НАПРЯМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ

Черноног О.О.
слухач 1-го курсу спеціальності 8.15010004
“Державне управління у сфері національної безпеки”

Анотація

Інтеграція України у світовий кіберпростір призвела до постійного утворення нових загроз національним інтересам держави, пов’язаних з функціонуванням комп’ютерних мереж та систем. Це спричиняє необхідність концептуального переосмислення нової кібербезпекової реальності, впорядкування внутрішнього нормативно-правового поля і вирішення комплексу проблем, пов’язаних із розбудовою національної системи кібербезпеки.

Тому досліджено питання підвищення ефективності забезпечення кібербезпеки в системі публічного управління в умовах відсутності концептуального розуміння кібербезпекової політики України. Досліджено кіберзагрози і складові кіберконфліктів XXI сторіччя та сформульовані основні напрямки їх розвитку по відношенню до України в 2015–2016 роках. Проведено аналіз стану мілітаризації кіберпростору та проблематики міжнародної кібербезпеки.

На основі одержаних результатів виконано огляд проблем національного нормативно-правового та організаційного забезпечення кібербезпеки, що дозволило розробити сучасну модель національної системи кібербезпеки.

Впровадження запропонованої моделі національної системи кібербезпеки дозволить підвищити ефективність забезпечення кібербезпеки в системі публічного управління, покращить імідж держави на світовій арені та забезпечить стійкий розвиток національного сегменту кіберпростору в умовах глобального протистояння найбільших держав у кіберпросторі.

Ключові слова: кіберпростір, кібербезпека, кіберзагрози, кіберконфлікти, суб’єкти та об’єкти забезпечення кібербезпеки, національна модель кібербезпеки.

Аннотация

Интеграция Украины в мировое киберпространство привела к постоянному образованию новых угроз национальным интересам государства, связанных с функционированием компьютерных сетей и систем. Это вызывает необходимость концептуального переосмысления новой кибербезопасностной реальности, упорядочения внутреннего нормативно-правового поля и решения комплекса проблем, связанных с развитием национальной системы кибербезопасности.

Поэтому исследован вопрос повышения эффективности обеспечения кибербезопасности в системе публичного управления в условиях отсутствия концептуального понимания кибербезопасностной политики Украины. Исследованы киберугрозы и составляющие киберконфликтов XXI столетия и сформулированы основные направления их развития по отношению к Украине в 2015–2016 годах.

Проведен анализ состояния милитаризации киберпространства и проблематики международной кибербезопасности.

На основе полученных результатов выполнено описание проблем национального нормативно-правового и организационного обеспечения кибербезопасности, что позволило разработать современную модель национальной системы кибербезопасности.

Внедрение предложенной модели национальной системы кибербезопасности позволит повысить эффективность обеспечения кибербезопасности в системе публичного управления, улучшит имидж государства на мировой арене и обеспечит устойчивое развитие национального сегмента киберпространства в условиях глобального противостояния наибольших государств в киберпространстве.

Ключевые слова: киберпространство, кибербезопасность, киберугрозы, киберконфликты, субъекты и объекты обеспечения кибербезопасности, национальная модель кибербезопасности.

Annotation

The Ukraine's integration into the global cyberspace has led to continuous formation of new threats to national interests related to the operation of computer networks and systems. This leads to the need for a new conceptual rethinking of cybersecurity reality, improvement of the internal legal framework and solution of problems related to the development of national cybersecurity systems.

That's why the problem of the increasing of effectiveness of cybersecurity in the system of public administration in the absence of conceptual understanding of cybersecurity Policy of Ukraine was investigated. Cyber threats and integrated parts of cyber conflicts of XXI century were investigated and the main spheres of it's development in relation to Ukraine in the years 2015–2016 were represented. The analysis of the militarization of cyberspace and international issues of cybersecurity were held.

On the basis of the results, the description of problems of national regulatory and organizational support for cybersecurity was carried that allowed the development of a modern model of the national cybersecurity.

The implementation of the proposed model of the national cybersecurity will improve the effectiveness of cybersecurity in the system of public administration, improve the image of the country on the world stage and ensure sustainable development of the national segment of cyberspace in conditions of a global confrontation of largest countries in cyberspace.

Key words: cyberspace, cybersecurity, cyber threats, cyber conflicts, subjects and objects to ensure cybersecurity, a national model of cybersecurity.

Перелік умовних позначень

CERT	–	Computer Emergency Response Team, команда реагування на комп'ютерні надзвичайні події.
CERT-UA	–	Computer Emergency Response Team of Ukraine, команда реагування на комп'ютерні надзвичайні події України.
CCD CoE	–	NATO Cooperative Cyber Defence Centre of Excellence, Центр кіберзахисту НАТО в м. Таллінні.
CSIRTs	–	Computer Security Incident Response Teams.

DDoS – Distributed Denial of Service, розподілена атака “на відмову в обслуговуванні”.
DNS – Domain Name System, система доменних імен.
DoS – Denial-of-Service (DoS), атака “на відмову в обслуговуванні”.
FIRST – Forum for Incident Response and Security Teams, Форум команд реагування на інциденти інформаційної безпеки.
GPS – Global Positioning System, система глобального позиціонування.
IT – Information Technology, інформаційні технології.
NATO – North Atlantic Treaty Organization, Організація Північноатлантичного договору.
NIST – National Institute of Standards and Technology, Національний інститут стандартів і технологій США.
ATEC – Азійсько-Тихоокеанське економічне співробітництво, The Asia-Pacific Economic Cooperation.
ЄС – Європейський Союз.
ЗС – Збройні Сили.
ІКТ – інформаційно-комунікаційні технології.
ІНПЗ – індивідуальне науково-практичне завдання.
КК – Кримінальний кодекс.
КНР – Китайська Народна Республіка.
МВС – Міністерство внутрішніх справ.
МЗС – Міністерство закордонних справ.
МО – Міністерство оборони.
МСЕ – Міжнародний союз електрозв’язку, International Telecommunication Union, ITU.
НАТО – Організація Північноатлантичного договору, North Atlantic Treaty Organization, NATO.
НСКБ – Національна система кібербезпеки.
ОБСЄ – Організація з безпеки і співробітництва в Європі, Organization for Security and Cooperation in Europe, OSCE.
ОЕСР – Організація економічного співробітництва та розвитку, Organisation for Economic Cooperation and Developmet, OECD.
ООН – Організація Об’єднаних Націй, United Nations Organisation.
РНБО – Рада національної безпеки і оборони.
РФ – Російська Федерація.
СБУ – Служба безпеки України.
США – Сполучені Штати Америки.
ТНК – транснаціональна корпорація.
ШОС – Шанхайська організація співробітництва.
ЮНЕСКО – Організація Об’єднаних Націй з питань освіти, науки і культури, United Nations Educational, Scientific and Cultural Organization, UNESCO.

Актуальність. На сьогоднішній день провідні держави світу та суспільство в цілому все більшою мірою покладаються і, відповідно, залежать від

безперешкодного функціонування п'ятого простору – кіберпростору, під яким пропонується розглядати сукупність взаємопов'язаних інформаційних ресурсів, програмного забезпечення, баз та банків даних, що обробляються в комп'ютерних мережах і пов'язаній з ними інфраструктурі, разом з об'єктами, що підпадають під їх контроль та управління.

Захист інтересів держав та громадян в кіберпросторі стає життєво важливим завданням, яке перетворює безперешкодне використання ІТ-мереж на питання безпеки й оборони. Потенційна небезпека може загрожувати системам державного та військового управління, економіки та промисловості.

Україна інтегрована у світовий кіберпростір і відповідно зазнає різних загроз і негативних впливів, пов'язаних з його розвитком (зокрема від наслідків суперництва США і ЄС з РФ та КНР), що гостро актуалізує проблеми кібербезпеки на загальнодержавному рівні. Це призводить до необхідності концептуального розуміння нової кібербезпекової реальності, впорядкування внутрішнього нормативно-правового поля, визначення повноважень відомств та організацій, задіяних у забезпеченні кібербезпеки держави і вирішення комплексу проблем, пов'язаних із розбудовою національної системи кібербезпеки.

Найбільш ефективним шляхом вирішення зазначених питань є побудова національної моделі кібербезпеки та розробка першочергових напрямків діяльності державного та приватного секторів у сфері кібербезпеки.

Метою ІНПЗ є розроблення обґрунтування заходів з підвищення ефективності забезпечення кібербезпеки в системі публічного управління в умовах відсутності концептуального розуміння кібербезпекової політики України.

Досягнення зазначеної мети здійснювалося шляхом розв'язання низки завдань:

дослідження кіберзагроз і складових кіберконфліктів XXI сторіччя для врахування наслідків їх реалізації по відношенню до органів публічного управління;

формулювання найбільш актуальних для України кіберзагроз і кіберконфліктів для визначення переліку органів публічного управління у сфері кібербезпеки;

аналіз стану мілітаризації кіберпростору та проблематики міжнародної кібербезпеки для уточнення складу органів публічного управління воєнної сфери;

огляд стану і проблем національного нормативно-правового та організаційного забезпечення кібербезпеки для визначення проблемних аспектів діяльності у цій сфері;

розробка сучасної моделі національної системи кібербезпеки для визначення складу та порядку взаємодії органів публічного управління в національній системі кібербезпеки України;

розробка першочергових напрямів діяльності у сфері кібербезпеки для обґрунтування заходів з підвищення ефективності забезпечення кібербезпеки в системі публічного управління.

Об'єктом дослідження є забезпечення кібербезпеки в системі публічного управління держави.

Предметом дослідження є склад органів публічного управління в національній системі кібербезпеки України.

Методи дослідження завдань ІНПЗ. Відповідно до конкретних завдань на різних етапах дослідження використано такі методи, як системно-структурний, кібернетичний, синергетичний, структурно-функціональний, аналогії, аналізу й синтезу, сходження від абстрактного до конкретного, індукції та дедукції, інтерпретації.

Новизна одержаних результатів:

сформульовано найбільш актуальні для України кіберзагрози і кіберконфлікти в 2015–2016 роках;

дістав подальшого розвитку огляд стану і проблем національного нормативно-правового та організаційного забезпечення кібербезпеки;

вперше, з урахуванням досвіду європейських країн, розроблено сучасну модель національної системи кібербезпеки та запропоновано першочергові напрями діяльності у сфері кібербезпеки.

Практичне значення одержаних результатів. Розроблена модель національної системи кібербезпеки та першочергові напрямки діяльності у сфері кібербезпеки призначені для удосконалення нормативно-правової бази України, структури органів державного управління, місцевого самоврядування та організацій приватного сектору за напрямком забезпечення кібербезпеки держави.

Результат дослідження. Система публічного управління України інтегрована у світовий кіберпростір і відповідно зазнає різних загроз і негативних впливів, пов’язаних з його функціонуванням, що гостро актуалізує проблеми кібербезпеки на загальнодержавному рівні. Пошук шляхів підвищення ефективності кібербезпеки в системі публічного управління потребує дослідження нової кібербезпекової реальності, впорядкування внутрішнього нормативно-правового поля, визначення повноважень відомств та організацій, задіяних у забезпеченні кібербезпеки держави і вирішення комплексу проблем, пов’язаних із розбудовою національної системи кібербезпеки. Найбільш ефективним шляхом вирішення зазначених питань є побудова національної моделі кібербезпеки та розробка першочергових напрямків діяльності державного та приватного секторів у сфері кібербезпеки.

Для забезпечення кібербезпеки надзвичайно важливо розуміти загрози кіберпростору, дослідження яких здійснюють провідні світові експерти та міжнародні організації [1, 2, 3]. Як приклад, можливо навести досі актуальну класифікацію кібернетичних загроз, одержану за результатами досліджень “ENISA Threat Landscape 2013” [1]: “Drive-By” експлойти; хробаки (worms)/трояни; ін’єкція коду; exploit kits: exploit kits; ботнет; відмова в обслуговуванні (denial-of-service (DoS) атака); фішинг і фармінг; компрометація конфіденційної інформації; roguaware (шахрайське програмне забезпечення)/scareware (псевдоантивірусні програми); спам; цільові атаки; фізична крадіжка/втрата/пошкодження; крадіжка особистих даних (Identity Theft); abuse of information leakage (зловживання витоком інформації); search engine poisoning (отруєння пошукових систем); система доменних імен Domain Name system (DNS); rogue certificates (підробні сертифікати).

Міркування щодо наведених кіберзагроз, вочевидь, будуть неповними без наведення конкретних випадків застосування кіберозброєнь (того, що під ним розуміється), та значущих кіберінцидентів, які суттєво вплинули на світову громадську думку щодо кібербезпекової проблематики загалом.

Сукупність відомих кіберконфліктів можна розділити на три ключових рівні:

перший – "класичні" кіберзлочини (шахрайство, здирництво, несанкціонований доступ до персональної інформації користувачів та автоматизованих баз даних, поширення порнографії, продаж зброї чи наркотиків тощо) – як абсолютно оригінальні, так і вже звичні для нас, для своєї реалізації вони потребують лише наявності сучасних інформаційних технологій;

другий – злочини, характерні для геополітичної боротьби (або такі злочини на місцевому рівні, які мають потенціал вплинути на політичне становище держави): хактивізм, або політично вмотивовані хакерські атаки; кібершпигунські акції; кібердиверсії [4];

третій – військові дії (операції) провідних країн у кіберпросторі, особливістю яких є нарощування потенціалу на знищення життєво важливої інфраструктури та отримання доступу до банківських, комерційних, військових та оборонних баз даних [5, 6].

Водночас політика країн Заходу у сфері внутрішнього інформаційного (кібер) простору дедалі частіше набуває рис політики тих країн, які традиційно відносять до авторитарних. Щоправда, у відповідних процесах мають місце суттєві відмінності. Якщо у країнах авторитарного типу реалізується передусім політика прямого обмеження доступу, то відповідно до досліджень Washington Post [7] країни Заходу збирають дані про користувачів, здійснюють моніторинг національного Інтернет-трафіку та створюють можливості цільового відключення окремих елементів мережі або її користувачів за рахунок засекреченого співробітництва безпекових структур та провідних приватних компаній, що працюють на світовому інформаційному ринку, – Microsoft, Yahoo, Google, Facebook, PalTalk та інших.

Можна констатувати, що в Україні в повному обсязі присутні всі ключові "класичні" кіберзлочини і щороку їх кількість зростає. Високий рівень загроз у кіберпросторі підтверджується дослідженнями відомого німецького оператора зв'язку Deutsche Telecom, за даними якого Україна опинилася на четвертій позиції у світі серед країн-джерел кібернетичних атак. Тільки протягом лютого 2013 року з території України їх було здійснено 566 тисяч [8].

Розглядаючи динаміку кількості карних справ, порушених Службою безпеки України за фактами виявлених кіберзлочинів, можна чітко прослідкувати їх істотне збільшення: від 39 справ у 2005 році до 114 за друге півріччя 2012 року та перше півріччя 2013 року [8].

Зростають масштаби як традиційного кардингу[1], так і більш складних кіберзлочинів. Крім того, й досі значними за обсягами та збитками залишаються такі злочини, як поширення порнографії, порушення авторських прав, чому особливо активно протидіє МВС.

Державі стає відомо лише про 5 % злочинів у кіберпросторі, а значна кількість потерпілих від них можуть тривалий час і не знати про те, що їх атакували. Іноді на виявлення факту "зламу" витрачаються місяці (якщо це спрямований "злам", здійснений фахівцями, – роки).

[1] Вид шахрайства, пов'язаний із використанням платіжних карток або їхніх реквізитів.

З урахуванням протиправної діяльності Російської Федерації, в 2015–2016 роках з високою ймовірністю найбільш актуальними для України кіберзагрозами і кіберконфліктами стануть:

посилення рівня небезпеки кібертероризму, враховуючи, що терористичні організації позиціонують дії у кіберпросторі як повноцінну форму ведення боротьби;

спрямування кібернетичних атак на окремі процеси обміну та обробки інформації з низьким рівнем захисту;

перманентний розвиток "чорного ринку" послуг зі здійснення цільових кібератак;

розширення масштабів таких видів кіберзлочиності, як шантаж, залякування та вимагання, у яких інформаційні ресурси відіграватимуть роль "заручників" та блокуватимуться або знищуватимуться у разі ігнорування (невиконання) вимог зловмисників;

активізація кібератак на "хмарні сховища даних" з метою викрадення інформації, що зумовлено перманентним зростанням популярності "хмарних сховищ" для зберігання даних та ігноруванням, у більшості випадків, елементарних вимог до забезпечення кіберзахисту інформації;

масштабне використання уразливостей мобільних пристроїв (смартфони, планшети тощо) для викрадення персональних даних їх власників (у т.ч. місцеположення, інформації фінансового характеру тощо). Крім того, персональні мобільні пристрої стануть одними з основних об'єктів цільових кібератак. Це зумовлено зростанням активності використання мобільних пристроїв у службовій діяльності, незважаючи на значно нижчий рівень їх захищеності від кібератак порівняно з корпоративними інформаційними системами;

нарощення активності та масштабів використання бот-мереж на базі мобільних пристроїв з метою несанкціонованого збору інформації, а також для проведення різного роду диверсій та заподіяння матеріальних збитків, кількість яких зростатиме з розширенням технічних можливостей доступу (насамперед, бездротового "Wi-Fi", 'Bluetooth" тощо) мобільних пристроїв до мережі Інтернет;

використання кібератак на окремі Інтернет-ресурси державних органів України для досягнення політичних цілей;

використання соціальних мереж та спеціалізованих веб-сайтів для дестабілізації ситуації в Україні, що на теперішній час проявляється у створенні російською стороною "фейкових" профілів (акаунтів) у соціальних мережах та сервісах електронної пошти (насамперед відомих публічних користувачів) та активізації незаконного отримання доступу до них з метою поширення дезінформації про події у південно-східних областях нашої держави, пошуку осіб для проведення антиурядових акцій і так званих "акцій громадської непокори", участі у бойових діях на боці незаконних збройних формувань, формування викривленого висвітлення ситуації в Україні в цілому;

створення нових антиукраїнських Інтернет-ресурсів, з яких окремої уваги потребують нові, спеціально створені для розміщення провокаційних матеріалів антиукраїнського характеру, зокрема "Русская весна" (http://rusvesna.su) та "Одеса-антимайдан" (http://odessa- antimavdan.com);

розробка нових та модифікація існуючих зразків шкідливого програмного забезпечення.

Попри зростаючу небезпеку від кіберзагроз різних рівнів складності, на шляху створення ефективних механізмів протидії кіберзлочинцям досі постають дві важливі проблеми – термінологічна та нормативно-правова.

Незважаючи на те, що такі поняття, як кіберпростір, кібервійна, кібератака, кібертероризм та кібермогутність широко використовуються в науковій і публіцистичній літературі, дотепер невизначеним є їх зміст, що значно ускладнює наукове осмислення та практичне освоєння проблеми забезпечення кібербезпеки.

Водночас теоретико-методологічні дискусії довкола термінологічної бази стикаються зі значно більш практичною проблемою – застосування чинного нормативно-правового поля (особливо міжнародного) щодо кіберзагроз і з'ясування самої можливості його застосування у відповідному контексті.

Особливо важливо вирішити кілька принципових ускладнень, що унеможливлюють формалізацію безпекової політики в кіберпросторі:

досі відсутні системні міжнародні нормативно-правові документи, які б чітко надавали визначення кіберпростору та всім його "безпековим" похідним;

не визначено правовий статус кіберпростору;

на міжнародному рівні відсутній консенсус щодо правил поведінки в кіберпросторі;

відсутні загальноприйняті методології оцінки наслідків кіберзлочинів та їх розгляду як об'єкта міжнародних норм і правил (зокрема щодо визнання кібератаки як акту війни).

Незважаючи на широкий інтерес до зазначеного безпекового напряму, наукові дослідження (чи навіть узагальнення з цього питання) досі є поодинокими й часто несистемними.

Спроби впорядкувати ці проблеми в межах нормативно-правового поля можна вважати лише частково успішними. Єдиним реальним документом кібербезпекового характеру є ратифікована Україною Конвенція про кіберзлочинність [9], однак вона, по-перше, присвячена доволі вузькому сегменту кіберзагроз (кіберзлочинам у сфері комп'ютерної інформації), а по-друге, по суті, є регіональним документом, який до того ж не сприймається значною кількістю геополітичних гравців.

Більшість потужних держав світу (США, Росія, ЄС, Китай, Індія та інші) перебувають нині на етапі створення і трансформації власних військових кібернетичних підрозділів з огляду на можливості використання мережі Інтернет проти їх національних інтересів, а також отримання можливості впливати на інші держави.

За даними керівника компанії McAfee, оприлюдненими на Всесвітньому економічному форумі в Давосі ще у 2010 році [10], вже у 2009–2010 рр. понад 20 країн планували або здійснювали різноманітні інформаційні операції. Скільки країн стурбовано створенням і модернізацією власних кібервійськ станом на 2013–2015 рр. – невідомо. Станом на кінець 2014 року згідно з офіційними заявами військові кіберпідрозділи з виразно захисними функціями створено у США (U.S. Cyber Command); Великобританії (урядовий Cyber Security Operations Centre); Німеччині (Internet Crime Unit та Federal Office for Information Security); Австралії (The Cyber

security operations centre); Індії; Ізраїлі та багатьох інших країнах. Готовність до створення кіберкомандування серед сусідів України висловила передусім Російська Федерація. Ще в лютому 2013 року перший заступник голови Комітету Держдуми з оборони В. Заварзін за результатами засідання Комітету, за участю глави Генерального штабу В. Герасімова, повідомив, що в Генштабі Збройних Сил Росії почав роботу спеціальний підрозділ з кібербезпеки [11]. Також у 2013 році з'явилася інформація про те, що створення кібервійськ починає Білорусь [12].

Активну позицію щодо протидії кіберзагрозам посідають провідні міжнародні безпекові організації такі як ОБСЄ та НАТО. В червні 2011 року міністри оборони стран-членів Альянсу погодили нову Концепцію кібербезпеки НАТО (Cyber Defence Concept), а Спільний центр передового досвіду в галузі кібербезпеки НАТО (NATO Cooperative Cyber Defence Centre of Excellence, CCD CoE) функціонує з 2008 р. [13]).

Цілісним баченням Урядом США найближчого майбутнього розвитку кіберпростору стала Міжнародна стратегія для кіберпростору (International Strategy for Cyberspace) [14]. Документ не лише визначив принципові положення, якими керуватимуться США в процесі формування власної політики щодо кіберпростору, а й окреслив бажане для США майбутнє кіберпростору. Значущість питань кібербезпеки для США загалом та Адміністрації Б. Обами зокрема ілюструє протистояння щодо прийняття комплексних нормативно-правових документів, спрямованих на повноцінне функціонування системи кібербезпеки США, яке розгорнулося протягом 2009–2014 рр. у Конгресі. Наприклад, проводиться просування таких законодавчих актів, як "Про підвищення кібербезпеки" [15], або "Про сприяння національній кібербезпеці" [16].

Активність ЄС є набагато скромнішою. Лише в лютому 2013 року Європейська Комісія спільно з Верховним представником ЄС у закордонних справах та з політики безпеки представили проект Стратегії з кібербезпеки "Відкритість, безпека та надійність" [17]. Стратегія спрямована на поліпшення взаємодії між державним і приватним сектором у подоланні кіберзагроз, створення єдиних баз даних щодо загроз у кіберпросторі тощо.

Аналогічні стратегії створено на рівні окремих країн ЄС, зокрема в Естонії, Фінляндії, Словаччині, Чеській Республіці, Франції, Німеччині, Литві, Люксембургу, Нідерландах, Великобританії, Польщі та Румунії.

У доктринальних безпекових документах КНР зростання ролі інформатизації у військовій справі зазначається принаймні від середини 90-х років XX сторіччя. У датованій 2008 роком "Національній обороні Китаю" [18] вказується на бажання досягти до 2020 року значного результату з питань інформатизації армії. Питанню розбудови інформаційного потенціалу збройних сил КНР присвячено також цілий пункт у Білій книзі з питань оборони за 2013 рік [19].

Рівень занепокоєння провідних держав світу щодо сфери кібербезпеки засвідчує в тому числі бажання врегулювати питання стосовно можливості визнання кібератаки актом війни на міжнародному рівні. Розгляд підходів США до організації та ведення бойових дій (операцій) у кіберпросторі проводиться в численних документах МО США: Стратегія Міністерства оборони США по операціях у кіберпросторі (Department of Defense Strategy for operating in Cyberspace) 2011 року

[20], Операції в кіберпросторі, план та концепція можливостей 2016–2028 (Cyberspace Operations Concept Capability Plan 2016–2028) [21] та інших.

На противагу США Російська Федерація просуває власні ініціативи, зокрема Конвенцію про забезпечення міжнародної інформаційної безпеки [22], та проводить власну політику шляхом розробки проекту Концепції стратегії кібербезпеки Російської Федерації та оприлюднення в серпні 2013 року Основ державної політики РФ у сфері міжнародної інформаційної безпеки на період до 2020 року [23].

Концептуальна ключова різниця у поглядах найбільших гравців полягає в тім, що США та значна частина європейських держав дотримуються погляду щодо необхідності розглядати на міжнародному рівні лише проблеми кібербезпеки, залишаючи осторонь проблеми інформаційно-психологічних впливів. Натомість РФ, КНР та інші держави "напівзакритого" типу шляхом просування зазначених вище документів послідовно обстоюють позицію, відповідно до якої кібербезпеку не можна розглядати як окремий техніко-технологічний напрям, тобто відособлено від соціальних, політичних, економічних і воєнних наслідків застосування сучасних інформаційних технологій.

Якщо не буде винайдений реальний формат взаємовідносин між країнами, існує суттєвий ризик переростання їх суперництва в нове "холодне" протистояння, полем якого стане саме кіберпростір. Уже зараз експерти кажуть про зародження "холодної війни v2.0.", основними інструментами якої стануть вже звичні методи класичної "холодної війни" – непрямі методи боротьби, шпигунство, гонка озброєнь – з перенесенням їх до кіберпростору. Відсутність ефективних міжнародних інструментів протидії цим процесам може спричинити цифровий аналог Карибської кризи.

Проблеми кібербезпеки є предметним полем діяльності кількох міжнародних інституцій, передусім спеціалізованих організацій ООН, зокрема ЮНЕСКО й МСЕ, а також таких міждержавних форумів, як G8, G20, ОЕСР, ШОС, АТЕС тощо.

На особливий інтерес заслуговує Резолюція Генеральної Асамблеї ООН A/RES/57/239 від 20 грудня 2002 року "Створення глобальної культури кібербезпеки" (Creation of a global culture of cybersecurity) [24], в якій вперше чітко використовувалося поняття кібербезпека. Продовження розгляду теми кібербезпеки відбулося у Резолюціях A/RES/58/199 "Створення глобальної культури кібербезпеки та захист найважливіших інформаційних інфраструктур" 2003 року [25] та A/RES/64/211 "Створення глобальної культури кібербезпеки та оцінка національних зусиль по захисту найважливіших інформаційних інфраструктур" 2009 року [26].

Активно до теми безпеки кіберпростору звертається МСЕ, який ухвалив низку резолюцій і рекомендацій, що безпосередньо стосуються проблеми кібербезпеки. На особливу увагу заслуговує Рекомендація МСЕ-Т59 Х.1205 від 2008 року [27], яка надає визначення кібербезпеки, представляє у систематизованій формі загрози кібербезпеці та уразливості (включно з переліком найпоширеніших інструментів хакерських атак). Крім того, в Рекомендації МСЕ від 2008 року зроблено огляд різноманітних технологій кібербезпеки включно з антивірусним захистом, системами виявлення вторгнень, моніторингу систем тощо, подано принципи захисту мереж, технологій і стратегій управління ризиками тощо.

Поміж важливих кроків МСЕ, спрямованих на подальше убезпечення кіберпростору, варто виокремити створення фахівцями цієї структури такого важливого документа, як "Розуміння кіберзлочинності: Керівництво для країн, що розвиваються" (Understanding Cybercraime: A Guaide for Developing Counries) [28]. У Керівництві викладено ключові погляди МСЕ на ситуацію у сфері кібербезпеки, запропоновано ключові визначення та універсальна модель взаємодії основних суб'єктів забезпечення кібербезпеки на національному рівні. Досі цей документ залишається достатньо актуальним і виваженим. Великий інтерес також являє собою книга "У пошуках кібермиру" [29] видана в 2011 році Міжнародним союзом електрозв'язку спільно зі Всесвітньою федерацією учених.

Крім ООН та пов'язаних з нею спеціалізованих організацій, проблемами кібербезпеки, як зазначалося, опікуються інші міжнародні структури, зокрема G8, яка вперше звернулася до проблем протидії "високотехнологічним злочинам" ще у 1997 році. Прийняті G8 документи цікаві тим, що в них закладено потенціал інформаційної "десуверенізації" у вигляді безпосередньо сформульованої тези (положення 7 "Принципів та Плану дій щодо боротьби з високотехнологічними злочинами" (Principles and Action Plan to Combat High-tech Crime) [30]) про надання правоохоронним органам певної країни можливості здійснювати частину своєї діяльності без отримання дозволу від іншої країни. Хоча на той час з цим положенням погодилися всі члени G8, однак вже за 5 років відповідний пункт став причиною, через яку РФ відмовилася підписувати цей документ.

Таким чином, на сьогоднішній день проблематика майбутнього глобального кіберпростору знаходиться на перетині двох рівнозначних трендів. З одного боку, офіційні зусилля спрямовані на демілітаризацію кіберпростору та недопущення перетворення його на нове поле збройного протистояння, а з іншого – де-факто продовжується процес протистояння. Міжнародні структури на кшталт ООН, МСЕ чи G8 (G20) хоча й роблять спроби впливати на цей процес, однак ці спроби є фрагментарними та надто обережними. Незважаючи на цілу низку рішень і резолюцій, ООН так реально і не наблизилася до вироблення дієвого міжнародного документа, що зміг би впорядкувати кібербезпекову проблематику.

Хоча Україна досі є на шляху розвитку, однак для неї проблеми глобалізованого кіберпростору не є чимось відірваним від політичної реальності. І чим інтенсивніше розвивається інформаційне суспільство в Україні, тим актуальнішою (як для держави в цілому, так і кожного громадянина зокрема) стає проблема самовизначення України щодо кіберпростору.

Розв'язанню проблеми відсутності реальних кроків України в кіберпросторі жодним чином не сприяє недосконале чинне законодавство, яке досі виходить з парадигми штучного розширення предмета інформаційної безпеки на максимальну кількість сфер. Це, по-перше, розмиває сам предмет інформаційної безпеки, а по-друге, обумовлює відсутність частини "кібер" у вітчизняних нормативно-правових документах. Натомість використовується в суто пострадянському дискурсі поняття інформаційна безпека та низка інших, тісно з ним пов'язаних: інформаційний суверенітет; інформаційна інфраструктура [31]; інформаційні впливи тощо. На виправдання зазначеного підходу зазвичай наводиться той аргумент, що терміни з

частиною “кібер” акцентують виключно на формальній стороні інформаційних процесів, ігноруючи сторону змістову.

Окремі аспекти, пов’язані із забезпеченням кібербезпеки держави, відображені в таких законах України: Закон України “Про основи національної безпеки України”; Закон України “Про інформацію”; Закон України “Про Державну службу спеціального зв’язку та захисту інформації України”; Закон України “Про державну таємницю”; Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” та інших. Крім того, в межах цієї проблематики чинними є два стратегічних документи: Стратегія національної безпеки України [32] та Доктрина інформаційної безпеки України, нова редакція якої готується з травня 2014 року. Важливе нормативно-стратегічне значення має також ратифікована Верховною Радою України Конвенція про кіберзлочинність.

Наприкінці 2010 року (Указ Президента України від 10 грудня 2010 року №1119/2010) набуло чинності рішення РНБО України від 17 листопада 2010 року “Про виклики та загрози національній безпеці України у 2011 році”. Відповідно до цього рішення органам виконавчої влади було поставлено завдання розробити та подати у двомісячний строк на розгляд РНБО України пропозиції щодо створення “єдиної загальнодержавної системи протидії кіберзлочинності” та “розробити та затвердити перелік об’єктів, що мають важливе значення для забезпечення національної безпеки і оборони України та потребують першочергового захисту від кібернетичних атак”.

На виконання цих завдань мав бути розроблений Закон України “Про кібернетичну безпеку України”, остаточна редакція якого на цей час відсутня, хоча протягом 2010–2014 рр. зроблено принаймні чотири спроби створення документа, жодна з яких не закінчилася заключним обговоренням.

Остання редакція проекту Закону України “Про основні засади забезпечення кібербезпеки України”, підготовлена за участю автора та яка пройшла міжвідомче погодження з усіма зацікавленими органами державної влади, була відхилена 5 листопада 2014 року на засіданні Кабінету Міністрів України. Відповідно до протокольного рішення засідання Уряду Адміністрації Держспецзв’язку разом з МВС, СБУ, МЗС та із залученням міжнародних експертів, зокрема зі складу організації ISACA, було доручено доопрацювати зазначений законопроект. Підготовлений Держспецзв’язку України (окремо від розглянутого законопроекту) проект Стратегії забезпечення кібернетичної безпеки України також знаходиться на доопрацюванні.

Водночас кібербезпекова тематика лише побіжно згадується у стратегічних документах воєнного сектору. Наприклад, у Воєнній доктрині України йдеться про кібернетичний складник або в контексті поширення тероризму (зокрема кібертероризму), або як про елемент переліку дій, які Україна вважає необхідними умовами для виникнення воєнного конфлікту та застосування воєнної сили [33]. Аналогічно незначна увага приділяється питанням кібербезпеки у Стратегічному оборонному бюлетені України [34].

Крім проблем суто нормативно-правового характеру, доводиться констатувати брак міжвідомчого координування з питань забезпечення кібербезпеки держави. Наразі в Україні відсутні загальнонаціональні міжвідомчі координаційні структури,

спроможні узгоджувати й координувати діяльність різних силових відомств під час розслідування злочинів у кіберпросторі та створення ефективної системи захисту вітчизняного кіберпростору.

Координування з питань забезпечення кібербезпеки держави має відбуватися на двох рівнях – стратегічному та оперативному. Стратегічне координування вочевидь є зоною відповідальності Ради національної безпеки і оборони, а оперативне, із врахуванням підпорядкованості безпекових та оборонних структур, доцільно здійснювати силами Національного центру кібербезпеки при Президентові України, який слід створити у найкоротший термін. Невиконання цієї вимоги матиме результатом небажання окремих структур сектору безпеки співпрацювати з іншими уповноваженими відомствами через законодавчу (нормативну) невизначеність прав та обов'язків цих структур чи невідповідність певних нормативних документів вимогам часу. Ця ситуація вже має місце, а в тих випадках, коли така співпраця існує, найчастіше вона здійснюється на рівні міжособистісних зв'язків керівників відповідних підрозділів. З погляду довгострокової перспективи така ситуація є прямою загрозою кібербезпеці держави. При цьому профільні науково-дослідні інститути, задіяні в комплексних дослідженнях кібербезпеки, майже відсутні.

Ще одна проблема полягає в тому, що Україна (особливо телекомунікаційний компонент її інформаційної інфраструктури) й досі є принципово уразливою до кіберзагроз і, не в останню чергу, через надміру широке транслювання іноземних програмних продуктів та використання матеріально-технічної бази іноземного виробництва. Пошук можливих "закладок" у цій продукції практично унеможливлюється через залежність Української держави від згаданих продуктів, що вийшла на дійсно загрозливий для національної безпеки рівень в усіх сферах.

Виходячи з проведеного аналізу стану сфери кібербезпеки в Україні, який склався в умовах протистояння провідних країн світу у кіберпросторі, автором пропонується до розгляду модель побудови національної системи кібербезпеки, розроблена з урахуванням досвіду країн Європейського Союзу та НАТО.

Для забезпечення кібербезпеки України держава у партнерстві із суспільством та приватним сектором, а також громадянами, має підвищити ефективність державного управління у цій сфері, здійснити впорядкування нормативно-правового поля та забезпечити розвиток інфраструктури кібербезпеки. Зокрема, має бути розроблено Національну стратегію кібербезпеки з впровадженням заходів оцінки її ефективності та створено Національну систему кібербезпеки.

Вбачається, що єдина загальнодержавна система кібербезпеки – Національна система кібербезпеки (НСКБ) – має об'єднати у форматі співробітництва центральні органи виконавчої влади, військові формування, правоохоронні органи, органи державного регулювання у сфері інформатизації, телекомунікацій та захисту інформації, органи місцевого самоврядування, наукові установи і організації, а також зацікавлені громадські організації, професійні асоціації, представництва міжнародних організацій в Україні, представників приватного сектору, а також підприємства, установи та організації незалежно від форм власності, які здійснюють діяльність, пов'язану із забезпеченням функціонування або безпеки національного сегмента кіберпростору, для своєчасного запобігання кіберзагрозам, забезпечення

належного рівня обороноздатності та безпеки держави в кіберпросторі, оперативного виявлення, запобігання, протидії та розслідування злочинних проявів, заснованих на використанні інформаційних та інформаційно-комунікаційних технологій.

В рамках НСКБ пропонується передбачити такі функціональні елементи:

система моніторингу та реагування на кіберзагрози (передбачає швидку ідентифікацію зловмисників, вжиття заходів із локалізації шкоди, викликаної їх діями, та проведення розслідування кіберзлочинів);

система кібербезпеки у воєнній сфері та сфері оборони;

система кіберзахисту критичної інформаційної інфраструктури.

При формуванні вітчизняної моделі побудови НСКБ слід врахувати такі особливості:

на сьогодні державні органи в секторах, які в європейських країнах належать до критичної інфраструктури, задіяні переважно для регулювання економічних і майнових питань, у той час як невизначеними залишаються структури, які мають відповідати власне за питання кібербезпеки;

забезпечення кібербезпеки у приватному секторі здійснюється на власний розсуд власника тієї чи іншої системи;

відсутність єдиного координаційного центру з питань забезпечення кібербезпеки суттєво ускладнює, уповільнює, а у деяких випадках й унеможливлює взаємодію органів державного управління та вжиття необхідних заходів з реагування на кібернетичні злочини та інциденти кібербезпеки, які відрізняються високим ступенем латентності;

важливими показниками ефективності НСКБ є: оперативність оцінки ситуації, термін прийняття відповідних рішень, час реагування, достатність вжитих заходів;

кібернетичний суверенітет і кібермогутність держави базуються на сукупності змістовних чинників, до яких належать [4]: інноваційний потенціал країни та її здатність самостійно створювати новітні технології; ступінь розвитку ІТ-компаній, а де-факто – наявність національних ІТ-ТНК; ступінь розвитку внутрішнього ринку (передусім відповідної вимогам сучасності ІТ-інфраструктури); гуманітарний показник впливу культури країни на загальний контент мережі; військовий потенціал держави (передусім можливість здійснювати кібератаки та захищатися від них); зовнішньополітична компонента (включно з можливостями впливу на міжнародні структури, задіяні в управлінні Інтернетом).

Для створення дієвої вертикалі органів державного управління у сфері кібербезпеки принциповим є питання визначення на державному рівні єдиного координаційного органу, іншими словами – Центрального органу виконавчої влади зі спеціальним статусом у сфері кібербезпеки.

Організаційно до НСКБ пропонується включити такі структурні (рис. 1):

1) керівник НСКБ – Президент України;

2) орган законодавчої влади – Верховна Рада України;

3) вищий орган координації діяльності органів виконавчої влади у сфері кібербезпеки – Кабінет Міністрів України;

4) орган стратегічного управління сферою кібербезпеки України – Рада національної безпеки і оборони України;

Рис. 1 – Модель національної системи кібербезпеки

5) орган оперативного управління сферою кібербезпеки України – Національний центр кібербезпеки при Президентові України (як центральний орган виконавчої влади зі спеціальним статусом у сфері кібербезпеки);

6) суб'єкти забезпечення кібербезпеки – органи державної влади та місцевого самоврядування, органи військового управління Збройних Сил України, інших військових формувань, правоохоронні органи, установи науково-методологічної підтримки, громадські організації та професійні асоціації, створені за участю представників приватного сектору, а також об'єднання підприємств, установ та організацій незалежно від форми власності, які здійснюють діяльність, пов'язану із забезпеченням функціонування або безпеки національного сегмента кіберпростору.

Зі складу зазначених суб'єктів доцільно виділити суб'єкти забезпечення кібербезпеки постійної готовності – органи державної влади, сили та засоби яких спеціально виділені для перебування у постійній готовності до реагування на кіберзагрози та оперативного вирішення завдань забезпечення кібербезпеки.

До складу суб'єктів забезпечення кібербезпеки постійної готовності доцільно віднести:

РНБО України;

Національний центр кібербезпеки при Президентові України;

Міністерство внутрішніх справ України;

Службу безпеки України;

Міністерство оборони України;

Генеральний штаб Збройних Сил України;

Державну службу спеціального зв'язку та захисту інформації України;

Головну професійну асоціацію (організацію) у сфері кібербезпеки приватного сектору держави.

До основних підрозділів суб'єктів забезпечення кібербезпеки постійної готовності слід віднести:

Центр за напрямком боротьби з кіберзлочинністю у складі Міністерства внутрішніх справ України;

Центр за напрямком боротьби з кібертероризмом у складі Служби безпеки України;

Центр за напрямком забезпечення захисту інформації та кібербезпеки у складі Збройних Сил України;

Центр за напрямком реагування на комп'ютерні надзвичайні події (CERT-UA) у складі Державної служби спеціального зв'язку та захисту інформації України;

Недержавний центр за напрямком забезпечення кібернетичного захисту у складі Головної професійної асоціації (організації) у сфері кібербезпеки приватного сектору держави.

У центральних органах виконавчої влади та органах місцевого самоврядування доцільно створити відділи за напрямом забезпечення кібернетичного захисту інформаційної інфраструктури.

У складі підприємств, установ або організацій будь-яких форм власності, діяльність яких пов'язана із забезпеченням функціонування критичної

інформаційної інфраструктури держави, доцільно створити відповідні відділи (відділення) за напрямком забезпечення кібернетичного захисту.

7) об'єкти кіберзахисту.

До складу об'єктів кіберзахисту належать об'єкти інформаційної інфраструктури, інформаційні, телекомунікаційні та інформаційно-телекомунікаційні системи, в яких здійснюється обробка державних інформаційних ресурсів або інформації, вимога щодо кіберзахисту якої встановлена законом або власником системи.

За узгодженими з усіма суб'єктами кібербезпеки держави критеріями, зі складу об'єктів кіберзахисту доцільно виділити об'єкти критичної інформаційної інфраструктури (об'єкти, що потребують першочергового захисту від кібератак).

До першочергових напрямів діяльності держави у сфері кібербезпеки (розвитку складових національної системи кібербезпеки) пропонується віднести такі:

ідентифікація всіх регуляторів та учасників сфери кібербезпеки в різноманітних галузях, наприклад: захист інформації в ІТС; інформаційна безпека інформаційних технологій; безпека електронних комунікацій банківської сфери тощо);

розміщення за пріоритетами критичних об'єктів кіберзахисту залежно від впливу на суспільство, економіку та громадян (за основу можна взяти стандарт "Framework for Improving Critical Infrastructure Cybersecurity" розробки Національного інституту стандартів і технологій США (NIST, National Institute of Standards and Technology) [35];

розробка базових вимог до систем кібербезпеки як державних, так і приватних організацій. Такі вимоги можуть базуватися на загальноприйнятих міжнародних стандартах та рекомендаціях;

розробка єдиної національної системи оцінки ризиків, з використанням міжнародних практик, наприклад, стандарту "COBIT for risk" [36], та проведення їх оцінки;

розробка єдиної класифікації інцидентів кібербезпеки на основі, наприклад, стандарту NIST "Computer Security Incident Handling Guide" [38];

впровадження єдиної системи оцінки загроз та реагування на інциденти кібербезпеки;

визначення порядку обміну інформацією про інциденти кібербезпеки та встановлення порядку реагування;

розробка механізмів оцінки зрілості систем кіберзахисту та його впровадження для використання усіма учасниками сфери кібербезпеки;

розробка Національної стратегії кібербезпеки у відповідності до двох основних етапів: розробка та впровадження стратегії; оцінка ефективності та врегулювання стратегії;

налагодження взаємодії між державним та приватним секторами;

забезпечення постійного представництва у консультаціях експертів з кібербезпеки різних націй для узагальнення відомостей про кібернетичні загрози і найкращі практики у сфері кібербезпеки;

розвиток наукової та науково-дослідної діяльності в галузі кібербезпеки;

організація регулярних зустрічей представників суб'єктів забезпечення кібербезпеки для розгляду актуальних питань;

оновлення та застосування кримінального права, процедур та законодавства, спрямованих на запобігання, стримування, реагування і переслідування кіберзлочинності в судовому порядку;

підвищення обороноздатності держави у кіберпросторі;

підвищення національної культури кібербезпеки та фахового рівня спеціалістів у цій галузі;

впровадження технічних стандартів і передових практик кібербезпеки;

розробка національних політик кібербезпеки та впровадження ефективного механізму їх реалізації.

Для забезпечення фінансування заходів з розвитку та функціонування НСКБ пропонується відкрити державну цільову оборонну програму по забезпеченню кібербезпеки держави та залучати кошти приватного сектору до розвитку НСКБ, від ефективності функціонування якої безпосередньо залежать ризики, в тому числі і приватного сектора.

Підводячи підсумок, слід зазначити, що Україна змушена у стислі строки сформувати цілісну позицію щодо забезпечення кібербезпеки кіберпростору, який є полем нового геополітичного протистояння. Саме тому робота була спрямована на пошук напрямів підвищення кібербезпеки держави, функціонування якої регулюється системою публічного управління.

В умовах відсутності концептуального розуміння кібербезпекової політики держави та практично повної відсутності термінологічного апарату, на основі аналізу кіберзагроз і складових кіберконфліктів XXI сторіччя в роботі вдалося сформулювати напрями їх розвитку по відношенню до України в 2015–2016 роках.

З метою якнайбільшого врахування сучасних вимог кібербезпекової тематики проведено аналіз стану мілітаризації кіберпростору та проблематики міжнародної кібербезпеки, результати якої показали, що зусилля основних світових гравців знаходяться в протилежних векторах розвитку кіберпростору: з одного боку, офіційні зусилля спрямовані на демілітаризацію кіберпростору та недопущення перетворення його на нове поле збройного протистояння, а з іншого – де-факто продовжується процес протистояння.

В умовах невизначеності кібербезпекової політики України та з урахуванням її знаходження на перетині інтересів основних геополітичних гравців такий стан речей зумовлює необхідність якнайшвидшої розбудови усіх основних секторів держави за напрямом забезпечення кібербезпеки. Тому з урахуванням досвіду провідних країн світу в роботі запропонована модель національної кібербезпеки та першочергові напрями діяльності державного та приватного секторів з розвитку її складових.

Впровадження одержаних результатів дасть можливість у найкоротші терміни розробити та впровадити ефективні організаційні заходи з підвищення рівня кібербезпеки України, що позитивно вплине на розвиток та стале функціонування усіх сфер діяльності держави.

Подальшими кроками з удосконалення сфери кібербезпеки держави мають стати пошук та вироблення науково-технічних рішень з удосконалення технічних складових національної системи кібербезпеки.

Список використаних джерел:

1. ENISA Threat Landscape [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment /enisa-threat-landscape/enisa-threat-landscape-mid-year-2013.
2. Годовой отчет Cisco по безопасности за 2014 год [Електронний ресурс]. – Режим доступу: http://www.cisco.com/assets/global/RU/pdfs/executive_ security/sc-01casr2014_cte_lig_ru_35330.pdf.
3. Kaspersky security bulletin 2014 [Електронний ресурс]. – Режим доступу: http://securelist.ru/files/2014/12/Kaspersky-Security-Bulletin-2014-RU.pdf.
4. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. : НІСД, 2014. – 328 с. Електронна версія: http://www.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf.
5. China's Secret Cyberterrorism [Електронний ресурс]. – Режим доступу: http://www.thedailybeast.com/blogs-and-stories/2010-01-13/chinas-secret-cyber-terrorism/full/.
6. "Chinese government has supported cyberattack…" [Електронний ресурс]. – Режим доступу: http://www.thedailybeast.com/articles/2010/01/13/the-great-google-coverup.html.
7. NSA slides explain the PRISM data-collection program // Washington Post [Електронний ресурс]. – Режим доступу: http://www.washingtonpost.com/ newssearch/search.html?st=NSA%20slides%20explain%20the%20PRISM%20data-collection%20program.
8. Доповідь про стан інформатизації та розвиток інформаційного суспільства в Україні за 2013 рік [Електронний ресурс]. – Режим доступу: http://www.dknii.gov.ua/sites/default/files/stan_informatyzacii_20132.pdf.
9. Конвенція про кіберзлочинність // Офіційний вісник України. – 2007. – № 65; 10 вересня. – С. 107.
10. В мире два десятка стран занимаются кибероружием – McAfee [Електронний ресурс]. – Режим доступу: http://www.cybersecurity.ru/armament/ 86546.html.
11. Кибервойска РФ рождаются в Генштабе [Електронний ресурс]. – Режим доступу: http://file-rf.ru/news/12209.
12. Минобороны Беларуси создает элитное подразделение кибервойск [Електронний ресурс]. – Режим доступу: http://www.bezpeka.com/ru/news/2013/ 09/18/belarus-cyberforce.html.
13. NATO Cooperative Cyber Defence Centre of Excellence [Електронний ресурс]. – Режим доступу: https://ccdcoe.org/about-us.html.
14. International Strategy for Cyberspace [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_ strategy_for_cyberspace.pdf.

15. ‘‘Cybersecurity Enhancement Act of 2014’’ [Електронний ресурс]. – Режим доступу: http://www.gpo.gov/fdsys/pkg/BILLS-113s1353es/pdf/BILLS-113s1353es.pdf.

16. National Cybersecurity Protection Act of 2014 [Електронний ресурс]. – Режим доступу: https://www.congress.gov/bill/113th-congress/senate-bill/2519/text.

17. EU Cybersecurity plan to protect open internet and online freedom and opportunity [Електронний ресурс]. – Режим доступу: http://eeas.europa.eu/ policies/ eu-cyber-security/cybsec_comm_en.pdf.

18. China’s National Defense in 2008 [Електронний ресурс]. – Режим доступу: http://fas.org/programs/ssp/nukes/2008DefenseWhitePaper_Jan2009.pdf.

19. White Papers. The Diversified Employment of China's Armed Forces [Електронний ресурс]. – Режим доступу: http://eng.mod.gov.cn/Database/ WhitePapers/index.htm.

20. Department of Defense Strategy for operating in Cyberspace, July 2011 [Електронний ресурс]. – Режим доступу: http://www.defense.gov/news/ d20110714cyber.pdf.

21. Cyberspace Operations Concept Capability Plan 2016-2028, February 2010 [Електронний ресурс]. – Режим доступу: https://fas.org/irp/doddir/army/ pam525-7-8.pdf.

22. Конвенция об обеспечении международной информационной безопасности (концепция) [Електронний ресурс]. – Режим доступу: http://www.scrf.gov.ru/documents/6/112.html.

23. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года [Електронний ресурс]. – Режим доступу: http://www.scrf.gov.ru/documents/6/ 114.html.

24. Створення глобальної культури кібербезпеки : резолюция A/RES/57/239 [Електронний ресурс]. – Режим доступу: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf.

25. Створення глобальної культури кібербезпеки та захист найважливіших інформаційних інфраструктур A/RES/58/199 [Електронний ресурс]. – Режим доступу: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N03/ 506/54/PDF/N0350654.pdf?OpenElement.

26. Створення глобальної культури кібербезпеки та оцінка національних зусиль по захисту найважливіших інформаційних інфраструктур A/RES/64/211 [Електронний ресурс]. – Режим доступу: http://daccess-dds-ny.un.org/doc/ UNDOC/GEN /N09/474/51/PDF/N0947451.pdf?OpenElement.

27. ITU-T X.1205 (04/2008) [Електронний ресурс]. – Режим доступу: http://handle.itu.int/11.1002/1000/9136-en.

28. Понимание киберпреступности : руководство для развивающихся стран [Електронний ресурс]. – Режим доступу: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFR.pdf.

29. У пошуках кібермиру // Міжнародний союз електрозв’язку [Електронний ресурс]. – Режим доступу: http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-R.pdf.

30. Action plan to combat high-tech crime [Електронний ресурс]. – Режим доступу: http://www.irational.org/APD/CCIPS/action.htm.

31. Дубов Д. Модернізація інформаційної інфраструктури як чинник забезпечення національних інтересів України / Д. Дубов // Стратегічні пріоритети. – 2013. – № 2. – С. 90–96.

32. Стратегія національної безпеки України «Україна у світі, що змінюється» [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/105/2007.

33. Воєнна доктрина україни [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/648/2004.

34. Стратегічний оборонний бюлетень України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/771/2012/paran16#n16.

35. Framework for Improving Critical Infrastructure Cybersecurity / 2012 / [Електронний ресурс]. – Режим доступу: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

36. COBIT for risk / 2013 / [Електронний ресурс]. – Режим доступу: http://www.isaca.org/COBIT/Documents/COBIT-5-for-Risk-Preview_res_eng_0913. pdf.

37. Computer Security Incident Handling Guide. NIST Special Publication 800-61 Revision 2 / 2012 / [Електронний ресурс]. – Режим доступу: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.