УДК 343.9:343.346.8:004

ГРЕБЕНЮК М.В., *кандидат юридичних наук, доцент,*
Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при РНБО України
ЛЕОНОВ Б.Д., *доктор юридичних наук, старший науковий співробітник,*
Національна академія Служби безпеки України

АКТУАЛЬНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЕЛЕКТОРАЛЬНИХ ПРОЦЕСІВ: АНАЛІЗ ЗАРУБІЖНОГО ДОСВІДУ

Анотація. *У статті аналізується зарубіжний досвід забезпечення інформаційної безпеки електоральних процесів. Висвітлюються проблеми боротьби з фейковими аккаунтами та деструктивною пропагандою у вітчизняному інформаційному просторі. Аналізуються законодавчі ініціативи США та окремих країн ЄС у сфері забезпечення інформаційної безпеки.*

Ключові слова*: інформаційна безпека, електоральні процеси, деструктивна пропаганда.*

Summary. *The article analyzes the foreign experience of ensuring the information security of electoral processes. The problems of combating fake accounts and destructive propaganda in the domestic information space are covered. Analysis the legislative initiatives of the United States and EU countries in the field of information security is provided.*

Keywords*: information security, electoral processes, destructive propaganda*.

Аннотация*. В статье анализируется зарубежный опыт обеспечения информационной безопасности электоральных процессов. Освещаются проблемы борьбы с фейковыми аккаунтами и деструктивной пропагандой в отечественном информационном пространстве. Анализируются законодательные инициативы США, а также отдельных стран ЕС в области обеспечения информационной безопасности.*

Ключевые слова*: информационная безопасность, электоральные процессы, деструктивная пропаганда.*

Постановка проблеми. Відповідно до Доктрини інформаційної безпеки України забезпечення інформаційного суверенітету, запобігання інформаційної агресії, експансії та інформаційній блокаді України з боку іноземних держав, організацій, груп та осіб є пріоритетним завданням політикуму нашої країни [1]. Інформаційна безпека визначається як стан захищеності життєве важливих інтересів людини, суспільства і держави, за якого відбувається завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [2].

Напередодні проведення президентських та парламентських виборів в Україні у 2019 році тематика інформаційної безпеки набуває надзвичайної актуальності з огляду на загрозу з боку РФ втручатися у хід та підсумки електоральних процесів з метою дестабілізації політичної ситуації. Не виключається, що РФ буде активно втручатися у виборчий процес в Україні, використовуючи різні засоби, починаючи від дезінформації і закінчуючи кібератаками. Тому на особливу увагу заслуговує захист виборчої системи, об’єкти якої залишаються досить уразливими. Йдеться, зокрема, про можливість злому електронних скриньок та витоку персональних даних ключових кандидатів у президенти, особливо тих, хто серйозно загрожує Кремлю [3].

У серпні 2018 року СБ України заблокувала діяльність мережі Інтернет-агітаторів, яких спецслужби РФ залучили для втручання у майбутні вибори. Російські спецслужби залучили до "співпраці" жителів Дніпра, Кривого Рогу і Нікополя, які є адміністраторами груп в соціальних мережах та поставили завдання з підготовки "плацдарму" для проведення заздалегідь запланованих заходів впливу на хід майбутніх президентських виборів шляхом маніпулювання громадською думкою Інтернет-користувачів. Також з метою маніпулювання свідомістю пересічних громадян спецслужби РФ з використанням проросійськи налаштованих громадян України створюють тисячі фейкових аккаунтів з російським корінням для майбутнього втручання у виборчий процес. Тому в Україні існує необхідність у розробці та впровадженні дієвого механізму запобігання такому втручанню.

Результати аналізу наукових публікацій. Інформаційна складова як один із факторів, який впливає на масову свідомість, докладно розглянута зарубіжними авторами, серед яких виділяються праці Г. Алмонда, Е. Вятра, Р. Даля, С. Верба, А. Вілдавскі, К. Дойча та ін.

Серед вітчизняних дослідників інформаційному протиборству приділяли увагу Бакалинський О.О., Гапеєва О.Л., Горбулін В.П., Гулай В.В., Жарков Я.М., Мосов С.П., Нижник Н.Р., Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін.

Однак в науковій літературі відсутні системні дослідження, присвячені вивченню зарубіжного досвіду забезпечення інформаційної безпеки електоральних процесів.

Метою статті є аналіз зарубіжного досвіду у сфері забезпечення інформаційної безпеки електоральних процесів для його можливого запозичення та використання державними органами України.

Виклад основного матеріалу. Як зазначається у Доктрині інформаційної безпеки України, застосування РФ технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України. Комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації [1]. Водночас, агресивна інформаційна війна здійснюється не тільки в Україні, а й на території інших країн світу.

У грудні 2016 року схвалено 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". У Доктрині відзначається відставання РФ від провідних західних країн у сферах комп'ютерних та телекомунікаційних технологій, що становить суттєву загрозу для Російської Федерації [4].

Невипадково протягом останнього часу відзначається надмірне посилення протиборства між країнами Заходу та РФ, перш за все, в інформаційній сфері, що пов'язано з активізацією спроб останньої здійснити вплив на політику США та ЄС у вигідному для себе напрямку. Найбільш резонансними проявами таких дій РФ стали спроби втручання в хід президентських виборів у США, а також у виборчі процеси окремих європейських країн, що викликає занепокоєння та негативну реакцію західних політичних кіл. Так, за результатами розслідувань дій Росії в ФРН, німецькі спецслужби

дійшли висновку щодо проведення російськими спецслужбами послідовної інформаційної політики з дестабілізації політичної обстановки в ФРН. Аналогічні дії російських спецслужб були відмічені спецслужбами Великої Британії, Франції, Австрії, Польщі та інших країн ЄС.

Розглянемо законодавчі ініціативи та практичні заходи, які вживаються євроспільнотою з метою протидії агресивній інформаційній експансії РФ та забезпечення власної інформаційної безпеки з урахуванням міжнародного досвіду забезпечення інформаційної безпеки електоральних процесів.

Після президентських виборів у США керівництвом Європейського Союзу було прийнято рішення щодо вироблення 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 включає положення щодо протидії "гібридним" війнам та засобам "м'якої сили" з боку супротивників ЄС, у т. ч. в інформаційній сфері. Зазначене рішення було конкретизовано у резолюції Європейського Парламенту "Стратегічні комунікації ЄС, як протидія пропаганді третіх сторін", яка була прийнята у листопаді 2016 року [5]. Ця резолюція вперше визнає застосування Росією агресивних методів з проведення ворожої пропаганди проти Європи, яка прирівнюється до загроз з боку терористичної організації "Ісламська держава". У резолюції наголошується, що пропаганда РФ є частиною "гібридної війни", яка спрямована на те, щоб "спотворити правду, посіяти сумніви і ворожнечу між країнами союзу, послабити стратегічну єдність ЄС і його північноамериканських партнерів, паралізувати процес прийняття рішення, дискредитувати інститут ЄС і трансатлантичне партнерство".

Серед основних методів такої пропаганди РФ виділяють: розповсюдження неправдивої інформації в європейському інформаційному просторі, надання інформаційної та фінансової підтримки ультраправим, популістським та проросійським силам в країнах ЄС, а також позиціювання окремих регіонів Європи як "сфери традиційного впливу Російської Федерації". Крім того, окремо відзначається використання РФ контактів з окремими європейськими партнерами з метою пропаганди та послаблення політичних позицій ЄС. За резолюцією головними організаторами інформаційних атак РФ є Міністерство закордонних справ РФ та Федеральне агентство "Россотрудничество", які застосовують комплекс відповідних інструментів, включаючи засоби масової інформації, інформаційно-аналітичні центри та спеціальні фонди [5].

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 резолюції визначається перелік заходів з посилення протидії інформаційному впливу з боку Росії, зміст яких передбачає: розробку нової інформаційної стратегії ЄС; вивчення форм та методів дій РФ в інформаційній сфері; поглиблення взаємодії між європейськими інституціями з питань інформаційної безпеки; активізацію дій європейських ЗМІ у регіонах, які в найбільше зазнають впливу російської пропаганди; підвищення поінформованості європейської та світової спільноти щодо політики ЄС; підтримку незалежних засобів масової інформації в Росії; викриття злочинів колишніх комуністичних режимів в країнах Центрально-Східної Європи [6].

Для практичної реалізації наведених заходів планується нарощування можливостей "Оперативної групи по стратегічним комунікаціям на Сході" (East StratCom Task Force), яка створена у складі Європейської служби зовнішніх зв'язків (фактично – міністерство

закордонних справ Європейського Союзу), і опікується питаннями протидії інформаційному впливу з боку РФ. Сьогодні ця група фактично трансформувалася у повноцінне відомство зі збільшенням кількості співробітників, які працюють у напрямах Східної Європи, а також Північної Африки та Близького Сходу. Крім того, у грудні 2016 року між ЄС та НАТО було досягнуто домовленості щодо поглиблення взаємодії сторін у розвитку оборонного потенціалу, включаючи протидію "гібридним" війнам та посилення захисту кіберпростору. З цією метою планується створення "Європейського центру протидії гібридним загрозам" з широким спектром функцій, у т.ч. інформаційного протиборства. Окремим напрямом дій США, НАТО та ЄС є сприяння посиленню здатності їх партнерів протистояти інформаційній експансії з боку Росії, що, зокрема, передбачено комплексним планом допомоги Україні, який був прийнятий під час Варшавського саміту НАТО в липні 2016 року [7].

З метою систематизації та встановлення мінімальних вимог для всіх країн-членів ЄС у 2016 році була схвалена Директива Європейського Парламенту та Ради № 2016/1148 "Про загальні заходи безпеки мережевих та інформаційних систем", положення якої зобов'язують уряди держав-членів визначати об'єкти критичної інфраструктури у різноманітних сферах [8]. Отже, з метою посилення кіберзахисту інформаційно-телекомунікаційних мереж та систем в ЄС були запроваджені Єдині нові правила. Виходячи із змісту вказаного документа, саме інформаційні мережі та системи відіграють життєво важливу роль в 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 необережні ці дії) можуть негативно впливати на окремі держави-члени ЄС.

Причиною прийняття нової Директиви ЄС стала необхідність розробки дієвого механізму запобігання інцидентам у сфері інформаційної безпеки, що стосується обчислювальних мереж, серверів, систем зберігання даних і мережевих вузлів. Таким чином, ефективне реагування 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. Ця 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 з метою надання підтримки та сприяння обміну інформацією між державами-членами про кіберзагрози та кіберінциденти;
- високий рівень безпеки у всіх секторах, які мають життєво важливе значення для економіки і суспільства, і крім того, значною мірою залежать від інформаційно-комунікаційних технологій (ІКТ), таких як: енергетика, транспорт, водопостачання, банківська сфера, інфраструктури фінансового ринку, охорони здоров'я та цифрової інфраструктури [8].

Окрім того, ключові постачальники цифрових послуг (пошукові системи, хмарні обчислення і он-лайнові торговельні майданчики) повинні відповідати вимогам безпеки і повідомляти про будь-які кіберінциденти. Також з метою досягнення високого рівня безпеки мережевих та інформаційних систем кожна країна ЄС зобов'язана розробити

Національні стратегії з безпеки мережевих та інформаційних систем, що визначають цілі і конкретні заходи, які повинні бути реалізовані.

У процесі здійснення імплементації положень цієї Директиви у серпні 2017 року декілька федеральних земель Німеччини звернулися до керівництва держави з проханням запровадити правила, які б зобов'язували 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 відправляють на адресу "Facebook" щодня більше десяти запитів про надання особистих даних користувачів, зокрема про їх облікові дані або IP-адреси. Крім того, на вимогу правоохоронців має бути максимально скорочений термін надання таких облікових даних або інформації про користувачів [9].

Проте, ситуація кардинально змінюється.

У травні 2016 року Європейський Парламент і Рада затвердили постанову про нові правила і порядок захисту персональних даних ("Пакет захисту даних" ЄС), який передбачає створення умов забезпечення узгодженої нормативно-правової бази на європейському рівні та для всіх країн світу, які мають відносини з державами-країнами ЄС. "Пакет захисту даних" ЄС набув чинності 25 травня 2018 року та складається з трьох документів, головним з яких є Загальний регламент захисту даних (GDPR – General Data Protection Regulation) [10].

GDPR стосується будь-якої обробки персональних даних, зокрема їх 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 порушника. З огляду на глобальний характер Інтернету, GDPR встановлює стандарт конфіденційності даних у всьому світі, а його дія поширюється практично всі великі Інтернет-компанії, включаючи "Google", "Facebook", "Twitter" та ін.

Один із великих світових провайдерів мережа "Facebook" на початку 2018 року прозвітував, що контролює фейкові записи, у зв'язку з чим удосконалила свої системи розпізнавання та видалення недостовірних записів та фейкових новин. Компанія "Twitter" може почати повідомляти користувачам, чи піддавалися вони впливу контенту, згенерованого російським сервісом для поширення пропаганди. Соціальна мережа працює, щоб ідентифікувати й особисто поінформувати її користувачів, які побачили під час президентської компанії 2016 року твіти акаунтів, пов'язаних із прокремлівським "Агентством Інтернет-досліджень". "Twitter" виявила 1062 аккаунта, пов'язаних з російським "Агентством Інтернет-досліджень", відомим також як "фабрика тролів".

У вересні 2018 р. Конгрес США ухвалив Закон "Про кіберстримування та відповідні заходи", відповідно до положень якого офіційний Вашингтон має право запроваджувати санкції проти осіб, закордонних держав чи організацій, винних у вчиненні кіберзлочинів проти США [10]. На думку авторів закону, такий захід зможе захистити вибори та важливі об'єкти інфраструктури від "фінансованих іноземними державами навмисних кібератак", а також створить основу стримування та реагування на кібератаки проти США в майбутньому. Новий закон зобов'язує президента формувати списки небезпечних осіб, які загрожують "національній безпеці, закордонним справам, економічному розвитку чи фінансовій стабільності країни" [11].

Також практично одноголосно ухвалено резолюцію про підтримку протидії російській пропаганді на рівні ЄС. Резолюція рекомендує країнам-членам ЄС заснувати органи (observatories) для відстежування дезінформації та фейків. У резолюції йдеться, що у деяких випадках державні засоби масової інформації були перетворені на

пропагандистські інструменти та використані для передачі фальшивих новин або розпалювання ненависті та ксенофобії проти меншин та певних груп. Це призводить до відсутності незалежності та низьких етичних стандартів у ряді засобів масової інформації та пояснює дедалі більшу недовіру населення. У зв'язку з цим Асамблея підтверджує свою підтримку рішення ПАРЄ від 2015 року про боротьбу з дезінформацією, яка походить із джерел ЗМІ та он-лайн-аккаунтів РФ, шляхом створення "Спеціальної групи East StratCom" [12].

Прояви російської інформаційної агресії також фіксує й політичне керівництво Франції, у зв'язку з чим у цій країні підготовлено проект закону для протидії фейкам на виборах. Минулорічна президентська кампанія у Франції ознаменовалася втручанням російських мас-медіа, кібератаками та загалом була визнана "брудною" за французькими стандартами. Враховуючи масштаби загроз в інформаційній сфері, у положеннях "Стратегічного огляду" (Revue stratégique) задекларовано, що питання дезінформації та її впливу стають одними з безпекових пріоритетів Франції [13].

Також у Франції на законодавчому рівні посилено заходи з контролю мас-медіа – для захисту країни від фальшивих новин – усі медіа, соцмережі, пошуковики, інформаційні портали матимуть певні зобов'язання стосовно "спонсорського контенту", який вони розміщують. Також очікується збільшення повноважень Вищої наглядової ради радіотелебачення (Conseil supérieur de l'audiovisuel, CSA) для "боротьби зі спробами дестабілізації телеслужбами, що знаходяться під впливом іноземних держав". Також з метою опору централізованій російській пропаганді у Франції законодавчо запроваджується право державного регулятора анулювати ліцензії телеканалів. Це стосується також й блокування контенту в соціальних мережах, що стане додатковим потужним інструментом з протидії російському впливу [14].

Не відстає від Франції й Німеччина, де також нещодавно було прийнято закон про боротьбу з фейковими новинами і з ненависницькими коментарями в соцмережах. Федеральне управління кримінальної поліції Німеччини (BKA) повідомило про те, що в десяти німецьких землях, в тому числі в Берліні, Баварії, Гессені, Північному Рейні-Вестфалії, Саксонії, поліція провела операцію проти осіб, яких підозрюють у публікації в Інтернеті коментарів, що виражають ненависть. Поліція провела обшуки в квартирах підозрюваних, їх було допитано за висунутими звинуваченнями. Ці заходи торкнулися 29 осіб, яких звинувачують у публічних закликах до здійснення правопорушень, ксенофобських і антисемітських висловлювань. Обшуки стали частиною заходів по боротьбі з коментарями, що містять вказані висловлювання. За даними німецької поліції, в минулому році було зареєстровано 2,3 тис. таких висловлювань [15]. Наприкінці минулого року в Німеччині набув чинності закон, метою якого є боротьба з фейковими новинами та ненависницькими коментарями в соцмережах. Відповідно до цього закону, такі висловлювання повинні бути максимально швидко видалені з соцмереж, а їх авторам може загрожувати до 5 років позбавлення волі [15].

Також євроспільнота постійно шукає ефективні механізми протидії російській інформаційній експансії, зокрема поширенню фейкових новин. Так, наприкінці 2018 року у Брюселі розпочала роботу група експертів, що протидіятиме поширенню неправдивої фейкової інформації у електронних ЗМІ. Ця комісія має розробити механізми розпізнавання фальшивих даних та запровадити обмеження щодо їх поширення. Перше завдання групи – дати визначення поняттю "фейкові новини" та підготувати пропозиції для подальших дій Єврокомісії. Група складається з 40 експертів, серед яких присутні фахівці із соціальних мереж, працівники ЗМІ, активісти, представники громадськості та провідні вчені [16].

Таким чином, світ вступає у нову виборчу фазу з урахуванням оновлень європейських інституцій. Сьогодні країни ЄС та США визнають глобальні масштаби російської агресивної інформаційної кампанії та вбачають в ній глобальну загрозу для їхнього інформаційного простору. У зв'язку з цим розроблюються нові законодавчі акти та впроваджуються практичні заходи, спрямовані на її суцільну нейтралізацію.

З урахуванням викладеного, саме результати активної фази протистояння між Заходом та РФ в інформаційній сфері визначатимуть розвиток ситуації в світі, яка безпосередньо впливає на Україну.

Висновки.

Враховуючи 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.

З метою реалізації цього завдання доцільним вбачається вжиття заходів щодо:

- виявлення та припинення деструктивних дій окремих державних та неурядових структур суміжних країн: РФ, Румунії, Угорщини, Республіки Польщі, мінімізувати іноземний вплив та нейтралізувати їх наміри, які можуть негативно вплинути на шкоду національним інтересам України;
- виявлення, запобігання та припинення спроб представників 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, у тому числі й з використанням соціальних мереж, що може спричинити дестабілізацію суспільно-політичної обстановки, особливо у регіонах;
- виявлення і недопущення використання закордонними неурядовими організаціями та їх функціонерами можливостей вітчизняних ЗМІ, ресурсів мережі Інтернет, представників мас-медійних громадських організацій та інших фахових об'єднань для створення механізмів впливу, у т.ч. 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.

Використана література

1. Доктрина інформаційної безпеки України: Указ Президента України від 25.02.17 р. № 47. *Офіційний Вісник України*. 2017. № 20. Ст. 554.

2. Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки: Закон України від 09.01.07 р. № 537-V. *Офіційний Вісник України*. 2007. № 8. Ст. 273.

3. 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 (дата звернення: 20.12.2018).

4. Доктрина информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 05.12.16 г. № 646. URL: https://rg.ru/2016/12/06/doktrina-infobezopasnost-site-dok.html (дата звернення: 20.12.2018).

5. Варшавський саміт НАТО і російська загроза. URL: https://www.bbc.com/ukrainian/politics/2016/07/160708_warsaw_nato_summit_ozh (дата звернення: 17.01.2019).

6. Нові аспекти інформаційного протистояння між Росією та Заходом. URL: http://bintel.com.ua/uk/article/02-18-infowar (дата звернення: 17.01.2019).

7. Про загальні заходи безпеки мережевих та інформаційних систем: Директива Європейського Парламенту та Ради № 2016/1148. URL: https://zakon.rada.gov.ua/laws/show/994_242/card5 (дата звернення: 17.01.2019).

8. Стосовно заходів щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі: Директива Європейського Парламенту та Ради від 6 липня 2016 р. № 2016/1148. URL: http://eur-lex.europa.eu/eli/dir/2016/1148/oj (дата звернення: 20.12.2018).

9. У Німеччині пропонують соцмережі зобов'язати до співпраці зі спецслужбами URL: http://www.eurointegration.com.ua/news/2016/08/7/7053101 9 (дата звернення: 20.12.2018).

10. Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних: збірник перекладу документів ("Пакет захисту даних" Європейського Парламенту і Ради від 2016 р.) пер. з англ. І. Майстренко / за ред. В. Брижко; передмова В. Пилипчука. – (НДІ інформатики і права Національної академії правових наук України). Київ: ТОВ "Видавничий дім "АртЕк", 2018. 180 с.

Регламент (ЄС) 2016/679 від 27 квітня 2016 р. (General Data Protection Regulation). URL: https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf (дата звернення: 17.01.2019).

11. У США схвалили закон про запровадження санкцій за кібератаки. URL: https://24tv.ua/u_ssha_shvalili_zakon_pro_zaprovadzhennya_sanktsiy_pro_kiberataki_n1027167 (дата звернення: 17.01.2019).

12. ПАРЄ прийняла резолюцію щодо протидії пропаганді РФ. URL: https://uatv.ua/parye-pryjnyala-rezolyutsiyu-shhodo-protydiyi-propagandi-rf (дата звернення: 17.01.2019).

13. Стратегічний огляд (Revue stratégique) URL:https://www.defense.gouv.fr/dgris/presentation/evenements/revue-strategique-de-defense-et-de-securite-nationale-2017 (дата звернення: 28.12.2018).

14. Якщо поглянути на Францію, то вона готує новий закон для протидії фейкам на виборах. Пропаганду забанять у Google. URL: https://www.eurointegration.com.ua/articles/2018/ 03/ 20/7079007 (дата звернення: 28.12.2018).

15. У Німеччині прийшли з обшуками до тих, хто пише ксенофобські коментарі в Інтернеті. URL: https://mind.ua/news/20185840-u-nimechchini-prijshli-z-obshukami-do-tih-hto-pishe-ksenofobski-komentari-v-interneti (дата звернення: 17.01.2019).

16. Соціальні мережі як чинник інформаційної безпеки. Огляд Інтернет-ресурсів (01. – 16.01.2018). URL: http://www.nbuviap.gov.ua/images/sozinfo/2018/1.pdf (дата звернення: 28.12.2018).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~