УДК 343.32
DOI https://doi.org/10.32782/2524-0374/2020-8/72

ШЛЯХИ МОДЕРНІЗАЦІЇ МЕХАНІЗМІВ РЕАЛІЗАЦІЇ СТРАТЕГІЇ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ В УКРАЇНІ НА ОСНОВІ ВИКОРИСТАННЯ МІЖНАРОДНОГО ДОСВІДУ

WAYS TO MODERNIZE IMPLEMENTATION MECHANISMS STRATEGIES TO COMBAT CYBERTERRORISM IN UKRAINE BASED ON THE USE OF INTERNATIONAL EXPERIENCE

Когут Ю.І., генеральний директор
ТОВ «Консалтингова компанія «СІДКОН»,
здобувач
Навчально-науковий інститут права імені князя Володимира Великого Міжрегіональної Академії управління персоналом

У статті досліджено механізми державного реагування на кіберзагрози, у тому числі загрози кібертероризму, в Україні. З метою модернізації механізмів реалізації державної стратегії протидії кібертероризму в Україні та з огляду на критично низький стан кібербезпекової складової частини вітчизняного сегменту кіберпростору, численні системні проблеми в організації кібербезпеки центральних органів виконавчої влади та об'єктів критичної інфраструктури запропоновано провести об'єктивний незалежний кібераудит державних електронних інформаційних ресурсів за міжнародними стандартами під егідою Національного координаційного центру кібербезпеки при РНБОУ та однієї з авторитетних міжнародних кібербезпекових організацій, а також створити національну експертну незалежну організацію з питань кібербезпеки та протидії кібертероризму за участю представників кібербізнесу, професійної кіберспільноти, науково-дослідницьких інституцій, вищих навчальних закладів, державних органів, міжнародних організацій та ін. У статті обґрунтована необхідність визначення державної структури (або державних структур), які будуть відповідальними за впровадження в Україні стандартів безпеки мережевих та інформаційних систем, єдиного контактного центру з питань безпеки мережевих та інформаційних систем, взаємовідносин та розподілу повноважень між такою державною установою (установами), контактним центром та CERT (Комп'ютерною групою (Командою) реагування на надзвичайні ситуації в кіберпросторі). Автор доводить необхідність обмеження об'єктів критичної інфраструктури, перерахованих у чинному законодавстві, залишивши в ньому винятково ті критично важливі об'єкти, які знаходяться у власності держави, скорочення переліку суб'єктів, чиї повноваження стосуються забезпечення кібербезпеки України, чіткого визначення компетенції кожного з державних органів – суб'єктів національної системи кібербезпеки для усунення дублювання їхніх функцій, а також обмеження повноважень Державної служби спеціального зв'язку та захисту інформації і СБУ у сфері забезпечення кібербезпеки з метою зменшення ризиків шпигунства та корупційних ризиків.

Ключові слова: кібертероризм, кібербезпека, кіберзагрози, критична інфраструктура, кіберзахист, кібератаки, кіберпростір, кібераудит, національна система кібербезпеки, стратегія протидії кібертероризму.

The article examines the mechanisms of state response to cyber threats, including threats of cyberterrorism, in Ukraine. In order to modernize the mechanisms of implementation of the state strategy to combat cyberterrorism in Ukraine and given the critically low state of cybersecurity component of the domestic segment of cyberspace, numerous systemic problems in the organization of cybersecurity of central executive bodies and critical infrastructure facilities. resources according to international standards under the auspices of the National Cyber Security Coordination Center at the National Security and Defense Council and one of the authoritative international cybersecurity organizations, as well as to create a national independent organization on cybersecurity and countering cyberterrorism with representatives of cyber business, professional community government agencies, international organizations, etc. The article substantiates the need to determine the state structure (or state structures) that will be responsible for the implementation in Ukraine of network and information systems security standards, a single contact center for network and information systems security, relationships and distribution of powers between such state institution (institutions), contact center and CERT (Computer Team (Team) for responding to emergencies in cyberspace). The author proves the need to limit the critical infrastructure facilities listed in the current legislation, leaving in it only those critical facilities that are owned by the state, reducing the list of entities whose powers relate to cybersecurity in Ukraine, clearly defining the competence of each of state bodies – subjects of the national cybersecurity system to eliminate duplication of their functions, as well as limit the powers of the State Service for Special Communications and Information Protection and the SBU in the field of cybersecurity in order to reduce the risks of espionage and corruption.

Key words: cyberterrorism, cybersecurity, cyber threats, critical infrastructure, cyber defense, cyber attacks, cyberspace, cyber audit, national cyber security system, strategy to combat cyberterrorism.

Постановка проблеми. Для забезпечення кібербезпеки України виняткового значення набуває обґрунтування ефективних механізмів забезпечення стратегії протидії кіберзагрозам, зокрема кібертероризму: деякі з них потребують удосконалення, інші взагалі не сформовані, а окремим елементам частини з них не вистачає концептуального обґрунтування.

Механізми державного реагування на кіберзагрози в Україні показують слабку ефективність: спостерігаються неспроможність органів державної влади налагодити цілісну стратегію інформаційно-комунікативної політики, слабка захищеність власного кіберпростору, постійний пошук рівня контролю за функціонуванням інформаційно-телекомунікаційних систем в інтересах національної безпеки.

Слід зазначити, що нині механізми реалізації державної стратегії протидії кібертероризму в Україні знаходяться на етапі становлення. Наявна система кібербезпеки не відповідає сучасним викликам та очікуванням суспільства. При цьому нормативно-правова база з питань кібербезпеки та протидії кібертероризму, незважаючи на значну кількість прийнятих останніми роками законодавчих та інших нормативних актів, потребує докорінних та невідкладних змін. Необхідність змін підтверджена атаками на об'єкти критичної інфраструктури, сумнозвісним NotPetya та багатьма іншими кіберінцидентами, які протягом останніх років створили Україні сумнівну репутацію одного з головних кіберполігонів [9]. Система управління кібербезпекою держави неефективна. Відсутнє централізоване управління силами реагування на кіберінциденти на загальнодержавному рівні.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [7] та низка нормативних документів про технічний захист інформації (НД ТЗІ) безнадійно застарілі, крім того, вони зобов'язують органи державної влади, об'єкти критичної інфраструк-

тури та приватні компанії, які хочуть надавати послуги державним органам (наприклад, Інтернет-провайдери), впроваджувати так звану Комплексну систему захисту інформації (КСЗІ) [9]. Вона, окрім того, що морально застаріла, впродовж багатьох років довела свою неефективність.

Аналіз публікацій, в яких започатковано розв'язання задекларованої проблематики. Проблемою кібертероризму займаються такі вчені, які зробили значний внесок у розробку заходів із протидії кібертероризму: В.А. Ліпкан, В.А. Мазуров, В.М. Бутузов, В.А. Васенин, В.А. Голубєв, І.В. Діордіца, О.Г. Широкова-Мурараш, Ю.Р. Акчурін, В.В. Топчій, Г.В. Форос, А.В. Форос, Є.А. Макаренко, М.М. Рижиков, М.А. Ожеван, В.К. Грищук, О.В. Кубишкін, В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа, О.Д. Довгань, І.М. Доронін, А.В. Тарасюк, В.Г. Пилипчук, О.С. Геращенко, О.В. Бойченко, С.О. Гнатюк, В.В. Мохор, С.Б. Гавриш, М.В. Гуцалюк, А.І. Марущак, С.Г. Петров, Л.М. Стрельбицька, М.П. Стрельбицький тощо. Зокрема, вагоме значення для подальшого висвітлення проблеми протидії кібертероризму мають наукові дослідження зарубіжних та вітчизняних вчених М. Делягіна, А. Фороса, Д. Деннінга, В. Ліпкана, І. Міхеєва, К. Герасименка та ін.

Однак, незважаючи на чималу увагу багатьох правознавців до досліджуваної проблематики, виняткового значення для забезпечення кібербезпеки України набуває наукове обґрунтування шляхів модернізації механізмів реалізації стратегії протидії кібертероризму в Україні на основі використання міжнародного досвіду.

Мета статті полягає в запропонуванні шляхів підвищення ефективності протидії кібертероризму, зокрема напрямів модернізації механізмів реалізації державної стратегії протидії кібертероризму в Україні.

Виклад основного матеріалу. Для того, щоб здійснити модернізацію механізмів реалізації державної стратегії протидії кібертероризму в Україні з огляду на критично низький стан кібербезпекової складової частини вітчизняного сегмента кіберпростору, численні системні проблеми в організації кібербезпеки центральних органів виконавчої влади та об'єктів критичної інфраструктури бажано якомога швидше провести об'єктивний незалежний аудит кібербезпеки критичних електронних інформаційних ресурсів (мережевої інфраструктури, політик, моделей загроз, наявності засобів захисту) за міжнародними стандартами на рівні як державних, так і недержавних інституцій під егідою Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України (РНБОУ) та однієї з авторитетних міжнародних кібербезпекових організацій (наприклад, європейського підрозділу Business Software Alliance (BSA)) за такими критеріями:

– правові підстави функціонування цього сегмента кіберпростору;
– організаційні інституції та механізми забезпечення кібербезпеки;
– стан державно-приватного партнерства;
– секторальна кібербезпека;
– кібербезпекове просвітництво [5, с. 123].

До цього аудиту можна додати проведення передбаченого Законом України «Про основні засади забезпечення кібербезпеки України» [8] незалежного аудиту за міжнародними стандартами діяльності Державної служби спеціального зв'язку та захисту інформації як головного органу національної системи кібербезпеки.

Однак нині варто констатувати таку проблему, як низька якість аудиту кібербезпеки, оскільки дозвіл на проведення аудиту мають лише акредитовані державою організації. Міжнародні сертифікати з інформаційної безпеки та ІТ-аудиту нині не визнаються, що негативно впливає на якість кібераудиту [9].

Для оцінки захищеності інформаційних систем пропонуємо впровадити кібераудити на відповідність міжнародним стандартам [9]. Такі кібераудити потрібно проводити регулярно, із залученням незалежних (бажано, зовнішніх) спеціалістів, які мають міжнародну сертифікацію.

З метою модернізації механізмів реалізації державної стратегії протидії кібертероризму в Україні доцільним є створення національної експертної незалежної організації (наприклад, ради) з питань кібербезпеки та протидії кібертероризму за участю представників кібербізнесу, професійної кіберспільноти, науково-дослідницьких інституцій, вищих навчальних закладів, державних органів, міжнародних організацій та ін. [4]. Наприклад, як пропонує К. Корсун [4], організаційна модель може бути аналогічною BRDO – Офісу ефективного регулювання – незалежного експертно-аналітичного центру, який фінансується Європейським Союзом. Прикладом такої організації є Національна Рада Кібербезпеки в Нідерландах [9].

Така національна експертна незалежна організація з питань кібербезпеки та протидії кібертероризму має готувати та подавати пропозиції до Стратегії кібербезпеки України, інших нормативно-правових актів у цій сфері, давати рекомендації з функціонування національної системи кібербезпеки, вирішувати інші завдання та проблеми, які потребують належної експертизи у кіберпросторі, розглядати спірні та неузгоджені питання функціонування національної системи кібербезпеки, розглядати та надавати рекомендації, консультувати з ключових питань кібербезпеки об'єктів критичної інфраструктури та центральних органів виконавчої влади, надавати експертну підтримку правоохоронним та судовим органам із технічних та технологічних аспектів питань кібербезпеки, які виникають під час розслідування та розгляду в судах відповідних кримінальних проваджень і які не чітко регламентуються чинним законодавством України, сприяти міжнародному співробітництву із зарубіжними організаціями з протидії кіберзлочинності та кібертероризму [4].

Ця організація сприятиме налагодженню горизонтальних зв'язків між об'єктами критичної інфраструктури, їхніми галузевими об'єднаннями, кіберспільнотою, громадськими організаціями, державними регуляторними органами тощо, сприятиме обміну інформацією про кіберінциденти, актуальні кіберзагрози, заходи протидії тощо між усіма об'єктами забезпечення кібербезпеки незалежно від форм власності.

І ще важливе зауваження щодо механізму реалізації Закону України «Про основні засади забезпечення кібербезпеки України» [8]: занадто широким є перелік об'єктів критичної інфраструктури, яких стосується цей закон. Це не дасть змоги повною мірою контролювати усі ці критично важливі об'єкти (КВО) та забезпечити нормальне регулювання питань забезпечення кібербезпеки для цих об'єктів. Таким чином, норми названого закону потребують суттєвого доопрацювання в окреслених напрямах.

До того ж через специфіку багатьох галузей (охорона здоров'я, енергетика, телекомунікації тощо) є гостра потреба у впровадженні окремих галузевих стандартів кібербезпеки [9]. Взагалі державі потрібен перехід на міжнародні стандарти кібербезпеки, зокрема галузеві. Є ціла низка міжнародних стандартів NIST, ISO, Cobit, які зарекомендували себе в розвинених країнах світу та пройшли перевірку часом. Наприклад, у США, Японії та Ізраїлю застосовують стандарт із кібербезпеки NIST Cybersecurity Framework. Так, National Institute of Standarts and Technology Cybersecurity Framework (NIST CSF) – розроблений американським Інститутом стандартів і технологій комплекс методологій та рекомендацій щодо зниження ІТ-ризиків, запобігання, моніторингу і реагування на кібератаки [1, с. 58].

Можна також виділити інші напрями модернізації механізмів реалізації державної стратегії протидії кібертероризму в Україні:

– чітке визначення та вимірювання критеріїв зарахування об'єктів до критичної інфраструктури;

– побудова чітко визначених процедур із реагування на кіберінциденти на об'єктах критичної інфраструктури;

– вдосконалення профільної освіти з кібербезпеки в Україні: створення онлайн-курсів у вищих навчальних закладах із підготовки спеціалістів із кібербезпеки, які зможуть правильно та ефективно реагувати на кібератаки і кіберінциденти;

– створення національного порталу кібербезпеки з метою підвищення обізнаності населення щодо кіберзагроз та протидії ним, а також формування культури кібербезпеки;

– визнання міжнародних сертифікацій та запровадження обов'язкової міжнародної сертифікації з кібербезпеки для посадовців, які займаються кібербезпекою та кібераудитом; заміна державної акредитації аудиторів із кібербезпеки, яка нині проводиться, акредитацією на основі міжнародних сертифікацій [9];

– створення галузевих центрів реагування на кіберінциденти (SOC) та центрів обміну інформацією про кібератаки (ISAC). Причому локальні SOC- та ISAC-центри мають налагодити тісну взаємодію з міжнародною мережею таких організацій [9].

У процесі нинішнього оновлення Стратегії кібербезпеки України доцільно провести таку роботу щодо модернізації механізмів її реалізації на практиці на основі імплементації в Україні положень європейських актів:

1) визначення державної структури (або державних структур), які будуть відповідальними за впровадження в Україні стандартів безпеки мережевих та інформаційних систем, визначення єдиного контактного центру з питань безпеки мережевих та інформаційних систем, взаємовідносин та розподілу повноважень між такою державною установою (установами), контактним центром та CERT (Комп'ютерною групою (Командою) реагування на надзвичайні ситуації в кіберпросторі) Державної служби спеціального зв'язку та захисту інформації (Держспецзв'язку).

Водночас варто вдосконалити правовий статус Національного координаційного центру кібербезпеки (НКЦК), який ч. 2 ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» [109] визначається робочим органом РНБОУ та який здійснює координацію та контроль за діяльністю суб'єктів сектора безпеки й оборони, що забезпечують кібербезпеку. Досі незрозумілим є правовий статус НКЦК, адже на практиці цей орган є суто інформаційно-аналітичним додатком до РНБОУ;

2) з метою здійснення адекватного та ефективного кіберзахисту КВО – визначення критеріїв «значної руйнівної дії» (з точки зору наявності та значимості кіберінцидентів на підставі реалізації кіберзагроз) з урахуванням особливостей надання послуг у певних секторах економіки, кількості користувачів сервісу конкретного оператора інформаційно-телекомунікаційних послуг чи провайдера цифрових послуг, залежності інших важливих секторів економіки від сервісу конкретного оператора чи провайдера, впливу (з урахуванням масштабу та тривалості) на соціально-економічну активність або громадську безпеку, ринкової частки оператора чи провайдера, географії поширення можливої руйнівної дії кіберінцидентів тощо.

Для того, щоб найточніше визначити критерії «значної руйнівної дії», варто скористатися Директивою NIS, згідно з якою операторами базових інформаційно-телекомунікаційних послуг є юридичні особи, які відповідають таким критеріям:

– підприємство (незалежно від форми власності) надає послугу, яка є базовою для підтримки критичної соціально-економічної діяльності;

– надання такої послуги потребує використання мережевих або інформаційних систем;

– порушення кібербезпеки матиме значний руйнівний вплив на надання базової послуги.

Як правило, оператори базових інформаційно-телекомунікаційних послуг функціонують у таких галузях: паливно-енергетичний комплекс, транспорт, фінансова галузь, у тому числі банківська, охорона здоров'я, телекомунікація, житлово-комунальний сектор, цифрова інфраструктура.

Своєю чергою до провайдерів цифрових послуг належать онлайнові торгівельні майданчики, постачальники «хмарних» послуг, пошукові системи.

Оператори базових інформаційно-телекомунікаційних послуг та провайдери цифрових послуг мають вжити необхідних (технічних та організаційних) заходів для того, щоб попередити ризики кіберінцидентів, забезпечити мережеву та інформаційну безпеку (відповідно до потенційних кіберризиків), належним чином відреагувати на кіберінциденти з метою мінімізації шкоди, повідомити компетентні органи про кіберінциденти.

Директивою NIS також передбачається дотримання міжнародних стандартів цими операторами та провайдерами, регулярне проведення ними моніторингу, кібераудіту та тестування;

3) стандартизації у сфері кібербезпеки. Так, приміром, у процесі впровадження стандартизації у зазначеній сфері від країн-членів ЄС вимагається дотримання мережевої нейтральності та міжнародних і європейських стандартів та забороняються введення окремих національних стандартів у сфері кібербезпеки, які не є сумісними з відповідними європейськими та міжнародними стандартами;

4) механізмів запровадження системи мережевої та інформаційної безпеки та її кібераудиту.

Установа, що відповідатиме за імплементацію в Україні Директиви NIS, або незалежний сертифікований аудитор має отримати доступ до документації оператора інформаційно-телекомунікаційних послуг чи провайдера цифрових послуг щодо оцінки ризиків кібербезпеки та запровадження системи управління ризиками кібербезпеки, а також оцінити ефективність такої системи. При цьому має вимагатись лише та інформація, яка є необхідною для проведення такого кібераудиту.

У разі виявлення недоліків у цій системі оператора інформаційно-телекомунікаційних послуг чи провайдера цифрових послуг аудитор має вказати на них та зробити приписи щодо їх усунення. І тільки в разі невиконання цих приписів має наставати відповідальність за недотримання вимог мережевої та інформаційної безпеки;

5) створення законодавчо-нормативної бази щодо функціонування системи сповіщення про кіберінциденти, впровадження системи кібераудиту та заходів мережевої та інформаційної безпеки.

Відповідно до вимог Директиви NIS передбачаються два варіанти сповіщення про кіберінциденти: обов'язковий та добровільний [3, с. 22]. Обов'язковість сповіщення про кіберінциденти має передбачатися для тих операторів та провайдерів, які були внесені відповідно до вимог постанови Кабінету Міністрів України від 09.10.2020 р. №,943 «Деякі питання об'єктів критичної інформаційної інфраструктури» [2] до офіційного переліку операторів базових інформаційно-телекомунікаційних послуг та провайдерів цифрових послуг та належать до кіберінцидентів, які підпадають під критерії «значної руйнівної дії».

Інформація від таких операторів і провайдерів та щодо таких кіберінцидентів має надсилатись до державної установи, що відповідатиме за імплементацію Директиви NIS, або до CERT (Команди реагування на надзвичайні ситуації в кіберпросторі) Держспецзв'язку.

Нині поки що з усіх перерахованих можливих та доцільних механізмів реалізації на практиці Страте-

гії кібербезпеки України впроваджені лише такі заходи на основі прийняття двох постанов Кабінету Міністрів України – від 09.10.2020 р. № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури» [2] та від 19.06.2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [6] щодо:

– визначення критеріїв, за якими буде складатись перелік операторів базових інформаційно-телекомунікаційних послуг та провайдерів цифрових послуг;

– створення переліку операторів базових інформаційно-телекомунікаційних послуг та провайдерів цифрових послуг.

Висновки. Для формування ефективної системи протидії кібертероризму в Україні необхідно вжити низку системних заходів у концептуальному, нормативно-правовому та інституціональному напрямах [6, с. 58]:

1) на концептуальному рівні:

– чітко визначити основні загрози кібербезпеці, зокрема загрози кібертероризму, та сформувати заходи, спрямовані на їх відвернення, нейтралізацію та попередження;

– створити систему технологічних засобів складника національної системи кібербезпеки;

– налагодити більш тісне співробітництво з міжнародними партнерами України;

2) на законодавчому рівні:

– по-перше, визначити єдиний державний орган, який би здійснював оперативне управління усіма суб'єктами, чиїм завданням є забезпечення кібербезпеки в мирний час;

– по-друге, обмежити повноваження Держспецзв'язку та Служби безпеки України у сфері забезпечення кібербезпеки з метою зменшення ризиків шпигунства та корупційних ризиків. Це стане можливим, зокрема, якщо кібераудит буде проводитись незалежними аудиторами, що знизить ризик корупціювання великого та середнього бізнесу з владними структурами;

– по-третє, скасувати проведення позапланових перевірок критичних об'єктів інфраструктури, що знаходяться у приватній власності;

– по-четверте, обмежити об'єкти критичної інфраструктури, перераховані в Законі України «Про основні засади забезпечення кібербезпеки України» [8], залишивши в ньому винятково ті КВО, які знаходяться у власності держави.

– по-п'яте, здійснити перерахування решти критичних об'єктів, які знаходяться у приватній власності, в окремому законопроєкті;

3) на інституціональному рівні:

– скоротити перелік суб'єктів, чиї повноваження стосуються забезпечення кібербезпеки України;

– чітко визначити компетенцію кожного з державних органів – суб'єктів національної системи кібербезпеки для усунення дублювання їхніх функцій.

ЛІТЕРАТУРА

1. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. доп. / за заг. ред. Д. Дубова. Київ : НІСД, 2018. 84 с.

2. Деякі питання об'єктів критичної інформаційної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 р., № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-п#Text.

3. Кольцов М., Аушев Є. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні (Policy Paper) / USAID. 2017. 28 с.

4. Корсун К. Щодо заснування національної експертної незалежної організації з питань кібербезпеки. URL: https://www.facebook.com/kostiantyn.korsun/posts/1156357737882659.

5. Ожеван М.А. Публічно-приватне партнерство у кібербезпековій сфері як модернізаційний виклик. *Актуальні проблеми управління інформаційною безпекою держави* : збірник тез наук. доп. наук.-практ. конф., Київ, 30 березня 2018 р. Київ : Нац. акад. СБУ, 2018. С. 120–124. URL: http://academy.ssu.gov.ua/upload/file/aktualn_problemi_upravl_nnya_nformac_ycnoyu_bezpekoyu_derzhavi.pdf.

6. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19.06.2019 р. № 518. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennya-zagalnih-vimog-do-kiberzahistu-obyektiv-kritichnoyi-infrastrukturi-i190619.

7. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР (із змінами). URL: https://zakon.rada.gov.ua/laws/main/80/94-вр#Text.

8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/main/2163-19#Text.

9. Янковський О. Україні потрібна нова кіберстратегія. URL: https://www.pravda.com.ua/columns/2019/09/14/7226291/.