УДК [1:[316.774:004.056]](4)
DOI: https://doi.org/10.21564/2663-5704.66.337888

Прудникова Олена Вікторівна, доктор філософських наук, професор, професор кафедри культурології, Національний юридичний університет імені Ярослава Мудрого, м. Харків, Україна
e-mail: elenvikprud@ukr.net
ORCID ID: 0000-0003-4610-908X

ІНФОРМАЦІЙНА БЕЗПЕКА ЄВРОПЕЙСЬКОГО СОЮЗУ: ВИКЛИКИ І ТЕНДЕНЦІЇ

У статті проаналізовано виклики та загрози інформаційній безпеці ЄС, що постали в сьогоденні. Розкрито діяльність європейських інституцій, які опікуються проблемами інформаційної безпеки, та законодавчу базу в цій сфері. Досліджено основні напрями протидії інформаційним викликам та загрозам, які реалізуються керівництвом Європейського Союзу. Охарактеризовано особливості європейської стратегії з кібербезпеки.

Ключові слова: *інформаційна безпека, кібербезпека, ЄС, інформаційна приватність, інформаційний простір, права і свободи людини, Інтернет-мережа.*

Постановка проблеми. Інформаційна безпека у XXI ст. є ключовим аспектом існування країн та державних об'єднань. Зокрема, Європейський Союз на тлі розгортання агресивних дій РФ у формі гібридних, інформаційних, мережевих і традиційних війн стикнувся з новими загрозами й викликами у сфері безпеки, у тому числі інформаційній. Характер таких загроз зумовлений внутрішніми й зовнішніми чинниками – ціннісно-політична неоднорідність європейських країн, наявність у ЄС політичних лідерів та громадян – симпатиків РФ, активна розвідувально-підривна діяльність російських спецслужб, яка спрямована на стимулювання конфліктів на теренах Європи та розпад ЄС. У контексті вітчизняних реалій, варто підкреслити, що рівень інформаційної безпеки ЄС опосередковано впливає на загальну безпекову ситуацію в Україні, яка є стратегічним партнером об'єднання. У зв'язку з вищенаведеним, актуальність дослідження інформаційної безпеки Європейського Союзу не викликає сумнівів.

Аналіз останніх досліджень і публікацій. Для обґрунтування ключових ідей і гіпотез дослідження ми спиралися на наукові праці низки фахівців. Зокрема, Я. Швечикова визначила таку негативну рису європейського простору, як фрагментація, що деструктивно впливає на безпекові процеси, у тому

числі в інформаційній сфері [1]. О. Фурсай проаналізувала законодавчу базу ЄС щодо протидії загрозам інформаційній безпеці та охарактеризувала їхню дієвість [2]. Натомість С. Троян дослідив створені ЄС інституції для посилення підвалин інформаційної безпеки [3], а Д. Гроза – діяльність агенції ENISA, яка визначила перелік ключових інформаційних загроз, що становлять значну небезпеку для Європейського Союзу [4].

Окремий блок наукових праць присвячено протидії інформаційним викликам та загрозам, спрямованим проти ЄС. Так, О. Запорожець [5] визначає комплекс першочергових дій, які мають бути реалізовані керівництвом Європейського Союзу, І. Милосердна [6] і С. Федонюк [7] аналізують основні напрями «Стратегії кібербезпеки для цифрового десятиліття», прийняту в ЄС.

Формулювання мети: дослідити сучасні виклики, загрози та тенденції у сфері інформаційної безпеки Європейського Союзу.

Виклад основного матеріалу. Протягом свого існування ЄС долає низку викликів і загроз, які час від часу виникають під впливом внутрішніх і зовнішніх чинників. Однією з таких загроз, яка активізувалась в останні роки, є агресивні інформаційні потоки, спрямовані проти єдності Європейського Союзу, його стабільного соціально-економічного та політичного розвитку. Інформаційні операції конкурентів та ворогів ЄС мають цілеспрямований характер, ставлячи за мету «активувати» культурну неоднорідність європейських країн, зменшити рівень інтегрованості та взаємодії держав, знизити ступінь політичної впливовості й економічної міцності об'єднання.

Аналізуючи характер таких загроз, Я. Швечикова зауважує, що на початку 90-х рр. XX ст. основним принципом для європейців постає зміцнення інтеграції. У контексті інформаційної безпеки цей принцип є одним із ключових, оскільки він міститься в основі механізму боротьби з основною загрозою для європейської спільноти – загрозою фрагментації. «Фрагментація в Європі неодмінно призводила до групування країн і створення системи балансу сил, а досвід демонстрував, що такий порядок у системі призводив до виникнення конфліктів, які не обмежувалися регіоном Європи. У свою чергу інтеграція в галузі безпеки (саме у її класичному розумінні) і зовнішньої політики за європейською моделлю є найвищою стадією інтеграції, а отже, завершує формування повноцінного комплексу безпеки» [1, с. 88].

Використовуючи інформаційно-комунікаційні засоби й технології, різноманітні деструктивні антиєвропейські сили здатні дестабілізувати ситуацію в будь-якому сегменті єдиного європейського простору. Для реалізації такої мети активно задіються як зовнішні канали впливу, так і відповідні суб'єкти, що перебувають на теренах ЄС, наприклад вихідці з неєвропейських країн,

які не поділяють європейські цінності й при цьому користуються благами, які надає перебування в Європейському Союзі.

У цьому сенсі, значною проблемою для ЄС, яка суттєво впливає на її безпекову ситуацію, в інформаційній сфері зокрема, є збільшення міграційних потоків різнорідного світоглядно-ціннісного характеру та посилення демографічної кризи серед місцевого населення. Збільшення кількості мігрантів у країнах ЄС, зниження рівня народжуваності у традиційних європейських сім'ях зумовлюють розмивання «європейської ідентичності» та загострюють необхідність для «корінних громадян» акцентуації на етнонаціональній ідентичності як підґрунтя для самозбереження. Міграційна проблема у свою чергу породжує низку інших супутніх проблем соціально-економічного, політико-правового, культурного і, врешті-решт, безпекового характеру, оскільки в Європі останнім часом почастішали випадки терористичної діяльності, яку здійснюють, наприклад, мусульмани. Отже, неоднорідний етнонаціональний склад ЄС із різноманітними духовно-ціннісними орієнтирами прямо та опосередковано впливає на стан інформаційної безпеки всього об'єднання.

З метою подолання загроз інформаційній безпеці Європейського Союзу, у 2001 р. Європейською комісією був розроблений базовий документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід» («Network and In formation Security: Proposal for A European Policy Approach»), у якому визначено пріоритети європейського розуміння проблем інформаційної безпеки. Варто підкреслити, що в документі використано поняття «мережева та інформаційна безпека», яка визначається «як здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, які становлять загрозу доступності, автентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через ці мережі і системи» [8].

З точки зору О. Фурсай, ЄС зміг створити достатньо дієвий захист у сфері інформаційної безпеки та інформаційної діяльності. Так, у рамках Європейського Союзу було розроблено та прийнято низку документів, що мають зміцнити у стратегічному вимірі інформаційну безпеку: «План боротьби з гібридними загрозами», «Зведення правил боротьби з дезінформацією», «План дій проти дезінформації». Також було утворено нові міжурядові та неурядові інституції, які спрямовані на проведення заходів інформаційної протидії та інформаційно-комунікаційного захисту. Ідеться про такі структури, як Центр передових технологій боротьби з гібридними загрозами SOMA, StratCom, яким вдалось викрити та нейтралізувати різноманітні дезінформаційні компанії спрямовані проти ЄС. «Європейський Союз досяг головної

мети – створив систему захисту європейських громадян та демократії від дезінформації. Інформаційна політика ЄС є позитивним чинником для зміцнення своїх позицій у світі, оскільки Європа підтримує дотримання миру, свобод, права націй на самовизначення, реалізацію спільної зовнішньої безпекової політики та формування єдиної системи європейського інформаційного простору» [2, с. 169].

З нашої точки зору, ЄС потребує подальшого вдосконалення системи інформаційної безпеки, оскільки загрози в цій сфері постійно модифікуються, масштабуються, ускладнюються, стаючи все більш непомітними для виявлення та нівелювання.

Важливо зазначити, що у 2004 р. було створено агенцію ЄС із питань мережевої та інформаційної безпеки (European Network and Information Security Agency – ENISA). Вона спеціалізується на діяльності, що спрямована на зміцнення інформаційної безпеки євроспільноти, країн ЄС та ділових кіл задля профілактики та реагування на проблемні ситуації в інформаційно-комунікаційній сфері. Як відомо, ENISA допомагає створити партнерські відносини між приватними і державними суб'єктами щодо обміну даними про кіберзлочини, а також між фінансово-економічним сектором і державними інституціями через Центри фінансової інформації та аналізу (FI–ISAC). «У 2008–2009 роках Агенцією створена структура / система, що допомагає зацікавленим сторонам краще ідентифікувати та розуміти поточні та майбутні ризики (Emerging and Future Risks), породжені новітніми інформаційними технологіями. Агенцією започаткований також Форум з безпекових питань та створені експертні групи, які дають оцінку та аналізують відповідні проблеми» [3, с. 29–30].

Отже, Європейський Союз посилює організаційну, технічну та правову спроможність у сфері інформаційної безпеки, намагаючись реагувати на нові виклики та загрози.

Вищезгадана агенція ENISA у 2023 р. визначила перелік ключових інформаційних загроз, що становлять значну небезпеку для Європейського Союзу:

1) програми-вимагачі – це різновид шкідливої атаки, коли кіберзлочинці зашифровують дані організації та вимагають плату за відновлення доступу. Про значну загрозу програм-вимагачів свідчать відповідні політичні ініціативи в ЄС;

2) шкідливе програмне забезпечення – використовується для виконання несанкціонованого доступу, який негативно впливатиме на конфіденційні дані, цілісність та доступність комп'ютерних систем. Фахівці ЄС констатують, що у 2023 р. кількість таких типів загроз збільшилася;

3) соціальна інженерія, яка вбирає значний спектр заходів, що спрямовані на використання людської помилки для доступу до необхідної інформації або відповідних послуг. Злочинці застосовують низку маніпулятивних форм для введення особи в оману для добровільного розголошення нею конфіденційної або секретної інформації. Для цього розсилаються відповідні шкідливі документи, електронні листи, рекламна продукція тощо;

4) порушення цілісності даних та їхній витік – це навмисна атака, що здійснюється злочинцем із метою отримання доступу до конфіденційної та захищеної інформації;

5) розподілені атаки типу «відмова в обслуговуванні» (DDoS), які заважають користувачеві мережі або системі отримувати вільний доступ до певної інформації або ресурсів. Науковці стверджують, що останніми роками (особливо з початком епідемії COVID-19 та агресії росії проти України) значно видозмінився характер загроз зі збільшенням спонсорованих певними країнами атак на критичну інфраструктуру інших держав;

6) інтернет-загрози – навмисні або ненавмисні перебої в Інтернет-мережі, електронних комунікаційних системах, які спричинюють його відключення. Такі проблеми Інтернет-мережі представлені такими різновидами, як від'єднання від мережі, відключення електроенергії, кібератаки, технічні проблеми, природні катаклізми та військові дії;

7) інформаційні маніпуляції – це незаконні дії та моделі поведінки, які загрожують (або негативно впливають) ціннісному світу людини, руйнують усталені політичні процедури та процеси. Під час інформаційних маніпуляцій використовуються сфабриковані фото-, відеоматеріали, поширюється неправдива інформація про державних та політичних діячів тощо. Маніпулятивна діяльність має скоординований, замовний характер;

8) «атаки на ланцюги поставок – спрямовані на відносини між організаціями та їх постачальниками. Такий різновид атак складається з комбінації принаймні двох атак – перша атака здійснюється проти постачальника, який потім використовується для атаки на ціль, щоб отримати доступ до своїх активів. До прикладу, російські хакери зосереджені на використанні програм-вимагачів для атак на ланцюжки поставок як в Україні, так і в європейських країнах, які використовуються для надання зброї та гуманітарної допомоги на підтримку українських військових» [4, с. 486–487].

Для ефективного захисту інформаційного простору ЄС, з точки зору О. Запорожця, необхідно реалізовувати такий комплекс дій:

1. Забезпечення відповідного професійного рівня підготовки у країнах – членах ЄС «національних комп'ютерних команд», які здатні швидко реагувати на безпекові загрози; активізація співробітництва між державним і при-

ватним секторами; утворення європейського постійно діючого форуму для обміну актуальною інформацією між країнами ЄС.

2. Запровадження в ЄС системи швидкого оповіщення про інформаційні загрози.

3. Посилення захисних спроможностей для критичної інформаційної інфраструктури Європейського Союзу, що включає в себе розроблення національних планів – заходів реагування на ситуативні та стратегічні загрози та проведення тренінгів для всебічного реагування на безпекові виклики; проведення загальноєвропейських тренувань із подолання інформаційно-безпекових інцидентів; посилення взаємодії між національними інформаційно-комп'ютерними силами швидкого реагування.

4. Розроблення ключових принципів європейської інформаційної безпеки та втілення їх у практичній площині.

5. «Визначення критеріїв ідентифікації європейської критичної інфраструктури для сектору інформаційно-комунікаційних технологій. Політичні пріоритети у сфері інформаційної безпеки, визначені керівними органами Європейського Союзу, які втілюються в життя на національному рівні як органами державної влади, так і неурядовими організаціями [5, с. 39–40].

На нашу думку, Європейський Союз має створити потужні кібервійська, які будуть самодостатні у своєму забезпеченні (наприклад, не залежати від США та інших країн технічно й технологічно) та професійно навчені, враховуючи, зокрема, досвід російсько-української війни.

Важливість такого завдання обумовлена, зокрема, й тим, що РФ уже багато років здійснює інформаційну війну, спрямовану проти європейської єдності, європейських цінностей, європейського способу життя. Одним з екзистенційних завдань такої війни РФ як проти Європейського Союзу, так і проти України є намагання посіяти недовіру громадян до європейських цінностей та інститутів, надати їм негативного забарвлення. Така діяльність РФ ще у 2020 р. вже мала відповідні результати. Згідно з опитуваннями GLOBSEC у Чехії, Угорщині та Словаччині, значна кількість респондентів вважала, що їхні держави мають додержуватись геополітичного балансу між умовними полюсами – «західним» і «східним» (55, 46, 46% відповідно) [9].

Оцінюючи такі настрої у країнах ЄС, Є. Булана, І. Паніна у 2020 р. констатували, що «така статистика є вкрай небезпечною для ЄС, адже великі групи населення можуть бути легко переконані в підтримці східного вектору. В умовах такого цілеспрямованого і послідовного наступу на свідомість громадян країн-членів Європейський Союз був змушений активізувати свої дії в інформаційному полі та посилити оборону від негативних сторонніх впливів» [10, с. 32].

Сьогодні можна стверджувати, що такі побоювання не були безпідставними – перемога на виборах проросійських сил в Угорщині та Словаччині, незначний відрив від проросійського кандидати на президентських виборчих перегонах в Румунії проєвропейського політика Нікушора Дана. Фактично, на сьогоднішній день, Угорщина та Словаччина стали союзниками РФ в інформаційній війні проти ЄС й України.

Цілком виправдано керівництво ЄС приділяє значну увагу такому різновиду інформаційної безпеки, як кібербезпека. Так, у 2020 р. Європейська комісія та Високий Представник Союзу з закордонних справ і політики безпеки презентували нову «Стратегію кібербезпеки для цифрового десятиліття» [11], яка спрямована на посилення колективної стійкості ЄС щодо кіберзагроз і гарантування надійності комунікаційно-інформаційних та цифрових систем. Для посилення захисту інформаційних систем Комісія також внесла оновлену Директиву NIS2 [12] про механізми забезпечення надійного загальноєвропейського рівня кібербезпеки в усьому ЄС та нову Директиву щодо стійкості критичних організацій [13].

Вищеназвана стратегія визначає чотири базові напрямки дій ЄС в інформаційно-цифровій сфері:

– стійкість безпекового середовища – норми ЄС для забезпечення захисту та стійкого функціонування критичної інфраструктури в інформаційно-комунікаційній сфері. Визначається важливість утворення Об'єднаного кіберпідрозділу як єдиної платформи для координації співробітництва та міжнародного партнерства для протидії кібератакам і підвищення рівня кібербезпеки країн-партнерів;

– боротьба з викликами й небезпеками, що посилюються. Вона передбачає зміцнення потенціалу правоохоронних органів у сфері інформаційно-цифрових розслідувань;

– активізація захисту європейських громадян від тероризму та оргзлочинності, що передбачає заходи з посилення законодавчої бази про безпеку кордонів і ефективного задіювання існуючих баз даних. Співпраця з міжнародними партнерами, що не є членами Європейського Союзу тощо;

– «сильна європейська екосистема безпеки, яка має формуватися на основі зміцнення мандату Європолу, та подальший розвиток Євроюсту для тіснішого зв'язку між судовими та правоохоронними органами» [6, с. 181].

У сукупності ці нормативні акти склали відповідний пакет з кібербезпеки. «Доповнення європейського вторинного права у сфері кібербезпеки стало логічним кроком після врахування виявлених недоліків попередніх нормативних актів і викликів, що з'явились у зв'язку з пандемією Covid-19. Стратегія описує кібербезпеку як багаторівневу проблему, для розв'язання якої сфор-

мовано сфери діяльності: стійкість, технологічний суверенітет та лідерство; нарощування оперативного потенціалу для запобігання, стримування й реагування; просування глобального та відкритого кіберпростору» [7, с. 150].

Отже, посилення кібербезпеки є необхідним складником зміцнення загальної системи інформаційної безпеки. Кожна підсистема такої системи відіграє свою особливу роль у протидії інформаційним атакам.

Піклуючись про інформаційну безпеку, країни Європейського Союзу мають вирішувати проблему дотримання прав і свобод громадян, не допускаючи зловживань під гаслом безпекових заходів.

У цьому контексті експерти RAND Corporation підкреслюють, що раціональний баланс між свободою та приватністю, з одного боку, і безпекою, з другого боку, має бути утворений у царині громадянських прав і свобод людини. Фахівці констатують, що громадяни та суспільство загалом, зіткнувшися з такою проблемою в реальному житті, маючи вибір відносно рівня свободи і безпеки, готові відмовитися від деяких свобод, прийняти обмеження щодо приватного життя, спонсорувати безпекові переваги, але з певними застереженнями. У будь-якому випадку влада має встановлювати чіткі правові рамки втручання у приватне життя громадян із метою забезпечення інформаційної безпеки. «Важливим аспектом транспарентизації інформаційної безпеки є підвищення поінформованості та розуміння проблеми безпеки, а також базових знань у цій сфері, що може бути пов'язано з процесом масового просвітництва та формуванням культури транспарентності та інформаційної безпеки» [14, с. 26].

Заходи держави з інформаційної безпеки будуть більш дієвими, коли громадяни матимуть чітке уявлення про їхнє значення, важливість, часові межі реалізації, особливо якщо йдеться про обмеження прав та свобод.

Загалом у Європейському Союзі приділяють значну увагу приватності, інформаційної зокрема. Основним законодавчим актом у цій царині (прийнятий 25 травня 2018 р.), який становить стандарт щодо захисту приватних інтересів та прав осіб в інформаційно-цифровому світі Інтернет-мережі та який унормовує збирання, зберігання, обробку та передачу персональних відомостей громадян Європейського Союзу, є Загальний регламент про захист даних (GDPR). Він визначає сутність поняття «порушення захисту персональних даних» – «це порушення безпеки, що призводить до випадкового чи незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до персональних даних, які передано, збережено або іншим чином опрацьовано. Саме недопущення випадкового чи незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до інформації, яка входить

у категорію «інформаційна приватність» – і є основною метою такої категорії, як «захист приватності в інформаційних мережах» [15, с. 1231].

Розмірковуючи про природу інформаційної приватності, ми трактуємо її як невід'ємне особисте право не робити публічною власну персональну інформацію, як-то домашня адреса, приватний телефонний номер, приватне листування або історія мережевого пошуку. Захист інформаційної приватності в Інтернет-мережі – це низка системних заходів, до яких можна віднести створення захищених паролів, використання та оновлення антивірусних програм, засоби шифрування даних тощо.

Висновки. Інформаційна безпека Європейського Союзу є багатовимірним і поліаспектним феноменом, який вбирає в себе інституційний та неінституційний рівні. Основними загрозами у сфері інформаційної безпеки для ЄС є кібер-тероризм, несанкціоноване втручання у функціонування інформаційно-комунікаційних систем в оборонному, політичному, економічному та інших сегментах об'єднання. На сьогоднішній день Європейський Союз створив достатньо дієву систему протидії інформаційним загрозам, яка в той же час потребує постійної модернізації у зв'язку з новими викликами з боку Росії, Китаю, США та ін.

ЛІТЕРАТУРА

1. Швечикова Я. П. Європейський регіональний комплекс безпеки в сучасній безпековій структурі світу. *Грані*. 2014. №9. С. 86–91.
2. Фурсай О. Політика інформаційної безпеки Європейського Союзу. *Літопис Волині*. 2023. №29. С. 165–170.
3. Троян С. С. Інформаційно-безпекова політика Європейського Союзу. *Зовнішні справи.* 2019. №2/3. С. 28–32.
4. Гроза Д. В. Окремі аспекти інформаційної безпеки ЄС. *Юридичний науковий електронний журнал :* електрон. наук. фах. вид. 2023. №12. С. 484–490. URL: http://lsej.org.ua/12_2023/12_2023.pdf (дата звернення: 02.07.2025).
5. Запорожець О. Ю. Політика Європейського Союзу в сфері інформаційної безпеки. *Актуальні проблеми міжнародних відносин.* 2009. Вип. 87, ч. ІІ. С. 36–45.
6. Милосердна І. М. Інформаційна безпека як елемент національної безпеки: теоретичний вимір та особливості впровадження. *Політикус :* наук. журн. 2024. Вип. 4. С. 179–185.
7. Федонюк С. Політика ЄС в аспекті основних глобальних концепцій інформаційної (кібер) безпеки. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2021. №3 (11). С. 144–168.
8. Communication from the European Commission. Network and Information Security: Proposal for a European Policy Approach. COM, 2001. 298 c. URL: http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf (дата звернення: 02.07.2025).

9. GLOBSEC Trends 2019: Central & Eastern Europe 30 years after the fall of the Iron Curtain. URL: http://aspeninstitute.ro/wp-content/uploads/2019/07/Central-Eastern-Europe-30-years-after-the-fall-of-the-Iron-Curtain_GLOBSEC-Trends-2019.pdf (дата звернення: 03.07.2025).
10. Булана Є. А., Паніна І. Г. Європейський союз та інформаційні впливи Російської Федерації. *Вісник студентського наукового товариства ДонНУ імені Василя Стуса.* 2020. Т. 1, № 12. С. 31–34.
11. Oint communication to the european parliament and the council. The EU's Cybersecurity Strategy for the Digital Decade. European Commission. Brussels, 16.12.2020 JOIN 2020 18 final. URL: https://ec.europa.eu/newsroom/dae/docu-ment.cfm?doc_id=72164 (дата звернення: 03.07.2025).
12. Revised Directive on Security of Network and Information Systems (NIS2). European Commission. Publication 16 December 2020. URL: https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2 (дата звернення: 03.07.2025).
13. Proposal for a Directive of the european parliament and of the council on the resilience of critical entities. Brussels, 16.12.2020 COM 2020 829 final. URL: https://ec.europa.eu/home-affairs/sites/default/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf (дата звернення: 4.07.2025).
14. Тихомирова Є. Б. Комунікативна політика ЄС: інформаційна безпека VS транспарентність. *Актуальні проблеми міжнародних відносин :* зб. наук. пр. 2011. Вип. 102, ч. 1. С. 22–28.
15. Мальцев С. Ю. Безпека інформаційних мереж та захист прайвесі: європейські стандарти й інтеграційні виклики для України. *Аналітично-порівняльне правознавство*. 2025. № 2. С. 1225–1233.

REFERENCES

1. Shvechykova, Ya.P. (2014). Yevropeiskyi rehionalnyi kompleks bezpeky v suchasnii bezpekovii strukturi svitu. *Hrani – Facets, 9, 86–91* [in Ukrainian].
2. Fursai, O. (2023). Polityka informatsiinoi bezpeky Yevropeiskoho Soiuzu. *Litopys Volyni – Chronicle of Volyn, 29, 165–170* [in Ukrainian].
3. Troian, S. S. (2019). Informatsiino-bezpekova polityka Yevropeiskoho Soiuzu. *Zovnishni spravy – Foreign Affairs, 2–3, 28–32* [in Ukrainian].
4. Hroza, D. V. (2023). Okremi aspekty informatsiinoi bezpeky YeS. *Elektronne naukove fakhove vydannia «Iurydychnyi naukovyi elektronnyi zhurnal» – Electronic professional scientific edition «Legal Scientific Electronic Journal», 12, 484–490.* URL: http://lsej.org.ua/12_2023/12_2023.pdf [in Ukrainian].
5. Zaporozhets, O. Yu. (2009). Polityka yevropeiskoho soiuzu v sferi informatsiinoi bezpeky. *Aktualni problemy mizhnarodnykh vidnosyn – Current Issues of International Relations, issue 87 (Chastyna II), 36–45* [in Ukrainian].
6. Myloserdna, I. M. (2024). Informatsiina bezpeka yak element natsionalnoi bezpeky: teoretychnyi vymir ta osoblyvosti vprovadzhennia*. Naukovyi zhurnal «Politykus» – Scientific journal «Politykus», issue 4, 179–185* [in Ukrainian].

7. Fedoniuk, S. (2021). Polityka YeS v aspekti osnovnykh hlobalnykh kontseptsii informatsiinoi (kiber) bezpeky. *Mizhnarodni vidnosyny, suspilni komunikatsii ta rehionalni studii – International relations, Public communications and Regional studies, 3(11), 144–168* [in Ukrainian].
8. Communication from the European Commission: Network and Information Security: Proposal for a European Policy Approach. (2001). COM. URL: http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf
9. GLOBSEC Trends 2019: Central & Eastern Europe 30 years after the fall of the Iron Curtain. (2019). URL: http://aspeninstitute.ro/wp-content/uploads/2019/07/Central-Eastern-Europe-30-years-after-the-fall-of-the-Iron-Curtain_GLOBSEC-Trends-2019.pdf
10. Bulana, Ye. A., Panina, I. H. (2020). Yevropeiskyi soiuz ta informatsiini vplyvy Rosiiskoi Federatsii. *Visnyk studentskoho naukovoho tovarystva DonNU imeni Vasylia Stusa – Bulletin of the Student Scientific Society of Vasyl Stus Donetsk National University, Vol. 1, 12, 31–34* [in Ukrainian].
11. Oint communication to the european parliament and the council. The EU's Cybersecurity Strategy for the Digital Decade. European Commission. (2020). Brussels, 16.12.2020 JOIN 18 final. URL: https://ec.europa.eu/newsroom/dae/docu-ment.cfm?doc_id=72164
12. Revised Directive on Security of Network and Information Systems (NIS2). (2020). European Commission. Publication 16 December. URL: https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2
13. Proposal for a Directive of the european parliament and of the council on the resilience of critical entities. (2020). Brussels, 16.12.2020 COM 829 final. URL: https://ec.europa.eu/home-affairs/sites/default/files/pdf/15122020_proposal_direc-tive_resilience_critical_entities_com-2020-829_en.pdf
14. Tykhomyrova, Ye.B. (2011). Komunikatyvna polityka YeS: informatsiina bezpeka vs transparentnist. *Aktualni problemy mizhnarodnykh vidnosyn: zbirnyk naukovykh prats – Current Issues of International Relations: Collection of Scientific Works*, *issue 102(1), 22–28* [in Ukrainian].
15. Maltsev, S. Yu. (2025). Bezpeka informatsiinykh merezh ta zakhyst praivesi: yevropeiski standarty y intehratsiini vyklyky dlia Ukrainy. *Analitychno-porivnialne pravoznavstvo – Analytical and Comparative Jurisprudence, 2, 1225–1233* [in Ukrainian].

Prudnykova Olena Victorivna, Doctor of Philosophical Sciences, Professor, Professor of the Department of Culturology, Yaroslav Mudryi National Law University, Kharkiv, Ukraine

INFORMATION SECURITY OF THE EUROPEAN UNION: CHALLENGES AND TRENDS

The article analyzes the current challenges and threats to the information security of the European Union. It outlines the activities of European institutions responsible for addressing

information security issues and examines the relevant legislative framework in this domain. The study explores the main directions of the EU leadership's response to information-related challenges and threats. It also highlights the key features of the European cybersecurity strategy.

Keywords: information security, cybersecurity, EU, information privacy, information space, human rights and freedoms, Internet network.