УДК 342.951:004.056](477-651.2)(045)
DOI https://doi.org/10.32782/2524-0374/2023-1/63

СУЧАСНІ ВИКЛИКИ АДМІНІСТРАТИВНО-ПРАВОВИХ ЗАСАД КІБЕРБЕЗПЕКИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

MODERN CHALLENGES OF ADMINISTRATIVE AND LEGAL FOUNDATIONS CYBER SECURITY OF UKRAINE UNDER MARTIAL LAW

Горінов П.В., к.ю.н.,
в.о. директора
Навчально-науковий інститут права,
доцент кафедри правознавства та галузевих юридичних дисциплін
Український державний університет імені Михайла Драгоманова

Драпушко Р.Г., к.ф.н.,
проректор з науково-педагогічної роботи,
доцент кафедри соціальної філософії, філософії освіти та освітньої політики
Український державний університет імені Михайла Драгоманова

Метою даної статті є зосередження уваги на актуальних проблемах, що існують в національному правовому регулюванні кіберпростору, особливостях адміністративно-правової охорони в сфері кібербезпеки в умовах воєнного стану, а також окреслити шляхи ефективного подальшого адміністративно-правового забезпечення кібербезпеки. У цьому сенсі констатуємо, що регулювання об'єктів і явищ кіберпростору на національному рівні є досить слабким і недостатнім у порівнянні з іншими країнами, тому доцільним є аналіз нормативно-правових практик, що ефективно функціонують у розвинених демократичних державах, з метою адаптації їх до реалій правової системи України. Методологічним підґрунтям слугувало використання низки методів: логічний метод використовувався для формулювання понять «адміністративно-правова охорона», «кіберпростір», «кібербезпека»; нормативний-догматичний застосовувався для вивчення змісту нормативних актів, що регулюють дану галузь; монографічний метод використаний при вивченні праць зарубіжних і українських науковців; системно-структурний дозволив досліджувати сучасний стан і перспективи вдосконалення адміністративно-правових основ кібербезпеки України; метод узагальнення застосовувався для формулювання висновків. Повномасштабне розгортання гібридної війни з боку росії чинить серйозний вплив на всі аспекти суспільного життя. Значною мірою саме від ефективної оперативності та якості правового реагування залежить стратегічний успіх протидії викликам гібридної війни. Підкреслено, що національна безпека держави значною мірою залежить від стану забезпечення кібербезпеки. Обґрунтовано, що гібридна війна значно посилює вплив кіберзагроз на українське суспільство та актуалізує небезпеку від цілеспрямованих кібератак як інструменту агресії проти нашої держави на фоні глобальних тенденцій щодо загроз у кіберпросторі. У процесі проведення дослідження нами сформульовано висновки, в яких особливу увагу приділено особливостям сучасного стану функціонування законодавства про кібербезпеку та розглядаються перспективні напрямки подальшого його вдосконалення, що, в свою чергу, слугуватиме підґрунтям удосконалення адміністративно-правового врегулювання кібербезпеки України.

Ключові слова: інформаційна безпека, кібербезпека, кіберпростір, адміністративно-правові основи кібербезпеки, воєнний стан.

The purpose of this article is to focus on the current problems that exist in the National Legal Regulation of cyberspace, the specifics of administrative and legal protection in the field of cybersecurity under martial law, as well as to outline ways to effectively further administrative and legal support for cybersecurity. In this sense, it is obvious that the regulation of objects and phenomena of Cyberspace at the national level is rather weak and insufficient in comparison with other countries, so it is advisable to analyze regulatory practices that effectively function in developed democratic states in order to adapt them to the realities of the legal system of Ukraine. The methodological basis was the use of a number of methods: the logical method was used to formulate the concepts of «administrative and legal protection», «cyberspace», «cybersecurity»; the normative-dogmatic method was used to study the content of normative acts regulating this industry; the monographic method was used in the study of the works of foreign and domestic scientists; the system-structural method allowed us to study the current state and prospects for improving the administrative and legal foundations of cybersecurity in Ukraine; the generalization method was used to formulate conclusions. The full-scale deployment of hybrid warfare by russia has a serious impact on all aspects of public life. To a large extent, the strategic success of countering the challenges of hybrid warfare depends on the effective efficiency and quality of legal response. It is emphasized that the state's national security largely depends on the state of cyber security. It is substantiated that the hybrid war significantly increases the impact of cyber threats on Ukrainian society and actualizes the danger from targeted cyber attacks as a tool of aggression against our state against the background of global trends regarding threats in cyberspace. In the course of the research, we formulated conclusions in which special attention is paid to the peculiarities of the current state of functioning of the cybersecurity legislation and consider promising directions for its further improvement, which in turn will serve as the basis for improving the administrative and legal regulation of cybersecurity in Ukraine.

Key words: information security, cybersecurity, cyberspace, administrative and legal foundations of cybersecurity, martial law.

Актуальність теми обумовлюється масштабами інформаційної війни, яку здійснює росія проти України та зростаючою роллю захисту кіберпростору України в війському контексті. Сьогодні, особливо в контексті військових дій, можна стверджувати, що «кіберпростір – це новий канал для створення та поширення різноманітної інформації, який став новим двигуном зростання економіки, новою платформою соціального управління, новим способом міжнародного співробітництва, до того ж і зовсім новою сферою державного суверенітету». Однак кіберпростір надає нам не тільки ресурси, можливості, але і містить загрози. Посилена цифровізація та зв'язок збільшують ризики кібербезпеки, тим самим роблячи суспільство загалом більш вразливим до кіберзагроз, посилюючи небезпеку, з якою стикаються люди, включаючи вразливих осіб, таких як діти [1].

Відзначаємо, що сьогоднішній день сектор високих технологій є однією з найбільш важливих і швидко мінливих сфер суспільного життя. Глобальний сектор високих технологій, крім іншого, акумулює значний обсяг фінансових, монетарних та інших ресурсів. Також визнається, що він має значний вплив практично на всі сфери розвитку як державного, так і приватного секторів. Яскравим прикладом, що підтверджує цю тезу є той факт, що високі технології дуже швидко і безповоротно змінили навколишній світ, тим самим вплинувши на навколишнє суспільство, в тому числі через кіберпростір.

Після ухвалення 20 грудня 2002 року Генеральною асамблеєю ООН резолюції 57/239 «Елементи для створення глобальної культури кібербезпеки» зазначений термін почав активно використовуватись в українській право-

вій термінології. Складніше було з імплементацією змісту резолюції. Зокрема, Генеральна асамблея ООН констатувала, що стрімкий розвиток інформаційної технології означає зміну підходів державних органів, організацій та індивідуальних користувачів до питання кібербезпеки [2, с. 104].

На думку окремих дослідників, – розвиток ІТ-законодавства в Україні, що регулює всі відносини всередині і навколо сектора високих технологій, ще не досягнув високої ефективності його функціонування в такому масштабі, як у розвинених західних країнах і деяких країнах Азії. У той час як правове регулювання сектора високих технологій у розвинених країнах допомагає як приватним особам, так і державі отримувати значні прибутки та пільги, Україна все ще страждає від слабкого правового регулювання цих процесів. Сучасна система забезпечення інформаційної безпеки та кібербезпеки в Україні повинна бути єдиною ефективною системою, що складається з таких обов'язкових компонентів, як юридичний, освітній і технічний [3, с. 34]. Усе вищевикладене свідчить про науковий та практичний інтерес до тематики правового врегулювання кібербезпеки в Україні, так і в світі, особливо в контексті використання кіберпростору в військових цілях. В умовах гібридизації кіберзагроз, їх зовнішній характер вказує на актуальність та гостру необхідність у розробці засобів захисту та моніторингу кіберцифрової безпеки. Світові уряди спрямовують відповідні ресурси та засоби для захисту власних кіберцифрових та кіберфізичних систем.

Паралельно, слід відмітити, що дана сфера є публічною, а тому предметом нашої уваги буде адміністративно-правове регулювання кіберпростору в контексті воєнних дій. Саме тому, метою статті є вивчення адміністративно-правового врегулювання кібербезпеки України в умовах воєнного стану, аналіз чинних національних і міжнародних нормативно-правових актів, практик їхнього застосування та реалізації.

Для проведення дослідження було використано наступні методи: системний метод дозволив охарактеризувати існуючі межі адміністративно-правового регулювання кібербезпеки в їх взаємозв'язку з нормами інших правових інститутів, у тому числі міжнародного права. Структурний метод був корисний для дослідження кібербезпеки як структурованого явища і категорії. Дедукція допомогла дослідити взаємозв'язок між міжнародними змінами та їх впровадженням, проблеми забезпечення інформаційної безпеки та кібербезпеки в Україні.

Джерельна база дослідження. Науково-теоретичним підґрунтям слугували наукові розвідки українських і зарубіжних вчених, а саме: Бакалінської О.О., щодо правового забезпечення кіберзахисту в Україні [1], Казанчук І. та Яценко В., які розмежовують концепцію кібербезпеки від інформаційної безпеки. Автори стверджують, що ці два терміни не схожі; кібербезпека виходить за рамки традиційного поняття «інформаційна безпека», оскільки включає в себе не тільки захист інформації, але і її носіїв, а також права людини, суспільства та держави в цій області [3, с. 36]. Лісовська Ю.П. досліджує кібербезпеку як інноваційну систему віртуальності сучасного інформаційного простору [4, с. 2], аналізуючи дослідження Діордіца І. щодо поняття і змісту кіберзагроз на сучасному етапі [5], який доводить, що потреба реалізації ефективних заходів із протидії сучасним кібернетичним загрозам на національному рівні призводить до збільшення ролі в системах кібербезпеки країн спеціальних служб і правоохоронних органів, що мають контррозвідувальні функції й виконують завдання з протидії протиправній діяльності спецслужб іноземних держав і тероризму.

Розглядаючи законодавчі визначення цього поняття, Рижкова Є.А., формулює своє власне тлумачення адміністративно-правового врегулювання кібербезпеки. На її думку, це стан захисту життєво важливого інтересу для особистості, суспільства та держави, при якому збиток запобігається за допомогою негативного інформаційного впливу шляхом несанкціонованого створення, використання інформації, свідомо спрямованої з певною метою; неповної, несвоєчасної, недостовірної і необ'єктивної інформації; негативний вплив кібертехнологій; несанкціоновані порушення режимів доступу до інформації з її подальшим поширенням і використанням [6, с. 59].

Тарасюк А. підкреслює, що адміністративно-правове врегулювання кібербезпеки забезпечує інформаційну безпеку, яку слід трактувати як юридичне поняття. Це означає стан захисту національних інтересів у кіберпросторі, яким визначається сукупність збалансованого інтересу особистості, суспільства та держави [7, с. 171].

Відповідно до Закону України «Про основні засади кібербезпеки України» кібербезпека – це захист життєво важливих інтересів особистості і громадянина, суспільства і держави при використанні кіберпростору, який забезпечує сталий розвиток інформаційного суспільства та цифрового комунікаційного середовища, своєчасне виявлення, запобігання та нейтралізацію реальних та потенційних загроз до національної безпеки України в кіберпросторі [8].

Суттєвим кроком у розвитку кіберправа є прийняття 12 січня 2023 року Верховною Радою України у першому читанні законопроєкту щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, яким пропонується внести зміни до ряду законів України, що спрямовані на нормативне забезпечення захищеності від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, на створення належної правової основи для здійснення заходів з попередження, виявлення та припинення актів агресії у кіберпросторі в умовах війни російської федерації проти України, а також на загальне удосконалення нормативно-правової бази у сфері кібербезпеки та захисту інформації задля посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам.

Надзвичайно швидкий розвиток інформаційного суспільства вимагає ефективного регулювання державної політики в області боротьби з зазіханнями на кібербезпеку. Стрімкий розвиток технологій створює нові можливості у використанні інформаційного простору, але нові можливості тягнуть за собою нові загрози в цій галузі [9, с. 140].

Транскордонний характер кіберпростору, його залежність від складних інформаційних технологій, активне використання сайтів і сервісів кіберпростору всіма верствами населення виявляють нові можливості, але також викликають нові загрози, в тому числі: а) шкоду правам, інтересам і життю окремих осіб, організацій, державних установ; б) кібератаки на інформаційні ресурси з боку кіберзлочинців і кібертерористів; в) використання кіберзброї на війні та г) кібервійни, в тому числі ті, які супроводжують традиційну ворожнечу. Незважаючи на всі публічні заклики до мирного використання кіберпростору в інтересах всіх людей і націй, уряди тих же країн, які закликають до цього, активно включилися в гонку кіберзброєння, відтворюючи класичну «дилему безпеки» на якісно новій основі. Це означає, що на тлі складних і суперечливих глобальних процесів політичного, економічного і соціального розвитку кіберпростір стає простором холодної війни, тобто основою нового протистояння (переважно в кіберпросторі) ключових геополітичних акторів.

Ми погоджуємось із дослідниками, які вказують, що кіберпростір слід вважати «досить специфічним простором, в якому держави змушені в умовах часткового суверенітету формувати свої позиції та захищати національні інтереси. Цікаво, що на рівні міжнародного права та усталених традицій розуміння, поняття суверенітет наявний, хоча й обмежений, суверенітет над телекомунікаційною інфраструктурою є досить неоднозначним. Фактично

саме це і створює центральне тло глобального протиборства між державами за майбутнє кіберпростору [10, с. 40]. Відповідно ми не здивовані, що сьогодні, на думку відповідних посадових осіб, відбувається і «перша у світі кібервійна» [1], що ставить додаткові виклики перед Україною.

Під час війни Інтернет стає потужною зброєю, яка значно посилюється технологіями штучного інтелекту. Кіберзброя включає в себе широкий спектр технічних і програмних засобів, які часто спрямовані на використання вразливостей у системах передачі даних. Варто нагадати, що країни Північноатлантичного альянсу відносять кібератаки до основних сучасних гібридних загроз, а кіберпростір – це оперативна зона бойових дій на рівні з сушею, морем і повітрям.

Так, сьогодні фахівці фіксують зростання кількості кіберінцидентів і кібератак на державні інформаційні ресурси та об'єкти критичної інформаційної інфраструктури України.

Про це повідомили в Державній службі спеціального зв'язку та захисту інформації. За допомогою засобів системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було опрацьовано 24 млрд подій інформаційної безпеки. Зросла кількість зареєстрованих та опрацьованих кіберінцидентів – від 64 до 115 порівняно з попереднім кварталом. Основною метою хакерів є кібершпіонаж, порушення доступності державних інформаційних сервісів і знищення даних інформаційних систем. Фахівці Державного центру кіберзахисту зафіксували істотне зростання розповсюдження шкідливого програмного забезпечення, що дає можливість хакерам викрадати дані чи й взагалі знищувати їх. Кількість атак із високим рівнем критичності зросла у 3,8 раза, а кількість зареєстрованих кіберінцидентів із високим рівнем критичності – на 128%. Варто зазначити, що за ці місяці кількість критичних подій інформаційної безпеки, джерелом яких є IP-адреси росії, зросла у 35 разів, порівняно з першим та другим кварталами 2022 року [11].

Важливим досягненням у розвитку національної кібербезпеки в умовах війни слугувало проведення у грудні 2022 року засідання Національного Кластера Кібербезпеки, під час якого було проаналізовано ключові здобутки та прогалини у сфері кіберзахисту, обговорювалися подальші кроки, які дозволять посилити національну систему кібербезпеки й ефективніше протидіяти загрозам у кіберпросторі, розроблено Стратегію кібербезпеки на 2023 рік. Для посилення кадрового потенціалу затверджено перші шість професійних стандартів для нових професій у галузі кібербезпеки.

Також доцільно вказати, що система правового регулювання повинна бути всеосяжною і включати як фактичні засоби правового регулювання, які можуть чітко описувати зміст і сутність публічних правовідносин, що виникають у кіберпросторі, так і методи та засоби, що дозволяють суб'єктам правовідносин у цій сфері бути захищеними від різних незаконних посягань. Саме з цієї причини вчені відзначають, що таку модель системи правового регулювання кіберпростору має бути створено в Україні.

Ми погоджуємось, що «інформаційна війна в сучасному світі є цілком реальним фактором геополітики, який тривалий час недооцінювався політичною елітою України [12], а тому так важливо проводити інформаційну компанію щодо протидії дезінформації та підвищення рівня правової та інформаційної культури населення України.

Правова культура є первинною категорією і основою для формування інформаційної культури та протидії інформаційним викликам, порушенням в сучасних умовах. Відповідно найважливішим фактором формування високого рівня правової культури молоді є «правовий всеобуч», що можна здійснювати через мережу закладів освіти, громадських організацій, різноманітних волонтерських проєктів, професійних організацій, юридичних установ, центрів з прав людини, правоохоронних органів тощо.

Окремо слід розширити сферу діяльності Міністерства освіти і науки України, Міністерства культури та інформаційної політики України, Департаменту кіберполіції Національної поліції, судових органів щодо попередження вчинення злочинів серед неповнолітніх шляхом проведення профілактичної просвітницької роботи серед молоді [13], в тому числі і в сфері кібербезпеки. Слід зазначити, що велика частина українського суспільства нехтує закликами військових, зокрема Міністерства оборони України, яке чітко попереджає на своєму офіційному сайті і зазначає, що соціальні мережі дають адміністрації сайту можливість збирати інформацію про персональні дані без відома окремих осіб, оскільки неможливо відстежити збір відповідної інформації в таких системах. Розміщення фотографій на сторінці соціальної мережі зі зброєю або військовою технікою, надання інформації про місцезнаходження навіть одного солдата може призвести до втрати цілого підрозділу, але фотографії пересування військових частин Збройних Сил України публікувалися і, на жаль, продовжують публікуватися. Тому, на нашу думку, хоча і з дуже великою затримкою, як це повинно було бути зроблено в 2014 році, Україна прийняла закон № 2160-IX, який ввів кримінальну відповідальність за фото- і відеозйомку пересування українських військових.

Паралельно, слід відзначити, що Україна має потужну мережу фахівців в IT середовищі, які забезпечують захист її інтересів в інформаційному середовищі. «Українські кібервійська успішно атакують сервіси доставок, сервіси регіональних підрозділів державної влади росії. Усі вони закриті в російському контурі, але IT-армії України вдається їх пробивати. Про це в ефірі телемарафону повідомив керівник із розвитку електронних послуг Міністерства цифрової трансформації Мстислав Банік [14].

Поряд з тим, ми погоджуємось із заступником Секретаря РНБО України, що через наявні виклики пов'язані з війною в Україні є «потреба постійно збільшувати якісний кадровий потенціал держави у сфері кібербезпеки як у приватному, так й державному секторах». Запровадження професійних стандартів сприятиме суттєвому підвищенню якості освіти. У 2022 році за підтримки проєкту USAID «Кібербезпека критично важливої інфраструктури України» було розроблено перші шість професійних стандартів для таких професій: розробник систем захисту інформації, адміністратор мереж і систем, фахівець сфери захисту інформації, аналітик з безпеки інформаційно-телекомунікаційних систем, фахівець з питань безпеки та інструктор-методист з інформаційної безпеки та кібербезпеки. З-поміж найближчих планів – підготовка профстандартів для інших професій у сфері кібербезпеки, а також створення системи кваліфікаційних центрів, де фахівці зможуть підтверджувати відповідність своїх знань та навичок посадам, на які претендують або які обіймають.

Крім позитивної динаміки розвитку законодавства в області кібербезпеки, слід зазначити, що необхідно привести національне законодавство у відповідність з міжнародними стандартами. Ми поділяємо думку вчених, які стверджують, що необхідно вдосконалювати державне управління в секторі безпеки і оборони, включаючи системи кібербезпеки, захисту інформації та збереження інформаційних ресурсів; важливо зміцнювати можливості органів розвідки і контррозвідки шляхом створення організаційних, матеріально-технічних і фінансових умов для концентрації їх оперативних можливостей на пріоритетних напрямах оперативної і службової діяльності, зміцнення потенціалу суб'єктів кібербезпеки щодо ефективної боротьби з кіберзагрозами військового характеру, кібершпигунством, кібертероризмом і кіберзлочинністю,

зміцнення інституційних і технічних можливості таких організацій, поглиблення міжнародного співробітництва в цій області.

Висновки. Під час війни проблема забезпечення інформаційної безпеки стає питанням національної безпеки, а також кожного громадянина і суспільства в цілому, саме тому це стратегічна проблема держави, яка вимагає всеохоплюючої системи підтримки кібербезпеки й інформаційного суверенітету, налагоджувати стратегічну комунікацію суб'єктів національної системи кібербезпеки, нарощувати можливості протидії кіберзагрозам, формувати відповідну інфраструктуру українського інформаційного простору.

Завданням держави є створення стандартів і рекомендацій з кіберзахисту, завданням керівників установ – будувати захист за єдиним стандартом. Завдання громадян – виконувати рекомендації, які надають державні органи, тому так важливо набувати навички кібергігієни. Навички кібергігієни вкрай важливі для кожного у країні сьогодні: адже, захищаючи себе, кожен захищає країну.

Законодавець зобов'язаний проводити політику передбачення і негайного реагування на динамічні зміни, що відбуваються в кіберпросторі, розробляти і впроваджувати ефективні засоби та інструментарій можливого реагування на агресію в кіберпросторі, які можуть бути використані як засіб стримування військових конфліктів і загроз у кіберпросторі. В умовах глобалізації кіберзагроз доцільно уніфікувати підходи до адміністративно-правового регулювання у сфері кібербезпеки та стандартизувати заходи безпеки для ефективної співпраці, координації зусиль на національному та міжнародному рівнях.

Прагнення України до європейської інтеграції зобов'язують удосконалювати національне законодавство в галузі кібербезпеки з урахуванням умов Угоди про асоціацію між Україною, з одного боку, і ЄС і державами-членами, з іншого. Впровадження досвіду та передової практики країн ЄС, стандартів НАТО має бути пріоритетом. Слід зазначити, що проблему ефективної кібербезпеки буде вирішено тільки шляхом скоординованих дій на національному, регіональному та міжнародному рівнях, тому, на наш погляд, незаперечним фактом є те, що сьогодні закони повинні відповідати вимогам сучасного рівня розвитку технологій.

ЛІТЕРАТУРА

1. Бакалінська О.О. Правове забезпечення кіберзахисту в Україні. URL: https://coordynata.com.ua/pravove-zabezpecenna-kiberzahistu-v-ukraini
2. Доронін І.М. Правове регулювання забезпечення кібербезпеки у регюванні окремих фанкцій держави. *Інформація і право.* 2017. № 1 (20). С. 104–111.
3. Казанчук І. та Яценко В. Особливості правового регулювання діяльності Національної поліції України у сфері забезпечення інформаційної безпеки в Україні. *Закон і безпека*. 2020. № 79 (4). С. 32–38.
4. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. К. : Видавничий дім «Кондор», 2019. 272 с.
5. Діордіца І. Поняття і зміст кіберзагроз на сучасному етапі. URL: http://pgp-journal.kiev.ua/archive/2017/4/22.pdf
6. Рижкова Є. Актуальні проблеми правового регулювання цифрової революції. *Юридичні дослідження*. 2021. № 8. С. 1–10.
7. Тарасюк А. Актуальні проблеми забезпечення кібербезпеки на глобальному та національному рівнях. *Visegrad Journal on Human Rights*. 2020. № 1, С. 167–172.
8. Закон України «Про основні засади кібербезпеки України» від 5 жовтня 2017 року. URL: https://zakon.rada.gov.ua/laws/show/2163-19
9. Лесько Н., Гулак С. Правові засади управління інтернетом. *Порівняльно-аналітичне право*. 2020. № 8. С. 140–143.
10. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. К. : НІСД, 2014. 328 с.
11. Перун В. Зросла кількість російських кібератак і розповсюдження шкідливого програмного забезпечення. *Держспецзв'язок*. URL: https://lb.ua/tech/2022/11/10/535470_zrosla_kilkist_rosiyskih.html
12. Сенченко М. Запорука національної безпеки в умовах інформаційної війни. *Вісник Книжкової палати.* 2014. № 6. С. 3–9.
13. Драпушко Р.Г., Горінов П.В. Сучасні виклики і загрози правової культури молоді. *Аналітично-порівняльне право.* 2021. № 4. С. 9–16.
14. Це перша у світі кібервійна. У Мінцифрі розповіли про українську ІТ-армію. https://suspilne.media/222186-ce-persa-u-sviti-kibervijna-u-mincifri-rozpovili-pro-ukrainsku-it-armiu/