УДК 32:005.21:316.774–049.5(4)

Копійка М. В.
аспірантка
кафедра міжнародних медіакомунікацій і комунікативних технологій
Інститут міжнародних відносин
Київський національний університет імені Тараса Шевченка
вул. Юрія Іллєнка, 46/1, м. Київ, 04119, Україна
E-mail: kopiikams@gmail.com
DOI: http://dx.doi.org/10.18524/2304-1439.2019.32.173847

СТРАТЕГІЧНІ РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЄВРОПЕЙСЬКИХ КРАЇН

Стратегічні ризики інформаційної безпеки пов'язуються зі швидкоплинним розвитком цифрових технологій, використанням штучного інтелекту у сфері безпеки, вдосконаленням інформаційних озброєнь та комунікативного інструментарію деструктивних впливів у геополітичному протиборстві провідних міжнародних акторів. Головними проблемами інформаційної і кібербезпеки визначено перспективні порушення конфіденційності інформаційних ресурсів державного, корпоративного і приватного характеру, що можуть призвести до значного впливу деструктивних чинників на критично важливі сфери життєдіяльності суспільства, спричинити руйнування механізмів правового захисту інформаційної безпеки, викликати появу нових інформаційних загроз в умовах швидкоплинного технологічного прогресу; зниження якості інформації для урядів, що забезпечує ухвалення керівних рішень; зростання контенту, створеного за допомогою систем «штучного інтелекту», і водночас прискореного реагування на «фейкові» повідомлення. В європейському регіоні стратегічні ризики інформаційної безпеки враховуються насамперед у рішеннях і програмних документах інтеграційного об'єднання ЄС, а також у стратегіях національної безпеки європейських країн з потужним економічним, науковим, технічним потенціалом і геополітичним впливом. Метою статті визначається дослідження реальних і потенційних стратегічних ризиків інформаційної безпеки Великої Британії, Франції та ФРН в умовах спрямованого використання технологічного і комунікативного інструментарію безпекової політики у міжнародному середовищі. У статті досліджуються оновлені стратегії безпекової політики ЄС, зокрема інформаційної й кібербезпеки, аналізується практика провідних європейських країн щодо протидії сучасним інформаційним викликам і загрозам. У висновках підкреслено важливість модернізації національних стратегій інформаційної безпеки в умовах турбулентності процесів у глобальному інформаційному середовищі.
Ключові слова: стратегічні ризики, інформаційна безпека, кібербезпека, деструктивні впливи, ЄС, Велика Британія, Франція, ФРН.

Постановка проблеми. Стратегічні ризики сучасної безпекової політики провідних європейських країн в умовах нових викликів і загроз полягають у захисті критично важливих сфер життєдіяльності держав та протидії

зовнішнім інформаційним загрозам, таким як спеціальні інформаційно-психологічні операції, інформаційний, медіа-, психо- і кібертероризм, кіберзлочинність, деструктивні інформаційні впливи тощо. Ініціативи щодо вирішення проблеми інформаційної безпеки політичних акторів Європи та посилення відповідальності щодо подолання дисбалансу між регіональними і національними пріоритетами потребують, на думку представників керівних інститутів наднаціональної організації, поліпшення координації ЄС та європейських країн у виробленні спільних підходів до проблем боротьби з кіберзлочинністю та ворожою пропагандою і мають сприйматися європейською спільнотою як стратегічний інтерес у зміцненні оборонного потенціалу і реформуванні механізмів європейської колективної безпеки з врахуванням національних інтересів. Відтак інформаційна й кібербезпека Великої Британії, Франції й ФРН розглядається як стратегічна парадигма, яка стосується всіх верств суспільства, слугує для забезпечення інформаційного суверенітету, безпеки і надійності національної інформаційної інфраструктури, конфіденційності інформаційних ресурсів і приватного життя, тобто практично виступає як модель вирішення проблеми інформаційної безпеки у зовнішньому і внутрішньому політичному середовищі, яка може бути запозичена для формування системи інформаційної безпеки іншими міжнародними акторами, зокрема такий досвід може бути врахований Україною з огляду на стратегічні ризики для системи інформаційної безпеки держави.

Аналіз попередніх досліджень. У сучасному науковому дискурсі з проблем прогнозування стратегічних ризиків безпеки здійснено перспективний аналіз доктрин та практики інформаційної безпеки, захисту конфіденційності інформаційних ресурсів (Е. Хон, Е. Парасіліті, С. Ефрон, С. Стронгін), розглянуто дискусійні погляди зарубіжних фахівців щодо сучасного стану інформаційної безпеки ЄС (С. Каррера, Ф. Рагацці, Ж. Джандесбоз) та інформаційної безпеки європейських країн (Д. Гомперт, Д. Кріз, Д. Рідлі-Джонсон, Л. Адам, П. Кахез, П. Генсінг, С. Штьобер та ін.), а також представлено підходи і погляди вітчизняних науковців (В. Бойко, Д. Дубов, Т. Ісакова, О. Кучмій, О. Литвиненко, Є. Макаренко, І. Мінгазутдінов, М. Ожеван, В. Петрик, Н. Піпченко, А. Покровська, Г. Почепцов, М. Рижков, О. Соснін, Є. Тихомирова, О. Фролова) з інформаційної безпеки, з'ясовано понятійно-категоріальні характеристики інформаційної безпеки, проаналізовано актуальні проблеми трансформації стратегій міжнародних акторів, зокрема державно-приватного партнерства у сфері кібербезпеки та протидії агресивним впливам на політичні і виборчі процеси в Європі. У дослідженнях підкреслюється, що стратегічні ризики інформаційної безпеки наразі визначають суперечності сучасного міжнародного розвитку і ставлять під загрозу забезпечення світового порядку загалом. Фахівці вважають, що національні стратегії інформаційної безпеки мають ґрунтуватися на врахуванні динамічних змін сучасної політичної реальності, еволюції концепцій сили у міжнародних відносинах та впровадженні механізмів забезпечення національної інформаційної безпеки як складової зовнішньої і безпекової політики.

Мета статті полягає у дослідженні стратегічних ризиків інформаційної безпеки Великої Британії, Франції та ФРН в умовах спрямованого використання технологічного і комунікативного інструментарію безпекової політики у міжнародному середовищі.

Дослідження ґрунтується на *методології*, яка включає герменевтико-політологічний аналіз документів і програм наднаціональних інститутів ЄС та порівняльний аналіз національних стратегій інформаційної безпеки зазначених європейських країн. Авторський підхід полягає у тому, що стратегії інформаційної безпеки аналізуються як через поточні політичні події, так і в контексті глобальних трендів щодо стратегічних ризиків інформаційної безпеки, які в європейському дискурсі ще не досліджувались.

Еволюція наукової думки і практика інформаційної безпеки вплинула на різноплановість визначень явищ і понять, що її характеризують, тому у статті використано термінологію, яка зафіксована в документах міжнародних організацій, доктринах зовнішньої і внутрішньої політики, в національних законодавствах та професійних кодексах, діяльності національних безпекових інституцій провідних міжнародних акторів.

Відтак для аналізу стратегічних ризиків інформаційної безпеки обрано поняття: «*інформаційна безпека*» — стан захищеності інтересів суспільства і держави в інформаційному просторі, включаючи інформаційно-телекомунікаційну інфраструктуру, забезпечення цілісності, об'єктивності, доступності і конфіденційності інформації; «*інформаційний суверенітет*» — право держав на формування і здійснення національної інформаційної політики відповідно до положень міжнародного права, конституцій і законодавства країн; «*національна інформаційна інфраструктура*» — сукупність організаційних структур і систем, які забезпечують функціонування та розвиток інформаційного простору, засобів інформаційної взаємодії та доступу до інформаційних ресурсів.

Виклад основного матеріалу дослідження. Критичний аналіз стратегічних ризиків інформаційної безпеки був запропонований дослідниками у доповіді «Discontinuities and Distractions-Rethinking Security for the Year 2040» (RAND Corporation, 2017 р.), яка містить прогноз глобальних тенденцій у сфері безпеки та непередбачуваних подій (чорних лебедів). Оскільки прогностичні дослідження корпорації RAND сприймаються політичними лідерами і фаховими експертами різних країн як можливість екстраполяції певних тенденцій та їх наслідків на національному рівні, вважаємо за потрібне врахувати висновки документу для аналізу стратегій інформаційної безпеки європейських країн.

Зауважимо, що головною проблемою інформаційної і кібербезпеки у дослідженні RAND визначено перспективні порушення конфіденційності інформаційних ресурсів державного, корпоративного і приватного характеру, що можуть призвести до значного впливу деструктивних чинників на критично важливі сфери життєдіяльності суспільства, спричинити руйнування механізмів правового захисту інформаційної безпеки, викликати появу нових інформаційних загроз в умовах швидкоплинного технологічного прогресу, зниження якості інформації для урядів, що забезпечує ухвален-

ня керівних рішень, зростання контенту, створеного за допомогою систем «штучного інтелекту», і водночас прискореного реагування на «фейкові» повідомлення [1].

Ці тенденції визначають зміну підходів міжнародних акторів Європи до формування стратегій інформаційної безпеки на регіональному і національному рівнях, переосмислення механізмів безпекової політики, спрямованої на протидію інформаційному тероризму, поширенню інформаційних озброєнь та деструктивних впливів, які зумовлюють порушення безпекової стабільності в Європі, а також до диференціації пріоритетів регіональної і національної інформаційної безпеки.

Слід підкреслити, що сучасна європейська стратегія зовнішньої і безпекової політики (A Global Strategy for the European Union's Foreign and Security Policy, 2016) включає принципи взаємодії щодо стабільності спільної безпеки й оборони, натомість конкретні цілі та заходи інформаційної безпеки формулюються у програмах і робочих планах інститутів ЄС, які передбачають необхідність знайдення спільних рішень об'єднання європейських країн щодо інформаційного протиборства та визначають необхідність трансформації програми європейської інформаційної безпеки. Як стратегічна проблема європейської безпеки також розглядається кібербезпека як політика посилення захищеності інформаційної інфраструктури та баз даних, а також важливості державно-приватного партнерства і співробітництва на міждержавному рівні. Варто зазначити, що Європейська Комісія ЄС підписала угоду (Agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats 2016) та план дій в галузі кібербезпеки для інтенсифікації зусиль, спрямованих на боротьбу з кіберзагрозами у форматі державно-приватного партнерства [2; 4]. У дослідженні глобального стану інформаційної безпеки (The Global State of Information Security Survey 2018) також зазначається, що кібербезпека, конфіденційність та етичність даних є все більш взаємопов'язаними і потребують ефективного управління інформаційними ризиками. Через це для надання підтримки для захисту від інформаційних загроз компанія PwC (PricewaterhouseCoopers) розробила нову платформу з кібербезпеки та конфіденційності (Digital Trusts Insights 2018) [5].

На регіональному рівні координацію безпекового співробітництва ЄС і європейських країн здійснює «Європейське агентство з мережевої та інформаційної безпеки» (ENISA), яке створювалося для ефективного захисту інформаційного суверенітету та інформаційної інфраструктури Європи, поглиблення відносин між ЄС та політичними акторами, представниками інформаційної індустрії та приватного сектора [6; 7, с. 401]. Варто підкреслити, що першу стратегію кібербезпеки «Національний план захисту інформаційної інфраструктури» у форматі співпраці з агентством ENISA було ухвалено урядом ФРН. У цій стратегії зазначалося, що забезпечення відкритості кіберпростору, а також цілісності, достовірності та конфіденційності інформаційних ресурсів в мережевому середовищі стало одним з важливих пріоритетів німецької держави як на національному, так і на міжнародному рівні. Франція також орієнтується на принципи агентства ENISA щодо

протидії загрозам, які можуть негативно вплинути на інформаційну безпеку країни, тому практичні дії Франції спрямовані на використання технічних засобів захисту інформації і боротьбу з кіберзлочинністю та тероризмом. Стратегія інформаційної безпеки Великої Британії у рамках співпраці з агентством ENISA забезпечує розвиток кібербезпеки як механізму впровадження інновацій, залучення інвестицій та поліпшення якості сервісів у сфері інформаційно-телекомунікаційних технологій, запобігання ризикам кібератак злочинних і терористичних угруповань [6]. Тобто, сприймаючи стратегію ЄС з інформаційної і мережевої безпеки, провідні європейські країни враховують національні пріоритети і засоби їх досягнення.

Всеосяжний характер інформаційних і кібернетичних загроз спонукає країни ЄС до спільних дій на європейському рівні, щоб не тільки ефективно протидіяти кібератакам, а й превентивно реагувати на них на оперативному, тактичному і стратегічному рівнях. Агентство ENISA розробило спеціальний практикум для країн Європи щодо формування національної політики інформаційної і кібербезпеки, в якому подано короткий аналіз поточного стану стратегій європейських країн і визначено загальні риси й відмінності в національних стратегіях, а також запропоновано рекомендації з впровадження стратегії кібербезпеки в країнах ЄС [7, с. 403]. Слід зауважити, що 27 квітня 2018 р. набув чинності і «Генеральний регламент про захист персональних даних» (GDPR) ЄС, за допомогою якого Європарламент, Рада ЄС та Єврокомісія уніфікують захист персональних даних. Важливість постанови підтверджується даними Євробарометра — дослідницької служби ЄС, де зазначається, що понад дві третини (67 %) респондентів поінформовані про «Загальний регламент захисту даних ЄС». Водночас 36 % — знають про зміст Регламенту, тоді як 31 % — знають про постанову, але не знають про її контент [4; 7].

Останнім часом до стратегічних ризиків інформаційної безпеки ЄС та європейських країн експерти відносять агресивну пропаганду авторитарних держав, «мову ворожнечі» і «фейкові» повідомлення деструктивного характеру. Так, на рівні ЄС було прийнято рішення щодо посилення протидії агресивній пропаганді, зокрема російській, а на рівні європейських країн було створено спеціальні установи й підрозділи відповідного спрямування: у Великій Британії боротьбу проти деструктивних впливів було віднесено до повноважень Національного підрозділу Ради національної безпеки; у Франції таку роботу здійснюють спеціальні державні і законодавчі інституції; у ФРН запроваджено програми для боротьби з «фейковими» новинами. Слід підкреслити, що координація дій ЄС і європейських країн у боротьбі з ворожою пропагандою розглядається як стратегічний інтерес організації щодо визнання його статусу міжнародного актора на рівні європейської інформаційної безпеки [8, с. 416].

Зазначимо, що європейські стандарти інформаційної безпеки підтримуються всіма країнами-членами ЄС, що свідчить про спільні підходи до критеріїв оцінки інформаційних загроз, однак їх диференціація у провідних європейських країнах є відмінною залежно від пріоритетів національної безпекової політики.

Так, стратегії інформаційної безпеки Великої Британії враховують як міжнародні, так і національні інтереси держави щодо формування комплексної системи захисту від сучасних інформаційних і кіберзагроз, оскільки у програмному документі «Стратегія національної безпеки» (2011 р.) зазначається, що серед низки критичних для безпеки держави викликів виокремлюються кіберзагрози та антитерористичні заходи. Кібератаки з боку держав, злочинних та екстремістських угруповань вважаються стратегічними ризиками для провідної європейської країни, а кібершпигунство з боку інших країн, хакерський вплив на критично важливі сфери діяльності держави і кіберзлочинність розглядаються як найбільш значимі загрози для безпеки Великої Британії загалом. «Стратегія кібербезпеки», проголошена британським урядом, передбачала реалізацію таких проектів, як створення громадських/приватних «хабів» з кібербезпеки, що дозволяє урядовому і приватному секторам обмінюватися інформацією про кіберзагрози і протидіяти кібератакам. Базові положення «Стратегії» передбачали також створення підрозділу «кіберфахівців», щоб вирішувати проблеми кіберзлочинності та широко використовувати чинні санкції щодо кіберзлочинів [9]. Крім того, у 2016 р. було ухвалено «Стратегію кібербезпеки Великої Британії (2016–2021 рр.), яка наразі вважається основоположним документом у сфері інформаційної безпеки, де сформульовано бачення Великої Британії як «захищеної та гнучкої до кіберзагроз держави за допомогою інноваційних технологій і знань для протидії всім формам агресії в кіберпросторі. Експерти вказують, що фінансування реалізації «Стратегії» збільшилося більш ніж удвічі: з 860 млн фунтів (2012–2016 рр.) до 1,9 млрд фунтів (2016–2021 рр.) [10; 11]. Головною координаційною інституцією Сполученого Королівства з інформаційної безпеки є Штаб-квартира урядових комунікацій (Government Communications Head Quarters, GCHQ), завданнями якої визначено співпрацю з розвідувальними та правоохоронними структурами для захисту урядових систем від кіберзагроз, зокрема кіберзлочинності, хакерства, інтернет-шпигунства, надання підтримки збройним силам і правоохоронним органам щодо забезпечення громадського порядку. Організаційно до складу Штаб-квартири з урядових комунікацій входить: Національний центр з питань кібербезпеки (National Cyber Security Centre, NCSC), що об'єднав різні установи, які займалися окремими питаннями інформаційної й кібербезпеки, а саме Офіс із питань кібербезпеки та інформаційного забезпечення, до компетенції якого належало координування програм із кібербезпеки, передбачених національною стратегією; Операційний центр із питань кібербезпеки, що відповідав за аналіз та оперативне інформування про потенційні кіберзагрози; Центр із питань захисту національної інфраструктури, який надавав рекомендації організаціям з питань управління національною інфраструктурою; Національний технічний головний орган із питань інформаційного забезпечення, що здійснював послуги інформаційного забезпечення уряду, оборонних відомств та ключових інфраструктурних організацій; Платформа «Спільне партнерство з кіберінформації», яка забезпечувала обмін інформацією про поточні загрози в інформаційній сфері між урядом та приватним сектором

в режимі реального часу тощо. У військовій сфері питаннями інформаційної безпеки займається Операційний центр з питань кібербезпеки, що структурно належить до Міністерства оборони держави і є відповідальним за захист військових мереж від кібератак. Наступальна складова кіберпотужності Великої Британії реалізується через Національну програму з кібернаступу (NOCP), що здійснюється Штаб-квартирою урядових комунікацій та Міністерством оборони і включає завдання щодо випередження хакерських і кібератак [12; 13]. Таким чином, у Великій Британії сформовано розвинену інституційно-організаційну базу системи інформаційної безпеки, що охоплює відповідне законодавство, національні стратегії в галузі безпеки й кібербезпеки, а також спеціалізовані урядові установи, призначені для забезпечення безпеки країни в інформаційному та кіберпросторі. Зважаючи на проблему виходу Великої Британії з ЄС, урядові інституції прагнуть підтвердити статус країни як провідного міжнародного актора у сфері інформаційної й кібербезпеки і беруть участь у спільних проектах з FIRST (Forum of Incident Response and Security Teams), Міжнародним союзом електрозв'язку, Групою центрів комп'ютерного реагування на надзвичайні ситуації європейських держав (EGC group), TF-CSIRT, а також у програмах НАТО, ОБСЄ та ООН. До інтересів Великої Британії у сфері інформаційної безпеки належать також: участь у розробці єдиного міжнародного акта щодо кібербезпеки (інформаційної безпеки) в рамках ООН; активізація двосторонньої співпраці з країнами ЄС як передумова налагодження відносин після виходу зі складу Європейського Союзу; міжнародна взаємодія в боротьбі з міжнародною комп'ютерною злочинністю та міжнародним кібертероризмом; технічна та експертна підтримка програм з кібербезпеки в інших країнах; зменшення ризиків у мережі Інтернет для безпечного користування ресурсами і послугами; забезпечення захисту персональних даних тощо [12].

Новітньою тенденцією у сфері кібербезпеки Великої Британії вважається державно-приватне партнерство як один з провідних механізмів попередження та мінімізації кіберзагроз для національної безпеки. Діяльність уряду щодо державно-приватного партнерства у сфері кібербезпеки, підкреслюється в експертному середовищі, полягає у залученні «приватного сектора до співпраці, просуванні інноваційних стартапів, координації інструментів забезпечення кібербезпеки, підтримці мереж фахівців з питань кібербезпеки». Можна стверджувати, що Велика Британія наразі характеризується високим рівнем розвитку національної системи кібербезпеки, що «забезпечується потужною стратегічною та законодавчою базою, а також низкою практичних заходів, спрямованих на розбудову широкого партнерства між державними структурами, приватним сектором, науковими установами та громадянським суспільством» [14].

На відміну від стратегії інформаційної безпеки Великої Британії до пріоритетів інформаційної безпеки Французької Республіки відносять «*цифровий суверенітет*» як здатність держави автономно приймати рішення та вдаватися до захисних дій національної безпеки в умовах глобалізації та інформатизації суспільства» та захист інформаційної інфраструктури

й інформаційного середовища країни, оскільки наявний постійний вплив деструктивної проросійської пропаганди на інформаційний простір держави і маніпулювання ззовні масовою свідомістю французької громадськості. Серед сучасних ризиків інформаційної безпеки Франції особливо виокремлюються кіберзагрози, оскільки кіберзлочинність, інтернет-шпигунство і хакерські атаки на інфраструктурні об'єкти розглядаються як атаки на критично важливі сфери життєдіяльності країни. Свого часу в межах безпекової доктрини 2008 р. Франція здійснила кардинальні зміни безпекової й оборонної політики та подальшу її модернізацію у 2013 р., коли у стратегічних документах кібербезпека була визначена основним пріоритетом національної безпеки держави. Французьке агентство з мережевої та інформаційної безпеки (ANSSI), яке було створене 2009 р., з часом стало загальнонаціональним відомством Франції із захисту інформаційних систем і критичної інфраструктури. У Міністерстві оборони країни було сформовано генеральний директорат з кіберзахисту, що ініціював ухвалення в 2014 р. «Стратегії кібербезпеки», в якій базовими засадами діяльності міністерства з управління та захисту національних інформаційних систем було вказано використання досвіду інших європейських країн зі становлення національної системи кіберзахисту на основі резервних мереж. Стратегією було передбачено збільшення фінансування кібербезпеки Франції в 2014–2019 рр., а також закріплення кібероперацій в якості складової військових операцій. У документі передбачено підтримку проектів державно-приватного партнерства у сфері інформаційної безпеки за участю державних органів влади, крупних промислових корпорацій, приватного сектора, науково-дослідницьких та освітніх установ з огляду на актуальність інвестування у кіберзахист і забезпечення інформаційного суверенітету країни. Секторами інформаційної сфери, що потребують державного захисту, визнано системи інформації обмеженого користування, інформаційні ресурси державної таємниці та спеціальних урядових і військових телекомунікацій. Аналіз оцінок французьких фахівців засвідчив, що загроза інформаційної чи глобальної кібервійни сприймається в експертному середовищі як реальна, хоча такі висновки нівелюються інерційністю системи військових витрат і недостатнім усвідомленням французьким політикумом всіх можливостей інформаційних озброєнь, що виходять за рамки традиційних засобів захисту інформаційних ресурсів [15].

Розвиток доктрини і практики інформаційної безпеки Франції відносять до 2015 р., коли було прийнято французьку національну цифрову стратегію, в якій ключовими цілями було визначено безпеку національних інформаційних систем і критично важливої інфраструктури, конфіденційність приватного життя та персональних даних, безпечність громадян у мережі Інтернет, сприяння французьким компаніям, які працюють у секторі цифрових продуктів та послуг, а також зміцнення впливу Франції у міжнародних організаціях через програми кібербезпеки для найменш захищених країн, загальну підтримку стабілізації кіберпростору. Для забезпечення кіберзахисту Франції передбачалося до 2017 р. збільшити чисельність співробітників французького Агентства з мережевої та інформаційної

безпеки (ANSSI) до 600 осіб, а також Міністерств оборони і внутрішніх справ, зміцнити безпеку суспільно важливих недержавних інформаційних систем, підтримати французькі організації, що розробляють системи виявлення і захисту від кібератак для малих і середніх компаній [16].

Новітню доктрину, спрямовану на організацію та роз'яснення захисту французьких інтересів у кіберпросторі було представлено 18 січня 2019 р.. в якій французький підхід до кібербезпеки та оборони визначає чітке розмежування між наступальними і оборонними кіберопераціями, а також інтеграцію кібероперацій у звичайні військові дії, запроваджуючи «принцип балансування ризику при підготовці та проведенні наступальних операцій, ескалації ризику в асиметричному середовищі або ризик побічної шкоди, або непередбачувані непрямі впливи на цивільну інфраструктуру» [8; 17]. Водночас підкреслимо, що за соціологічними дослідженнями, поінформованість французької спільноти щодо проблем у сфері кібербезпеки впродовж 2017–2018 рр. становила лише 54 % — добре ознайомлених громадян, 44 % — взагалі не ознайомлених з такою проблемою; 93 % громадян Франції не розміщували персональні дані у режимі он-лайн, 89 % — вбачали в цьому ризик від кіберзлочинів, 80 % — вважали, що інформаційні ресурси не забезпечують належний захист персональних даних, а 71 % громадян заперечили можливості державних інституцій щодо захисту конфіденційності персональної інформації [17].

До стратегічних ризиків інформаційної безпеки Франції відносять кібертероризм, зважаючи на те, що за допомогою веб-сайтів здійснюються пропаганда тероризму, психологічні впливи на французьку спільноту, вербування прихильників терористичних організацій, пошук фінансових ресурсів і планування терористичних акцій. Експерти підкреслюють, що терористи поширюють деструктивну інформацію через мас-медіа, яка детально висвітлює теракти, ситуації із захопленням заручників, реагування влади на заяви терористичних угруповань і таким чином посилює контент негативу й фактично примножує присутність терористичних груп в інформаційному середовищі країни [17].

Крім того, фахівці у сфері інформаційної й кібербезпеки Франції звертають увагу не лише на зовнішні чинники впливу щодо інформаційної інфраструктури, а й на деструктивну діяльність фабрик «тролів», «ботів», пропаганду гібридних війн, а також рекомендують урядовим відомствам Франції створити централізований орган для боротьби з «фейковими» новинами, який здійснюватиме спростування та недопущення маніпулятивних повідомлень в інформаційне середовище держави [18]. У парламенті Франції для протидії «фейковим новинам» було запропоновано проект закону, згідно з яким діяльність мас-медіа, причетних до поширення «фейків», буде припинятися за прискореною судовою процедурою. Наразі протидія поширенню недостовірної інформації у Франції відбувається за законом про пресу 1881 р., що вже не відповідає вимогам сучасності. Як заявив президент Франції Е. Макрон, «юридичний механізм для захисту від фейкових новин уможливить закриття за рішенням суддів акантів в мережі Інтернет, видалення інформації сумнівного змісту та обмеження доступу до окремих

сайтів». Таким чином, можна стверджувати, що реакція Франції на сучасні загрози в досяжній перспективі буде зосереджена на внутрішніх чинниках інформаційної безпеки як з погляду організації протестів «жовтих жилетів», які можуть бути інспіровані ззовні, так і поширення публікацій, проплачених опозиційними політичними рухами [19].

Проблема стратегічних ризиків інформаційної безпеки ФРН дискутувалися на 10-й конференції Федерального відомства з питань захисту Конституції «Нові загрози для інформаційної безпеки та інформаційного суверенітету держави» (Neue Gefahren für Informationssicherheit und Informationshoheit) в Берліні (2016). Тематика конференції стосувалася таких нагальних питань, як відповідальність урядових структур за інформаційний суверенітет держави, захист інфраструктури від несанкціонованого втручання і кібершпигунства, поширення дезінформації для впливу на громадськість, формування програми державно-приватного партнерства у сфері кібербезпеки, порушення конфіденційності приватної інформації, діяльність мас-медіа в умовах зовнішніх деструктивних впливів.

Фахівці наголошували, що принципи захисту цифрової інфраструктури було сформульовано в Стратегії цифрової безпеки (Cyber-Sicherheitsstrategie für Deutschland, 2016), якими забезпечення свободи та безпеки суспільства й корпорацій, запобігання і переслідування злочинів, вчинених у кіберпросторі, визнається одним з основних завдань держави. Враховуючи потенціал цифрових інновацій, йшлося у дискусії, відповідним урядовим інституціям на основі аналізу ризиків важливо перспективно визначати можливі події та їх потенційний вплив на системи кібербезпеки, надавати пропозиції для ухвалення керівних рішень та інтегрувати їх у політичні концепції, щоб гарантувати інформаційний суверенітет Німеччини у цифровому світі. Зазначалося, що політика кібербезпеки дає змогу повною мірою скористатися значними можливостями та потенціалом цифрових технологій в інтересах суспільства в цілому та запобігти ймовірним ризикам. Основними заходами при цьому визначалися застосування ефективних продуктів та стандартів безпеки, тісне співробітництво для запобігання, виявлення, відстеження та знешкодження кібератак. У стратегії підкреслюється, що в Німеччині забезпечується формування такого цифрового й інформаційного середовища, в якому ризики, спрямовані на дестабілізацію безпеки всередині країни, зводяться до рівня, коли можна запобігти їхнім проявам. Серед принципів стратегії кібербезпеки виокремлені положення про те, що держава, бізнес, наука та суспільство мають спільну відповідальність за безпеку кіберпростору, тому мають надавати скоординовані відповіді на виклики. Також підтверджено позицію щодо необхідності тісної взаємодії у сфері інформаційної безпеки з європейськими та міжнародними акторами. Зауважимо, що забезпечення захисту кіберпростору Німеччини здійснюють Федеральне міністерство оборони та Бундесвер, а відповідальність за міжнародну політику у сфері цифрової та інформаційної безпеки є компетенцією Федерального міністерства закордонних справ [20].

Актуальним механізмом для інформаційної безпеки ФРН вважається запровадження державно-приватного партнерства в кібернетичній сфері,

що передбачає «створення простору безпеки та зменшення ризиків, збалансування безпеки із забезпеченням свободи в мережі Інтернет, права на втручання держави у децентралізований кіберпростір». Фахівці посилаються на практику ФРН щодо функціонування різних платформ державно-приватного партнерства у сфері кібербезпеки, зокрема на дії Федерального міністерства інформаційної безпеки ФРН, яке 2018 р. нейтралізувало в країні кібератаки, що були спрямовані на вилучення інтелектуальної власності та корпоративне шпигунство. За даними німецьких спецслужб, у країні зросли кількість і масштаб хакерських атак на життєво важливі інфраструктурні об'єкти: повідомляється про 157 хакерських атак на системи критичної інфраструктури ФРН у 2018 р. Посилаючись на неопубліковану статистику Федерального відомства з безпеки у сфері інформаційних технологій, Welt am Sonntag зазначає істотне зростання кіберпорушень порівняно з 2017 р., коли тоді було зафіксовано 145 кібератак такого характеру, роком раніше — лише 34. Експерти підкреслюють, що насправді кількість атак є більшою, оскільки провайдери не розголошують інформацію щодо хакерських зламів [21].

Моніторинг деструктивної кіберактивності Росії щодо урядових мереж та мереж приватних компаній в європейських країнах уможливив відомству ФРН здійснити запобіжні заходи через Національний центр кіберзахисту та попередити операторів критичної інфраструктури про небезпеку несанкціонованого втручання у функціонування інфраструктури. Крім того, модернізація стратегії кібербезпеки зумовлює нові спільні підходи уряду, приватних компаній та спільноти ФРН до усвідомлення ризиків кібербезпеки, а також залучення ефективного менеджменту щодо управління ризиками [22; 23].

Важливим питанням забезпечення інформаційної безпеки ФРН наразі стала й боротьба з дезінформацією та спростування недостовірних даних, що загрожують життєдіяльності суспільства на внутрішньому і зовнішньому рівнях діяльності держави. Йдеться про інформаційно-пропагандистські впливи Росії у ФРН, що свідчать про наявність численних мереж проросійської пропаганди в європейських країнах [24]. Зокрема у тижневику Der Spiegel (жовтень, 2014 р.) було опубліковано матеріал про «кремлівську пропаганду», структури якої створили у ФРН мережу промосковських експертів, щоб переконати німецьке суспільство у тому, що «Німеччина підтримує Росію» в російсько-українському конфлікті. На думку аналітиків, саме ФРН є пріоритетним об'єктом російської пропаганди в Європі, оскільки наявність понад чотирьох мільйонів російськомовних мешканців країни надає РФ можливість здійснювати потужний вплив на їхню мотивацію щодо політичних і виборчих процесів в крані. Зокрема інструментом російської пропаганди в Німеччині вважається телеканал Russia Today з річним бюджетом в 350 млн дол в той час, коли фінансування російської служби «Голосу Америки» на рік становить лише 13 млн доларів. Саме за підтримки «Газпрому» і «Россотрудничества» у ФРН здійснюються деструктивні пропагандистські кампанії, в яких для маніпуляцій використовуються суперечності між політичними партіями, антимігрантські й антиамерикан-

ські настрої окремих суспільних груп та проросійських націоналістичних організацій [25].

Таку діяльність вважають складовою гібридної війни не тільки проти німецького уряду, а й проти засобів масової інформації країни, щоб сформувати опозиційну громадськість, яка б споживала російські медіа з фейковими новинами і спотвореними фактами як достовірні повідомлення. Ефективним інструментом протидії російській пропаганді у ФРН і викриття дезінформації, зазначають дослідники, можуть стати якісні медіа для російськомовної меншини Німеччини. Така політика інформаційної безпеки, на думку експертів, є винятково важливою для ефективної боротьби зі шкідливим інформаційним ресурсом, оскільки інформаційні загрози у модифікованих формах стали «надто багатомірним, небезпечним та складним явищем», з яким практично складно воювати, оскільки потрібно здійснювати оперативний моніторинг дезінформації, яка може загрожувати національній безпеці і психологічному благополуччю суспільства, її аналіз та направлення спростування до інформаційних агентств, координувати заходи національних відомств з аналогічними державними та наддержавними об'єднаннями за кордоном [8, с. 277].

Загалом концепт інформаційної безпеки для ФРН оцінюється як значний виклик для безпеки держави і суспільства, що зазнає зовнішніх впливів внаслідок турбулентності сучасного світу, оскільки, крім позитивних наслідків, що несе з собою відкритість інформаційного та цифрового середовища, роль інформаційних технологій у поширенні політичних меседжів має потенційний негатив для державної політики й зростання деструктивних ризиків. Відтак аналіз дає підстави стверджувати, що стан безпекового простору сучасної Німеччини є вразливим до новітніх тенденцій зовнішнього впливу, оскільки сучасний розвиток інформаційних технологій надав державі, її економіці та суспільству надзвичайної нестійкості перед потенційними кіберзагрозами і зумовив необхідність відповідно реагувати на інтенсифікацію загроз для національної й інформаційної безпеки держави.

Висновки. Порівняльний аналіз стратегічних ризиків інформаційної безпеки європейських країн уможливив висновки щодо спільних і відмінних пріоритетів діяльності держав у захисті інформаційного суверенітету, критично важливої інфраструктури і громадськості.

Спільними пріоритетами можна вважати політику підтримки стратегії інформаційної безпеки ЄС, що стосується інформаційного тероризму, кібератак, а також зовнішніх інформаційних впливів деструктивного характеру. Ініціативи щодо вирішення проблем інформаційної та кібербезпеки Європейського Союзу полягають у поглибленні координації дій наднаціональних і національних інститутів та у виробленні спільних підходів до протидії інформаційним загрозам. Ці ініціативи розглядаються провідними міжнародними акторами Європи в контексті національного інтересу щодо посилення оборонного потенціалу і реформування програми європейської колективної безпеки.

Що стосується відмінних характеристик, то зазначимо, що до сучасних загроз безпеці Великої Британії відносять загрози гібридного харак-

теру щодо цілісності інформаційного суверенітету країни. Як випливає з аналізу національної стратегії інформаційної безпеки цієї країни, забезпечення надійного рівня захисту інформаційних ресурсів та інфраструктури покладається на дотримання єдиних національних стандартів і норм, пов'язаних з інформаційною та кібербезпекою, співпрацею з провідними міжнародними акторами задля вирішення поточних і перспективних проблем кібербезпеки держави, посилення контролю за охороною персональних і конфіденційних даних, а також залучення приватного сектора і громадських об'єднань до формування середовища інформаційної культури.

Натомість стратегія інформаційної безпеки Франції спрямована на поглиблення міждержавного співробітництва щодо вирішення загальних безпекових проблем ЄС, створення механізмів для подолання інформаційних загроз, узгодження на європейському і двосторонньому рівні правових питань кібербезпеки та притягнення до відповідальності за скоєння передусім терористичних кібератак. За Планом дій з інформаційної безпеки Франції передбачаються здійснення стратегічного аналізу щодо протидії інформаційним загрозам у співробітництві з Радою Безпеки ООН, встановлення стратегічного партнерства з провідними міжнародними акторами у сфері кібербезпеки, поглиблення нормативної бази держави з інформаційної безпеки через ухвалення законів, рекомендацій і резолюцій про інформаційну безпеку та конфіденційність електронних комунікацій, визначення та оцінка інформаційних і кіберзагроз для критично важливих сфер життєдіяльності французької спільноти, впровадження основних положень національної політики інформаційної безпеки і включення країни у програми забезпечення регіональної інформаційної безпеки.

Проблематика інформаційної безпеки ФРН є стратегічним викликом для посилення заходів безпеки в суспільстві внаслідок потужних зовнішніх впливів в умовах всеосяжної інформатизації сучасного світу. Окрім позитивних наслідків для інформаційного середовища і німецької спільноти, що несе з собою відкритість інформаційного та цифрового просторів, новітні технології та їхня роль у здійсненні передачі політичних меседжів несуть потенційні загрози, до яких відносять зростання ризиків та їхніх непередбачуваних наслідків, спричинених і використанням інструментарію зовнішніх впливів. Тому важливим для політики інформаційної безпеки ФРН вбачається здійснення ефективної стратегії для виявлення та пом'якшення ризиків, оскільки держава, її сфери життєдіяльності та суспільство виявилися недостатньо стійкими перед потенційними інформаційними і кіберзагрозами.

Список використаної літератури

1. Hoehn A., Parasiliti A., Efron S., Discontinuities and Distractions — Rethinking Security for the Year 2040. URL: https://www.rand.org/pubs/conf_proceedings/CF384.html (дата звернення: 28.05.2019).
2. A Global Strategy for the European Union's Foreign And Security Policy URL: http://eeas.europa.eutop_stories/pdf/eugs_review_web.pdf (дата звернення: 28.05.2019).

3. The Commission adopts a new European Agenda on Security 2015–2020 to support better cooperation between Member States in the fight against terrorism, organised crime and cybercrime. URL: http://ec.europa.eu/news/2015/04/20150428_en.htm (дата звернення: 28.05.2019).
4. European Commission — Press release Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats. URL: http://europa.eu//press-release_IP-12321_en.htm (дата звернення: 28.05.2019).
5. The Global State of Information Security® Survey 2018. URL: https:// www.pwc. com/ us/en/ services/ consulting/ cybersecurity/ library/information-security-survey.html (дата звернення: 28.05.2019).
6. National Cyber Security Strategies Guidelines & tools — ENISA. URL: https:// www.enisa. europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies -guidelines-tools (дата звернення: 28.05.2019).
7. Регіональні стратегії США і Європи: зовнішньополітичний і безпековий вимір: монографія. К. : Центр вільної преси, 2016. 528 с.
8. Макаренко А. Є. Стратегічні комунікації в міжнародних відносинах: монографія. К. : Вадекс, 2018. 442 с.
9. Kriz D. A Global Model: UK's «National Cyber Security Strategy». URL: https://www.securityroundtable.org/global-model-uks-national-cyber-security-strategy/ (дата звернення: 28.05.2019).
10. UK Parliament's Joint Committee publish government response to UK's National Security Strategy. URL: https:// www. nccgroup. trust/uk/about-us/newsroom-and-events/ news/2019/march/joint-committee-publish-government-response-to-national-security-strategy/ (дата звернення: 28.05.2019).
11. Steed D. The UK's National Cyber Security Strategy Beyond 2021: The International Dimension. URL: https://rusi.org/commentary/The_UKs_National_Cyber_Security_Strategy_Beyond_2021_The_International_Dimension (дата звернення: 28.05.2019).
12. The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World. London : Whitehall, November 2011. 43 p.
13. The National Cyber Security Centre. URL: https://www.ncsc.gov.uk/home (дата звернення: 28.05.2019).
14. Покровська А. В., Ісакова Т. О. Державно-приватне партнерство у сфері кібербезпеки: досвід Великої Британії. URL: http://old2.niss.gov.ua/content/articles/files/cybersecurity-6ddd7.pdf (дата звернення: 28.05.2019).
15. French national digital security strategy. URL: https://euagenda.eu/publications/french-national-digital-security-strategy (дата звернення: 28.05.2019).
16. Laudrain A. France's New Offensive Cyber Doctrine. URL: https://www.lawfareblog.com/ frances–new–offensive–cyber–doctrine (дата звернення: 28.05.2019).
17. Adam Л. Appel de Paris sur la cybersécurité: comment la France veut tracer sa voie. URL: https://www.zdnet.fr/actualites/appel-de-paris-sur-la-cybersecurite-comment-la-france-veut-tracer-savoie39876349.htm (дата звернення: 28.05.2019).
18. Cahez P. Élections européennes: lutte contre la propagande mensongire. URL: https://blogs. mediapart.fr/patrick-cahez/blog/110419/elections-europeennes-lutte-contre-la-propagande-mensongere (дата звернення: 28.05.2019).
19. Lutter contre la désinformation et protéger les journalistes. URL: https://www.robert-schuman.eu/fr/questions-d-europe/0498-lutter-contre-la-desinformation-et-proteger-les-journalistes
20. Neue Gefahren für Informationssicherheit und Informationshoheit. URL: https://www.verfassungsschutz.de/.../tagungsband-2016–10-sicherheitstagung-2016.pdf (дата звернення: 28.05.2019).
21. Cyber-Sicherheitsstrategie für Deutschland 2016. URL: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (дата звернення: 28.05.2019).
22. Waidner M. Cybersicherheit in Deutschland — T-Systems. URL: https://www.t-systems. com/de/de/ueber-uns/ unternehmen/ newsroom/ news/news/fraunhofer-cybersicherheit-in-deutschland-680672 (дата звернення: 28.05.2019).
23. Бойко В. О. Досвід Німеччини у функціонуванні платформ державно-приватного партнерства в сфері кібербезпеки. URL: http://old2.niss.gov.ua/content/articles/files/1_AZ_Boyko_var77_FIN-4d2ef. Pdf (дата звернення: 28.05.2019).

24. Gensing P., Stöber S. Pro-russische Netzwerke: Moskautreue Rechte. URL: https://www.tagesschau. de/ inland/ neurechte–russland–101.html (дата звернення: 28.05.2019).
25. Pörzgen G. Informationskrieg in Deutschland? Zur Gefahr russischer Desinformation im Bundestagswahljahr. *Aus Politik und Zeitgeschichte/bpb.de*. URL: https://www.bpb.de/apuz/248506/informationskrieg-in-deutschland-zur-gefahr-russischer-desinformation-im-bundestagswahljahr?p=all (дата звернення: 28.05.2019).

References

1. Hoehn, A. , Parasiliti, A., Efron, S. «Discontinuities and Distractions—Rethinking Security for the Year 2040.» Accessed May 5, 2019. https://www.rand.org/pubs/conf_proceedings/CF384.html
2. A Global Strategy for the European Union's Foreign And Security Policy. Accessed May 5, 2019. http://eeas.europa.eutop_stories/pdf/eugs_ review_web.pdf
3. The Commission adopts a new European Agenda on Security 2015–2020 to support better cooperation between Member States in the fight against terrorism, organised crime and cybercrime. Accessed May 5, 2019. http://ec.europa.eu/news/2015/04/20150428_en.htm
4. European Commission — Press release Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats Accessed May 5, 2019. http:// europa.eu/ /press-release_IP-16–2321_en.htm
5. The Global State of Information Security Survey 2018. Accessed May 5, 2019. https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html
6. National Cyber Security Strategies Guidelines & tools — ENISA. Accessed May 5, 2019. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies -guidelines-tools
7. Rehional′ni stratehiyi SSHA i Yevropy: zovnishn′opolitychnyy i bezpekovyy vymir. Monohrafiya. K. : Tsentr vil′noyi presy, 2016.
8. Makarenko, E. O. Stratehichni komunikatsiyi v mizhnarodnykh vidnosynakh. Monohrafiya. K. : Vadeks, 2018.
9. Kriz, D. «A Global Model: UK's «National Cyber Security Strategy.» Accessed May 5, 2019. https://www.securityroundtable.org/global-model-uks-national-cyber-security-strategy/
10. UK Parliament's Joint Committee publish government response to UK's National Security Strategy Accessed May 5, 2019. https:// www. nccgroup. trust/uk/about-us/newsroom-and-events/news/2019/march/joint-committee-publish-government-response-to-national-security-strategy/
11. Steed, D. «The UK's National Cyber Security Strategy Beyond 2021: The International Dimension.» Accessed May 5, 2019. https://rusi.org/commentary/The_UKs_National_Cyber_Security_Strategy_Beyond_2021_The_International_Dimension
12. The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World. — London : Whitehall, November 2011.
13. The National Cyber Security Centre. Accessed May 5, 2019. https://www.ncsc.gov.uk/home
14. Pokrovs′ka, A. V., Isakova, T. O. «Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: dosvid Velykoyi Brytaniyi.» Accessed May 5, 2019. http://old2.niss.gov.ua/content/articles/files/cybersecurity-6ddd7.pdf
15. French national digital security strategy Accessed. May 5, 2019. https://euagenda.eu/publications/french-national-digital-security-strategy
16. Laudrain, A. France's New Offensive Cyber Doctrine. Accessed May 5, 2019. https://www.lawfareblog.com/frances–new–offensive–cyber–doctrine
17. Adam, Л. «Appel de Paris sur la cybersécurité : comment la France veut tracer sa voie.» Accessed May 5, 2019. https://www.zdnet.fr/actualites/appel -de-paris-sur-la-cybersecurite-comment-la-france-veut-tracer-savoie39876349.htm
18. Cahez, P. «Élections européennes: lutte contre la propagande mensongиre.» Accessed May 5, 2019. https://blogs.mediapart.fr/patrick-cahez/blog/110419/elections-europeennes-lutte-contre-la-propagandemensongere
19. «Lutter contre la désinformation et protéger les journalists.» Accessed May 5, 2019. https://www.robert-schuman.eu/fr/questions-d-europe/0498-lutter-contre-la-desinformation-et-proteger-les-journalistes

20. Neue Gefahren für Informationssicherheit und Informationshohei. Accessed May 5, 2019. https://www.verfassungsschutz.de/.../tagungsband-2016–10-sicherheitstagung-2016.pdf
21. Cyber-Sicherheitsstrategie für Deutschland 2016. Accessed May 5, 2019. https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf
22. Waidner, M. «Cybersicherheit in Deutschland — T-Systems.» Accessed May 5, 2019. https://www.t-systems.com/de/de/ueber-uns/ unternehmen/ newsroom/ news/news/fraunhofer-cybersicherheit-in-deutschland-680672
23. Boyko, V. O. «Dosvid Nimechchyny u funktsionuvanni platform derzhavno-pryvatnoho partnerstva v sferi kiberbezpeky.» Accessed May 5, 2019. http://old2.niss.gov.ua/content/articles/files/1_AZ_Boyko_var77_FIN-4d2ef. pdf
24. Gensing, P., Stöber, S. «Pro-russische Netzwerke: Moskautreue Rechte Accessed.» May 5, 2019. https:// www. tagesschau. de/ inland/ neurechte–russland–101.html
25. Pörzgen, G. Informationskrieg in Deutschland? Zur Gefahr russischer Desinformation im Bundestagswahljahr. *Aus Politik und Zeitgeschichte/bpb.de* Accessed May 5, 2019. URL: https://www.bpb.de/apuz/248506/informationskrieg-in-deutschland-zur-gefahr-russischer-desinformation-im-bundestagswahljahr?p=all

Стаття надійшла до редакції 12.06.2019

Копейка М. В.
кафедра международных медиакоммуникаций и коммуникативных технологий, Институт международных отношений КНУ им. Тараса Шевченко
ул. Юрия Ильенко, 46/1, г. Киев, 04119, Украина

СТРАТЕГИЧЕСКИЕ РИСКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЕВРОПЕЙСКИХ СТРАН

Резюме

Стратегические риски информационной безопасности обусловливаются развитием цифровых технологий, совершенствованием инструментария деструктивных воздействий в геополитическом противоборстве ключевых акторов. В европейском регионе стратегические риски информационной безопасности учитываются, прежде всего, в программных документах и деятельности ЕС, а также в стратегиях национальной безопасности европейских стран, обладающих значительным геополитическим, экономическим и научно-техническим потенциалом, таких как Великобритания, Франция и Германия. Целью статьи определяется исследование факторов модернизации стратегий информационной безопасности Великобритании, Франции и ФРГ. Исследование основывается на методологии, которая включает анализ документов и программ наднациональных институтов ЕС и национальных стратегий по информационной безопасности определенных европейских стран, исследований зарубежных и отечественных ученых, аналитических публикаций специалистов экспертной среды. Автором продемонстрировано, что инициативы по решению проблем информационной и кибербезопасности ЕС заключаются в углублении координации действий наднациональных и национальных институтов по противодействию информационным угрозам. Показано, что в документах Великобритании противодействие угрозам информационному суверенитету страны и обеспечение защиты информационных ресурсов и инфраструктуры видятся посредством установления стандартов информационной безопасности, усиления контроля за охраной персональных и конфиденциальных данных, привлечения частного сектора и общественных объединений к формированию среды информационной культуры и международного сотрудничества. Стратегия информационной безопасности Франции направлена на создание механизмов преодоления информационных угроз, согласование на европейском уровне правовых вопросов кибербезопасности и привлечение к ответственности за совершение террористических кибератак. Политика информационной безопасности ФРГ ориентирована на сохранение открытости информационного и цифрового пространства.

Ключевые слова: стратегические риски, кибербезопасность, деструктивные воздействия, ЕС, Великобритания, Франция, ФРГ.

Kopiika M. V.
Department of International Media Communication and Communication Technologies, Institute of International Relations, Taras Shevchenko National University of Kyiv, st. Yuriya Ilyenka, 46/1, Kiev, 04119, Ukraine

STRATEGIC RISKS OF INFORMATION SECURITY OF THE EUROPEAN COUNTRIES

Summary

The strategic risks of information security are determined by the development of digital technologies, the improvement of tools for destructive impacts in the geopolitical confrontation of key actors. In the European region, strategic risks of information security are taken into account, first of all, in the EU policy documents and activities, as well as in the national security strategies of European countries with significant geopolitical, economic, scientific and technological potential, such as the UK, France and Germany. The purpose of the article is to study the factors of modernization of information security strategies in the UK, France and Germany. The study is based on a methodology that includes analysis of documents and programs of supranational institutions of the EU and national information security strategies of certain European countries, studies of foreign and domestic scientists, analytical publications of experts from the expert community. The author has demonstrated that initiatives to address the EU's information and cybersecurity problems are to deepen coordination of supranational and national institutions to counter information threats. It is shown that in the UK documents, countering threats to the country's information sovereignty and ensuring the protection of information resources and infrastructure is seen through the establishment of information security standards, strengthening control over the protection of personal and confidential data, involving the private sector and public associations in creating an information culture environment and international cooperation. France's information security strategy aims to create mechanisms to overcome information threats, coordinate European cyber security legal issues and hold accountable terrorist cyber attacks. The information security policy of Germany is focused on maintaining the openness of the information and digital space.

The article explores updated EU security policy strategies, including information and cybersecurity, and analyzes the practices of leading European countries in addressing current information challenges and threats. The conclusions underline the importance of modernizing national information security strategies in the context of turbulent processes in the global information environment.

Key words: strategic risks, cybersecurity, destructive impacts, EU, UK, France, Germany.