УДК 329.09.5

***Піскорська Г.А.*[*], *Яковенко Н.Л.*[**]**

СУЧАСНІ ВИКЛИКИ І ЗАГРОЗИ В КІБЕРПРОСТОРІ: ФОРМУВАННЯ МЕХАНІЗМУ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

***Анотація**. Одним зі світових трендів є тенденція до значного зростання кількості кібератак, які стають все більш витонченими і малопрогнозованими. Інформаційні операції РФ можуть привести до повсюдного використання інформаційно-комунікаційних технологій в міждержавних конфліктах. Питання забезпечення кібербезпеки є надзвичайно актуальними для України, проте заходи з протидії викликам і загрозам у зазначеній сфері не мають комплексного характеру. Поява Закону України про кібербезпеку і посилення міжнародного співробітництва в сфері захисту кіберпростору з США і Європейським Союзом стало актуальним як ніколи.*

***Ключові слова:** кіберпростір, кібербезпека, кібератака, критичні об'єкти інфраструктури держави, міжнародне співробітництво в сфері захисту кіберпростору.*

***Annotation.** One of the world trends is the tendency to a significant increase in the number of cyber attacks, which are becoming more sophisticated and less predictable. Information operations of the Russian Federation can lead to the widespread use of information and communication technologies in interstate conflicts. Ensuring cybersecurity is extremely important for Ukraine in conditions of a hybrid war. The Law of Ukraine on Cybersecurity and further development of international cooperation in the field of cyberspace protection with the United States and the European Union is more urgent than ever. It is*

[*] кандидат історичних наук, доцент, старший науковий співробітник Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

[**] доктор історичних наук, професор, професор Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

necessary to improve international mechanisms and a common international policy to develop and implement effective methods for combating cyber threats.

Key words: *cyberspace, cybersecurity, cyber attack, critical objects of state infrastructure, international cooperation in the field of cyberspace protection.*

Аннотация. *Одним из мировых трендов является тенденция к значительному росту количества кибератак, которые становятся все более изощренными и малопрогнозируемыми. Информационные операции РФ могут привести к повсеместному использованию информационно-коммуникационных технологий в межгосударственных конфликтах. Вопросы обеспечения кибербезопасности чрезвычайно актуальны для Украины, однако меры по противодействию вызовам и угрозам в указанной сфере не имеют комплексного характера. Появление Закона Украины о кибербезопасности и усиление международного сотрудничества в сфере защиты киберпространства с США и Европейским Союзом актуально как никогда.*

Ключевые слова: *information, Internet, types of telecommunications, communications, contemporary system of international relations.*

Постановка проблеми. Завдяки потужній інформаційній кампанії США та їх союзників, а також Росії та її союзників події в Україні та Сирії перетворилися на запеклу боротьбу за визнання/невизнання Росії як «великої держави». Захід фактично проігнорував Росію, відмовивши їй у статусі «великої держави», тоді як Росія проігнорувала думку Заходу.

В умовах протидії російській гібридній агресії дедалі більше країн робитимуть ставку на мілітаризацію інформаційного простору й розвиток технологій його безпеки. Нинішній рівень інформатизації України у цілому й органів державної влади зокрема засвідчує актуальність загрози використання проти української держави кібернаступальних технологій.

Мета статті – дослідити сутнісні характеристики формування механізму міжнародної інформаційної безпеки. Завдання статті: проаналізувати особливості забезпечення кібербезпеки України.

Виклад основного матеріалу. Особливою метою кіберзлочинців є критично важливі об'єкти інфраструктури країни. У червні 2017 року сталась найбільша кібератака в історії країни, що заблокувала роботу тисяч українських компаній і державних органів. Головною жертвою вірусу-шифрувальника Petya.A стала Україна, де зареєстровано понад 75% всіх випадків зараження [1].

Впродовж лише одного дня комп'ютерний вірус "Ransom: Win32/Petya" атакував приватний і державний сектори економіки України, зокрема банки, аеропорти, державну залізничну компанію, телекомпанії, телекомунікаційні компанії, великі мережеві супермаркети, енергетичні компанії, державні фіскальні служби, органи державної влади і місцевого самоврядування та ін. Вірусом були вражені також приватні та державні суб'єкти інших держав [2].

Вірус-вимагач, який блокує доступ до даних і вимагає викуп у розмірі 300 доларів в біткоінах за розблокування, атакував десятки енергетичних, телекомунікаційних та фінансових компаній і організацій по всьому світу. Фахівці в цій галузі сходяться в тому, що найбільше постраждала Україна. Держава виявилася не в змозі протистояти такій атаці, яка, в свою чергу, виявила незахищеність життєво важливих інтересів людини й громадянина, суспільства і держави при використанні кіберпростору і відсутності можливості своєчасного виявлення, попередження і нейтралізації реальних і потенційних загроз національній безпеці в кіберпросторі.

Вперше в Україні проект Закону про кібербезпеку був зареєстрований групою депутатів з різних фракцій в червні 2015 р. На початку 2016 р. у зв'язку з затвердженням президентом «Стратегії кібербезпеки України» документ втратив актуальність і був відкликаний.

Пізніше був зареєстрований вже новий суттєво доопрацьований проект. У жовтні 2017 р. закон був остаточно прийнятий парламентом та набере чинності 9 травня 2018 року [3].

Новий закон спрямовано на формування загальної державної політики кібербезпеки, а також розподіл функцій між різними відомствами. Зокрема, він дає повноваження спецслужбам для здійснення кіберзахисту країни. За законом, координувати дії в сфері кібербезпеки буде Президент через Раду національної безпеки та оборони (РНБО). Також передбачено створення Національної системи кібербезпеки, яка об'єднає низку міністерств та відомств. До неї увійдуть Держслужба спеціального зв'язку та захисту інформації, Національна поліція, Служба безпеки України, Міністерство оборони і Генеральний штаб, Національний банк, а також розвідувальні органи. Закон чітко визначає, яке відомство і за що буде відповідати в сфері кіберзахисту. Координація та здійснення державної політики стають відповідальністю Держспецзв'язку. Нацполіція повинна буде забезпечувати захист громадян, суспільства і держави в кіберпросторі, а також вживати заходів для запобігання кіберзлочинності. Серед завдань СБУ – розслідування кіберінцидентів та кібератак, здійснених проти державних інфосистем. При цьому Міноборони і Генштаб мають готувати державу «до відбиття військової агресії в кіберпросторі». Нацбанк є відповідальним за кібербезпеку в банківській сфері, зокрема, шляхом створення центру кіберзахисту НБУ. До того ж, в Україні буде створено Національну телекомунікаційну мережу, до якої увійдуть інформаційні системи бюджетної сфери (органи державної влади та держпідприємства). Порядок її формування покладено на уряд. За захищений доступ держорганів, антивірусний захист і аудит інформаційної безпеки відповідатиме Державний центр кіберзахисту.

Закон передбачає появу переліку об'єктів критичної інформаційної інфраструктури. Відповідальність за розробку правил його формування і функціонування, а також критеріїв включення об'єктів до цього реєстру

покладено на Кабмін. Такий самий реєстр, але в банківській сфері, має створити і НБУ. До об'єктів критичної інфраструктури можуть бути віднесені підприємства, що працюють в сфері енергетики (наприклад, АЕС), хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, а також підприємства банківського і фінансового секторів. Крім того, до реєстру можуть увійти підприємства сфер централізованого водопостачання, постачання електроенергії та газу, виробництва продуктів харчування і охорони здоров'я. До реєстру таких підприємств також потрапляють ті, що мають потенційно небезпечне виробництво та стратегічне значення для економіки і безпеки держави.

В разі включення підприємства до такого переліку, відповідно до Закону, його власники або керівники автоматично стають відповідальними за забезпечення кіберзахисту комунікаційних систем і захист технологічної інформації. Крім того, керівники підприємств матимуть терміново інформувати урядову команду реагування на комп'ютерні надзвичайні події – CERT-UA – про інциденти кібербезпеки. CERT-UA аналізуватиме дані щодо інцидентів, допомагатиме запобіганню кібератак і усуненню їх наслідків в разі потреби. Крім того, на критично важливих підприємствах щорічно здійснюватиметься незалежний аудит щодо ефективності систем кіберзахисту. В правове поле також вводиться державно-приватна взаємодія як один з принципів забезпечення кібербезпеки. Взаємодія передбачає обмін інформацією про інциденти кібербезпеки, реалізацію спільних науково-дослідних проектів, навчання кадрів у цій сфері та ін.

Закон також передбачає поглиблення міжнародного співробітництва в сфері захисту кіберпростору передусім з Європейським Союзом і НАТО. Відповідно, Закон обмежує участь в кіберзахисті будь-яких компаній і установ з Росії, а також підсанкційних осіб або інших країн. Фінансування кібербезпеки, за Законом, можливе як за бюджетні кошти, так і приватні або кредитні. Припустимо також використання міжнародної технічної допомоги або інших джерел, які не заборонені законодавством.

Одним з істотних моментів в прийнятому Законі є фактичне прирівнювання злочинів в кіберпросторі до звичайних. Так, Закон вводить в правову площину саме поняття «кіберзлочини», яке позначається як суспільно небезпечне діяння, за яке передбачена кримінальна відповідальність.

У США підтримали діяльність українських законотворців, і в лютому 2018 конгресмени схвалили проект Закону про співпрацю з Україною з питань кібербезпеки, спрямований на просування активної взаємодії між Україною та США в сфері кібербезпеки [4]. Законопроект розроблено на Капітолійському пагорбі під керівництвом члена комітету з міжнародних справ палати представників Брендана Бойла – безпосередньо для української держави. В ході обговорення документа Бойл заявив: «Впродовж останніх років Росія використовувала Україну як полігон для кібератак, які ставлять під загрозу національну безпеку нашого великого союзника, України, а також її сусідів по регіону» [5].

Експерти зазначають, що це буде перший закон США в сфері кібербезпеки, де слово Україна винесено в заголовок. При цьому в тексті згадується Будапештський меморандум, і Україні пропонується разом з Америкою виконувати лідерську роль в поліпшенні кібербезпеки у всій Центральній і Східній Європі. Закон свідчить про відповідальне ставлення наддержави до безпеки в регіоні. Підтверджується прихильність США Хартії про стратегічне партнерство між США і Україною та прихильність США до підтримці співпраці між НАТО і Україною [6].

Конгрес дав зрозуміти, що усвідомлює небезпеку неконвенційної війни, і що поза увагою конгресменів не залишаються все напади на енергетичні об'єкти, газо-транспортну систему, аеропорти, метро в Україні. Варто зазначити, що американські експерти давно попереджали про реальну кіберзагрозу Заходу, яка виходить від РФ. Так, ще в березні 2015 р. директор національної розвідки Джеймс Клеппер повідомив Комітету з питань Збройних Сил Сенату в ході презентації «Оцінки всесвітньої

загрози службою розвідки США» (2015): «Хоча я не можу вдатися до деталей тут, російська кіберзагроза є більш суворою, ніж ми раніше оцінювали». У доповіді складні кібератаки визначено основною загрозою національній безпеці США. Наголошено, що «кібернетичні загрози національній і економічній безпеці США зростають за частотою, масштабом, витонченістю та ступенем тяжкості впливу». Росію вирізнено як одну з найрозвинутіших держав-гравців у міжнародному кіберпросторі. Доповідь містить інформацію про те, що Міністерство оборони Росії створює власну кибернетичну команду, відповідальну за проведення наступальних комп'ютерних заходів (подібно до Cyber Command Сполучених Штатів), яка діятиме на кшталт свого американського колеги при проведенні кіберпропагандистських операцій та кібератак проти супротивника та ворожих управлінських систем. Наголошено, що «неідентифіковані російські кіберактори» досягли спроможності вражати промислові системи управління і таким чином атакувати електроенергетичні мережі, управління повітряним рухом та нафтогазові мережі [7].

У Законі США про співробітництво з Україною з питань кібербезпеки містяться певні положення, які фактично є зобов'язаннями для американської влади. Наприклад, Державному Секретарю – вживати заходів, відповідно до інтересів США, щодо допомоги Україні в підвищенні її кібербезпеки. Департамент енергетики буде нести відповідальність для створення українсько-американської робочої групи з розробки Програми кібернетичної безпеки України. Тобто, є чіткі положення, що це – завдання Держдепу і Міністерства енергетики, і чим саме вони мають допомогти українській стороні. Встановлюється формат відносин, констатується, якими вони повинні бути, оскільки до цього часу офіційних документів, в яких це закріплено, не існувало. Американська влада має робити певні кроки по захисту критичної інфраструктури [8].

Проте варто зазначити, що поняття «кібербезпека» в документі стоїть далеко не на першому місці. Велика частина його положень підтверджує інші двосторонні американсько-українські ініціативи: США повинні допомогти Україні в боротьбі з російською пропагандою в соціальних мережах, а також розширити співпрацю по лінії політики, економіки, торгівлі і культури. Зокрема, США мають організувати допомогу щодо захисту урядових українських комп'ютерних мереж, обмін інформацією, позбавлення від російського програмного забезпечення. Це рамковий документ, який дозволяє почати ефективний двосторонній діалог, а як він буде наповнюватися, залежить від учасників діалогу, від комісії, яка буде працювати як в США, так і в Україні [9].

Можна розглянути і інші аспекти американської політики. Наприклад, вивчення активності РФ в кіберпросторі в зв'язку з підсумками президентських виборів в США 2016 г. почалося ще до вступу Д. Трампа на посаду глави Білого дому. Комітети американського Сенату оголосили про це завчасно (Комітет з міжнародних зв'язків, 04.01.2017; Комітет з питань збройних сил, 05.01.2017; Комітет з розвідки, 06.01.2017). Варто згадати і ту обставину, що в травні 2017 р. Міністерство юстиції США призначило колишнього главу ФБР Роберта Мюллера на посаду спеціального прокурора для розслідування втручання Росії в президентські вибори США 2016 р. [10]. У наказі Мін'юсту безпосередньо зазнвчається, що Мюллер повинен розслідувати: 1. спроби російського уряду втручатися в американські вибори 2016 р.; 2. будь-які зв'язки або координацію між Росією і особами, пов'язаними з передвиборчим штабом Дональда Трампа.

Ситуацію щодо зростаючих загроз з боку Росії в інформаційно-комунікаційній сфері розглядають і в інших державах Євроатлантичної спільноти, де представники спеціальних служб періодично заявляють про небезпеку, що виходить із РФ. Наприклад, 15 лютого Лондон поклав відповідальність на Москву за масштабну кібератаку з використанням вірусу NotPetya в Україні. За заявою заступника глави МЗС

Великобританії Таріка Ахмада, який відповідає в британському відомстві за питання кібербезпеки, дана атака продемонструвала «тривалу неповагу до українського суверенітету» з боку РФ [11].

З метою протидії інформаційній політиці Москви працює робоча група Євросоюзу зі стратегічних комунікацій (StratCom Task Force), яка була створена рішенням глав держав і урядів ЄС у березні 2015 р. для протидії російським дезінформаційним кампаніям. Група задіяна в розробці комунікаційних матеріалів і кампаній, покликаних роз'ясювати політику ЄС в країнах Східного партнерства (СП) (Азербайджан, Вірменія, Білорусь, Грузія, Молдова та Україна). Вона працює в тісній співпраці з інститутами ЄС та його представництвами в країнах Східного партнерства. Оперативна робоча група підтримує спільні прагнення ЄС щодо зміцнення медійного середовища в країнах СП в тісній співпраці з іншими суб'єктами ЕС. Група аналізує і доповідає про тенденції дезінформації, пояснює і спростовує її наративи, а також підвищує обізнаність щодо цієї проблеми [12].

На 2018-2020 рр. її бюджет складе 1,1 млн євро. Субсидія на зазначену суму вже закладена в бюджет Євросоюзу, а становлення проекту пройшло в ході саміту «Східне партнерство», де британський Прем'єр-міністр заявила, що в наступні 5 років тільки Лондон витратить 100 млн фунтів стерлінгів на боротьбу з «пропагандою Кремля» в східноєвропейських країнах. До речі сказати, що незабаром після цієї заяви Британія уклала двосторонню угоду з Польщею з метою узгоджено протидіяти «російській дезінформації».

Восени 2017 року в Гельсінкі в районі Серняйнен офіційно почав роботу Європейський центр з протидії гібридним загрозам на чолі з начальником відділу Поліції безпеки Фінляндії (Supo) Матті Саарелайненом. Відомо, що до проекту долучилися США і європейські держави, включаючи Великобританію, Іспанію, Німеччину, Францію, Норвегію, Швецію, Польщу, і колишні радянські республіки Прибалтики;

основне фінансування структури здійснюється за рахунок Фінляндії. Як заявив начебто випадково опинившись на семінарі в день відкриття Центру заступник Генерального секретаря НАТО Арндт Фрейтаг фон Лорінгхофен, «Росія є однією з країн, за якою ведеться спостереження в Центрі».

У вересні 2017 р. на саміті з цифрових технологій президент Литви Даля Грібаускайте виступила з ініціативою «кібернетичного Шенгену» – створення в рамках ЄС сил швидкого реагування на кібернетичні атаки. На її думку, дана структура буде доповнювати НАТО в боротьбі з гібридними загрозами, тероризмом і допомоги третім країнам. Вже в грудні учасники європейської програми Постійного структурованого співробітництва (PESCO) схвалили надання взаємодопомоги для забезпечення кібернетичної безпеки і створення кібергрупи швидкого реагування, включивши цю ініціативу в число 17 затверджених проектів. Як зазначають європейці, створення таких сил виведе взаємодію держав ЄС в кібернетичній сфері на новий рівень, коли країни-учасниці не обмежуватимуться лише національним форматом. Керуватиме проектом Литва.

Вищенаведене свідчить про високу зацікавленість ряду західних країн в керуванні процесами в кіберпросторі. Рішення проблем в сфері кіберзлочинності є важливим насамперед з огляду на формування надійного механізму міжнародної інформаційної безпеки. Транскордонний характер кіберзлочинів, використання серверів та технічних майданчиків різних країн обумовлює необхідність розвитку співпраці на міждержавному рівні. Поки ж, в спробах пояснити власні політичні негаразди, з Євроатлантики лунають звинувачення про «втручання Росії» за допомогою інформаційно-комунікаційних технологій в електоральні та інші політичні процеси, що аж ніяк не сприяє вирішенню назрілих протиріч в даній сфері. Мілітаризація кіберпростору сягне уже в найближчому майбутньому критичної позначки, коли виникнуть

об'єктивні передумови для укладання на міжнародному рівні спеціальних регулюючих договорів з питань інформаційної безпеки та оборони. Подібні договори з міжнародної інформаційної безпеки, ініційовані ще в 90-ті роки РФ та КНР поки що вперто торпедуються США. Проте, неможливість США забезпечити власне лідерство в сфері ІКТ та їхня вразливість до чисельних кібернападів змусить їх піти на поступки в питаннях укладання договору з міжнародної інформаційної безпеки, який прирівняє інформаційну зброю до зброї масового ураження та заборонить на рівні міжнародного права її «проліферацію».

Проблеми кібернападів і кібератак, як зазначено, постійно зростають, і способи подобних нападів змінюються, удосконалюються, особливо збільшуються кібердари по Інтернету, в результаті чого відбувається збій в системі кіберпростору і інтернет-мережі. Почастішали випадки нанесення кібератак з метою ослаблення зовнішньої політики і політики безпеки окремих держав, інфраструктурних та соціальних систем, банківських і фінансових структур. Такі кіберзагрози вимагають об'єднання зусиль всіх держав для координації співпраці, обміну важливою інформацією з зарубіжними партнерами в сфері кібербезпеки. Проблеми забезпечення кібербезпеки в контексті глобальних загроз обумовлюють створення нових механізмів щодо вирішення глобальних проблем кіберпростору і протидії кібератакам, злочинним діям зловмисників, стабільності системи кібербезпеки та інформаційної безпеки загалом.

Україна як повноправний член ООН має всі шанси виступити одним з ініціаторів подібного масштабного міжнародного договору з питань «нерозповсюдження» інформаційної зброї, боротьби з кібертерором та шпигунством в Інтернет-просторі. МЗС України доцільно активізувати роботу у форматі комісій, експертних груп, інших дорадчих та координуючих органів ООН, задіяних у формування політики ООН в сфері міжнародної інформаційної безпеки та глобальної кібербезпеки. З метою посилення кібербезпеки та протидії кібертерору й кіберзлочинності

потребує детального вивчення та впровадження в Україні досвід діяльності «Центру міжнародного багатостороннього партнерства проти кіберзагроз» та «Центру глобальної відсічі в кіберпросторі». МЗС України також доцільно ініціювати обговорення питань кібербезпеки як в рамках двосторонніх українсько-російських відносин, так і в рамках співробітництва України з міжнародними організаціями – Вишеградською групою, ЄС, НАТО, ОДЕР-ГУАМ, ОЧЕС.

Формування системи забезпечення міжнародної інформаційної безпеки визначається ступенем політичної довіри між урядами держав з урахуванням принципів взаєморозуміння, рівноправності і узгодженості інтересів. Очевидна необхідність ведення діалогу з усього спектру цих питань, розробка і вдосконалення міжнародних договорів і національного законодавства в сфері інформаційної безпеки. Неодмінною умовою вирішення питань щодо правового та організаційного забезпечення інформаційної безпеки є розуміння того, що держава знаходиться в нерозривному зв'язку і взаємодії з іншими аналогічними структурами і суб'єктами, реалізуючи функції стратегічного і тактичного партнерства, співпраці й добросусідства.

Питання кібербезпеки здатні ускладнити міжнародні відносини, привести до кібервійни, тому вкрай необхідним є посилення взаємодії дії між країнами світу щодо неприпустимості зростання напруженості в світовому кіберпросторі.

Висновки. Забезпечення міжнародної безпеки в інформаційній сфері і в світовому кіберпросторі вимагає не тільки зусиль окремих країн світу, а й розробку і здійснення максимально ефективних міжнародних інструментів. Тому всі економічні і політичні ресурси з протидії загрозам міжнародної інформаційної та кібербезпеки повинні розглядатися на найвищому світовому рівні за участю основних кібердержав. Забезпечення кібербезпеки в контексті глобальних загроз, поряд з спільними зусиллями міжнародного співтовариства, диктує важливість розробки і здійснення

превентивних дієвих заходів проти кібератак і кіберзлочинів в світовому кіберпросторі, що обумовлено наступними факторами:

– в світовому кіберпросторі з'явилися небезпечні тенденції, зростає кількість кіберзлочинів, кібератак, кібершпигунства й інших злочинних діянь зловмисників;

– зростає напруженість між країнами, особливо провідними країнами світу в сфері кіберпростору, в наявності всі компоненти кібервійни;

– країнам світу необхідно розробити адекватні моделі державної політики та національні концепції з кібербезпеки, що відповідають вимогам національної безпеки держав в контексті глобальних викликів та інших тенденцій сучасності;

– необхідно вдосконалити міжнародні механізми і загальну міжнародну політику по розробці і здійсненню дієвих та ефективних інструментів;

– при цьому відмінність в інтересах країн, а також відсутність міжнародної правової бази перешкоджає розвитку співробітництва між державами.

Список використаних джерел

1. Главной жертвой вируса-шифровальщика Petya.A стала Украина, где зарегистрировано более 75 % всех случаев заражения [Електронный ресурс]. – Режим доступа : http://itc. ua/blogs/eset-glavnoy-zhertvoy-virusa-shifrovalshhika-petya-a-stala-ukraina-gde-zaregistrirovanobolee-75-vseh-sluchaev-zarazheniya/

2. Від кібератаки вірусом Petya.A постраждали до 10 % комп’ютерів в Україні – Шимків [Електронний ресурс] / Новое Время. – Режим доступу : http://nv.ua/ukr/ukraine/events/vid-kiberatakivirusom-petya-a-postrazhdali-do-10-komp-juteriv-v-ukrajini-shimkiv-1442363.html

3. Про основні засади забезпечення кібербезпеки України Закон від 05.10.2017 № 2163-VIII [Електронний ресурс] – Режим доступу : http://zakon5.rada.gov.ua/laws/show/2163-19

4. Ukraine Cybersecurity Cooperation Act of 2017 [Electronic resource]. – Mode of Access : https://www.congress.gov/bill/115th-congress/house-bill/1997

5. Конгрес США розглядатиме законопроект щодо України [Електронний ресурс]. – Режим доступу : https://ukrainian.voanews.com/a/zakonoproect-po-ukraini/4239695.html

6. Спільно з Україною в ролі лідерів з кібербезпеки: Законопроект Конгресу США [Електронний ресурс] – Режим доступу : https://www.ukrinform.ua/rubric-polytics/2399870-spilno-z-ukrainou-v-roli-lideriv-z-kiberbezpeki-zakonoproekt-kongresu-ssa.html

7. Russia Tops China as Principal Cyber Threat to US [Electronic resource]. – Mode of Access : https://thediplomat.com/2015/03/russia-tops-china-as-principal-cyber-threat-to-us/

8. Кібербезпека України: американці зробили перший крок [Електронний ресурс] – Режим доступу : https: //www.ukrinform.ru/rubric-polytics/2400079-kiberbezopasnost-ukrainy-amerikancy-sdelali-pervyj-sag.html

9. Ukraine Cybersecurity Cooperation Act of 2017 [Electronic resource]. – Mode of Access : https://www.congress.gov/bill/115th-congress/house-bill/1997

10. Экс-главе ФБР поручили расследовать роль России в выборах в США [Електронный ресурс]. – Режим доступа : https://www.bbc.com/russian/news-39957238

11. Лондон официально обвинил Москву в атаке вируса-вымогателя NotPetya [Електронный ресурс]. – Режим доступа : https://www.bbc.com/russian/news-43067377

12. ЕС выделяет отдельный бюджет на борьбу с дезинформацией из России [Електронный ресурс]. – Режим доступа : https://www.bbc.com/russian/news-42115898?ocid=socialflow_twitter