УДК 004.056.5:351
DOI: https://doi.org/10.26642/jen-2021-3(97)-36-40

К.Х. Герасимюк, к.держ.упр., доц.
Комунальний заклад вищої освіти
«Вінницька академія безперервної освіти»

Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення

Нагальна необхідність формування системи кібер- та інформаційної безпеки зумовлена насамперед проблемою гібридних воєн, світовою пандемією, міжнародними та регіональними коливаннями економіки тощо, адже це несе цілу низку загроз державам, бізнесу, суспільству в цілому та кожному громадянину зокрема. В умовах же тотальної діджиталізації управління проблема ризиків розповсюдження і захисту інформації стає надзвичайно актуальною для органів публічної влади всіх рівнів. Саме тому держава потребує вироблення дієвих механізмів державного управління в цій сфері, й насамперед механізмів кібер- та інформаційної безпеки. Значний всебічний розгляд науковцями кібербезпеки та інформаційної безпеки свідчить про нагальність та актуальність цієї проблеми, проте малодослідженими залишаються питання механізмів державного управління цією сферою та, в цьому контексті, підготовки фахівців публічного управління та адміністрування, здатних адекватно протидіяти зазначеним загрозам. Аналіз нормативно-правової бази та наукових досліджень дав можливість визначити: два ключові напрями розвитку кіберзахисту; проблемні питання правового та організаційного механізму державного управління інформаційною та кібербезпекою; сучасні підходи до формування політики підготовки та підвищення кваліфікації фахівців ІТ-сфери й публічного управління та адміністрування тощо. Зазначено, що сьогодні виникає необхідність більш ретельного підходу до забезпечення органів публічної влади технічним обладнанням, програмним забезпеченням, до підготовки / перепідготовки кадрів, які б не лише бути впевненими користувачами цих програм, а і розуміли свою відповідальність за безпеку в цій сфері. Крім того, всі зазначені вище заходи кіберзахисту в сфері публічного управління мають набути системного характеру.

Ключові слова: *інформаційна безпека; кібербезпека; механізми державного управління кібербезпекою та інформаційною безпекою; інформаційні системи органів публічного управління.*

Актуальність теми. Перехід практично всіх сфер діяльності людства у віртуальний простір спонукає до необхідності напрацьовувати все нові й нові системи кібер- та інформаційної безпеки. Сьогодні ж, в умовах гібридних воєн, світової пандемії, міжнародних та регіональних коливань економіки тощо, це питання особливо актуальне, адже несе цілу низку загроз державам, бізнесу, суспільству в цілому та кожному громадянину зокрема. Органів публічної влади зазначена проблема стосується насамперед ризиками розповсюдження і захисту інформації. А саме: тотальна діджиталізація інформації, її обіг, зберігання, загрози неналежного використання та зміни / пошкодження, зовнішнього несанкціонованого втручання та використання на шкоду як державі, так і кожному громадянину. Саме тому держава потребує вироблення дієвих механізмів державного управління в цій сфері, й насамперед механізмів кібер- та інформаційної безпеки.

Аналіз останніх досліджень та публікацій, на які спирається автор. Проблеми інформаційної та кібербезпеки останнім часом стають предметом дослідження науковців різних галузей. Зокрема, А.О. Азарова, Л.М. Ткачук, Л.О. Нікіфорова, А.А. Шиян, О.М. Хошаба розглядають публічне управління та адміністрування в контексті захисту інформаційного простору [1, с. 149–156]. Присяжнюк М.М. та Цифра Є.І. аналізують передумови виникнення понять «кіберпростору», «кібербезпеки», «кіберзагроз», дають порівняльний аналіз стратегій кібербезпек провідних країн світу тощо [12]. Кібербезпеку як важливу складову системи захисту національної безпеки, правові та організаційні засади кібербезпеки в ЄС досліджує А.В. Войціховський [2]. З точки зору економіки проводить аналіз вихідних даних для формування політики інформаційної безпеки на підприємстві І.Ю. Маковський [7, с. 38–43].

Трофименко О., Прокоп Ю., Логінова Н., Задерейко О. визначають політичні, науково-технічні, організаційні та просвітницькі питання, вирішення яких є необхідним у межах комплексної протидії кіберзагрозам задля випереджального реагування на динамічні змінення, що відбуваються у кіберпросторі України [16]. Значний доробок стосовно кібербезпеки з точки зору захисту комп'ютерних систем напрацьовано О.Трофименко (медичних комп'ютерних систем) [15]; О.В. Потій, А.І. Семенченко, Д.В. Дубовим, О.О. Бакалинським, Д.В. Мялковським (організаційно-технічна модель кіберзахисту України) [9] та іншими. Крім зазначених вище досліджень, варто також звернути увагу і на доробки дослідників щодо інформаційної безпеки держави (див., наприклад, Г.Почепцов [10]).

Значний всебічний розгляд кібербезпеки та інформаційної безпеки свідчить про нагальність та актуальність цієї проблеми, проте малодослідженими залишаються питання механізмів державного управління цією сферою та, в цьому контексті, підготовки фахівців публічного управління та адміністрування, здатних адекватно протидіяти зазначеним загрозам.

Мета статті – на основі аналізу результатів загальнотеоретичних та галузевих досліджень сучасного стану формування та задіяння механізмів державного управління кібер- та інформаційної безпеки виявити існуючі проблеми в цій сфері та запропонувати напрями їх вирішення.

Викладення основного матеріалу. На сучасному етапі функціонування органів публічного управління актуалізується питання інформаційної та кібербезпеки через значну інформатизацію надання всіх видів послуг громадянам на різних рівнях державної влади та місцевого самоврядування (наприклад, від документообігу, реєстрації речових прав до видачі ID-паспортів усім громадянам країни, зберігання такої інформації, неможливість її зміни / використання без відповідного дозволу, якісного вітчизняного програмного забезпечення тощо).

Крім того, глобальні виклики зміни клімату та інновації в міжнародній економіці та фінансовій сфері (той же біткоїн), які, здавалося б, не зовсім стосуються електронного урядування та тотальної діджиталізації всієї сфери публічного управління, сьогодні можуть банально внести небажані корективи простим відключенням електроенергії на тривалий час як в окремо взятій громаді, так і в цілому регіоні. Тим самим паралізувавши на певний час роботу не лише органів влади, а і порушивши права громадян щодо їх майнового стану, визнання особи тощо.

Вітчизняні проблеми в цій сфері на сучасному етапі є і в нормативно-правовому забезпеченні. Так, наприклад, в 2021 році чинним є Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [14]. І деякі його положення ще досить актуальні щодо: відсутності координації зусиль державного і приватного секторів економіки з метою ефективного використання наявних ресурсів; ефективності використання фінансових, матеріальних, кадрових ресурсів, спрямованих на інформатизацію, впровадження ІКТ у соціально-економічну сферу; недостатності розвитку нормативно-правової бази інформаційної сфери; незначної частки в Інтернет-просторі україномовних інформаційних ресурсів; нерівномірності забезпечення можливості доступу населення до комп'ютерних і телекомунікаційних засобів; невирішення у повному обсязі питання захисту авторських прав на програмне забезпечення тощо.

Звичайно певний розвиток та напрацювання нормативної бази можна простежити в Законі України «Про основні засади забезпечення кібербезпеки України» [13], який є логічним втіленням у вітчизняну нормативну базу Конвенції про кіберзлочинність (ратифікована у 2005 році) [6]. Так в зазначеному Законі законодавець вже подає визначення термінів «кібербезпека», «кіберзахист», «кіберпростір». Саме кібербезпека та кіберзахист, згідно з цим Законом, покликані забезпечити захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору. А для цього має бути розроблено та впроваджено сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем [13]. Тобто, умовно кіберзахист держави можна поділити на два ключові напрями:

1) організаційно-правові заходи;

2) ІТ-заходи.

Власне, й науковці, а саме: О.В. Потій, А.І. Семенченко та інші, подають кіберзахист як структуровану систему з трьох інфраструктур кіберзахисту: організаційно-керуючу інфраструктуру (сукупність суб'єктів забезпечення кібербезпеки, що формують та/або реалізують державну політику у сфері кібербезпеки); технологічну інфраструктуру кіберзахисту (сили та засоби кіберзахисту); інфраструктуру, що забезпечує функціонування сил кіберзахисту, інформаційно-комунікаційних мереж та їх ресурсів тощо [9]. Таким чином, дослідники також схиляються до поділу кіберзахисту на ці два напрями, проте акцентують увагу саме на технічних аспектах.

У Стратегії реформування державного управління України до 2025 року від 21.07.2021 року [3] визначено мету – побудова в Україні спроможної сервісної та цифрової держави, яка забезпечує захист інтересів громадян на основі європейських стандартів та досвіду. Згідно зі Стратегією, державна служба має бути професійною, доброчесною, політично нейтральною, базуватися на заслугах, бути орієнтованою на громадян. Для цього передбачається здійснити низку заходів, в тому числі й навчання та підвищення кваліфікації фахівців публічного управління та адміністрування, адже сучасна система не забезпечує своєчасне навчання щодо майбутніх пріоритетів розвитку державного управління. [3]. Крім цього, Стратегія передбачає подальшу цифровізацію адміністративних послуг із забезпеченням розвитку дієвої електронної інфраструктури, що слугуватиме фундаментом для збільшення кількості адміністративних послуг, що надаються з використанням інформаційних технологій.

Таким чином, Стратегія визначає чіткий вектор цифровізації послуг та підвищення кваліфікації посадовців місцевого самоврядування та державних службовців і в цьому контексті також, прямо зазначаючи, що зміст професійного навчання державних службовців та посадових осіб місцевого самоврядування не повною мірою відповідає потребам у такому навчанні [3].

Варто зазначити, що й питання ІТ-освіти сьогодні є нагальною для нашої держави. Так Міністерство освіти та науки України спільно з Міністерством цифрової трансформації продовжують процес розробки концепції трансформації ІТ-освіти в Україні [8]. Проте акцент у зазначеній концепції робиться саме на потребах ринку ІТ-індустрії в приватній сфері (див. [5]) та на підвищенні професійного рівня таких фахівців, і, що особливо заслуговує уваги, профорієнтаційна робота в цьому напрямі вже на рівні закладів загальної середньої освіти.

Робота Уряду щодо впровадження ІТ-заходів проводиться і в процесі створення в регіонах Центрів Індустрії 4.0 на базі індустріальних і наукових парків та університетів. Основне завдання цих Центрів – координація процесу впровадження та розроблення перспективних технологій, підготовка відповідних спеціалістів, формування зв'язків між бізнесом, який розробляє сучасні технології, та виробничими підприємствами [11].

Тобто, ми можемо зауважити, що визначені два вектори кіберзахисту мають цілу низку напрацювань на рівні держави та вітчизняних науковців, але вони не набрали ще системного характеру їх поєднання саме в публічному управлінні. Ми вважаємо, що в сфері публічного управління ці два вектори мають бути систематизовані, підсилені механізмами державного управління не лише стосовно захисту інформації технічно та створенням низки управлінських структур державного та регіонального рівня цією галуззю, але й підготовкою кваліфікованого фахівця, здатного не лише технічно захищати та розповсюджувати інформацію (так званого айтішника), але і розуміти важливість та наслідки розповсюдження недостовірної, пропагандистської інформації, уміти її аналізувати та нівелювати негативні наслідки для держави та громадянина від неї тощо.

Сьогодні в Україні (та й у світі) накопичилася ціла низка кібер- та інформаційних загроз і викликів. Адже значною загрозою безпеці держави є і тотальне використання невітчизняного програмного забезпечення та сервісного зберігання інформації щодо всіх сфер діяльності органів публічної влади. До цього часу немає на 100 % нормативно урегульованих конкретних стандартів і вимог до інформаційних систем державних органів влади та місцевого самоврядування. А це означає, що сьогодні значна частина цих органів послуговуються програмним продуктом досить сумнівного походження (в тому числі і з країни-агресора, і з приватних міжнародних структур). Наприклад, з настанням пандемії всі структури публічного та приватного секторів, звичайні громадяни вимушені були для дистанційної роботи / навчання використовувати платформу Zoom, яка при завантаженні апріорі має доступ до налаштувань гаджета користувача, а отже і до всієї інформації на ньому з можливістю її подальшого відстеження. Отже, сьогодні досить умовно можна говорити про відповідальність державного службовця та посадовця місцевого самоврядування, та, зрештою, навіть лікаря, про дотримання службової таємниці. Крім того, на законодавчому рівні ці питання також до кінця не врегульовані.

В цих умовах виникає необхідність більш ретельного підходу не лише до забезпечення органів публічної влади технічним обладнанням, програмним забезпеченням, а і підготовки / перепідготовки кадрів, які б не лише були впевненими користувачами цих програм, а і розуміли свою відповідальність за безпеку в цій сфері. Звичайно, сьогодні в державі робляться певні кроки до виправлення ситуації. Так Міністерство юстиції України повідомило, що Мінцифри запустило Цифрограм для держслужбовців (безкоштовний національний тест, який дає можливість перевірити свою цифрову грамотність. Він розроблений на основі європейської концептуально-еталонної Рамки цифрових компетентностей для громадян ЄС (DigComp 2.1). Цей варіант тестування містить 90 запитань та оцінює 30 цифрових компетентностей, необхідних для роботи сучасного держслужбовця) [4].

Проте, як ми вже зазначали, ці кроки не набули системного характеру. А починатися ця система має, на нашу думку, з підготовки висококваліфікованих спеціалістів для роботи в органах публічної влади з особливими компетентностями щодо поєднання роботи ІТ зі сферою публічного управління та адміністрування й державної безпеки. Сьогодні можливість підготовки таких спеціалістів може бути реалізована на базах політехнічних університетів, до яких приєднані регіональні інститути державного управління. На їх базі можна розробити та запровадити нові освітньо-професійні програми на кшталт «Інформаційна / кібербезпека публічного управління та адміністрування» як для бакалаврів, так і для магістрів. Адже об'єднання цих закладів дає надзвичайні можливості для реалізації таких програм вже сьогодні – це і наявність матеріальної бази, і висококваліфікованих спеціалістів обох сфер. На нашу думку, такі фахівці будуть надзвичайно затребувані та конкурентоздатні на ринку праці. А необхідність їх в державному секторі мала б підтверджуватися державним замовленням.

Крім того, НАДС разом з Мінцифри та Міністерством освіти і науки України могли б також розробити Концепцію трансформації підготовки кадрів з публічного управління та адміністрування. Врахувавши в ній профорієнтаційну роботу на рівні закладів загальної середньої освіти, адже навіть цьогорічний набір

на освітні програми спеціальності 281 Публічне управління та адміністрування за освітнім рівнем «бакалавр» демонструє небажання (чи нерозуміння?) молоді обирати цю спеціальність. Так значна кількість абітурієнтів, які й подали заявки, проте не надавали перший пріоритет цій спеціальності (див., наприклад, https://vstup.osvita.ua/). А це вже загроза не лише перспективі розвитку державного управління та місцевого самоврядування, а й держави в цілому.

Висновки та перспективи подальших досліджень. Розглянувши та проаналізувавши нормативно-правову базу, доробки дослідників, було визначено, що кібербезпека держави забезпечується за двома ключовими напрямами: організаційно-правовими та ІТ-заходами. На сучасному етапі активно йде напрацювання щодо формування нормативної бази, хоча є ціла низка недоліків – від застарілих правових актів до неунормованості ключових потреб публічного управління в цій галузі (наприклад, регламентування відповідальності посадових осіб за несанкційне розповсюдження / пошкодження / розголошення службової таємниці через незахищені інформаційні системи тощо). ІТ-заходи все ще не вирішують проблеми якісного програмного забезпечення органів публічної влади. Організаційні заходи поки що обмежуються створенням низки владних структур, але залучення висококваліфікованих фахівців до роботи в них все ще потребує удосконалення. Значної роботи потребує розробка заходів стосовно інформаційної безпеки в умовах кібервоєн (від втручання у вибори до розповсюдження регіональних фейкових новин).

Тобто, можемо констатувати, що на сучасному етапі всі зазначені вище заходи кіберзахисту в сфері публічного управління не набули системного характеру, немає напрацьованих дієвих механізмів державного управління цією сферою. Тотальна ж інформатизація суспільства ставить перед державою глобальні завдання подолання загроз, які вона несе з собою. І від їх вирішення сьогодні залежить не лише розвиток, а і в цілому існування держави як незалежної та конкурентоздатної. І саме професіонали можуть протистояти цим загрозам. Саме тому ми пропонуємо внести в систему механізмів державного управління інформаційною та кібербезпекою ключову ланку – підготовку кваліфікованих фахівців публічного управління, здатних забезпечувати кіберзахист як технічно, так і з точки зору інформаційної (і як результат – соціальної, воєнної, екологічної тощо) безпеки.

Подальші дослідження цієї теми можуть відбуватися в бік конкретизації кожного з векторів механізмів державного управління інформаційною та кібербезпекою на різних рівнях управління, їх взаємозв'язків та взаємовпливів.

Список використаної літератури:

1. Публічне управління та адміністрування в контексті захисту його інформаційного простору / *А.О. Азарова, Л.М. Ткачук, Л.О. Нікіфорова та ін.* // Вісник ЖДТУ. Серія : Економіка, управління та адміністрування. – Житомир. – 2019. – № 2 (88). – С. 149–156.
2. *Войціховський А.В.* Кібербезпека як важлива складова системи захисту національної безпеки європейських країн / *А.В. Войціховський* // Журнал східноєвропейського права. – 2018. – № 53 [Електронний ресурс]. – Режим доступу : https://cutt.ly/gWy5Jck.
3. Деякі питання реформування державного управління України : Розпорядження Кабінету Міністрів України від 21 липня 2021 р. № 831-р. [Електронний ресурс]. – Режим доступу : https://www.kmu.gov.ua/npas/deyaki-pitannya-reformuvannya-derzhavnogo-upravlinnya-t210721.
4. Для держслужбовців запустили Цифроґрам [Електронний ресурс]. – Режим доступу : https://sud.ua/ru/news/ukraine/203598-dlya-derzhsluzhbovtsiv-zapustili-tsifrogram?fbclid=IwAR3AJISmR6qPYsQRg2OOShMq3IktsmrHJYXk7Bil_3SI_smaS5q16jp_N_A.
5. Експрес-аналіз поточного стану ІТ-освіти в Україні [Електронний ресурс]. – Режим доступу : https://cutt.ly/jWu79GO.
6. Конвенція про кіберзлочинність : Документ 994_575, ратифікація від 07.09.2005 р., підстава – 2824-15 [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/994_575#Text.
7. *Маковський І.Ю.* Аналіз вихідних даних для формування політики інформаційної безпеки на підприємстві / *І.Ю. Маковський* // Економіка, управління та адміністрування. – Житомир : Державний університет «Житомирська політехніка». – 2020. – № 1 (91).– С. 38–43.
8. Оприлюднено результати експрес-аудиту щодо ІТ-освіти в Україні [Електронний ресурс]. – Режим доступу : https://mon.gov.ua/ua/news/oprilyudneno-rezultati-ekspres-auditu-shodo-it-osviti-v-ukrayini?fbclid=IwAR0RvlRI8tiTW5xZS326Q6uXDBKyoHH0pAHOHHiILKbFVL7aO_dMPgTkXKQ.
9. Концептуальні засади впровадження організаційно-технічної моделі кіберзахисту України / *О.В. Потій, А.І. Семенченко, Д.В. Дубов та ін.* // Захист інформації. – 2021. – Т. 23, № 1 [Електронний ресурс]. – Режим доступу : https://jrnl.nau.edu.ua/index.php/ZI/article/view/15434.
10. *Почепцов Г.* Сучасні інформаційні війни / *Г.Почепцов.* – К. : Києво-Могилян. акад., 2015. – 496 с.
11. Прем'єр-міністр: Розпочинаємо створення в регіонах Центрів Індустрії 4.0 [Електронний ресурс]. – Режим доступу : https://www.kmu.gov.ua/news/premyer-ministr-rozpochinayemo-stvorennya-v-regionah-centriv-industriyi-40.
12. *Присяжнюк М.М.* Особливості забезпечення кібербезпеки / *М.М. Присяжнюк, Є.І. Цифра* // Реєстрація, зберігання і обробка даних. – 2017. – Т. 19, № 2. – С. 61–68 [Електронний ресурс]. – Режим доступу : http://dspace.nbuv.gov.ua/bitstream/handle/123456789/131678/06-Prysiazhniuk.pdf.

13. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VII [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19?find=1&text=%D0%BD%D0%B0%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD#w1_26
14. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 9 січня 2007 року № 537-V [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/537-16#Text.
15. *Трофименко О*. Питання кібербезпеки медичних комп'ютерних систем / *О.Трофименко* // Захист інформації. – 2021. – Т. 23, № 1. DOI: 10.18372/2410-7840.23.15153.
16. Кібербезпека України: аналіз сучасного стану / *О.Трофименко, Ю.Прокоп, Н.Логінова, О.Задерейко* // Захист інформації. – 2019. – Т. 21, № 3. – С. 150–157 [Електронний ресурс]. – Режим доступу : https://jrnl.nau.edu.ua/index.php/ZI/article/view/13951.

References:

1. Azarova, A.O., Tkachuk, L.M. and Nikiforova, L.O. etc. (2019), «Publichne upravlinnja ta administruvannja v konteksti zahystu jogo informacijnogo prostoru», *Visnyk ZhDTU*, Serija *Ekonomika, upravlinnja ta administruvannja*, Zhytomyr, No. 2 (88), pp. 149–156.
2. Vojcihovs'kyj, A.V. (2018), «Kiberbezpeka jak vazhlyva skladova systemy zahystu nacional'noi' bezpeky jevropejs'kyh krai'n», *Zhurnal shidnojevropejs'kogo prava*, No. 53, [Online], available at: https://cutt.ly/gWy5Jck
3. KMU (2021), «Dejaki pytannja reformuvannja derzhavnogo upravlinnja Ukrai'ny», *Rozporjadzhennja vid 21 lypnja 2021 r.*, No. 831-r., [Online], available at: https://www.kmu.gov.ua/npas/deyaki-pitannya-reformuvannya-derzhavnogo-upravlinnya-t210721
4. «Dlja derzhsluzhbovciv zapustyly Cyfrogram», *Sudebno-yuridicheskaya gazeta v Ukraine*, [Online], available at: https://sud.ua/ru/news/ukraine/203598-dlya-derzhsluzhbovtsiv-zapustili-tsifrogram?fbclid=IwAR3AJISmR6qPYsQRg2OOShMq3IktsmrHJYXk7Bil_3SI_smaS5q16jp_N_A
5. «Ekspres-analiz potochnogo stanu IT-osvity v Ukrai'ni», [Online], available at: https://cutt.ly/jWu79GO
6. VRU (2005), «Konvencija pro kiberzlochynnist'», Dokument 994_575, ratyfikacija vid 07.09.2005 r., pidstava – 2824-IV, [Online], available at: https://zakon.rada.gov.ua/laws/show/994_575#Text
7. Makovs'kyj, I.Ju. (2020), «Analiz vyhidnyh danyh dlja formuvannja polityky informacijnoi' bezpeky na pidpryjemstvi», *Ekonomika, upravlinnja ta administruvannja*, Derzhavnyj universytet «Zhytomyrs'ka politehnika», Zhytomyr, No. 1 (91), pp. 38–43.
8. Ministerstvo osvity ta nauky Ukrai'ny (2021), «Opryljudneno rezul'taty ekspres-audytu shhodo IT-osvity v Ukrai'ni», [Online], available at: https://mon.gov.ua/ua/news/oprilyudneno-rezultati-ekspres-auditu-shodo-it-osviti-v-ukrayini?fbclid=IwAR0RvlRI8tiTW5xZS326Q6uXDBKyoHH0pAHOHHiILKbFVL7aO_dMPgTkXKQ
9. Potij, O.V., Semenchenko, A.I., Dubov, D.V. etc. (2021), «Konceptual'ni zasady vprovadzhennja organizacijno-tehnichnoi' modeli kiberzahystu Ukrai'ny», *Zahyst informacii'*, Vol. 23, No. 1, [Online], available at: https://jrnl.nau.edu.ua/index.php/ZI/article/view/15434
10. Pochepcov, G. (2015), *Suchasni informacijni vijny*, Kyjevo-Mogyljan. akad., Kyi'v, 496 p.
11. KMU, «Prem'jer-ministr: Rozpochynajemo stvorennja v regionah Centriv Industrii' 4.0.», [Online], available at: https://www.kmu.gov.ua/news/premyer-ministr-rozpochinayemo-stvorennya-v-regionah-centriv-industriyi-40
12. Prysjazhnjuk, M.M. and Cyfra, Je.I. (2017), «Osoblyvosti zabezpechennja kiberbezpeky», *Rejestracija, zberigannja i obrobka danyh*, Vol. 19, No. 2, pp. 61–68, [Online], available at: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/131678/06-Prysiazhniuk.pdf
13. VRU (2017), «Pro osnovni zasady zabezpechennja kiberbezpeky Ukrai'ny», *Zakon Ukrai'ny* vid *5 zhovtnja 2017 roku*, No. 2163-VII, [Online], available at: https://zakon.rada.gov.ua/laws/show/2163-19?find=1&text=%D0%BD%D0%B0%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD#w1_26
14. VRU (2007), «Pro Osnovni zasady rozvytku informacijnogo suspil'stva v Ukrai'ni na 2007-2015 roky», *Zakon Ukrai'ny* vid 9 sichnja 2007 roku No. 537-V, [Online], available at: https://zakon.rada.gov.ua/laws/show/537-16#Text
15. Trofymenko, O. (2021), «Pytannja kiberbezpeky medychnyh komp'juternyh system», *Zahyst informacii'*, Vol. 23, No. 1, doi: 10.18372/2410-7840.23.15153.
16. Trofymenko, O., Prokop, Ju., Loginova, N. and Zaderejko, O. (2019), «Kiberbezpeka Ukrai'ny: analiz suchasnogo stanu», *Zahyst informacii'*, Vol. 21, No. 3, pp. 150–157, [Online], available at: https://jrnl.nau.edu.ua/index.php/ZI/article/view/13951

Герасимюк Костянтин Харитонович – кандидат наук з державного управління, доцент, доцент кафедри управління та адміністрування Комунального закладу вищої освіти «Вінницька академія безперервної освіти».

https://orcid.org/0000-0002-5189-8418.

Наукові інтереси:

– децентралізація влади;
– формування та розвиток механізмів державного (публічного) управління;
– адміністративно-територіальний устрій;
– державна служба, формування компетентностей у посадовців публічного управління.

E-mail: kgerasymyuk@ukr.net.

Стаття надійшла до редакції 21.06.2021.