УДК 004.7.056.5(477)(045)

КІБЕРБЕЗПЕКА УКРАЇНИ: НАУКОВІ ТА ПРАКТИЧНІ ВИМІРИ СУЧАСНОСТІ

Валюшко І. О.,
аспірант,
Дипломатична академія України при МЗС України

У статті розкриваються проблеми кібербезпеки України. Звертається увага на наукове осмислення термінів «кіберпростір», «кібербезпека» як вітчизняними, так і зарубіжними дослідниками цього питання. Вказано, що дотепер ще не існує чітко визначеного змісту зазначених термінів, що ускладнює наукове осмислення та подальше практичне подолання тих проблем і викликів, які постають у кіберпросторі. Актуалізується питання кібермогутності держави. Відзначається, що для кіберпростору можуть застосовуватися модернізовані, проте за суттю ті ж самі підходи, які були сформульовані класиками геополітики. Описано основні загрози кібербезпеці України в контексті російської інформаційної- та кіберагресії. В колі уваги – питання реалізації патріотичних волонтерських проектів метою яких є протистояння російським кібератакам. Вказано, що з початком російської військової агресії проти України розпочалася трансформація національного інформаційного законодавства, в тому числі щодо кібербезпеки. У статті проаналізовано основні нормативно-правові акти України, які були прийняті з 2014 року та регулюють сферу кібербезпеки.

В статье раскрываются проблемы кибербезопасности Украины. Обращается внимание на научное осмысление терминов «киберпространство», «кибербезопасность» как отечественными так и зарубежными исследователями этого вопроса. Указано, что до сих пор еще не существует четко определенного смысла указанных терминов, что затрудняет научное осмысление и дальнейшее практическое преодоление стоящих в киберпространстве проблем и вызовов. Актуализируется вопрос кибермогущества государства. Отмечается, что для киберпространства могут применяться модернизированные, но по сути те же подходы, которые были сформулированы классиками геополитики. Описаны основные угрозы кибербезопасности Украины в контексте русской информацийной- и киберагресии. Обращается внимание к вопросу деятельности патриотических волонтерских проектов, целью которых является противостояние российским кибератакам. Указано, что с началом российской военной агрессии против Украины началась трансформация национального информационного законодательства, в том числе по кибербезопасности. В статье проанализированы основные нормативно-правовые акты Украины, которые были приняты с 2014 года и регулируют сферу кибербезопасности.

The article discusses the problems of cybersecurity in Ukraine. Attention is drawn to the scientific understanding of the terms ‘cyberspace’ and , ‘cybersecurity’ by domestic and foreign researchers of this subject. It is noted that there is still no clear definition of these terms and this complicates the scientific comprehension as well as further practical overcoming of the problems and challenges that arise in cyberspace. The article discusses the issue of cyber-power of the state. It is noted that essentially the same, yet modernised, approaches that were formulated by the classics of geopolitics can be applied for cyberspace. The article describes the main threats to the cyber security of Ukraine in the context of Russian aggression in cyberspace. Attention is drawn to the issue of patriotic volunteer projects with the goal to confront the Russian cyberattacks. It is indicated that with the beginning of the Russian military aggression against Ukraine, the transformation of legislation concerning the information, including on cybersecurity has began. The article analyses the main legal acts in Ukraine that have been adopted since 2014, which regulate the sphere of cyber security.

Ключові слова: кібепростір, кібербезпека, кіберагресія, кібермогутність, кіберзагроза.

Постановка наукової проблеми та її значення. Питання забезпечення кібербезпеки стоїть на порядку денному для багатьох країн світу. Нині кіберпростір розглядається як важливий безпековий імператив, оскільки від його реалізації залежать економічна, військова, соціальна та інші сфери діяльності держави. Розуміння нових викликів, які постали у сучасну інформаційну добу та необхідність їх нейтралізації, призвели до виникнення поняття «кібербезпека». Вважається, що вперше це поняття з'явилося у середині 1990-х років, коли уряд США став досліджувати цю тему [7]. Однак нині ще досі не існує єдиного універсального визначення терміну кібербезпека, що ускладнює процес дослідження питання. У сучасних умовах війни з РФ забезпечення безпеки України у кіберпросторі є одним із найактуальніших завдань. Реальна ситуація у цій сфері характеризується частими кібератаками на інформаційні ресурси держави, що є компонентом гібридної війни, яку веде Росія проти України. Загалом джерелами загроз у кіберпросторі України можуть бути як окремі злочинці або їх групи, підготовлені у сфері ІТ, а й іноземні державні органи, політичні структури та неформальні об'єднання. З огляду на важливість даного питання Україні необхідно удосконалювати механізми забезпечення кібербезпеки, зокрема термінологічну, технічну, професійну базу та законодавство.

Аналіз попередніх досліджень і публікацій. Серед зарубіжних науковців, які досліджували питання кібербезпеки з позиції провадження зовнішньої політики держави варто виділити М. Лібіцкі, Дж. Ная, С. Старра. Слід відмітити, що з початком Російської збройної агресії дещо збільшилася кількість публікацій з даної тематики серед вітчизняних вчених. Зокрема, варто відзначити праці Д. Дубова, присвячені стратегічним аспектам кібербезпеки України. Велике значення має його монографічне дослідження «Кіберпростір як новий вимір геополітичного суперництва», де серед іншого проаналізовані питання забезпечення національних інтересів України в глобальному та національному кіберпросторах. Питанням щодо тлумачення поняття кібербезпека присвячені роботи А. Погорецького, В. Шеломенцева О. Баранова. Проблема кібертероризму та кібератак розкрита у статті С. Гнатюка. Про філософське осмислення кіберпростору та природу російського месіанізму у ньому пише О. Добродум. Узагальнення існуючих робіт уможливлює поглиблення знань щодо окресленої теми, та виявити основні шляхи її подолання.

Мета і завдання статті. Метою статті є теоретичне осмислення питання кіберпростору, кібербезпеки та дослідження стану кібербезпеки України в контексті російської збройної агресії; аналіз законодавчої бази у цій сфері. Досягнення поставленої мети передбачає вирішення таких завдань: охарактеризувати поняття кіберпростору та кібербезпеки; проаналізувати основні загрози кібербезпеці України в контексті російської агресії; проаналізувати основні проблеми та визначити основні зрушення в законодавчій базі у сфері кібербезпеки, які відбулися після російського вторгнення.

Виклад основного матеріалу. Проблема дослідження кіберпростору характеризується рядом невизначеностей як у самій термінології, так і в нормативно-правовій сфері. Нині кіберпростір розглядається полем міждержавних протистоянь.

Вперше термін «кіберпростір» було використано письменником В. Гібсоном у 1982 р. у новелі «Спалення Хром» («Burning Chrome»). У 1984 р. це поняття було більш детально розкрито у творі «Нейромант» («Neuromancer»). І хоч цей термін часто зустрічається в міжнародно-правових актах, національних джерелах права, а також в працях зарубіжних та вітчизняних науковців, його застосування є достатньо умовним та суперечливим, він не має чітких загальноприйнятих рамок, часто пов'язується чи ототожнюється з поняттями: «інформаційний простір», «віртуальний простір», «комп'ютерна сфера», «Інтернет», «Інформаційно-комунікаційні системи і мережі» [30].

Широких масштабів проблема кібербезпеки набула тоді, коли держави усвідомили усі можливі наслідки від реалізації загроз у сферах, де використовувались комп'ютерні системи. При незначному обсязі ресурсів для реалізації цих загроз досягаються значні результати, здатні паралізувати цілі компанії та держави.

Американський підхід до питання кіберпростору визначився Національною військовою стратегією для операцій у кіберпросторі 2006 р. У документі кіберпростір визначений як «сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікування та обміну даними через мережеві системи та пов'язаної з ними фізичної інфраструктури» [6, с. 9].

Водночас Дж.Ліпман наполягає [4], що подібний підхід є характерним саме для фахівців з Міністерства оборони США. Останнім часом відбувається часткова зміна цієї точки зору, зокрема з-поміж військових спеціалістів, у бік розуміння кіберпростору як теоретичного (чи, швидше, віртуального) поняття.

«Огляд політики щодо кібепростору» від 2009 року – комплексний документ з оцінки стану кібербезпекового простору США та можливих способів його поліпшення – розуміє кібербезпеку відповідно до визначення, запропонованого в Директиві Президента з національної безпеки 54, Директиві Президента з внутрішньої безпеки 23 від 2008 року. Вони визначають кіберпростір як «взаємозалежні мережі, комп'ютерні системи, ІТ-інфраструктури, що включають інтернет, телекомунікаційні мережі, комп'ютерні процесори (embedded processors) та контролери у критично важливих сферах» [2, с. 1].

У Стратегії Франції, присвяченій питанням кібербезпеки, дано таке визначення: кібербезпека – це бажаний стан інформаційної системи, за якого вона може протистояти подіям з кіберпростору, що можуть поставити під загрозу доступність, цілісність або конфіденційність даних, які зберігаються, обробляються або передаються, і пов'язаних з ними послуг, які ці системи пропонують або роблять доступними [3].

З урахуванням того, що проблема кібербезпеки носить глобальний характер, цікавою видається позиція міжнародних організацій. Так, Міжнародний телекомунікаційний союз (International Telecommunication Union, ITU) у своїй Рекомендації дає таке визначення: кібербезпека – це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування та технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації та користувача [24].

У вітчизняній науці можна виділити наступні дефініції поняття кіберпростору.

О. Манжай вважає, що кіберпростір – це інформаційне середовище (простір), яке виникає (існує) за допомогою технічних (комп'ютерних) систем при взаємодії людей між собою, взаємодії технічних (комп'ютерних) систем та управлінні людьми цими технічними (комп'ютерними) системами» [18, с. 145]. А. Погорецький та В. Шеломенцев під кіберпростором вважають «штучне електронне середовище існування інформаційних об'єктів у цифровій формі, що утворене в результаті функціонування кібернетичних комп'ютерних систем управління й оброблення інформації та забезпечує користувачам доступ до обчислювальних й інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання інформаційних послуг, ведення електронної комерції тощо)» [20, с. 80].

О. Баранов дає таке визначення: кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації [9].

В. Фурашев визначає кібербезпеку як стан здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу (управління) інформації [29].

Деякі американські науковці слушно зазначають, що для кіберпростору мають застосовуватися суттєво модернізовані, проте за суттю ті ж самі підходи, які були сформульовані класиками геополітики, передусім американцями Х.Маккіндером і Н.Спайкменом. Наприклад, дослідники Ф.Крамер, С.Старр та Л.Вентц зазначають з цього приводу: «теж саме, що Макіндер та Спайкмен визначили для «земельної могутності» (land power), ті, хто розвиватиме теорію кібермогутності, мають визначити ключові ресурси та основні точки для кіберпростору» [1, с. 258].

Все більше науковців зосереджують увагу на питанні кібермогутності держави як здатності втілювати її волю та забезпечувати національні інтереси в кіберпросторі. Кібермогутність є досить складним питанням для науковців, адже включає в себе аспекти військової, політологічної, юридичної, телекомунікаційної та інших сфер і потребує ще подальшої розробки.

Нині для України питання кібербезпеки, нарощування потенціалу кібермогутності стоять на порядку денному. З початком російської гібридної війни, де кіберагресія є однією з її визначних складових, Україні необхідно самостійно шукати шляхи і механізми забезпечення кібербезпеки від сучасних загроз, які постають. Дуже слушно про це пише Д. Дубов, який вважає, що кіберзагрози Український державі та суспільству умовно можна розділити на два ключових рівні. Перший – «класичні» кіберзлочини – як абсолютно оригінальні, так і вже звичні для нас, для своєї реалізації вони потребують лише сучасних інформаційних технологій. Другий – злочини, характерні для геополітичної боротьби (або такі злочини на місцевому рівні, які мають потенціал вплинути на політичне становище держави): хактивізм, кібершпигунство та кібердиверсії. Водночас техніки здійснення атак в обох випадках демонструють чимало спільного. Наприклад, фішингові техніки можуть бути використані як для заволодінням коштами громадян, так і з кібершпигунською метою [14, с. 210].

Масовані кібератаки Росії вже неодноразово вражали сайти органів державної влади України (сайти Адміністрації Президента, Кабміну, Держспецзв'язку та ін.) та українських компаній; іде війна в соцмережах, яку розгорнули російські «фабрики троллів». Відомі численні російські хакерські групи «Sandworm», «Кіберберкут», «Спрут» які здійснюють різні диверсії в інформаційному просторі України. Нині вже не секрет, що за ними стоять і керують їх діяльністю російські спецслужби.

Вивчаючи матеріали Інтернету, присвячені месіанізму Росії в кіберпросторі, можна стверджувати про її прагнення відігравати творчу роль і здійснити сотеріологічне покликання в прийдешню

епоху. Меседж Ру-нету в цьому зв'язку – виступати засобом реінтеграції універсальної постнаціональної спільноти СРСР, формування нової ідентичності як суми «Homo Rosianus» і «Homo Runeticus», відновлення в кіберпросторі російсько-радянської національної ідентичності [12].

З метою протистояння кібервикликам в Україні було створено такі волонтерські проекти, як «Українські кібервійська», «Кіберальянс» (об'єднання груп «FalconsFlame», «Trinity», «Рух8» і «КіберХунта»). Наявність ефективної мережі громадських структур стає за сучасних умов однією з умов забезпечення національної безпеки. Однак наука в Україні до цього часу комплексно не досліджувала недержавну систему безпеки як громадський механізм, а громадські об'єднання – як суб'єкти забезпечення національної безпеки держави. Діяльність окремих різновидів громадських об'єднань не пов'язувалася з державною стратегією забезпечення національної безпеки [8].

До прикладу, «Інформаційний спротив» – неурядовий проект, головною ціллю якого є протидія в інформаційному полі зовнішнім загрозам, які виникають у військовій, економічній, енергетичній сферах України, а головне – у сфері інформаційної безпеки. Проект «Інформнапалм» був створений у лютому-березні 2014 року як спроба прориву інформаційної блокади та демонстрації доказів російської агресії, яка спочатку маскувалася під дії «кримської самооборони» і внутрішньоукраїнське громадянське протистояння. Велика заслуга активістів цієї організації полягає в тому, що українські патріоти помітили розгубленість офіційних структур і взяли на себе збір доказів та інформування світової спільноти на кількох мовах про повномасштабну воєнну інтервенцію Російської Федерації в Крим [16].

Крім того сама державна система та бюрократія не дозволяють державним структурам бути настільки мобільними, оперативними та використовувати соціальні мережі як патріотичні хакерські організації.

CERT-UA (Computer Emergency Response Team of Ukraine) при Державній службі спецзв'язку в 2014 р. зафіксувала 216 кібератак ззовні (більше половини з них – на державні установи). У 2015 р. число атак збільшилося в півтора рази.

До прикладу можна назвати атаку, яка відбулася 23 грудня 2015 року. Російським зловмисникам вдалось успішно атакувати комп'ютерні системи управління «Прикарпаттяобленерго» та вимкнули близько 30 підстанцій, залишивши близько 230 тисяч мешканців без світла. Ця атака стала першою у світі підтвердженою атакою, спрямованою на виведення з ладу енергосистеми[(використовувався небезпечний вірус BlackEnergy [15].

6 грудня 2016 р. внаслідок хакерської атаки була заблокована робота сайтів Державного казначейства, Міністерства фінансів, Пенсійного фонду. Згодом були атаковані Інтернет-ресурси Укрзалізниці і Міністерства оборони.

27 червня 2017 р. потужний комп'ютерний вірус паралізував роботу низки державних та приватних установ. Серед постраждалих – уряд України, національна пошта, метрополітен Києва, міжнародний аеропорт «Бориспіль», Чорнобильська АЕС, а також низка ЗМІ, банків, комерційних структур. За даними фахівців, вірус називається DOS/Petya.A. Вірус поєднує в собі функції блокувальника і шифрувальника. На відміну від схожого вірусу WannaCry, який блокував доступ до окремих файлів, Petya.A заблокував доступ не до диска, а до комп'ютера в цілому. Вірус поширювався не тільки в Україні, однак, на нашу державу припало 75,24% заражень від загальної кількості у світі. На Німеччину – 9,06%, на Польщу – 5,81%, Сербію – 2,87%, Грецію – 1,39%, Румунію – 1,02%. На Росію ж припало 0,8% [19].Чітких висновків про те, хто винен у поширенні вірусу досі немає. При цьому в Україні заявляють, слід кібератак веде до Росії [19].

За інформацією компанії Lookinglass Cyber Solutions, починаючи з середини 2013 року російські безпекові органи проводять масштабну кібероперацію «Армагедон», метою якої є отримання данних про плани та оцінки українських органів державної влади щодо розвитку конфліту на Сході України та про дії владних структур.

Доповідь «Операція Армагеддон: кібершпигунство як стратегічний компонент російської сучасної війни» – це один з перших досліджень кіберкампанії, де в часових рамках демонструється, як використовували кібервійни та шпіонаж в координації з кінетичною війною, плануванням бою та рухом військ разом з іншими стратегічними військовими тактиками та активами.

Ключові висновки доповіді полягають в наступному:

- Операція Армагеддон – це російська державна кампанія з підтримки кібершпигунства, яка діє щонайменше з середини 2013 року та орієнтується на українську владу, правоохоронні органи та військових посадовців з метою виявлення українських військових стратегій;
- Росія є провідним національним актором, що загрожує кібербезпеці, яка використовує наступальні кібероперації разом із кінетичними нападами в переслідуванні політичних та військових цілей;
- російська військова доктрина 2010 року визнає активізацію діяльності в галузі інформаційних боїв як особливості сучасної війни [5].

Крім того стало відомо, що італійська компанія Hacking Team, яка спеціалізується на розробці «наступальних» програмних продуктів, а також тих, що можуть використовуватися для стеження за користувачами, співпрацювала з ФСБ РФ. Остання виявила зацікавленість у продуктах компанії, що дозволяють отримувати доступ до пристроїв фірми Apple, а також мобільних пристроїв. Є підтвердження, що зазначені програмні комплекси будуть застосовуватися і проти України [13].

Реакцією української влади на тотальні кібератаки стало створення Кіберполіції. 5 жовтня 2015 року вона була створена, як структурний підрозділ Національної поліції. Метою створення Кіберполіції в Україні було реформування та розвиток підрозділів МВС України, що забезпечило підготовку та функціонування висококваліфікованих фахівців в експертних, оперативних та слідчих підрозділах поліції, задіяних у протидії кіберзлочинності, та здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності [17].

Очевидно, що нині Україна потребує висококваліфікованих кадрів у сфері кібербезпеки для реагування на нові виклики часу. Національне агентство із забезпечення якості вищої освіти України узгодило новий стандарт вищої освіти для спеціальності «Кібербезпека». Стандарт розробили у секторі вищої освіти Науково-методичної ради Міністерства освіти. Таким чином, «Кібербезпека» став першим затвердженим стандартом бакалаврського рівня [11]. До прикладу, з 2016 року в ДВНЗ «КНЕУ ім. В. Гетьмана» на факультеті інформаційних систем і технологій відкрита і проліцензована нова спеціальність «Безпека інформаційних і комунікаційних систем», галузь знань «Інформаційна безпека».

Перебуваючи вже четвертий рік у стані фактичної війни з Росією Україна змушена була вибудовувати оборону в кібербезпеці, адже з початків незалежності вони були відсутні, не кажучи вже про напрацювання наступальних механізмів у цій сфері.

2014 рік цілком можна вважати поворотним в усвідомленні державою усієї важливості інформаційної складової у забезпеченні національної безпеки. Адже інформаційний компонент гібридної агресії виявився не менш потужним, ніж військовий. За усі роки незалежності Україні не вдавалося позбутися системної проблеми – невідповідності законодавства в інформаційній сфері, у тому числі і щодо кіберпростору, сучасним реаліям. З початком російської військової агресії проти України розпочалася трансформація національного інформаційного законодавства.

Стартовим нормативно-правовим актом у цьому напрямку стало рішення РНБО «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 28 квітня 2014 року, введене в дію Указом в. о. Президента України від 1 травня 2014 року № 449/2014. Цим документом було поставлено завдання розроблення Стратегії кібернетичної безпеки України.

24 вересня 2015 року була прийнята Воєнна Доктрина України. Воєнна політика є невід'ємним компонентом діяльності кожної держави. Серед головних тенденцій, які впливають на воєнно-політичну обстановку в регіоні довкола України, Доктрина чітко визначає інформаційну війну Російської Федерації проти України, спроби несанкціонованого доступу до об'єктів інформаційної інфраструктури України [25]. Однак військові експерти, зокрема Д. Васильєв, наголошує на тому, що в доктрині слабко розкрита тема кібербезпеки, адже чимала частина гібридної війни відбувається в інформаційному просторі [10].

6 травня 2015 року РНБО схвалила проект нової Стратегії національної безпеки, яка розрахована до 2020 року. Цей стратегічний документ передбачає забезпечення національної безпеки, окрім іншого у сфері інформаційних ресурсів, критичної інфраструктури та кібербезпеки.

Окремими загрозами інформаційній, кбербезпеці, а також інформаційним ресурсам Стратегія визначає:

- ведення інформаційної війни проти України;
- відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства;
- уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак;
- фізичну і моральну застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

Пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів Стратегія визначає:

- розвиток інформаційної інфраструктури держави;
- створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT);
- моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації;
- розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів;

- забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмову від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації;
- реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав – членів НАТО та ЄС;
- створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони;
- розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікацію співпраці України та НАТО, зокрема, в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки [26].

Важливим і визначним документом стало прийняття Стратегії кібербезпеки України. Документ був введений в дію Указом Президента України № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України».

Стратегія визнає, що агресія Російської Федерації, що триває, інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України вимагають невідкладного створення національної системи кібербезпеки як складової системи забезпечення національної безпеки України. Метою Стратегії кібербезпеки України (далі – Стратегія) є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [27].

Документ визначає основні загрози кібербезпеці, пріоритети та напрями її забезпечення. Визначальними у ній є концептуальні положення, які вказують, що державна політика у сфері кібербезпеки має бути спрямована на досягнення сумісності з відповідними стандартами ЄС та НАТО. Окрім того документ передбачає конкретні кроки для розбудови національної системи забезпечення захисту кіберпростору, своєчасного виявлення та нейтралізації кіберзагроз, а також запобігання їм з урахуванням практики провідних держав-членів НАТО та ЄС. Також у Стратегії йдеться про пріоритети та напрямки забезпечення кібербезпеки, координацію, взаємодію і розподіл повноважень та відповідальності органів сектору безпеки і оборони України в питаннях кібербезпеки, кіберзахисту та протидії кібертероризму і кіберзлочинності.

Крім цього Стратегія передбачає залучення експертного потенціалу наукових установ, професійних і громадських об'єднань до підготовки проектів концептуальних документів у цій сфері; підвищення цифрової грамотності громадян та культури безпеки поведінки в кіберпросторі; розвиток міжнародного співробітництва і підтримку міжнародних ініціатив у сфері кібербезпеки. Згідно з документом, основу національної системи кібербезпеки складуть Міністерство оборони, Державна служба спеціального зв'язку та захисту інформації, СБУ, Національна поліція, НБУ, розвідувальні органи [22]. Головним недоліком Стратегії вважаємо те, що у ній відсутні визначення понять «кіберзлочин», «кібербезпека», «кіберпростір» та похідні від них.

Позитивним зрушенням у формуванні цілісної державної політики в інформаційній сфері стала Доктрина Інформаційної безпеки, яка була введена в дію Указом Президента України від 25 лютого 2017 року № 47/2017. У загальних положеннях Доктрини вказується, що «…застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства…» Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни [28]. І хоч Доктрина не згадує питання кібербезпеки як таке, однак, вода опосередковано служить цілісній політиці держави в забезпеченні кібербезпеки.

Основним недоліком Доктрини можна визначити те, що вона не має достатнього правового регулювання потенційного залучення громадянського суспільства до заходів забезпечення інформаційної безпеки.

Крім того, до Верховної Ради україни було подано законопроект «Про основні засади забезпечення кібербезпеки України» від 19.06.2015 р. N 2126а. У пояснювальній записці зазначається, що метою проекту закону є «створення національної системи кібербезпеки як сукупності політичних, соціальних, економічних та інформаційних відносин разом із організаційно-адміністративними та техніко-технологічними заходами шляхом комплексного підходу у тісній взаємодії державного і приватного секторів та громадянського суспільства» [21].

Даний документ важливий тим, що він уперше на законодавчому рівні може закріпити визначення понять «кібербезпека», «кіберпростір», «кіберзагроза», «кіберзахист», «кібероборона», «кібертероризм», «національна система кібербезпеки» та деякі інші терміни. Важливим є те, що серед іншого законопроект окреслює основні принципи та напрями забезпечення кібербезпеки, об'єкти кіберзахисту, визначає завдання Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, регулює державно-приватна взаємодію у сфері кібербезпеки тощо [23]. Станом на липень 2017 року законопроект підготовлений до повторного другого читання.

Висновки та перспективи подальшого дослідження. Нині питання забезпечення кібербезпеки є вкрай важливими для України. У сьогоднішній ситуації наша держава є об'єктом кіберагресії з боку Кремля. З огляду на ведення російської гібридної війни, де кіберпростір є ареною ведення військових дій, Україні необхідно розбудовувати не тільки оборонні спроможності у кіберпросторі, а й наступальні.

У протистоянні існуючим викликам і загрозам кібербезпеці заважають дві основні проблеми. Перша – це відсутність загальної термінології. Такі поняття, як кіберпростір, кібербезпека, кібервійна, кібератака, кібертероризм широко використовуються у науці, проте, дотепер ще не існує чітко визначеного їх змісту. Це у свою чергу ускладнює наукове осмислення та подальше практичне подолання тих проблем і викликів, які постають у кіберпросторі.

Другою проблемою є те, що за період незалежності і безпосередньо до 2014 року була відсутня якісна нормативно-правова база у сфері кібербезпеки. Однак відзначимо, що за останні роки вона значно удосконалилася.

Загалом, не зважаючи на певну розпорошеність, законодавство у сфері кібербезпеки України в останні роки було переглянуто і трансформовано відповідно до нових викликів та загроз. Це дає підстави вважати, що законодавча база у поєднанні із реструктуризацією системи національної безпеки дозволять створити потужний механізм стримування зовнішньої кіберагресії.

Разом з тим зауважимо, що побудова законодавства у такій важливій сфері, як кібербезпека, відбувається за принципом надолуження згаяного. Натомість, потрібно навчитися стратегічно планувати, прогнозувати.

Відзначимо, у сучасних умовах громадські об'єднання, як невід'ємний елемент громадянського суспільства, є повноцінним учасником процесу забезпечення інформаційної безпеки України. Взаємодія між громадським сектором та державними інститутами є важливим аспектом безпекової політики, однак, потребує додаткового вивчення та дослідження.

Література:

1. Cyberpower and National Security / ed.by Franklin D.Kramer, Stuart H.Starr, Larry Wentz.– Washington, D.C.: Potomac Books,2009.– 642 p.
2. Cyberspace Policy Review [Електронний ресурс].– Режим доступу: http://www.whitehouse.gov/assets/documents/Cyberspace_ Policy_ Review_final.pdf
3. Information systems defence and security: France's strategy. – French Network and Information Security Agency. – 2011. – С. 23. – Режим доступу : //www.gouvernement.fr/sites /default/files/fichiers_joints/livre-blanc-sur-la-defense-et-la-securite-nationale_2013.pdf
4. Liepman M.J., Jr.Cyberspace: The Third Domain / James M.Liepman, Jr.[Електронний ресурс].– Режим доступу: https://www.hsdl.org/?view&doc=89385&coll=public
5. Lookingglass Report: Russia Backed Cyber Attack on Ukraine Gov't Leaders. – [Електронний ресурс]. – http://blog.executivebiz.com/2015/04/lookingglass-report-russia-backed-cyber-attacks-on-ukrainian-govt-leaders/
6. National Military Strategy for Cyberspace Operations [Електронний ресурс].– Режим доступу: http://www.dod.gov/pubs/foi/ ojcs/07-F-2105doc1.pdf
7. Stubley D. What is Cyber Security? – [Електронний ресурс]. – www.7elements.co.uk/resources/blog/what-is-cyber-security
8. Антонюк В. Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці. – [Електронний ресурс]. – http://www.dy.nayka.com.ua/?op=1&z=747
9. Баранов О. Про тлумачення та визначення поняття «кібербезпека» // Інформація і право. – 2014. – № 2 (42). – С. 54-62.
10. Беззуб І. Нова Воєнна доктринаУкраїни: керівництво до дії чи декларація? – [Електронний ресурс]. – http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=1495:novavoenadoktruna2&catid=71&Itemid=382
11. В Україні вперше ввели бакалаврську спеціальність із «Кібербезпека». – [Електронний ресурс]. –
12. https://lviv.com/lab/v-ukrayini-vpershe-vvely-bakalavrsku-spetsialnist-iz-kiberbezpeky/
13. Добродумов О. Месіанізм та антимесіанізм Росії у кібепросторі. – [Електронний ресурс]. – http://dspace.nbuv.gov.ua/bitstream/handle/123456789/34971/36-Dobrodym.pdf?sequence=1
14. Дубов Д. «Питання створення «Огляду сектору кібербезпеки України». Аналітична записка. – [Електронний ресурс]. – http://www.niss.gov.ua/articles/1911/
15. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К: НІСД, 2014. – 328 с.

16. Зеттер К. Хакерська атака Росії на українську енергосистему: як це було. – [Електронний ресурс]. – http://texty.org.ua/pg/article/newsmaker/read/66125/Hakerska_ataka_Rosiji_na_ukrajinsku_jenergosystemu_jak
17. Історія InformNapalm. Відповіді на запитання, які ставлять найчастіше (FAQ). – [Електронний ресурс]. – https://informnapalm.org/ua/istoriya-informnapalm-vidpovidi-na-zapytannya-yaki-stavlyat-najchastishe-faq/
18. Кіберполіція (Україна) – [Електронний ресурс]. – https://uk.wikipedia.org/wiki/Кіберполіція_(Україна)
19. Манжай О.В. Використання кіберпростору в оперативнорозшуковій діяльності / О.В.Манжай // Право і безпека.Науковий журнал. – 2009. – № 4. – С. 142–149.
20. Опубліковано карту поширення вірусу Petya.A: Україна зазнала наймасштабнішої атаки. – [Електронний ресурс]. – https://www.unian.ua/politics/2003496-opublikovano-kartu-poshirennya-virusu-petyaa-ukrajina-zaznala-naymasshtabnishoji-ataki.html
21. Погорецький М. Поняття кіберпростору як середовища вчинення злочинів / М.Погорецький, В.Шеломенцев // Інформаційна безпека людини, суспільства, держави. – 2009. – № 2. – С. 77–81.
22. Пояснювальна записка до проекту Закону України «Про основні засади забезпечення кібербезпеки» – [Електронний ресурс]. – http://search.ligazakon.ua/l_doc2.nsf/link1/GH1N268B.html
23. Президент затвердив Стратегію кібербезпеки України. – [Електронний ресурс]. – https://dt.ua/POLITICS/prezident-zatverdiv-strategiyu-kiberbezpeki-ukrayini-202619_.html
24. Проект Закону України «Про основні засади забезпечення кібербезпеки України» – [Електронний ресурс]. – http://search.ligazakon.ua/l_doc2.nsf/link1/JH1N268W.html
25. Рекомендация МСЭ-Т X.1205. Обзор кибербезопасности. – Женева : МСЭ, 2009. – С. 55. – [Електронний ресурс]. – www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru
26. Указ Президента України Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України». – [Електронний ресурс]. – http://zakon2.rada.gov.ua/laws/show/555/2015
27. Указ Президента України Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» – [Електронний ресурс]. – http://zakon2.rada.gov.ua/laws/show/287/2015
28. Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» – [Електронний ресурс]. – http://zakon3.rada.gov.ua/laws/show/96/2016
29. Указ Президента України Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» – [Електронний ресурс]. – http://www.president.gov.ua/documents/472017-21374
30. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності // Інформація і право. – 2012. – № 2. – С. 162-169.
31. Шипка Р. Безпека в кібепросторі. – [Електронний ресурс]. – http://www.ispc.org.ua/wp-content/uploads/2015/07/conference_05_17.pdf#page=98