоб посилити та покращити співпрацю між правоохоронними органами та інструментами правосуддя, він використовує електронні докази для розслідування та приписування злочинних і терористичних дій у кіберпросторі через Європейський ордер про видачу та Європейський ордер про збереження [26]. Європейська судова кіберзлочинна мережа підтримується Євроюстом і сприяє співпраці між компетентними судовими органами.

Огляд політики та стратегій, прийнятих ЄС за останні два десятиліття, показує, що Брюссель нерішуче використовує термін кібертероризм, пов'язуючи його з певним типом дій: кіберзлочинність і кібербезпека.

Серед причин, по-перше, з огляду на те, що ЄС є інституцією економічного характеру, існувала невід'ємна тенденція позначати загрози як злочини. Таким чином, проблеми, пов'язані з комп'ютерною безпекою, зазвичай, позначаються як онлайн-злочинна діяльність, комп'ютерні та інформаційні системи і злочини у сфері високих технологій.

По-друге, технічне визначення кібератак залишається складним завданням. Тому виявити мотиви кібератаки та охарактеризувати її як терористичну атаку все ще є складним завданням.

По-третє, політичне приписування кібератаки терористу, а не злочинній групі, піднімає питання політичної легітимації. Брюссель не бажає пропонувати таку легітимізацію, тому утримується від позначення таких дій кібертерористичними.

Тим не менш, ЄС не байдужий до викликів безпеці, які кібертероризм представляє для своїх держав-членів. Зокрема, політика ЄС щодо кібербезпеки стосується діяльності, пов'язаної з тероризмом, у кіберпросторі, як-от радикалізація, вербування, пропаганда та фінансування. Проте ЄС значно виграє від гармонізації законодавства і процедур розслідування, судового переслідування та криміналізації цих дій. Крім того, у рамках зусиль зі зміцнення своєї культури кібербезпеки ЄС має посилити співпрацю між своїми державами-членами та з відповідними міжнародними організаціями. Нарешті, протистояння кіберзагрозам залежить від обміну інформацією, передового досвіду, а також освіти та навчання.

Війна Росії проти України, підкреслила також важливу роль космосу. Якщо космічний потенціал Європи буде підірваний, то здатність ЄС забезпечувати безпеку та захист своїх громадян буде піддана серйозному випробуванню. Слід зазначити, що на початку лютого 2022 р., напередодні повномасшбатного вторгнення РФ, російські хакери атакували систему "ViaSat", перервавши Інтернет-послуги в Україні. Наслідком цієї кібератаки стали перебої у зв'язку між користувачами, державними органами та підприємствами України, зокрема, атака завдала шкоди декільком країнам-членам ЄС (Польщі та Франції) [1].

Як відомо, ЄС може похвалитися автономними космічними можливостями, які допомагають у глобальному позиціонуванні ("Galileo") і моніторингу ("Copernicus"). Через Європейський оборонний фонд і постійне структуроване співробітництво (PESCO) ЄС також працює над заповненням прогалин у своїх можливостях космічної оборони. Нарешті, такі організації, як Супутниковий центр ЄС ("SatCen"), продовжують надавати цінні дані геопросторової розвідки для ЄС та його партнерів, у тому числі для України [16, с. 86–87].

Щоб протистояти російському впливу на технологічну сферу, ЄС має будувати цифрові альянси з країнами-однодумцями. ЄС має прагнути до більшого зближення зі США та іншими західними союзниками та запропонувати глобальному Півдню привабливий альтернативний шлях до цифрового розвитку.

Війна в Україні вже показала, що великі цифрові компанії та громадянське суспільство є важливими акторами міжнародної політики. Значна частина рішень щодо боротьби з російською дезінформацією в ЄС, Україні та РФ була покладена на приватні компанії та неурядові організації через відсутність регулювання модерації контенту. У відповідь на громадський тиск, який часто спричиняють представники громадянського суспільства, великі західні технологічні компанії фактично запровадили власні санкції проти РФ, зупинивши послуги та продажі в РФ навіть у регіонах, навмисно виключених із режимів урядових санкцій. Щоб гарантувати, що цілі зовнішньої політики Європи не будуть підірвані діями приватного сектору та громадянського суспільства, важливо, щоб ЄС постійно співпрацював із цими суб'єктами в питаннях цифрової дипломатії [28].

Висновки. Підсумовуючи, варто зазначити, що в умовах російської гібридної війни, міжінституційний підхід дозволить суб'єктам ЄС розробити свої заходи з посилення інформаційної безпеки, включаючи кібербезпеку та відповіді на кіберзагрози і потенційні атаки. У своїй резолюції від березня 2021 р. Рада ЄС наголосила на важливості надійної та послідовної системи безпеки для захисту всього персоналу ЄС, даних, комунікаційних мереж, інформаційних систем і процесів прийняття рішень. Цього можна досягти лише шляхом посилення стійкості та покращення культури безпеки інституцій, органів, офісів та агентств ЄС.

Цифрова трансформація може бути успішною, лише якщо ЄС зможе забезпечити безпечне та стійке державне управління в цьому процесі. Нові правила допоможуть суб'єктам ЄС запобігати та протистояти кібератакам, які стали частими за останні кілька років. Усі суб'єкти ЄС взаємопов'язані, і в цьому ланцюзі не повинно бути слабкої ланки.

У сучасних політичних умовах породжених російською гібридною війною, ЄС також досяг значного прогресу в протидії кіберзагрозам. Наприклад, у травні 2022 р. Рада схвалила висновки щодо розвитку кіберпозиції ЄС, метою яких є висвітлення рішучості ЄС надати відповідь суб'єктам загрози, які прагнуть позбавити ЄС безпечного та відкритого доступу до кіберпростору та вплинути на його інтереси. Також у травні 2022 р. інституції ЄС досягли політичної згоди щодо переглянутої Директиви про мережеву та інформаційну безпеку (NIS-2), яка, зокрема, посилить правила кібербезпеки та запровадить суворіші наглядові заходи та вимоги до виконання. Ключовими елементами пропозиції для всіх інституцій, органів, офісів та агентств ЄС є наступні: 1) мати структуру управління, управління ризиками та контролю у сфері кібербезпеки; 2) проводити регулярні оцінки зрілості; 3) впроваджувати заходи кібербезпеки для усунення виявлених ризиків; 4) розробити план покращення кібербезпеки; 5) негайно надсилати інформацію про інцидент із CERT-EU.

Важливою подією в інституційному забезпеченні інформаційної безпеки ЄС стало те, що 9 листопада 2023 р. – Європейський парламент ухвалив текст Закону про європейські дані. Закон про дані ЄС також підтримує цифрову трансформацію державних послуг і запровадження спільної європейської цифрової ідентичності, яка оптимізує транскордонні цифрові транзакції та послуги, водночас захищаючись комплексною структурою європейських стандартів і вказівок.

Усе це означає, що ЄС почав грати в глобальну технологічну гру. Війна в Україні сприяє цьому процесу Стратегії ЄС у сфері інформаційної безпеки. Російсько-українська війна стала прискорювачем існуючих тенденцій і викликів, перетворивши технології на ще одне ключове поле битви. Інституції ЄС намагаються сформувати глобальні стандарти конфіденційності та захисту даних, цифрових платформ і штучного інтелекту відповідно до європейських цінностей, використовуючи привабливість і силу свого внутрішнього ринку.

Список використаної літератури

1. Бережанський І. За масштабною кібератакою на супутниковий інтернет в Україні стояла Росія – ЄС і Британія // ТСН.ua. 2022. 10 травня. URL: https://tsn.ua/ato/za-masshtabnoyu-kiberatakoyu-na-suputnikoviy-internet-v-ukrayini-stoyala-rosiya-yes-i-britaniya-2058739.html
2. Перун Т. Інформаційна безпека країн Європейського Союзу: проблеми та перспективи правового регулювання. Правові засади європейської та євроатлантичної інтеграції України: досягнення та перспективи: матеріали учасників ІІ заочної науковопрактичної конференції (Львів, 23 листопада 2018 р.). Львів, 2018. С. 140–143.

3. Троян С. С. Інформаційно-безпекова політика Європейського Союзу. Саміт-книга, 2019. С. 1–9. URL: https://er.nau.edu.ua/handle/NAU/43324
4. Фурсай О. Політика інформаційної безпеки Європейського Союзу. Літопис Волині. Всеукраїнський науковий часопис. 2024. С. 165–170. URL: http://litopys.volyn.ua/index.php/litopys/article/view/489/423
5. Хмель А., Білоусов М. Механізми та правове забезпечення захисту інформації в ЄС // Вісник Львівського університету. Серія філос.-політолог. студії. 2020. Випуск 33. С. 167-176; Хмель А. О. Боротьба із гібридними загрозами в ЄС (за нормативно-правовою базою Європейського Союзу). Acta de Historia & Politica: Saeculum XXI. Вип. 4. 2022. С. 91–101.
6. A new strategic agenda for the EU (2019–2024) // European Council. URL: https://www.consilium.europa.eu/en/eu-strategic-agenda-2019-2024/
7. Cavelty M. D. Europe's cyber-power', European Politics and Society. Vol. 19. № 3. January, 2018. P. 304-320. URL: https://www.tandfonline.com/doi/full/10.1080/23745118.201 8.1430718
8. Charter of fundamental rights of the European Union // European Parliament: official web-site. URL: https://www.europarl.europa.eu/charter/pdf/text_en.pdf
9. Christou G. Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy New Security Challenges. Springer, 2016. 222 p.
10. Commission welcomes political agreement on new rules to boost cybersecurity in EU institutions, bodies, offices and agencies. 2023. 26 of June. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3483
11. Cyber Defence: EU boosts action against cyber threats // European Commission. 10 of November. 2022. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6642
12. Cyber threats // European Parliamentary Research Service. December, 2022. P. 29–30.
13. Cybersecurity at the EU institutions, bodies, offices and agencies: Council and Parliament reach provisional agreement. 2023. 26 of June. URL: https://www.consilium.europa.eu/en/press/press-releases/2023/06/26/cybersecurity-at-the-eu-institutions-bodies-offices-and-agencies-council-and-parliament-reach-provisional-agreement/
14. European Parliament approves EU Data Act // European Parliament. 2023. URL: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0385_EN.html
15. EU Security Union Strategy: connecting the dots in a new security ecosystem // European Commission. 24 of July. 2020. URL: https://ec.europa.eu/commission/presscorner/ detail/en/IP_20_1379
16. Fiott D. Rethinking the EU's Approach to Space: The Case of Security and Defence // Facing war: rethinking Europe's security and defence edited by Serena Giusti and Giovanni Grevi introduction by Paolo Magri. Institute for International Political Studies. 2022. P. 86–87.
17. General Data Protection Regulation // EU GDPR: official web-site. URL: https://gdpr-info.eu/
18. Internet Organized Crime Threat Assessment (IOCTA) // Europol. 9 of October. 2019. URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organisedcrime-threat-assessment-iocta-2019
19. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace // European Commission. 7 of February. 2013. P. 3. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/ PDF/?uri=CELEX:5201 3JC0001&from=EN

20. Joint Cybercrime Action Taskforce (J-CAT) // Europol. URL: https://www.europol.europa.eu/ activities-services/services-support/joint-cybercrime-action-taskforce
21. Matlé A. A. New Burden-Sharing Formula in the Making? How the EU and NATO Can Organize Security Together. 2023. 27 of June. URL: https://dgap.org/en/research/publications/new-burden-sharing-formula-making
22. Mercado-Kierkegaard S. 'EU Tackles Cybercrime', in Cyber Warfare and Cyberterrorism. IGI Global Publisher of Timely Knowlegde. January, 2007. P. 431–438. URL: https://www.europol.europa.eu/abouteuropol/european-cybercrime-centre-ec3
23. Monár A., Fiott D., Asderaki F., Paile-Calo S. Challenges of the Common Security and Defence Policy. ESDC 2nd Summer University Book. Luxembourg: Publications Office of the European Union. 314 p.
24. New rules to boost cybersecurity of the EU institutions enter into force // European Commission. 2024. 8 of January. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6782
25. Parliament backs plans for better access to, and use of, data // European Parliament. 2023. URL: https://www.europarl.europa.eu/news/en/press-room/20231106IPR09025/parliament-backs-plans-for-better-access-to-and-use-of-data
26. Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters // European Commission. 17 of April. 2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=PT
27. Rehrl J. Handbook on Cybersecurity: the Common Security and Defence Policy of the European Union. Vienna: Federal Ministry Republic of Austria, Luxembourg Publications Office of the European Union, 2018. 232 p.
28. Ringhof J. The geopolitics of technology: How the EU can become a global player. 2022. 17 of May. URL: https://ecfr.eu/publication/the-geopolitics-of-technology-how-the-eu-can-become-a-global-player/
29. Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the EU // Council of the European Union. 10 of May. 2022. URL: https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/
30. Sliwinski K. F. Moving beyond the European Union's Weakness as a Cybersecurity Agent // Contemporary Security Policy 35. № 3. September 2014. P. 468-486. URL: https://www.tandfonline.com/doi/full/10.1080/13523260.2014.959261
31. Special Eurobarometer 464a Report: Europeans' attitudes towards cyber security // European Commission. September 2017. URL: https://ec.europa.eu/commfrontofce/publicopinion/index.cfm/ResultDoc/download/DocumentKy/79735
32. Weber V. Rethinking European Cyber Defence Policy: Towards a Defence Superiority Doctrine // German Council on Foreign Relations. 8 of April. 2022. 11 p.
33. What is GDPR, the EU's new data protection law? // EU GDPR: official web-site. URL: https://gdpr.eu/what-is-gdpr/

THE POLITICAL FRAMEWORK AND INSTITUTIONAL SUPPORT FOR EU INFORMATION SECURITY

Mykyta Bilousov
Petro Mohyla Black Sea National University,
Faculty of Political Sciences,
Department of International Relations and Foreign Policy
68 Desantnykiv str., 10, 54000, Mykolaiv, Ukraine

The scientific article examines the political framework and institutional support for EU information security during 2014-2024.

The author notes that since 2014, new challenges have arisen for the EU in the sphere of information security. But the EU's reaction to the actions of the Russian Federation, which posed a potential hybrid threat, appeared somewhat late, in particular in institutional terms.

The author draws attention to the fact that after the Russian invasion of Ukraine in 2014, in particular after a full-scale one in 2022, the EU began to highlight new challenges or threats in the field of information security, because targeted attacks from Russia created a large-scale risk given the interconnectedness EU institutions. It should be noted that after February 24, 2022, the EU began to follow the path of adapting its legislation taking into account all the changes generated by the Russian hybrid war.

In the article, the author analyzed the system of regulations governing EU information security issues, namely: EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace (2013); EU Network and Information Security Directive (NIS-1) (2016); General Data Protection Regulation (GDPR) (2018); EU Strategic Agenda for 2019–2024; EU Network and Information Security Directive (NIS-2) (2022); The Eropean Data Act (2023); the Cybersecurity Regulation establishing measures for a high overall level of cybersecurity in EU institutions, bodies, offices and agencies starting from 2024.

The author comes to the conclusion that if the EU can ensure safe and sustainable public administration in the field of digital transformation, then only under such conditions can this process be successful. The new rules will help EU entities prevent and counter information threats and challenges, in particular cyber attacks, the number of which has increased rapidly since February 24, 2022.

Key words: information security, cybersecurity, EU, Ukraine, the Russian Federation.