DOI: 10.15421/151846 УДК: 35.08 (477)

Теоретичні підходи до понятійно-категоріального апарату кібербезпеки в системі публічного управління

Кубанов Є. В., Міжрегіональна академія управління персоналом

У статті аналізуються наукові підходи до поняття «кібербезпека». Визначено поняття «кібербезпека системи публічного управління», яке розуміється як основа національної безпеки України, яка формує захищеність держави, суспільства, системи публічного управління, населення країни в кібернетичному просторі через створення легітимних механізмів забезпечення кібербезпеки публічного управління. Виокремленні внутрішні та зовнішні загрози. Виділені основні елементи системи кібербезпеки публічного управління, зокрема: інформація, інформаційно-комунікативні системи; загрози; механізми забезпечення кібербезпеки системи публічного управління; суб'єкти забезпечення кібербезпеки системи публічного управління.

Інтеграція України в європейський простір та реформування сфер економіки, промисловості та оборони викликали необхідність створення принципово нового підходу до інформаційної та кібернетичної безпеки. Кіберпростір як арена конфліктів між державами, організаціями, посадовими особами є однією з найактуальніших проблем сьогодення.

У статті проаналізовані наукові підходи до поняття «кібербезпека» та визначено, що кібербезпека системи публічного управління – це основа національної безпеки України, яка формує захищеність держави, суспільства, системи публічного управління, населення країни в кібернетичному просторі через створення легітимних механізмів забезпечення кібербезпеки публічного управління. Виокремленні внутрішні (корупційні дії; апаратні закладки у мікросхемах і прошивках комп'ютерного і мережного обладнання; слабку організацію системи управління кіберпростором) та зовнішні загрози (таргетовані атаки; кібертероризм; кібервійни; хактивізм; атаки на банківські системи; атаки на електронний уряд).

Ключові слова: *національна безпека; кібербезпека; публічне управління; зовнішні та внутрішні загрози; інформація; інформаційно-комунікативні системи*

Theoretical approaches to the conceptual-categorical apparatus of cybersecurity in the system of public administration

Kubanov E. V., Interregional Academy of Personnel Management

The article analyzed the scientific approaches to the concept of «cybersecurity». The author defined the concept of «cybersecurity of the public administration system», which is understood as the basis of the national security of Ukraine, which forms the security of the state, society, public administration system, and the population of the country in the cybernetic space through the creation of legitimate mechanisms for ensuring the cybersecurity of public administration. The article identified internal and external threats. The author highlighted the main elements of the cybersecurity system of public administration, in particular: information, information and communication systems; threats; mechanisms of providing cybersecurity of the public administration system; subjects of the cybersecurity of the public administration system.

Integration of Ukraine into the European space and the reform of the spheres of economy, industry and defense has called for a radically new approach to information and cybernetic security. Cyberspace as an arena of conflicts between states, organizations, and officials is one of the most pressing problems of the present.

The article analyzes the scientific approaches to the concept of «cyber security» and states that cybersecurity of the system of public administration is the basis of the national security of Ukraine, which forms the security of the state, society, public administration system, and the population of the country in the cybernetic space through the creation of legitimate mechanisms for ensuring the cybersecurity of public administration. Separate internal (corruption actions; hardware bookmarks in chips and firmware of computer and network equipment; weak organization of the cyberspace management system) and external threats (targeted attacks, cyberterrorism, cyberwar, hatcism, attacks on banking systems, attacks on e-government).

Keywords: national security; cybersecurity; public administration; external and internal threats; information; information and communication systems

Теоретические подходы к понятийно-категориальному аппарату кибербезопасности в системе публичного управления

Кубанов Е. В., Межрегиональная академия управления персоналом

В статье анализируются научные подходы к понятию «кибербезопасность». Определено понятие «кибербезопасность системы публичного управления», которое понимается как основа национальной безопасности Украины, которая формирует защищенность государства, общества, системы публичного управления, население страны в кибернетическом пространстве посредством создания легитимных механизмов обеспечения кибербезопасности публичного управления. Выделении внутренние и внешние угрозы. Выделены основные элементы системы кибербезопасности публичного управления, в частности: информация, информационно-коммуникативные системы; угрозы; механизмы обеспечения кибербезопасности системы публичного управления; субъекты обеспечения кибербезопасности системы публичного управления.

Интеграция Украины в европейское пространство и реформирования сфер экономики, промышленности и обороны вызвали необходимость создания принципиально нового подхода к информационной и кибернетической безопасности. Киберпространство как арена конфликтов между государствами, организациями, должностными лицами являются одной из самых актуальных проблем современности.

В статье проанализированы научные подходы к понятию «кибербезопасность» и определено, что кибербезопасность системы публичного управления - это основа национальной безопасности Украины, которая формирует защищенность государства, общества, системы публичного управления, население страны в кибернетическом пространстве посредством создания легитимных механизмов обеспечения кибербезопасности публичного управления. Выделении внутренние (коррупционные действия; аппаратные закладки в микросхемах и прошивках компьютерного и сетевого оборудования; слабую организацию системы управления киберпространством) и внешние угрозы (таргетированной атаки; кибертерроризм; кибервойны; хактивизм; атаки на банковские системы; атаки на электронное правительство).

Ключевые слова: *национальная безопасность; кибербезопасность; публичное управления; внешние и внутренние угрозы; информация; информационно-коммуникативные системы*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями.

Стрімкий розвиток інформаційного суспільства, розвиток глобального інформаційного суспільства, впровадження в діяльність органів державної влади електронного документообігу, обмін інформаційними базами між органами влади, в мережі системи державного управління вимагає формування захисту інформаційних потоків від атак та витоків. На сьогодні стоїть гостро проблема розробки дієвих механізмів забезпечення інформаційної безпеки як основної системи національної безпеки України.

Інтеграція України в європейський простір та реформування сфер економіки, промисловості та оборони викликали необхідність створення принципово нового підходу до інформаційної та кібернетичної безпеки. Кіберпростір як арена конфліктів між державами, організаціями, посадовими особами є однією з найактуальніших проблем сьогодення.

На сьогодні проблеми забезпечення кібербезпеки в України регламентують нормативно-правові документи, у тому числі законами України: «Про основи національної безпеки України», «Про захист інформації в інформаційно-телекомунікаційних мережах», «Про телекомунікації», «Про інформацію», «Про наукову-технічну інформацію», «Про доступ до публічної інформації», Стратегія національної безпеки України, Стратегія кібербезпеки України, Доктрина інформаційної безпеки України та ін.

У зазначених нормативно-правових документах визначається актуальність теми забезпечення кібербезпеки в системі публічного управління.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми, виділення не вирішених раніше частин загальної проблеми.

Аналіз наукових джерел із даної проблематики свідчить, що в Україні лише в останні десятиріччя українські вчені почали предметно розглядати проблему кібербезпеки, і більшість уваги приділено юридичному аналізу забезпечення кібербезпеки.

Крім того аналіз вітчизняних наукових публікацій, присвячених питанням забезпечення кібербезпеки, свідчить, що вказаний тематичний напрям був аналізований у наукових працях наступних вчених: О. Баранов [1], В. Богданович [2], В. Бурячок [7], М. Грайворонський [3], І. Діордіца [4; 8], Д. Дубов [5], Є. Живило [6], В. Ліпкан [8], Н. Логінова [9], А. Мовчан [10], В. Петров [11], О. Черноног [6], В. Фурашев [14], В. Шеломенцев [15]. Так, Є. Живило та О. Черноног [6] аналізують національну систему кібербезпеки, у тому числі формує єдину загальнодержавну модель побудови Національної системи кібербезпеки.

Водночас, на сьогодні не розроблено поняття «кібербезпека», «кібербезпека системи публічного управління», не визначена сучасна модель кібербезпеки в системі публічного управління.

Формулювання цілей статті (постановка завдання).

Мета статті – проведення системного аналізу наукових підходів до понятійно-категоріального апарату «кібербезпека в системі публічного управління», визначення авторської дефініції «кібербезпека в системі публічного управління».

Виклад основного матеріалу дослідження з обґрунтуванням отриманих наукових результатів.

Спочатку дослідження проаналізуємо поняття «кібербезпека». Так, кібербезпека це:

по-перше, 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 [15];

по-друге, сукупність узгоджених за завданнями елементів кібернетичної безпеки, які комплектуються та розгортаються за єдиним замислом і планом у кібернетичному просторі з метою забезпечення кібернетичної безпеки інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [4];

по-третє, стан захищеності державних електронних інформаційних ресурсів у кіберпросторі від ризику стороннього впливу, виявлення та запобігання різних зовнішніх втручань через інформаційні системи, а також загрози національним та особистим інтересам [9, с. 575];

по-четверте, стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кібернетичному просторі, в якому є можливим безперешкодне створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації, а у вузькому сенсі – стан індивіда, суспільства та держави, де відсутня будь-яка небезпека [8];

по-п'яте, стан здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу (управління) інформації [14];

по-шосте, 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 [1].

Таким чином, кібербезпека системи публічного управління – це основа національної безпеки України, яка формує захищеність держави, суспільства, системи публічного управління, населення країни в кібернетичному просторі через створення легітимних механізмів забезпечення кібербезпеки публічного управління.

Тепер проаналізуємо загрози кібербезпеки в системі публічного управління.

Відповідно до Стратегії національної безпеки України, до загроз кібербезпеці і безпеці інформаційних ресурсів віднесені [13]:

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.

Відповідно до Стратегії кібербезпеки України загрози кібербезпеці актуалізуються через дію таких чинників, зокрема, як [12]:

невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;

недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;

безсистемність заходів кіберзахисту критичної інформаційної інфраструктури;

недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів;

недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;

недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

Проведений аналіз дає підстави зазначити, що загрози в кібернетичному просторі можуть бути:

1) залежно від можливості прогнозування: передбачувані або не передбачувані;

2) залежно від об'єкта безпеки:

- люди (організації),
- технічне оснащення,
- інформація,
- технології,
- імідж (репутація),
- матеріальні та нематеріальні активи;

3) залежно від походження: зовнішні та внутрішні;

Слід зазначити, що у науці найбільш поширено класифікувати загрози від сфери виникнення. Проаналізуємо основні зовнішні та внутрішні загрози кібербезпеки.

До зовнішніх загроз кібербезпеки в системі публічного управління належать:

по-перше, таргетовані атаки. В залежності від цілей, можна виділити дві протилежні тактики атак на комп'ютерні системи. Перший варіант – застосувати для атаки програмне забезпечення (вірус, троянський кінь), маючи на меті компрометацію якомога більшої кількості систем. Другий варіант – проводити атаку прицільно (звідки й назва «таргетовані», тобто націлені), для компрометації комп'ютерів конкретної установи або навіть конкретних користувачів (як правило, посадових осіб високого рангу або їхніх помічників, науковців, взагалі людей, які мають справу з особливо цінною інформацією);

по-друге, кібертероризм (вплив на системи керування). Те, що, власне, і називають кібертерроризмом – можливість впливу через комп'ютерну мережу (зокрема, Інтернет) на системи керування транспортом, промисловими об'єктами, будинками та будь-якими технологічними процесами. ІКТ надають терористам кілька інструментів: застосування комп'ютерних мереж для керування, координації дій і підготовки терактів; можливість терористам напряму звертатись до широкого кола людей, використовуючи сервіси сучасного Інтернету; потенційно будь-який технологічний процес, яким керує цифрова система керування (або SCADA), може стати об'єктом атаки кібертерористів;

по-третє, кібервійни. Stuxnet – це є прообраз кіберзброї для ведення кібервійни, використовується для здійснення диверсій або відключення систем (наприклад, комплексів протиповітряної чи протиракетної оборони);

по-четверте, хактивізм – зловживання інформацією у соціальних мережах (вплив на суспільство). Як правило, йдеться про викриття таємних операцій, змов, корупції та інших дій на рівні урядів чи окремих політичних сил, які суперечать закону, принципам демократії й іншим загальнолюдським цінностям;

по-п'яте, атаки на банківські системи (викрадення грошей);

по-шосте, атаки на електронний уряд. «Електронний уряд» – інформаційно-комунікаційна система, або об'єднання інформаційно-комунікаційних систем, що автоматизує інформаційну взаємодію органів

державної влади та органів місцевого самоврядування з громадянами та суб'єктами господарювання з метою підвищення ефективності надання державних послуг. Атаки на електронний уряд можуть зашкодити функціонуванню такої системи, а у країнах з низьким рівнем впровадження інформаційно-комунікаційних технологій – підірвати довіру до демократичних перетворень і технічного прогресу [3, с. 17].

До внутрішніх загроз кібербезпеки слід віднести: корупційні дії, апаратні закладки у мікросхемах і прошивках комп'ютерного і мережного обладнання, слабку організацію системи управління кіберпростором, відсутність корпоративної політики тощо.

Проведений аналіз дає підстави виділити основні елементи системи кібербезпеки публічного управління, зокрема: інформація, інформаційно-комунікативні системи; загрози; механізми забезпечення кібербезпеки системи публічного управління; суб'єкти забезпечення кібербезпеки системи публічного управління.

На схемі нижче представлена система забезпечення кібербезпеки публічного управління (рис.1).

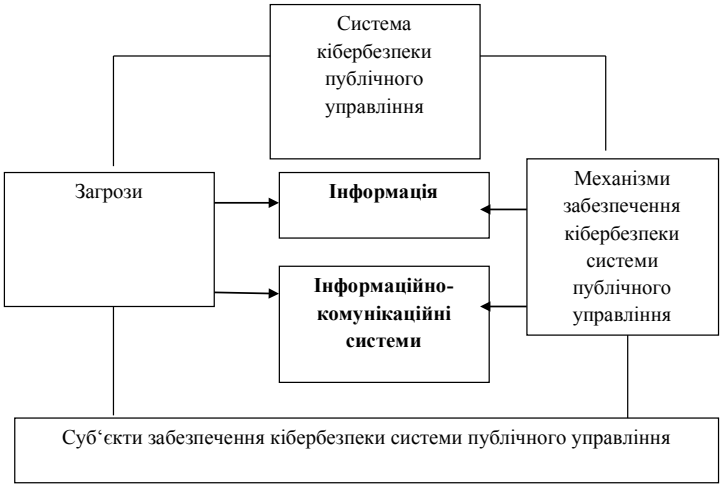

Рис. 1. Система забезпечення кібербезпеки публічного управління.

Висновки.

У статті проаналізовані наукові підходи до поняття «кібербезпека» та визначено, що кібербезпека системи публічного управління – це основа національної безпеки України, яка формує захищеність держави, суспільства, системи публічного управління, населення країни в кібернетичному просторі через створення легітимних механізмів забезпечення кібербезпеки публічного управління. Виокремленні внутрішні (корупційні дії; апаратні закладки у мікросхемах і прошивках комп'ютерного і мережного обладнання; слабку організацію системи управління кіберпростором) та зовнішні загрози (таргетовані атаки; кібертероризм; кібервійни; хактивізм; атаки на банківські системи; атаки на електронний уряд).

У перспективі подальших розвідок передбачається проаналізувати закордонний досвід забезпечення кібербезпеки системи публічного управління, виокремити механізми забезпечення кібербезпеки системи публічного управління.

БИБИЛИОГРАФИЯ

1. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека» / О. А. Баранов // Правова інформатика. – 2014. – № 2. – С. 54-62.
2. Богданович В. Ю. Методологічний підхід до обґрунтування режимів функціонування системи забезпечення кібернетичної безпеки / В. Ю. Богданович, М. М. Алексєєв // Сучасний захист інформації. – 2013. – № 4. – С. 68-77.
3. Грайворонський М. В. Сучасні підходи до забезпечення кібернетичної безпеки / М. В. Грайворонський // Матеріали XIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», м. Київ, 21-23 травня 2015. – Київ : НТУУ «КПІ». – 2015. – С. 10-17.
4. Діордіца І. В. Поняття та зміст національної системи кібербезпеки / І. В. Діордіца. – Режим доступу: http://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/.
5. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – Київ: НІСД, 2014. – 328 с.
6. Живило Є. О. Напрями створення та розбудови національної системи кібербезпеки / Є. О. Живило, О. О. Черноног // Збірник наукових праць ВІТІ. – 2017. – № 3. – С. 60-65.
7. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. – Київ: ДУТ, 2015. – 288 с.
8. Ліпкан В. Національна система кібербезпека як складові частина системи забезпечення національної безпеки / В. Ліпкан, І. Діордіца // Підприємництво, господарство і право. – 2017. – № 5. – С. 174-180.
9. Логінова Н. І. Правові основи кібербезпеки в Україні / Н. І. Логінова // Правові та інституційні механізми забезпечення розвитку держави та прав в умовах євроінтеграції: матеріали міжнар. наук.-практ. конференції. – Одеса: 2016. –Т. 1. – С. 575-577.
10. Мовчан А. В. Кібернетична безпека України в умовах глобальної нестабільності / А. В. Мовчан // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2015. – № 1. – С. 159-163.
11. Петров В. В. Щодо формування національної системи кібербезпеки України / В. В. Петров // Стратегічні пріоритети. – Київ: НІСД, 2013. – № 4. – С. 127-130.
12. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 № 96. – Режим доступу: http://www.president.gov.ua/documents/962016-19836
13. Стратегія національної безпеки України: затверджена Указом Президента України від 26 трав. 2015 р. № 287. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/287/2015.
14. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності // Інформація і право. – 2012. – № 2. – С. 162-169.
15. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – № 1. – С. 312-320.

REFERENCES

1. Baranov, O.A. (2014). Pro tlumachennia ta vyznachennia poniattia «kiberbezpeka» [About the interpretation and definition of «cyber security»]. *Pravova informatyka, 2,* 54-62 [in Ukrainian].
2. Bohdanovych, V.Yu., & Aleksieiev, M. M. (2013). Metodolohichnyi pidkhid do obgruntuvannia rezhymiv funktsionuvannia systemy zabezpechennia kibernetychnoi bezpeky [Methodological approach to the substantiation of the modes of functioning of the system for ensuring cybernetic security]. *Suchasnyi zakhyst informatsii, 4,* 68-77 [in Ukrainian].
3. Hraivoronskyi, M.V. (2015). Suchasni pidkhody do zabezpechennia kibernetychnoi bezpeky [Modern approaches to the provision of cybernetic security]. *Materialy XIII Vseukrainskoi naukovo-praktychnoi konferentsii studentiv, aspirantiv ta molodykh vchenykh «Teoretychni i prykladni problemy fizyky, matematyky ta informatyky» – Proceedings from the XIII All-Ukrainian Scientific and Practical Conference of Students, Postgraduates and Young Scientists «Theoretical and Applied Problems of Physics, Mathematics and Informatics».* Kyiv: NTUU «KPI» [in Ukrainian].
4. Diorditsa, I.V. *Poniattia ta zmist natsionalnoi systemy kiberbezpeky [Concept and content of the national system of cyber security]*. Retrieved from: http://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/ [in Ukrainian].

5. Dubov, D.V. (2014). *Kiberprostir yak novyi vymir heopolitychnoho supernytstva [Cyberspace as a New Dimension of Geopolitical Competition]*. Kyiv: NISD [in Ukrainian].
6. Zhyvylo, Ye.O., & Chernonoh, O.O. (2017). Napriamy stvorennia ta rozbudovy natsionalnoi systemy kiberbezpeky [Directions of creation and development of the national system of cyber security]. *Zbirnyk naukovykh prats VITI, 3,* 60-65 [in Ukrainian].
7. Buriachok, V.L., Tolubko, V.B., Khoroshko, V.O., & Toliupa, S.V. (2015). *Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt [Information and Cybersecurity: Socioeconomic Aspect]*. Kyiv: DUT [in Ukrainian].
8. Lipkan, V., & Diorditsa, I. (2017). Natsionalna systema kiberbezpeka yak skladovi chastyna systemy zabezpechennia natsionalnoi bezpeky [National cyber security system as an integral part of the system of ensuring national security]. *Pidpryiemnytstvo, hospodarstvo i pravo, 5,* 174-180 [in Ukrainian].
9. Lohinova, N.I. (2016). *Pravovi osnovy kiberbezpeky v Ukraini / N. I. Lohinova [Legal bases of cybersecurity in Ukraine]. Pravovi ta instytutsiini mekhanizmy zabezpechennia rozvytku derzhavy ta prav v umovakh yevrointehratsii – Legal and institutional mechanisms for ensuring state and rights development in the conditions of European integration: Proceedings from the International Scientific and Practical Conference.* (Vol. 1). (pp. 575-577). Odesa [in Ukrainian].
10. Movchan, A.V. (2015). Kibernetychna bezpeka Ukrainy v umovakh hlobalnoi nestabilnosti [Cybernetic security of Ukraine in the conditions of global instability]. *Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka), 1,* 159-163 [in Ukrainian].
11. Petrov, V.V. (2013). Shchodo formuvannia natsionalnoi systemy kiberbezpeky Ukrainy [On the formation of the national system of cyber security of Ukraine]. *Stratehichni priorytety, 4,* 127-130. Kyiv: NISD [in Ukrainian].
12. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku «Pro Stratehiiu kiberbezpeky Ukrainy» [On the decision of the Council of National Security and Defense of Ukraine dated January 27, 2016 «On the Strategy of Cybersecurity of Ukraine»]. *Ukaz Prezydenta Ukrainy vid 15.03.2016 № 96. – Decree of the President of Ukraine dated March 15, 2016 № 96.* Retrieved from: http://www.president.gov.ua/documents/962016-19836 [in Ukrainian].
13. *Stratehiia natsionalnoi bezpeky Ukrainy: zatverdzhena Ukazom Prezydenta Ukrainy vid 26 trav. 2015 r. № 287 [Strategy of National Security of Ukraine: approved by Decree of the President of Ukraine from May 26. 2015 p. № 287].* Retrieved from: http://zakon2.rada.gov.ua/laws/show/287/2015 [in Ukrainian].
14. Furashev, V.M. (2012). Kiberprostir ta informatsiinyi prostir, kiberbezpeka ta informatsiina bezpeka: sutnist, vyznachennia, vidminnosti [Cyberspace and information space, cybersecurity and information security: essence, definition, differences]. *Informatsiia i pravo, 2,* 162-169 [in Ukrainian].
15. Shelomentsev, V.P. (2012). Pravove zabezpechennia systemy kibernetychnoi bezpeky Ukrainy ta osnovni napriamy yii udoskonalennia [Legal support of the system of cybernetic security of Ukraine and the main directions of its improvement]. *Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka), 1,* 312-320 [in Ukrainian].

Кубанов Євген Васильович
Аспірант
Міжрегіональної академії управління персоналом
03039, м. Київ, вул. Фрометівська, 2

Kubanov Yevhen
Postgraduate student
Interregional Academy of Personnel Management
2, Frometivska St., 03039, Kyiv, Ukraine

Email: balashov.kiev@gmail.com

Цитированння: Кубанов Є. В. Теоретичні підходи до понятійно-категоріального апарату кібербезпеки в системі публічного управління / Є. В. Кубанов // Аспекти публічного управління. – 2018. – Т. 6. – № 8. – С. 49-55.

Citation: Kubanov, Y. V. (2018). Teoretychni pidkhody do poniatiino-katehorialnoho aparatu kiberbezpeky v systemi publichnoho upravlinnia [Theoretical approaches to the conceptual-categorical apparatus of cybersecurity in the system of public administration]. *Public administration aspects, 6 (8),* 49-55.

Стаття надійшла / Article arrived: 09.07.2018 Схвалено до друку / Accepted: 24.08.2018