УДК 342.9

ДОВГАЛЬ Ю.С.

ДЕЯКІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: АНАЛІЗ ЄВРОПЕЙСЬКОГО ДОСВІДУ

У статті досліджується актуальність питання теоретичних та практичних підходів до забезпечення інформаційної безпеки країни та аналіз європейського досвіду. Розглянуто інформаційну безпеку європейських країн. Акцентовано увагу на значенні інформаційної безпеки держави напередодні проведення президентських та парламентських виборів в Україні у 2019 році. Тематика забезпечення інформаційної безпеки набуває неабиякої актуальності, особливо враховуючи прагнення країни-агресора втручатися у перебіг та підсумки електоральних процесів із метою дестабілізації політичної ситуації та фальсифікації результатів виборів.

Ключові слова: *національна безпека, інформаційна безпека, інформаційне суспільство, інформаційні війни, Україна.*

В статье исследуется актуальность вопроса теоретических и практических подходов к обеспечению информационной безопасности страны и анализ европейского опыта. Рассмотрено информационную безопасность европейских стран. Акцентировано внимание на значении информационной безопасности государства накануне проведения президентских и парламентских выборов в Украине в 2019 году. Тематика обеспечения информационной безопасности приобретает актуальность, особенно учитывая стремление страны-агрессора вмешиваться в ход и итоги электоральных процессов с целью дестабилизации политической ситуации и фальсификации результатов выборов.

Ключевые слова: *национальная безопасность, информационная безопасность, информационное общество, информационные войны, Украина.*

The article investigates the relevance of theoretical and practical approaches to ensuring information security of the countries, and an analysis of European experience. The information security of European countries is considered. The emphasis on the importance of information security of the state on the eve of the presidential and parliamentary elections in Ukraine in 2019, the subject of information security is becoming extremely relevant, especially considering the country's aggressor's desire to interfere with the course and outcome of electoral processes in order to destabilize the political situation and falsify election results.

Key words: *national security, information security, information society, information wars, Ukraine.*

Вступ. Відповідно до фундаментальних положень Доктрини інформаційної безпеки України [1], забезпечення інформаційного суверенітету, запобігання інформаційній агресії, експансії та інформаційній блокаді України з боку іноземних держав, організацій, груп та осіб є пріоритетним завданням політикуму нашої країни. Інформаційна безпека держави є невід'ємним складником кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки, яка характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз і є сукупністю інформаційно-психологічної (психофізичної) та інформаційно-технологічної безпеки держави.

© ДОВГАЛЬ Ю.С. – молодший науковий співробітник відділу з вивчення проблем забезпечення інформаційної та кібернетичної безпеки, захисту вітчизняного інформаційного простору (Міжвідомчий науково-дослідний центр із проблем боротьби з організованою злочинністю при Раді національної безпеки й оборони України)

Напередодні проведення президентських та парламентських виборів в Україні у 2019 році тематика забезпечення інформаційної безпеки набуває неабиякої актуальності, особливо враховуючи прагнення країни-агресора втручатися у перебіг та підсумки електоральних процесів із метою дестабілізації політичної ситуації та фальсифікації результатів виборів. Невипадково протягом останнього часу спостерігається надмірне посилення протиборства між РФ та країнами Заходу в інформаційній (зокрема кібернетичній) сфері, що пов'язано з активізацією спроб Кремля здійснити вплив на політику США та ЄС у вигідному для себе напрямку. Найбільш резонансними проявами таких дій РФ стали втручання в перебіг президентських виборів у США, а також у виборчі процеси в низці європейських країн, що викликає суттєве занепокоєння та негативну реакцію західних політичних кіл, які вживають заходів щодо стримування інформаційної експансії Москви. Найбільш активні позиції в цьому питанні займають Конгрес США та керівництво Європейського Союзу і НАТО, які вбачають у діях РФ безпосередню загрозу власним інтересам і безпеці.

Так, наприкінці 2016 року в рамках ухвалення Конгресом США проекту закону про витрати на розвідку у 2017 році було прийнято окреме положення щодо посилення боротьби із завуальованим впливом Росії на США. Із цією метою вживалися заходи, спрямовані на створення спеціального міжвідомчого Комітету із завданнями координації дій американських спецслужб у цій сфері (що визначено одним з основних пріоритетів роботи). До складу зазначеного органу було залучено представників офісу директора Національної розвідки, ФБР, Державного департаменту, а також міністерств юстиції, фінансів та енергетики США. Окрім того, згідно з рішенням Конгресу США, створено спеціальну комісію з розслідування спроб РФ вплинути на результати президентських виборів у США, яка має незалежний статус і вміщує представників як Республіканської, так і Демократичної партій США. Основними завданнями комісії є визначення масштабів та форм дій Москви із застосування кіберінструментів для злому систем, які застосовуються на виборах, та розповсюдження дезінформації.

Активні позиції зі стримування інформаційної експансії Москви займають країни ЄС. Так, за результатами розслідувань дій Росії у ФРН, німецькими спецслужбами було зроблено висновок про проведення Москвою послідовної загрозливої інформаційної політики, спрямованої на підрив позицій А. Меркель та дестабілізацію ситуації у ФРН. Аналогічні дії Росії спостерігалися також у Великобританії, Франції, Австрії, Польщі та деяких інших країнах ЄС.

Зважаючи на це, керівництвом Європейського Союзу було ухвалено рішення щодо застосування якісно нових підходів в інформаційному протиборстві з РФ. Так, у листопаді 2016 року Європейський парламент ухвалив План імплементації нової Стратегії європейської політики безпеки і оборони, яка вміщує положення щодо протидії «гібридним» війнам та засобам «м'якої сили» з боку противників ЄС,зокрема в інформаційній сфері.

Зазначене питання було конкретизовано в резолюції Європейського парламенту **«Стратегічні комунікації ЄС як протидія пропаганді третіх сторін»**, яка була прийнята в листопаді 2016 року [2]. Документ уперше прямо визнає застосування Росією агресивних методів та інструментів для проведення ворожої пропаганди проти Європи, що прирівнюється до рівня загроз із боку терористичної організації «Ісламська Держава». У резолюції наголошено, що пропаганда, яку проводить РФ, є частиною «гібридної війни», а також вона спрямована на те, щоб «спотворити правду, посіяти сумніви і ворожнечу між країнами союзу, послабити стратегічну єдність ЄС і його північноамериканських партнерів, паралізувати процес ухвалення рішення, дискредитувати інститут ЄС і трансатлантичне партнерство».

Серед основних методів таких дій РФ виокремлюють такі, як розповсюдження підривної інформації в європейському інформаційному просторі, несанкціоноване проникнення в комп'ютерні системи європейських країн, надання інформаційної та фінансової підтримки ультраправим, популістським та проросійським силам у країнах ЄС, а також позиціювання окремих регіонів Європи як «сфери традиційного впливу Російської Федерації». Крім того, окремо визначається використання РФ контактів із європейськими партнерами з метою пропаганди та послаблення міжнародних позицій ЄС. Згідно з документом, головними організаторами інформаційних атак РФ на Європу є Міністерство закордонних справ РФ та Федеральне агентство «Россотрудничество», які застосовують комплекс відповідних інструментів, вміщуючи засоби масової інформації, інформаційно-аналітичні центри та спеціальні фонди.

За оцінками європейських експертів, **найбільшу загрозу для Європейського Союзу становлять російські псевдоновинні агентства та мультимедійні служби, зокрема агентство Sputnik, телеканал RT («Russia Today») та фонд «Русский мир».** З урахуванням наведених обставин, у документі визначається перелік заходів щодо посилення протидії інформаційному

впливу з боку Росії, які передбачають розробку нової інформаційної стратегії ЄС, вивчення форм та методів дій Кремля в інформаційній сфері, поглиблення взаємодії між європейськими інституціями з питань інформаційної безпеки, активізацію дій європейських ЗМІ у регіонах, які найбільше піддаються російській пропаганді, підвищення поінформованості європейської та світової спільноти щодо політики ЄС, підтримку незалежних засобів масової інформації в Росії, викриття злочинів колишніх комуністичних режимів у країнах Центрально-Східної Європи.

Для практичної реалізації наведених заходів планується нарощування можливостей **«Оперативної групи стратегічних комунікацій на Сході» (East StratCom Task Force),** яка була створена у складі Європейської служби зовнішніх зв'язків (міністерство закордонних справ Європейського Союзу) і займається питаннями протидії інформаційному впливу з боку РФ. Згодом групу було перетворено на повноцінне відомство зі збільшенням кількості співробітників, які працюють на напрямах Східної Європи, а також Північної Африки, Близького Сходу та Західних Балкан. Водночас ще у грудні 2016 року між ЄС та НАТО було досягнуто домовленості щодо поглиблення взаємодії сторін у розвитку оборонного потенціалу, вміщуючи протидію «гібридним» війнам та посилення захисту кіберпростору. Із цією метою планується створення «Європейського центру протидії гібридним загрозам» із широким спектром функцій, зокрема щодо інформаційного протиборства. Окремим напрямом дій США, НАТО та ЄС є сприяння посиленню здатності партнерів протистояти інформаційній експансії з боку Росії. Так, це передбачено в Комплексному плані допомоги Україні, який було ухвалено під часі Варшавського саміту НАТО в липні 2016 року [3].

Також слід указати, що держава-агресор із метою підвищення ефективності інформаційної політики РФ 5 грудня 2016 року схвалила **нову Доктрину інформаційної безпеки РФ,** у положеннях якої чітко визначено, що головною метою дій РФ в інформаційній сфері визначається «прорив інформаційної блокади з боку США та ЄС» у рамках побудови «рівноправних міждержавних відносин в інформаційному просторі» та «формування вільного середовища обігу інформації». При цьому наголошується на «загальнолюдських правах» отримання та розповсюдження інформації, що подається в контексті звинувачень на адресу Заходу в блокуванні роботи російських ЗМІ. Вагоме значення надається вдосконаленню системи інформаційного захисту Збройних сил РФ. Водночас у новій Доктрині інформаційної безпеки РФ визнається відставання від провідних західних країн у сферах комп'ютерних та телекомунікаційних технологій, що становить суттєву загрозу для Російської Федерації. У наведеному контексті окремо визначається небезпека підривних дій проти Росії через мережу Інтернет.

Зважаючи на викладене, можемо стверджувати, що саме результати активної фази протистояння, зокрема між Заходом та РФ в інформаційній сфері, мають стати визначальним чинником у розвитку ситуації у світі, Європі та безпосередньо навколо України. Так, певними «досягненнями» інформаційного протиборства РФ із країнами заходу вже стали такі: обрання проросійських президентів Румена Радева у Болгарії (2017 рік) Ігоря Додона в Молдові (2017), Мілоша Земана у Чехії (2018 рік), перемога Соціал-демократичної партії (СДП) на парламентських виборах у Румунії. Водночас наслідки таких дій Росії можуть бути значно нівельовані ЄС шляхом цілеспрямованого застосування заходів із протидії інформаційній експансії Москви.

Розглянемо законодавчі ініціативи та практичні заходи, які вживаються євроспільнотою з метою протидії інформаційній експансії РФ та забезпечення власної інформаційної безпеки.

ЄС не стоїть на місці, постійно змінюючи та вдосконалюючи підходи до регулювання сфери інформаційної безпеки. Із метою систематизації та встановлення мінімальних вимог для всіх країн-членів ЄС у 2016 році було схвалено Директиву Європарламенту та Ради Європи №2016/1148 «Про загальні заходи безпеки мережевих та інформаційних систем» [4], положення якої зобов'язують уряди держав-членів визначати об'єкти критичної інфраструктури в різноманітних сферах. Отже, в ЄС із метою посилення рівня кіберзахисту інформаційно-телекомунікаційних мереж та систем було запроваджено Єдині нові правила.

Виходячи зі змісту вказаного документа, саме інформаційні мережі та системи відіграють життєво важливу роль у європейському суспільстві. Зважаючи на те, що глобальні мережі мають транснаціональний характер, істотні порушення штатного функціонування інформаційних систем цивільного або військового управління, незалежно від того, навмисні чи ненавмисні ці дії, а також від місця скоєння, можуть негативно впливати на окремі держави-члени ЄС.

Причиною ухвалення нової Директиви ЄС стала необхідність розроблення дієвого механізму запобігання інцидентам у сфері інформаційної безпеки, що стосується обчислювальних мереж, серверів, систем зберігання даних і мережевих вузлів. Таким чином, ефективне реагуван-

ня на вказані виклики безпеці мережевих та інформаційних систем вимагає глобального підходу на рівні ЄС, що охоплює загальне зміцнення технічного потенціалу, налагодження інформаційного обміну, співпраці і загальних вимог безпеки для операторів цифрових послуг. Зазначена Директива передбачає впровадження таких заходів щодо підвищення загального рівня кібербезпеки в ЄС, які забезпечать:

– відповідний рівень готовності держав-членів, що передбачає створення Команд швидкого реагування на кіберінциденти (Computer Security Response (CSIRT)), і компетентних відповідальних національних органів;

– комплексну співпрацю між усіма державами-членами ЄС із метою надання підтримки та сприяння обміну інформацією між державами-членами про кіберзагрози та кіберінциденти;

– високий рівень безпеки у всіх секторах, які мають вагоме значення для економіки і суспільства і, крім того, значно залежать від таких інформаційно-комунікаційних технологій (далі – ІКТ), як енергетика, транспорт, водопостачання, банківська сфера, інфраструктури фінансового ринку, охорона здоров'я та цифрова інфраструктура.

Крім того, ключові постачальники цифрових послуг (пошукові системи, хмарні обчислення і онлайнові торговельні майданчики) мають відповідати вимогам безпеки і здійснювати повідомлення про будь-які кіберінциденти. Із метою досягнення високого рівня безпеки мережевих та інформаційних систем кожна держава-член ЄС також зобов'язана розробити **Національні стратегії з безпеки мережевих та інформаційних систем,** що визначають цілі і конкретні заходи, які мають бути реалізовані.

У процесі здійснення імплементації положень цієї Директиви у серпні 2017 року декілька федеральних земель Німеччини звернулися до політикуму держави з проханням запровадити норму законодавства, яка б зобов'язувала соціальні мережі, зокрема «Facebook», надавати на вимогу правоохоронців конфіденційну інформацію про користувачів, оскільки влада федеральних земель обурюється тим, що керівництво «Facebook» залишає без відповіді в середньому 2/3 таких запитів: протягом останніх років поліція, прокуратура і спецслужби Німеччини щодня відправляють на адресу «Facebook» більше ніж десять запитів про надання особистих даних користувачів, зокрема про облікові дані або IP-адресу. Крім того, на вимогу має бути максимально скорочено термін надання таких облікових даних або інформації про користувачів [5].

Проте у 2018 році ситуація кардинально змінилася. Із травня 2018 року в ЄС запроваджено нові вимоги до захисту персональних даних. Із 25 травня 2018 року в юридичному полі Європейського Союзу вступив у силу новий нормативний акт Загальний Регламент Захисту Даних, більш відомий як GDPR (General Data Protection Regulation) [6]. Євросоюз перейшов на нові правила поводження з персональними даними, а Регламент стосується будь-якої роботи з персональними даними, зокрема збору, зберігання і передачі. За недотримання вимог GDPR компаніям загрожує втрата європейських клієнтів і ринків, а також штрафи до 20 млн. євро, або 2–4% від річного фінансового обігу компанії порушника. Хоча закон ухвалений для захисту європейських даних, глобальний характер Інтернету означає, що GDPR установлює стандарт конфіденційності даних у всьому світі. Майже всі великі інтернет-компанії, зокрема Google, Facebook і Twitter, мають дотриматися вимог GDPR.

Цілком реально, що напередодні виборів Україна очікує від Кремля посилення тиску і нових масштабних хакерських атак. Можливо, РФ буде активно втручатися у виборчий процес в Україні, використовуючи різні засоби, починаючи від дезінформації і закінчуючи кібератаками, тому підвищену увагу доцільно приділяти передусім саме захисту виборчої інфраструктури. Так, Великобританія анонсувала готовність направити до України експертів, які допоможуть захистити електоральну систему від хакерського втручання РФ та фейкових повідомлень.

Тобто Кремль використовує всі можливі варіанти, щоб повернути Україну у свою сферу впливу. Одним із таких варіантів є широкомасштабні кібератаки на українські державні установи, банківську систему, об'єкти критичної інформаційної інфраструктури. У 2017 році ЦРУ з'ясувало, що за атакою вірусу «Petya» в Україні стоять військові РФ. За інформацією, розміщеною у The Washington Post, комп'ютерний вірус Petya потрапив в Україну і поширився на міжнародні комп'ютерні системи в США. Хоча ці кібератаки ніколи не були формально пов'язані з Кремлем, вони, найімовірніше, здійснювалися з боку Росії і можуть повторитися в наступному році під час виборів. Також можливими є зломи персональних електронних скриньок, як це було під час президентської кампанії в США 2016 року. Виборча система і технології країни залишаються досить уразливими. Імовірно, ці слабкі місця будуть використовуватися для зламу електронних скриньок та виявлення персональних даних ключових кандидатів у президенти, особливо тих, хто серйозно загрожує Кремлю [7].

Не можуть залишитися поза увагою світової спільноти нахабні спроби російських хакерів групи «Fancy Bear», які намагалися отримати несанкціонований доступ до електронного листування верховних помічників Вселенського Патріарха Варфоломія І, який вирішує те, чи надавати автономію Українській помісній автокефальній церкві. Виокремлення незалежної Української православної церкви має стати великим ударом по ролі російської православної церкви у світі, тому російська влада намагається зберегти вплив московського патріархату будь-якою ціною [8].

Так, у вересні 2018 року Палата представників Конгресу США ухвалила Закон «Про кіберстримування та відповідні заходи» [9], відповідно до положень якого офіційний Вашингтон має компетенцію запроваджувати санкції проти осіб, закордонних держав чи організацій за скоєні кіберзлочини проти США. На думку авторів Закону, такий захід зможе захистити вибори в країні та важливі об'єкти інфраструктури від «спонсованих іноземними державами навмисних кібератак», а також створить основу для стримування та реагування на кібератаки проти США в майбутньому. Новий закон вимагає, щоб президент формував списки небезпечних осіб, які загрожують «національній безпеці, закордонним справам, економічному здоров'ю чи фінансовій стабільності країни». Крім того, цей документ ухвалено на основі заяв директора нацрозвідки США про те, що «РФ, Китай, Іран і Північна Корея стануть найбільшими кіберзагрозами для США» [10].

Прояви російської інформаційної агресії також передбачає політичне керівництво Франції, тому в цій країні підготовлено проект закону, спрямований на протидію фейкам на виборах. Минулорічна президентська кампанія у Франції ознаменувалася втручанням російських медіа, кібератаками, а також загалом була «брудною» за французькими стандартами. Ураховуючи масштаби загроз в інформаційній сфері у Франції у положеннях Стратегічного огляду (Revue stratégique) [11] задекларовано, що питання дезінформації та її впливу стають одними з безпекових пріоритетів.

Отже, у Франції на законодавчому рівні посилюються заходи з метою контролю мас-медіа, особливо напередодні виборів – для захисту країни від фальшивих новин – усі медіа, соцмережі, пошуковики, інформаційні портали матимуть певні зобов'язання стосовно «спонсорського контенту», який вони розміщують. Крім того, очікується збільшення повноважень Вищої наглядової ради радіотелебачення (Conseil supérieur de l'audiovisuel, CSA) для «боротьби зі спробами дестабілізації ситуації телеслужбами, що перебувають під впливом іноземних держав». У Франції також законодавчо запроваджується право державного регулятора анулювати ліцензії телеканалів із метою протистояння централізованій російській пропаганді. Це також стосується блокування контенту в соціальних мережах, що стане додатковим, ще потужнішим інструментом із протидії російському впливу [12].

Великі світові провайдери, зокрема мережа «Facebook», на початку 2018 року прозвітувала, що контролює фейкові записи, тому вдосконалила свої системи розпізнавання та видалення недостовірних записів і фейкових новин. Таким чином, демократичний світ вступає у новий виборчий цикл, зокрема це стосується оновлення європейських інституцій у 2019 році. Країни ЄС та США одночасно визнали глобальні масштаби російської інформаційної експансійної кампанії та вбачають у ній глобальну загрозу для свого інформаційного простору.

Ураховуючи такі виклики, розробляються нові законодавчі акти та впроваджуються практичні заходи, спрямовані на повну нейтралізацію російської інформаційної експансії. Україна не стоїть осторонь цих процесів.

Так, у квітні 2018 року Президент України в Ситуаційному центрі РНБО України провів нараду щодо стану забезпечення інформаційної безпеки держави та протидії російській пропаганді, під час якої надав старт роботи Системи протидії антиукраїнському мовленню в зоні проведення Антитерористичної операції, що стало новою прогресивною фазою у захисті України від факторів російської гібридної агресії. Загалом, система комплексної протидії російській інформаційній агресії в зоні проведення Антитерористичної операції блокує аналогові та цифрові телевізійні сигнали більше як 40 каналів російського і проросійського телебачення на території проведення АТО. Вона спрямована на протидію інформаційній експансії та поширення пропаганди Росії на території проведення АТО і дозволяє захистити від її впливу громадян України, які проживають більше ніж у 150 населених пунктах на лінії розмежування [13].

У серпні 2018 року Служба безпеки України заблокувала діяльність мережі інтернет-агітаторів, яких спецслужби РФ залучили з метою підготовки до втручання у майбут-

ні вибори. Російські спецслужби залучили до «співпраці» жителів Дніпра, Кривого Рогу і Нікополя, які стали адміністраторами груп у соціальних мережах, та поставили завдання щодо підготовки «плацдарму» для проведення заздалегідь запланованих заходів впливу на перебіг майбутніх виборів Президента України шляхом маніпулювання громадською думкою інтернет-користувачів. Також із метою маніпулювання населенням України спецслужби РФ із використанням проросійськи налаштованих громадян України намагаються створити тисячі фейкових аккаунтів із російським корінням для майбутнього втручання РФ у виборчий процес. Зважаючи на це, необхідними є розробка та запровадження дієвого механізму попередження такого втручання.

У США 06.11.2018 відбулися проміжні вибори до Конгресу. Використовуючи маніпулятивні інформаційні технології, російські спецслужби застосували нову тактику втручання в електоральний процес шляхом розповсюдження суперечливого та фейкового контенту з метою впливу на кінцеві результати. Розповсюдження дезінформації відбувалося в соціальних мережах Facebook, Twitter, Reddit та інших платформах шляхом так званих компаній з інформаційних операцій, щоб витримати чистки, які здійснюють великі соціальні мережі, та уникнути перевірок із боку уряду [14].

Висновки. Ураховуючи масштаби російської інформаційної експансії та загрозливі тенденції у цій площині напередодні президентських та парламентських виборів у 2019 році в Україні, першочерговим завданням держави є системна боротьба з фейковими аккаунтами та російською пропагандою у вітчизняному інформаційному просторі. Можливо, російські куратори планують проведення низки заходів із метою загострення суспільно-політичної ситуації напередодні та під час проведення виборів Президента України, тому потенційно можливим є утворення в соціальних мережах груп нібито «патріотичного спрямування». Згодом із використанням цих ресурсів планується публікація деструктивних матеріалів, зокрема із закликами до насильницької зміни конституційного ладу України та порушення її територіальної цілісності.

Окрім того, доцільним убачається вживання заходів, спрямованих на:

– виявлення та припинення деструктивних дій окремих державних та неурядових структур суміжних країн: РФ, Румунії, Угорщини, Республіки Польщі; мінімізацію іноземного впливу та нейтралізацію намірів, які можуть завдати шкоди національним інтересам України;

– виявлення, попередження та припинення спроб представників громадсько-політичних і релігійних об'єднань (насамперед проросійських) політизувати та радикалізувати свою діяльність за підтримки закордонних центрів, інспірувати сепаратистські настрої та прояви релігійної ворожнечі серед етнічних громад, зокрема з використанням соціальних мереж, що може спричинити дестабілізацію суспільно-політичної ситуації, особливо в окремих регіонах України;

– виявлення і недопущення використання закордонними недержавними організаціями та функціонерами можливостей вітчизняних ЗМІ, ресурсів мережі Інтернет, представників мас-медійних громадських організацій та інших фахових об'єднань для створення механізмів впливу, зокрема фінансових, на вітчизняну інформаційну сферу, суспільно-політичні процеси, здійснення дискредитації діяльності органів державної влади, а також проведення антиукраїнських інформаційних акцій, особливо напередодні виборів 2019 року.

Доцільно також уживати заходів, спрямованих на попередження деструктивної діяльності окремих закордонних інформаційних структур, медійних та навколомедійних організацій, провайдерів програмних послуг *(РФ, Республіка Польща, Угорщина, Румунія),* які намагаються сформувати механізми впливу на суспільно-політичну ситуацію в Україні шляхом створення позицій в інформаційному просторі держави, використання ЗМІ, мережі Інтернет, видавничо-поліграфічної та рекламної галузей, власних інформаційних можливостей для здійснення антиукраїнських інформаційних акцій, інспірування в середовищі національних меншин автономістських та сепаратистських настроїв, особливо на Закарпатті.

Правоохоронним органам необхідно консолідувати спроможності з метою недопущення своєчасного виявлення та припинення, зокрема шляхом вживання профілактичних заходів, підготовки та поширення у вітчизняних ЗМІ, друкованих виданнях, мережі Інтернет (видання, соціальні мережі, блогосфера) інформаційних матеріалів, поліграфічної продукції із закликами до вчинення терористичних актів, насильницької зміни чи повалення конституційного ладу, захоплення державної влади, порушення територіальної цілісності, а також таких, які розпалюють національну, расову чи релігійну ворожнечу, пропагують ідеї расизму, ксенофобії або інші антиконституційні та протиправні діяння, особливо під час проведення виборів.

Список використаних джерел:

1. Доктрина інформаційної безпеки України: Затверджена Указом Президента України від 25 лютого 2017 року №47/2017. URL: http://zakon.rada.gov.ua/laws/show/47/2017?lang=ru.

2. Резолюція Європейського парламенту «Стратегічні комунікації ЄС, як протидія пропаганді третіх сторін» від 23 листопада 2016 року. URL: http://www.europarl.europa.eu/news/en/press-room/20161118IPR51718/meps-sound-alarm-on-anti-eu-propaganda-from-russia-and-islamist-terrorist-groups.

3. Варшавський саміт НАТО від 9 липня 2016 року. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_09/20160923_1609-factsheet-warsaw-summit-key-ukr.pdf.

4. Директива Європарламенту та Ради Європи №2016/1148 від 6 липня 2016 року «Про загальні заходи безпеки мережевих та інформаційних систем». URL: https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-20161148.pdf.

5. У Німеччині пропонують зобов'язати соцмережі до співпраці зі спецслужбами. URL: https://www.eurointegration.com.ua/news/2016/08/7/7053101/.

6. ДирективаЗахисту GDPR (General Data Protection Regulation) від 27 квітня 2016 року. URL :https://eu-ua.org/sites/default/files/inline/files/es-2016679.pdf.

7. Кремль використовує всі можливі варіанти, щоб повернути Україну в свою сферу впливу. URL: https://ru.tsn.ua/ukrayina/pyat-sposobov-kak-rossiya-mozhet-povliyat-na-ukrainskie-vybory-atlantic-council-1173792.

8. Російські хакери атакували електронну пошту в оточенні патріарха Варфоломія. URL: https://ukr.segodnya.ua/world/russia/rossiyskie-hakery-atakovali-okruzhenie-patriarha-varfolomeya-ap-1165911.html.

9. Закон США «Про кіберстримування та відповідні заходи» від 6 вересня 2018 року. № H.R.5576. URL: https://www.congress.gov/bill/115th-congress/house-bill/5576/text.

10. Палата представників Конгресу США прийняла закон про санкції за кібератаки. URL: https://dt.ua/WORLD/palata-predstavnikiv-kongresu-ssha-priynyala-zakon-pro-sankciyi-za-kiberataki-287588_.html .

11. Стратегічний огляд оборони та національної безпеки Франції (Revue stratégique) від 22 грудня 2017 року. URL: URL: https://www.defense.gouv.fr/dgris/politique-de-defense/revue-strategique/revue-strategique.

12. Франція, готує новий закон для протидії фейкам на виборах. Пропаганду забанять у Google. URL: https://www.eurointegration.com.ua/articles/2018/03/20/7079007/.

13. Президент Петро Порошенко в Ситуаційному центрі провів нараду щодо інформаційної безпеки держави та протидії російській пропаганді. URL :https://www.president.gov.ua/news/prezident-dav-start-roboti-sistemi-protidiyi-antiukrayinskom-47058.

14. У США 06.11.2018 відбулися проміжні вибори до Конгресу. URL: https://tsn.ua/svit/u-ssha-vidbudutsya-promizhni-vibori-kogo-obiratimut-ta-yaki-naslidki-voni-matimut-dlya-amerikanskoyi-politiki-1244310.html?_ga=2.23938362.1806568433.1541426855-1140103669.1538578270.