УДК 342.9
DOI https://doi.org/10.15421/392117

Діордіца І. В.,
доктор юридичних наук, доцент,
професор кафедри приватного та публічного права
Київського національного університету технологій та дизайну

АДМІНІСТРАТИВНО-ПРАВОВИЙ ЗМІСТ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ ЯК СКЛАДНИКА СИСТЕМИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

ADMINISTRATIVE AND LEGAL CONTENT OF THE NATIONAL CYBERSECURITY SYSTEM AS A COMPONENT OF THE NATIONAL SECURITY SYSTEM OF UKRAINE

У статті пропонуються до розгляду авторські результати визначення концептуальних положень адміністративно-правового змісту національної системи кібербезпеки як складової частини системи національної безпеки України. Розглянуто зміст сучасного стану державної політики у сфері формування системи кібербезпеки. Проаналізовано теоретичні та практичні аспекти організаційного забезпечення системи кібербезпеки. Визначено загальні та спеціальні суб'єкти забезпечення кібербезпеки. Запропоновано власне бачення щодо виокремлення в системі кібернетичної безпеки України таких основних елементів (відповідно до основних видів загроз кібербезпеці): 1) загальнодержавна система протидії кіберзлочинності; 2) загальнодержавна система протидії кібертероризму; 3) загальнодержавна система протидії кібершпигунству; 4) загальнодержавна система протидії інформаційним війнам та новим комплексним видам загроз, у тому числі гібридним війнам; 5) загальнодержавна система кібернетичного захисту об'єктів національної критичної інфраструктури. Встановлено адміністративно-правове розуміння поняття загальнодержавної системи кібербезпеки – сукупність спеціальних суб'єктів національної системи кібербезпеки, засобів і методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних інформаційних, кібернетичних, правових, організаційних, технічних та заходів стратегічних комунікацій, що ними здійснюються. Висновується, що оскільки система національної безпеки є багатокомпонентною, постає потреба в існуванні спеціальної підсистеми, мета функціонування якої полягала б у забезпеченні функціонування та розвитку цієї системи, тобто в забезпеченні життєздатності її системостворювальних елементів, зокрема національних інтересів людини, суспільства, держави. Такою системою і є система забезпечення національної безпеки, а також національна система кібербезпеки. Ці фактори підтверджують висновок щодо розгляду національної системи кібербезпеки не лише як підсистеми державної інформаційної політики, а й передусім як складового компонента системи забезпечення національної безпеки України.

Ключові слова: *кібербезпека, національна безпека, система кібербезпеки, забезпечення кібербезпеки, кіберзлочин.*

The article offers for consideration the author's results of determining the conceptual provisions of the administrative and legal content of the national cybersecurity system as a component of the national security system of Ukraine. The content of the current state of state policy in the field of formation of the cybersecurity system is considered. Theoretical and practical aspects of organizational support of the cybersecurity system are analyzed. General and special subjects of cybersecurity are identified. The own vision of the following main elements in the system of cyber security of Ukraine (according to the main types of threats to cybersecurity) is proposed: 1) national system of combating cybercrime; 2) national system for combating cyberterrorism; 3) a nationwide system for combating cyber espionage; 4) national system of counteraction to information wars and new complex types of threats, including hybrid wars; 5) national system of cyber protection of national critical infrastructure. The administrative and legal understanding of the concept of national cybersecurity system is established – a set of special subjects of the national cybersecurity system, means and methods used by them, as well as a set of relevant interconnected information, cybernetic, legal, organizational, technical and strategic communications measures carried out by them. It is concluded that since the national security system is multicomponent, there is a need for a special subsystem, the purpose of which would be to ensure the functioning and development of this system, ie to ensure the viability of its system-forming elements, including national interests, society, state. Such a system is the national security system, as well as the national cybersecurity system. These factors confirm the conclusion that the national cybersecurity system is considered not only as a subsystem of the state information policy, but also primarily as a component of the national security system of Ukraine.

Key words: *cybersecurity, national security, cybersecurity system, ensuring cybersecurity, cybercrime.*

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий, глобальний та інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади й активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади.

Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій зумовили виникнення нових загроз національній та міжнародній безпеці. Поряд з інцидентами природного (ненавмисного) походження зростає кількість і потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Поширюються випадки незаконного створення, збирання, одержання, зберігання, використання, поширення інформації, незаконних фінансових операцій, крадіжок та шахрайства в мережі Інтернет. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави загалом.

Агресія Російської Федерації, що триває донині, інші докорінні зміни в зовнішньому та внутрішньому безпековому середовищі України вимагають невідкладного створення національної системи кібербезпеки як складової частини системи забезпечення національної безпеки України. Ці та інші фактори зумовлюють *актуальність цього дослідження*.

Незважаючи на значний масив наукової літератури [1–9], питанням побудови саме системи кібербезпеки і правового регулювання її діяльності приділялось замало уваги.

Нині провідні держави світу та суспільство загалом дедалі більше 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 із ними інфраструктурі, разом з об'єктами, що підпадають під їх контроль та управління. Захист інтересів держав та громадян у кіберпросторі стає життєво важливим завданням, яке перетворює безперешкодне використання ІТ-мереж на питання безпеки й оборони.

Найбільш ефективним шляхом вирішення зазначених питань є побудова моделі національної системи кібербезпеки та розроблення з обов'язковим зазначенням у законодавстві пріоритетних напрямів та відповідальності діяльності як державних, так і недержавних суб'єктів цієї системи.

Зазначу, що зміст будь-якого явища – це його сутність, внутрішня особливість [10, с. 373], отже, адміністративно-правовий зміст національної системи кібербезпеки становитимуть її певні ознаки та особливості.

Під *системою* розуміється сукупність якихнебудь елементів, одиниць, частин, об'єднуваних за спільною ознакою, призначенням [10, с. 1126].

У першому Словнику зі стратегічних комунікацій поняття «система» визначено як множина взаємопов'язаних елементів та відносин між ними, які у своїй органічній єдності утворюють нову якість. Система задається (описується) такими параметрами (характеристиками): метою і завданнями (конкретизованою в просторі і часі метою); входами і виходами системи; обмеженнями, які необхідно враховувати під час побудови (модернізації, оптимізації, реструктуризації) системи; процесами всередині системи, які забезпечують перетворення входів у виходи [11, с. 327].

Отже, *система кібербезпеки* – це не проста сукупність органів, задіяних на забезпечення кібербезпеки через визначення їхньої предметної компетенції у профільному законі, це, передусім, взаємопов'язана спільними цілями та завданнями щодо реалізації національних інтересів у кіберпросторі множина органів, які внаслідок спільної, узгодженої за принципами та методами діяльності досягають спільних результатів із використанням притаманних форм і методів реалізації предметної компетенції, визначеної в законодавстві України.

На думку В.П. Шеломенцева, *система кібернетичної безпеки* (система кібербезпеки) розглядається як сукупність спеціальних суб'єктів забезпечення кібернетичної безпеки, засобів та методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних та технічних заходів, що ними здійснюються [7, с. 300].

Інші автори під терміном *система кібернетичної безпеки* розуміють сукупність узгоджених за завданнями елементів кібернетичної безпеки, які комплектуються та розгортаються за єдиним замислом і планом у кібернетичному просторі для забезпечення кібернетичної безпеки інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [8].

Погоджуюся з тим, що побудова дієвої національної системи кібербезпеки вимагає від державних органів України чіткого визначення державної політики в цій сфері та випереджального реагування на динамічні зміни, що відбуваються у світі у сфері забезпечення кібернетичної безпеки. При цьому вибір конкретних засобів і шляхів забезпечення кібернетичної безпеки України зумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру та масштабам реальних і потенційних кібернетичних загроз життєво важливим інтересам людини і громадянина, суспільства і держави. Організаційне забезпечення системи кібербезпеки також можна розглядати як цілеспрямовану діяльність суб'єкта забезпечення кібербезпеки, пов'язану зі:

– створенням і впорядкуванням (розвитком) організаційних структур, найбільш доцільних для забезпечення безпеки в кіберпросторі;

– впорядкуванням (налагодженням) процесу управління у сфері забезпечення безпеки в кіберпросторі, забезпеченням найліпших умов для прийняття та реалізації відповідних управлінських рішень.

Організаційне забезпечення системи кібербезпеки характеризується місцем і роллю спеціальних суб'єктів (відповідних державних органів та їх спеціалізованих підрозділів), їхніми функціями, повноваженнями, а також підставами, умовами і напрямами їх взаємодії в процесі здійснення заходів із забезпечення безпеки в кіберпросторі.

Серед суб'єктів забезпечення кібернетичної безпеки виділяють загальні та спеціальні.

До *загальних суб'єктів* забезпечення кібернетичної безпеки належать: Президент України; Верховна Рада України; Рада національної безпеки і оборони України; Кабінет Міністрів України; Збройні сили України, інші військові формування, утворені відповідно до закону; Служба безпеки України; Служба зовнішньої розвідки України; Національний банк України; інші міністерства та центральні органи виконавчої влади; місцеві державні адміністрації та органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; суб'єкти підприємницької діяльності різних форм власності у сфері виробництва інформаційних продуктів та надан-

ня інформаційних послуг; підприємства, установи та організації, зараховані до об'єктів критичної інфраструктури.

Спеціальними суб'єктами забезпечення кібернетичної безпеки є державні органи, які, крім загальних функцій, уповноважені на здійснення боротьби з кіберзлочинністю та кібертероризмом, протидію кібершпигунству, а також на забезпечення кібернетичного захисту об'єктів національної критичної інфраструктури, здійснення кібероборони. До таких суб'єктів належать Національний координаційний центр з кібербезпеки, Міністерство внутрішніх справ України, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України, Міністерство юстиції України, Генеральна прокуратура України.

Підтримую думку про доцільність виокремлення в системі кібернетичної безпеки України таких основних елементів відповідно до виділених основних видів загроз кібербезпеці: 1) загальнодержавна система протидії кіберзлочинності; 2) загальнодержавна система протидії кібертероризму; 3) загальнодержавна система протидії кібершпигунству; 4) загальнодержавна система протидії інформаційним війнам та новим комплексним видам загроз, у тому числі гібридним війнам; 5) загальнодержавна система кібернетичного захисту об'єктів національної критичної інфраструктури [12].

При цьому під *загальнодержавною системою* загалом варто розуміти сукупність спеціальних суб'єктів національної системи кібербезпеки, засобів і методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних інформаційних, кібернетичних, правових, організаційних, технічних та заходів стратегічних комунікацій, що ними здійснюються.

Наприклад, в Європейському Союзі у зв'язку з розумінням важливості проблеми кібербезпеки в 2004 році було створено Європейське агентство з мережевої та інформаційної безпеки, місією якого є допомога Спільноті в забезпеченні високого рівня мережевої та інформаційної безпеки, Комісії, державам-членам та бізнес-спільнотам у виконанні вимог мережної та інформаційної безпеки, а тому числі удосконаленні нинішнє та майбутнє законодавство Спільноти [13].

Основними *завданнями* агентства є інформування громадськості про нові віруси, атаки хакерів і проблеми з безпекою інформаційного простору Європи, а також розслідування епідемій електронних вірусів і електронних атак. Особливо підкреслюється, що ENISA не збирається відігравати роль кіберполіцейських, оскільки для силових операцій є інші структури, а слугує консультативним органом, що надає посильну допомогу як у затриманні злочинців, так і в запобіганні вчиненні злочинів. Агентство планує розробляти і поширювати навчальні посібники, а також проводити навчання персоналу інформаційним ризикам і способам захисту даних. Планується і проведення науково-дослідницької роботи в галузі захисту інформації [13].

Щодо України, то варто зазначити, що практично всі національні стратегії щодо забезпечення кібербезпеки і більшість експертів пов'язують проблематику кібербезпеки саме з використанням у процесі людської діяльності комп'ютерних систем і телекомунікаційних мереж (до останніх належить і мережа Інтернет) [14], а Національний координаційний центр кібербезпеки має стати системоутворювальним елементом всієї системи кібербезпеки та кіберзахисту України. До складу Центру увійшли представники ключових державних органів, які відповідають за весь спектр питань протидії широкому спектру кіберзагроз [15].

У розвинених країнах кібербезпека і стратегія кібероборони – важливі складники забезпечення миру. Найбільше в цій сфері досягли успіху США й Ізраїль, де є відповідні підрозділи кібервійськ, а в США утворено окреме кіберкомандування.

Кіберпростір давно перетворився на п'ятий вимір ведення війни, крім суші, моря, повітря і космосу. Загальносвітовою є стійка тенденція зростання числа комп'ютерних атак на важливі об'єкти національних інфраструктур іноземних країн, що призводило й призводить до завдання шкоди державам через спотворення та витоки важливої для них інформації, блокування виробничих процесів на стратегічних об'єктах. Зазначене зумовило зміну зовнішньополітичних доктрин провідних ядерних країн світу, згідно з якими кібератаки прирівнюються до військових дій та передбачають можливість завдання воєнних ударів у відповідь.

Протистояння в кіберпросторі є небезпечною складовою частиною гібридної війни, розв'язаної проти України, тому потрібно швидко, надійно та ефективно реагувати на будь-які кіберзагрози, що неможливо без інтегрування та чіткої взаємодії всіх наявних ресурсів суб'єктів кібербезпеки. Окрім відпрацювання ефективного реагування на кібератаки та кіберінциденти, необхідно вибудувати активний захист кіберпростору, створюючи належні умови для інституційного та технологічного забезпечення кібербезпеки [16].

Очевидною є необхідність створення національної системи кібербезпеки як одного з елементів системи забезпечення національної безпеки держави, коли нею займатимуть відповідні підрозділи СБУ, кіберзахистом – підрозділи ДССЗЗІ (Державної служби спеціального зв'язку та захисту інформації), а боротьбою з кіберзлочинністю – підрозділи кіберполіції. Координацію та ефективну взаємодію буде забезпечувати відповідний підрозділ РНБО України [17], тобто нагальною є потреба підготовки та ухвала відповідних нормативно-правових актів та внесення змін до наявних.

Нині у ДССЗЗІ відсутні як повноваження, так і інструментарій та важелі впливу в цій сфері. Водночас доволі позитивним є той факт, що в системі Держспецзв'язку функціонує спеціалізований підрозділ – команда реагування на комп'ютерні інциденти (CERT-UA) [9, с. 128].

Розвиток національної системи кібербезпеки має супроводжуватись відповідними коригувами

в процесі реформування усієї системи національної безпеки.

Зауважу, що Верховна Рада України ухвалила Закон України «Про основні засади забезпечення кібербезпеки України». Метою 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 в тісній взаємодії державного і приватного секторів та громадянського суспільства.

Незрозумілим є те, що у Положенні про Національний координаційний центр кібербезпеки закріплені його завдання і, з-поміж інших, здійснення аналізу стану кібербезпеки та результатів проведення огляду національної системи кібербезпеки, стану забезпечення кадрами національної системи кібербезпеки та підготовка пропозицій щодо її удосконалення [18], а от нормативно-правовий акт, в якому тлумачилися б усі аспекти цієї системи, досі відсутній.

Національна система кібербезпеки як насамперед система організованої та цілеспрямованої взаємодії суб'єктів кібербезпеки, має об'єднати широкий спектр правоохоронних, розвідувальних та контррозвідувальних органів, центральних органів виконавчої влади, органів місцевого самоврядування, інших державних органів, що здійснюють регулювання у сфері інформатизації, телекомунікацій та захисту інформації для своєчасного виявлення, попередження та припинення кіберзагроз, усунення передумов до їх настання та мінімізації негативних наслідків від їх реалізації.

Функціонування вказаної системи є неможливим без тісної співпраці з приватним сектором – операторами та провайдерами телекомунікації, власниками та розпорядниками критичних об'єктів інформаційної інфраструктури держави, компаній, діяльність яких пов'язана зі сферою інформаційної безпеки [9, с. 128].

Для ефективного правового регулювання кібербезпеки надзвичайно важливо розуміти правову природу загроз кіберпростору.

Як зазначено у Стратегії національної безпеки України, то актуальними загрозами кібербезпеці і безпеці інформаційних ресурсів є уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

За своїм алгоритмом будови функціоналу національної системи кібербезпеки вона має будуватись за принципом адекватності: кожній конкретно визначений загрозі має відповідати або напрям державної кібербезпекової політики, або конкретне завдання в рамках визначеного напряму цієї політики.

Пріоритетами забезпечення кібербезпеки та безпеки інформаційних ресурсів є 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, відмова від програмного забезпечення, зокрема антивірусного, розробленого в 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 сектора безпеки і оборони, розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки [19].

Останнім часом проблема забезпечення національної безпеки зміщується у бік не стільки декларованої, скільки реально розглядуваної. Передусім це зумовлено активізацією зовнішніх загроз безпечного розвитку України: посиленням мілітаризації держав у регіоні, наявністю відкритих збройних конфліктів на території України та поряд з її кордонами, використанням положення енергетичної та торговельно-економічної залежності нашої країни, посиленням економічного та інформаційного тиску на неї, веденням гібридної війни тощо.

Водночас зовнішні загрози посилюються наявністю внутрішніх викликів національній безпеці, зокрема, йдеться про розбалансованість та незавершеність системних реформ, перманентний конфлікт інтересів між центральними органами виконавчої влади, зниження обороноздатності держави, боєздатності Збройних сил України, незадовільний стан фінансування, складне економічне становище, глибоку та системну корупційну кризу.

Слід констатувати, що сучасний стан системи національної безпеки не забезпечує в повному обсязі нейтралізацію сучасних загроз і викликів. Незважаючи на вжиття низки заходів, реалізація державної безпекової політики ще не може характеризуватися як системна.

Висновок. Національна безпека має забезпечуватися проведенням єдиної узгодженої державної політики у всіх сферах життєдіяльності, системою заходів інформаційного, організаційно-правового, фінансово-економічного, соціально-політичного характеру, котрі є адекватними загрозам і небезпекам життєво важливим інтересам особи, суспільства і держави. З огляду на той факт, що система національної безпеки є багатокомпонентною, постає потреба в існуванні спеціальної підсистеми, мета функціонування якої полягала б у забезпеченні функціонування та розвитку цієї системи, тобто у забезпеченні життєздатності її системостворювальних елементів, зокрема, національних інтересів людини,

суспільства, держави. Такою системою і є система забезпечення національної безпеки, а також національна система кібербезпеки. Ці та інші фактори і підтверджують висновок щодо розгляду національної системи кібербезпеки не лише як підсистеми державної інформаційної політики, а й передусім як складового компонента системи забезпечення національної безпеки України.

ЛІТЕРАТУРА:

1. Ліпкан В.А., Никифорчук Д.Й., Руденко М.М. Боротьба з тероризмом : монографія. Київ : Знання, 2002. 254 с.

2. Ліпкан В.А., Діордіца І.В. Національна безпека України: кримінально-правова охорона : навчальний посібник. Київ : КНТ, 2007. 292 с.

3. Ліпкан В.А., Сопілко І.М., Кір'ян В.О. Правові засади розвитку інформаційного суспільства в Україні : монографія / за заг. ред. В.А. Ліпкана.Київ : О.С. Ліпкан, 2015. 664 с.

4. Ліпкан В.А., Харченко Л.С., Логінов О.В. Інформаційна безпека України : глосарій. Київ : Текст, 2004. 136 с.

5. Рудник Л.І. Право на доступ до інформації : дис. … канд. юрид. наук : 12.00.07. Київ, 2015. 247 с.

6. Запорожець О.Ю. Політика Європейського Союзу в сфері інформаційної безпеки. *Актуальні проблеми міжнародних відносин* : збірник наук. пр. / Київський нац. ун-т ім. Тараса Шевченка; Ін-т міжнар. відносин. Київ, 2009. Вип. 87, ч. 2. С. 36–45.

7. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. № 2 (28). С. 299–309.

8. Розширення термінології сучасного кіберпростору / В.В. Куцаєв, Є.О. Живило, С.П. Срібний, Ю.О. Черниш. URL: mino.esrae.ru/pdf/2014/3Sm/1387.doc.

9. Петров В.В. Щодо формування національної системи кібербезпеки України. *Стратегічні пріоритети*. Київ, 2013. № 4 (29). С. 127–130.

10. Великий тлумачний словник сучасної української мови / [уклад. і голов. ред. В.Т. Бусел]. Київ ; Ірпінь : Перун, 2003. 1440 с.

11. Попова Т.В., Ліпкан В.А. Стратегічні комунікації : словник /за заг. ред. д-ра юрид. наук. В.А. Ліпкана. Київ : О. С. Ліпкан, 2016. 416 с.

12. Діордіца І. Поняття і зміст кіберзагроз на сучасному етапі. *Підприємництво, господарство і право*. 2017. № 4. URL: http://pgp-journal.kiev.ua/archive/2017/4/22.pdf.

13. Cyber Security Strategy for Germany. URL: https://www.enisa.europa.eu.

14. Аналітична записка щодо Законопроекту «Про основні засади забезпечення кібербезпеки України». URL: www.inau.org.ua/download.php?bd189ae6a731113f59c7d7fcacf193f3.

15. Турчинов О. Національний координаційний центр кібербезпеки повинен мобілізувати весь наявний потенціал для забезпечення надійного кіберзахисту країни. *Рада національної безпеки і оборони України* : сайт. URL: http://www.rnbo.gov.ua/news/2528.html 11.07.2016

16. Ми повинні швидко реагувати на всі кіберзагрози, – Турчинов. URL: http://ua.censor.net.ua/n409349.

17. В Україні буде створена Національна система кібербезпеки. *ZAXID. NET.* 2016. 27 січня. URL: http://zaxid.net/news/showNews.do?.

18. Положення про Національний координаційний центр кібербезпеки : затв. указом Президента України від 7 черв. 2016 р. № 242/2016. URL: http://zakon2.rada.gov.ua/laws/show/242/2016.

19. Стратегія кібербезпеки України : затв. указом Президента України від 15 берез. 2016 р. № 96/2016. URL: http://www.president.gov.ua/documents/962016-19836.