DOI: [10.32702/2307-2156-2019.7.25](https://doi.org/10.32702/2307-2156-2019.7.25)

УДК: 343.37:321:004.9

*В. С. Гнатенко,
Дружківський міський голова, кандидат економічних наук
ORCID:0000-0003-2659-9202*

ІНФОРМАЦІЙНІ ВИКЛИКИ ЕКОНОМІЧНІЙ БЕЗПЕЦІ ДЕРЖАВИ

*V. S. Hnatenko
Druzhkivka mayor, Candidate of Economic Sciences*

INFORMATION CHALLENGES FOR THE ECONOMIC SECURITY OF THE STATE

Досягнення економічної безпеки є однією з життєво важливих проблем розвитку держави, суспільства, підприємства, особистості. Всі сфери життєдіяльності людини містять ризики та небезпеки, які необхідно враховувати при визначенні та здійсненні цілей, висунутих суспільством. Економічна безпека, як складова національної безпеки, має першорядне значення для її розвитку, так як вона дає орієнтири для прийняття вірних соціально-економічних рішень.

У ХХІ столітті основний вектор розвитку світової цивілізації лежить в інформаційній сфері, яка представляє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, які здійснюють збір, обробку, розповсюдження та використання інформації, а також системи регулювання виникаючих при цьому економічних відносин. У всіх без винятку випадках технологічного та економічного прогресу сучасного суспільства констатується, що розвиток сучасних інформаційно-комунікаційних технологій стає технологічним пакетом, який претендує на керуючу функцію у всіх сценаріях розвитку.

В умовах турбулентних явищ, нестійкості економіки та трансформації соціально-економічної системи проблеми економічної безпеки значно актуалізуються. Світ динамічно змінюється, і загрози змінюються з калейдоскопічною швидкістю. Пріоритети безпеки, визначені на конкретному етапі економічного розвитку, не є постійними і зазнають значних змін в умовах конкретних ситуацій. Система потенційних і реальних загроз також не може бути постійною: вони з'являються і зникають, наростають і зменшуються, при цьому змінюється їх місце і значення впливу на економічну безпеку. Економічна, соціальна і політична ситуації в світі кардинально змінюється, чимало загроз втрачають свою значимість і гостроту, в той же час з'являються нові виклики і загрози національній безпеці.

У статті доказывается, що небезпека являє собою об'єктивно існуючу можливість негативного впливу на суспільство, державу, підприємство, особистість, а також природне середовище, в результаті чого їм може бути завдано збитків, що погіршує їх становище і надає негативну динаміку розвитку. Виявлено, що високий ступінь інформатизації та автоматизації, до яких звернулося сучасне суспільство, породжує стан його залежності від безпеки використовуваних інформаційних технологій.

Achieving of the economic security is one of the vital problems of the development of the state, society, enterprise and a personality. All spheres of a human life-sustaining activity contain risks and dangers that must be taken into account when defining and implementing the goals set by society. Economic security, as a component of the national security, is of paramount importance for development, as it provides guidelines for making correct socio-economic decisions.

In the 21st century, the main vector of the world civilization development lays in the information sphere, which is a collection of information, information infrastructure, specimen that collect, process, promote and use information, as well as systems for regulation of the economic relations originating in this case. In all variants of technological and economic progress of the modern society, without exception, it is stated that the development of modern information and communication technologies transforms into a technological package that pretends to be a control function in all development scenarios.

Under conditions of turbulent phenomena, instability of the economy and the transformation of the socio-economic system, the problems of economic security are actualized significantly. The world is changing dynamically, and threats are changing at a kaleidoscopic speed. As a result, the security priorities identified at a particular stage of economic development are not constant and undergo significant changes in specific situations. The system of potential and real threats also cannot be constant: they appear and disappear, grow and decrease, while their place and significance of influence on economic security changes. The economic, social and political situations change dramatically in the world; many threats lose their significance and urgency, while new challenges and threats to national security appear.

It has been proved in this article that the danger is an objectively existing possibility of negative impact on society, state, enterprise and a person, as well as on the natural environment, as a result of which they can be damaged, and this harm will worsen their situation and afford negative dynamics to development. It has been determined that the highest degree of informational support and automation, to which modern society has rushed, creates its dependence on the security of the used information technologies.

Ключові слова: економічна безпека; національна безпека; інформаційна сфера; інформаційні загрози; небезпека; джерела небезпеки; інформаційна економіка; інформаційна війна.

Keywords: Economic security; national security; information sphere; information threats; danger; sources of danger; information economy; and information war.

Постановка проблеми. У сучасній економіці без інформаційних технологій неможливо досягнення ефективного економічного зростання, підвищення рівня освіти і кваліфікації населення, створення сучасної кредитно-фінансової системи, раціональне управління суспільними процесами, підвищення рівня життя громадян. Застосування нових інформаційних технологій в усіх галузях і сферах економіки є безсумнівним благом.

Однак основні тенденції розвитку інформатизації суспільства і економіки показують, що ці процеси створюють для розвитку держав не тільки нові можливості, але й нові проблеми та ризики. Високий ступінь інформатизації ставить сучасне суспільство і економіку в залежність від ступеня безпеки інформаційних технологій. Сучасна «залежність» економіки від інформаційних технологій може негативно відбитися на економічній безпеці держави, суспільства, підприємства і особистості. Відомо, що інформаційні технології та мережа Інтернет в «неправильних» руках перетворюються в небезпечну зброю: з їх допомогою можливі цілеспрямовані шкідницькі дії, які здатні паралізувати цілі галузі економіки.

Таким чином, в умовах сучасної економіки виникає необхідність переосмислення підходів до побудови системи економічної безпеки з урахуванням розширення інформаційної сфери. Розуміння специфіки впливу інформаційних загроз на економічну безпеку держави дозволяє вийти на визначення детермінант, що впливають на механізм забезпечення економічної безпеки держави в майбутньому, що відноситься до числа ключових завдань економічної політики.

Аналіз останніх досліджень і публікацій. Економічна безпека держави є визнаним об'єктом наукової уваги, як в нашій країні, так і за кордоном. Дослідженню проблем економічної безпеки присвячено багато робіт, розроблено значну кількість концепцій і теорій. Основний характер в дослідженні економічної безпеки мають праці таких закордонних вчених, як С. Гудвін [1], Ю. Цзян [2], С.Джонсон, Д.Кауфман, Д.Макміллан, К.

Вудруфф [3], М. Калер [4], Д.К. Нанто [5], Х.С. Несадурі [6], Ф. Шнайдер [7], Е. де Сото [8], Дж. Досі, Р. Нельсон [9], С. Уінтер [10] та інших.

Вітчизняною економічною наукою теоретичні аспекти проблем економічної безпеки найактивніше почали розроблятися з середини 1990-х років. Питання забезпечення економічної безпеки держави містяться в дослідженнях А.А. Ананьєва [11], А.І. Барановського [12], О.А. Белькова [13], А.А. Бочурова, А.Х. Курбанова, А.Н. Литвиненка [14], А.В. Загребельної [15], М.Н. Руденко, Я.А. Долганової [16], Е.Н. Чижикова, Е.Н. Бардуліна, В.І. Бабенкова [17] та інших. У роботах цих вчених детально досліджені загрози економічній безпеці в період трансформації і розкриті механізми виявлення, запобігання і нейтралізації даних загроз.

Разом з тим господарська практика останнього десятиліття показує, що все більш істотний вплив на економічну безпеку держави надають інформаційні фактори. Основні ідеї концепції інформаційної економіки сформульовані в працях С.Д. Бодрунова, Д.С. Демиденка, В.А. Плотнікова [18], О.А. Панченка, Н.В. Банчук [19], А.Е. Шаститка [20], А.В. Харламова, К.В. Адаменка [21] та інші.

Мета дослідження: виокремити та проаналізувати інформаційну складову в економічній безпеці держави.

Результати дослідження.

Проблема економічної безпеки є життєво важливою як в аспекті існування і розвитку будь-якої країни, так і в плані міждисциплінарних напрямків наукових досліджень. Можна абсолютно правомірно стверджувати, що всі сфери життєдіяльності людини в певній мірі містять певні індикатори, що сигналізують про можливі ризики і загрози, облік яких необхідний при визначенні та здійсненні цілей, висунутих державою, фірмами і окремою особистістю. Крім того, значення проблеми безпеки в даний час зростає через посилення альтернативності і багатоваріантності розвитку економіки. Неможливо вибрати той чи інший варіант розвитку економіки, інвестування, складання бюджетного плану країни, не оцінюючи їх соціально-економічні наслідки за допомогою виведення критеріїв економічної безпеки. Цей висновок особливо актуальний в період трансформації економічної системи, який завжди загрожує виникненням кризи. Без правильної оцінки безпеки економічних реформ для суспільства, держави, регіонів, корпорацій і громадян вони можуть привести до руйнування держави і його життєзабезпечуючих систем. Тому в сучасних умовах економічна безпека країни набуває першочергового значення, так як вона дає орієнтири для прийняття вірних соціально-економічних рішень.

Небезпечним явищем є виникнення «інциденту економічної небезпеки» - будь-якої непередбаченої або небажаної події, яка може порушити економічну діяльність. Тобто це ті випадки, які зі своєю появою ведуть до порушення економічної безпеки.

Природа появи визнаного інциденту вельми різноманітна: від випадкової помилки персоналу або неправильного функціонування технічних засобів, впливу природного фактора (пожежа, повінь тощо) до навмисних злочинних дій, які можуть привести до порушення цілісності, секретності, доступності інформації тощо.

Небезпека являє собою об'єктивно існуючу можливість негативного впливу на суспільство, державу, підприємство, особистість, а також природне середовище, в результаті чого їм може бути завдано збитків, що погіршує їх становище і надає негативну динаміку їх розвитку. Небезпека є цілком усвідомлюваною, але при цьому не фатальною ймовірністю нанесення збитку або шкоди будь-якому об'єкту. Вона визначається об'єктивними і суб'єктивними факторами, що володіють вражаючими властивостями. Небезпека - це вихідна передумова при дослідженні проблем економічної безпеки.

Джерелами небезпеки є умови і чинники, що містять в собі наміри ворожого характеру, деструктивну природу, шкідливі якості. Джерела небезпеки класифікуються за їх походженням, в їх числі природні, техногенні і соціальні.

Загроза являє собою найбільш конкретну та безпосередню форму небезпеки. Це система умов і факторів, які створюють небезпеку національним цінностям і національному способу життя. Загрози припускають можливість негативних змін у зовнішньому середовищі (політичної, економічної або природної), що завдають значний потенційний або реальний збиток як державі в цілому, так і його окремих структурних елементів.

Джерела формування загроз економічній безпеці країни відбуваються з різноманіття внутрішніх і зовнішніх протиріч економічного розвитку в різних сферах господарської діяльності людини. Це одночасно є головним вихідним критерієм для виділення суспільних відносин, що формують систему економічних взаємодій в сфері безпеки країни.

Високий ступінь інформатизації та автоматизації, до яких звернулося сучасне суспільство, породжує стан його залежності від безпеки використовуваних інформаційних технологій. У свою чергу, від цього залежить благополуччя багатьох людей. Особливої гостроти набувають проблеми захисту інформації, що циркулює в стратегічно важливих інформаційних системах. Уразливість такої інформації зростає. При цьому особливу небезпеку становить «інформаційний тероризм», можливість якого обумовлена існуванням глобальних комп'ютерних мереж, запобігти які важко, а ліквідувати наслідки надзвичайно дорого.

В останні роки дедалі більше набуває розуміння необхідності підвищення інформаційної безпеки, а також усвідомлення того, що захист інформації є важливим для економічної і політичної безпеки будь-якої держави. Зростаюча загроза кібер-атак змусила уряди і компанії гостріше усвідомлювати необхідність захисту

контрольованих комп'ютером систем управління комунальними підприємствами та іншої критично важливою інфраструктурою країни.

З огляду на вкрай постійний і цілеспрямований характер більшості сучасних кібер-атак, - порушення безпеки даних практично неминуче для більшості організацій. Незалежно від того, наскільки добре захищена організація, досвідчений противник завжди знайде спосіб прослизнути всередину її системи просто тому, що сучасні мережі настільки великі, складні і взаємопов'язані, що майже неможливо зберегти кожну точку входу постійно безпечною.

Однією з найбільших проблем, з якою стикаються підприємства реального сектору економіки, є аналіз всіх даних, що генеруються різними системами безпеки в Інтернет-мережах. Антивірусні засоби, системи виявлення та запобігання вторгнень, уніфіковані пристрої для управління загрозами і інші технології можуть генерувати безліч додаткових даних, з якими проблематично впоратися навіть адміністраторам по інформаційному захисті. Якщо додати до цього розмови з мобільних пристроїв, інформацію віртуалізованих систем і хмарних ресурсів, обсяг даних може стати для організації величезним.

Більш того, за даними компанії Hewlett Packard, в середньому підприємства отримують щотижня 17 тис. попереджень про шкідливе програмне забезпечення, переважна більшість яких виявляється хибним [22]. Для великих компаній переслідування таких помилкових попереджень обходиться близько 1,3 млн. Дол. США в рік. Фактично, тільки 19% відсотків попереджень, що генеруються системами безпеки, зазвичай надійні, а через величезний обсяг даних адміністратори в кінцевому підсумку дивляться лише близько 4% повідомлень, які вони отримують, створюючи величезну вразливість для організацій.

Так у 2017 році було зареєстровано 4149 порушень в різних великих системах, які оприлюднили понад 4,2 млрд. Особистих даних користувачів. У той же час шкоди світовій економіці від розкрадань того чи іншого типу інформації склав близько 445 млрд. Дол. Найбільший збиток був нанесений таким компаніям, як Yahoo, MySpace, Adobe Systems, eBay, LinkedIn і так далі. Саме на бізнес-сектор припадає найбільша кількість кібер-атак (51%), друге місце займає урядовий сектор (23%), третє - медичний сектор (12%) [23]. Однак з цього зовсім не випливає, що в більшості своїй ризику небезпеки даних схильні до великих компаній і корпорацій. З найбільшим ризиком втрати даних стикаються саме дрібні і середні фірми, за допомогою яких досвідчені хакери, згодом, шукають доступ до більш закритих систем.

В умовах інформаційної економіки інформація перетворилася в потужний засіб конкурентної боротьби. Вартість інформації безпосередньо залежить від величини прибутку від її використання або розміру ймовірного збитку її власника. Витягнута з суб'єкта реального сектору економіки інформація може бути використана проти нього. Тому найбільш серйозною загрозою для корпоративного сектору є витік інформації. За цією інформацією ведеться справжнє полювання, як ззовні, так і зсередини. Мета - домогтися певних переваг, наприклад, при веденні ділових переговорів. Уже в процесі встановлення відносин з потенційними партнерами компанії наймають хакерів, які ламали комп'ютери інших компаній, бухгалтерів, консультантів і юристів для отримання інформації, що схиляє чашу терезів на їхню користь. А якщо викрасти дані про плани інвестицій (де, коли, в яких обсягах) і технологічних інновацій, про заходи протидії конкурентам, про факти поглинання інших компаній або наближається банкрутство, то такої інформації немає ціни. Подібне вторгнення може викликати як прямий, так і непрямий збиток (витрати на відновлення та заміну програмного забезпечення та ін.).

Разом із тим, Інтернет перетворився в робочий інструмент, без якого вже практично неможлива повсякденна діяльність фірм і підприємств: це і глобальна довідкова система, і доступ до технологій, і спосіб передачі даних, і ефективний та недорогий засіб комунікації. Атака на web-сервери фірми, зміна існуючої на ньому інформації можуть спричинити за собою зниження довіри до фірми, і в результаті, втрату клієнтів і доходів.

Німецькі компанії щорічно втрачають від комп'ютерного промислового шпигунства більше 20 млрд. євро. Електронні атаки на комп'ютери фірм і державні структури Німеччини відбуваються із завидною регулярністю (як мінімум 4 рази на тиждень). Цікаво відзначити, що в цій справі широко використовуються програми - «троянці», які запускаються в чужий комп'ютер через Інтернет і за кілька секунд копіюють всю інформацію з жорстких дисків, переглядають електронну пошту і передають дані зацікавленим особам. Атакам таких програм піддаються 750 тис. комп'ютерів промислових компаній і установ країни.

Сучасні засоби і способи масової інформації дозволяють забезпечувати керованість в суспільстві. При цьому мова йде не про військове захоплення, а про ідеологічне: в систему цінностей країни вносяться невластиві для неї ідеали і прагнення. Іншими словами, можна говорити про ведення так званої інформаційної війни.

У «колонізованих» країнах примусово можна створити соціальний і політичний лад колоніальної демократії, яка є штучною, нав'язаною країні всупереч існуючим в ній традицій і тенденцій розвитку. При цьому може зберігатися зовнішня видимість суверенітету, однак економіка потрапляє під контроль іноземних банків або спільних підприємств. Таким чином, колоніальна демократія використовується як засіб не демократичного режиму, а засіб маніпуляції масами.

В даний час склад країн, що піддаються інформаційній колонізації не обмежується країнами третього світу. Глобальний інформаційний простір уніфікує інформаційні та телекомунікаційні технології всіх країн - суб'єктів мережевого простору, а ступінь інформатизації необхідного рівня доступна лише країнам з високим промисловим і науково-технічним потенціалом, а також високим рівнем освіти населення. Це дозволяє сильним постіндустріальним державам нарощувати своє політичне, соціально-економічне та військову перевагу за

рахунок переваг в інформатизації. В результаті вони здійснюють інформаційний контроль і нав'язують свої норми і правила усій світовій спільноті.

Використання сучасних інформаційно-телекомунікаційних технологій представляють принципово нові можливості для вдосконалення державного управління, перегляду взаємовідносин між державою, її органами управління і самоврядування та суспільством, а створення «електронних урядів» виводить на об'єктивно новий вид взаємозв'язків «громадянин - держава», заснованих на відкритості прийнятих рішень, виключення суб'єктивних факторів з управління як процесу прийняття рішення.

Розвиток інформатизації та електронних технічних засобів вплинув на структури і процеси державного управління, в тому числі і економічної безпеки держави. Якщо спочатку це вплив виразилося в підвищенні ефективності збору, обробки та використання інформації в процесі прийняття рішень, то в подальшому почали відбуватися помітні трансформації в інститутах і методах організації всієї системи державного управління.

Держава повинна виробити і реалізувати єдину державну інформаційну політику в сфері інформатизації управління національним економічним, соціальним і суспільним розвитком. Державна інформаційна політика в сфері інформатизації управлінських відносин може і повинна стати продовженням і механізмом реалізації державної адміністративної та соціально-економічної політики, сприяючи в умовах ринкових відносин високу ефективність функціонування як державного, так і недержавного секторів національної економіки, забезпечуючи цілісність управління країною як єдиним виробничо-споживчим комплексом і єдиним суб'єктом управління. Інформатизація системи державного управління повинна передбачати конструктивну взаємодію органів державного управління різних гілок, рівнів і ланок в рамках єдиної методології їх спільної діяльності, встановленої законодавчо, і єдиного національного інформаційно-економічного простору, що відображає поточну динаміку соціально-економічного середовища і суспільства.

Висновки та перспективи подальших досліджень.

1. Для того щоб забезпечити економічну безпеку в умовах інформаційної економіки, необхідно створити відповідну цьому завданню систему правових відносин. Однак для цього необхідний перегляд категоріального апарату, доктринального і концептуального фундаменту з метою подолання декларативного характеру сучасного законодавства в інформаційній сфері.

2. Скорочення розриву між практикою і законодавством. В даний час між законодавством і практикою - величезна прірва. Вона об'єктивно зумовлена тим, що інформаційні технології та Інтернет припускають стрімкість і масштабність дії. Нові загрози для економічної безпеки можуть з'являтися миттєво і в сотнях тисячах місць. Законодавчий процес, навпаки, має на увазі довгий шлях. У зв'язку з цим, найважливіше (і найважче) - це створити механізм, що дозволяє узгодити процес розробки законів з реаліями і прогресом розвитку сучасного суспільства, і зокрема, інформаційних технологій. Закони не можуть випереджати життя, але важливо, щоб відставання не було занадто великим, так як на практиці, крім інших негативних моментів, це може привести до зниження економічної безпеки в інформаційній сфері. Подолання розриву між практикою і законодавством необхідно для зниження і нейтралізації загроз економічній безпеці, обумовлених випередженням розвитку інформаційних технологій і виникненням прогалин в законодавстві.

3. Формування наднаціонального законодавства в інформаційній сфері. Протистояти злочинам, які вчиняються в Інтернеті, в рамках однієї країни неможливо. Навіть недоцільно вдаватися до заборонних заходів на національному рівні. Зловмисники найчастіше перебувають за кордоном, але їх деструктивна Інтернет-діяльність впливає на ту чи іншу країну. Боротися з ними безглуздо, поки не домовляться про консолідацію зусиль на міжнародному рівні. В умовах інформаційної економіки необхідне прийняття зводу міжнародних правил поведінки в Інтернет-просторі. Формування наднаціонального законодавства в сфері інформаційної безпеки дозволить подолати обмеженість національних законодавств в інформаційній сфері та в сфері кіберзлочинності.

4. Створення нових інститутів, що визначають рамки взаємодії і правил поведінки в Інтернет-просторі. Настав час вводити в міжнародне право такі нові поняття, як «електронна межа», «електронний суверенітет», «електронний податок» та інші. Необхідні закони, які дозволять боротися з економічними злочинами в Інтернеті на міжнародному рівні. Це сприятиме подоланню латентності кіберзлочинності, тобто підвищення показників розкриття кіберзлочинів.

Список використаних джерел.

1. Goodwin, C.D. Economics and National Security: A History of Their Interaction. – Durham, Duke University Press, 1991. – 217 p.
2. Jiang, Y. Economic Security: Redressing Imbalance. *China Security* – 2007. – V. 3, № 2. – P. 66–85.
3. Johnson S., Kaufmann D., McMillan J., Woodruff C. Why Do Firms Hide? Bribes and Unofficial Activity After Communism. *Journal of Public Economics*. Vol. 76. June 2000.
4. Kahler M. Economic security in an era of globalization: definition and provision. *The Pacific Review*. – 2004. – T. 17, № 4. – P. 485– 502.
5. Nanto D.K. Economics and National Security. 6 Issues and Implications for U.S. Policy. *Congressional Research Service*, 2011. – 82 p.
6. Nesadurai H.S. Conceptualising economic security in an era of globalization: what does the East Asian experience reveal? – 2005. – P. 1–26.

7. Schneider F. Shadow Economies around the World: What do we Really Know? *European Journal of Political Economy*. 2005. № 21. pp. 598-642.
8. Де Сото Э. Иной путь. Невидимая революция в третьем мире/Пер. с англ. Б.Пинскер. – М.: Catallaxy, 1995.
9. Доси Дж., Нельсон Р. Введение в эволюционную экономическую теорию. *Вестник молодых ученых. Экономические науки*. 1999. № 4.
10. Нельсон Р., Уинтер С. Эволюционная теория экономических изменений. М.: Финстатинформ, 2000.
11. Ананьев А.А. Международная экономическая безопасность: анализ сущности, подходов и факторов. *Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки*. 2012. С. 270–275.
12. Барановский А.И. Финансовая безопасность в Украине (методология оценки и механизмы обеспечения). Киев: КНТЭУ, 2004. 760 с.
13. Бельков О.А. Понятийно-категориальный аппарат концепции национальной безопасности. *Информационный сборник «Безопасность»*. №3. 2004. с. 91-94.
14. Бочуров А.А., Курбанов А.Х., Литвиненко А.Н. Сравнительный анализ отечественного и зарубежного опыта обеспечения экономической безопасности оборонно-промышленного комплекса. *Известия Санкт-Петербургского государственного экономического университета*. 2018. № 3 (111). С. 99-106.
15. Загребельная А.В. Классификация угроз экономической безопасности. *Томский политехнический университет, г. Томск*. 2015. №1-008 С. 35.
16. Руденко М.Н., Долганова Я.А. Исследование и оценка факторов, влияющих на функционирование регионального механизма экономической безопасности. *Национальные интересы: приоритеты и безопасность*. 2018. Т. 14, № 3 (360). С. 465-479.
17. Чижиков Э.Н., Бардулин Е.Н., Бабенков В.И. Анализ угроз экономической безопасности в чрезвычайных ситуациях. *Известия РАН*. 2017. № 2 (97). С. 31-37.
18. Бодрунов С.Д., Демиденко Д.С., Плотников В.А. Реиндустриализация и становление «цифровой экономики»: гармонизация тенденций через процесс инновационного развития. *Управленческое консультирование*. №2 (10). 2018. С. 43-57.
19. Панченко О.А., Банчук Н.В. Информационная безопасность личности в современном информационном обществе. *Український журнал телемедицини та медичної телематики*. 2012. Т. 10, № 1. с. 106-107.
20. Шаститко А.Е. Новая институциональная экономическая теория. М.: Теис, 2002. с. 90
21. Харламов А.В., Адаменко К.В. Новая конкурентоспособность хозяйствующих субъектов и проблема обеспечения экономической безопасности. *Известия Санкт-Петербургского государственного экономического университета*. 2016. № 2 (98). С. 13-16.
22. Hewlett Packard website – Available at: <http://www.hp.com/country/us/en/welcome.html> – Title screen. (дата звернення: 28.06.2019).
23. Data Breach QuickView. 2017 Report. [Електронний ресурс]. – 2017. Available at: <https://pages.riskbasedsecurity.com/2017-ye-breach-quickview-report>. (дата звернення: 28.06.2019).

References.

1. Goodwin, C.D. (1991), *Economics and National Security: A History of Their Interaction*, Duke University Press, Durham, UK.
2. Jiang, Y. (2007), Economic Security: Redressing Imbalance, *China Security*, vol. 3, no. 2, pp. 66–85.
3. Johnson S., Kaufmann D., McMillan J., & Woodruff C. (2000), Why Do Firms Hide? Bribes and Unofficial Activity After Communism, *Journal of Public Economics*. vol. 76.
4. Kahler, M. (2004), Economic security in an era of globalization: definition and provision, *The Pacific Review*, vol. 17, no. 4, pp. 485– 502.
5. Nanto, D.K. (2011), Economics and National Security. 6 Issues and Implications for U.S. Policy, *Congressional Research Service*, p.82.
6. Nesadurai, H.S. (2005), Conceptualising economic security in an era of globalization: what does the East Asian experience reveal? vol. 5, pp. 1-26.
7. Schneider, F. (2005), Shadow Economies around the World: What do we Really Know? *European Journal of Political Economy*, vol. 21, pp. 598-642.
8. De Soto E (1995), *Inoy put. Nevidimaya revolyutsiya v tretyem mire* [Another way. An invisible revolution in the third world], Catallaxy, Moscow, Russia.
9. Dosi, J., & Nelson, R. (1999), “An introduction to evolutionary economics”, *Vestnik molodykh uchenykh. Ekonomicheskije nauki*, vol. 4.
10. Nelson, R., & Winter, S (2000), *Evoljutsionnaya teoriya ekonomicheskikh izmeneniy* [Evolutionary theory of economic change]. Finstatinform, Moscow, Russia.
11. Ananjev, A.A. (2012), “International economic security: analysis of the essence, approaches and factors”, *Nauchno-tehnicheskiye vedomosti Sankt-Peterburgskogo gosudarstvennogo politehnicheskogo universiteta. Ekonomicheskije nauki*, pp. 270-275.

12. Baranovskiy, A.I. (2004), *Finansovaya bezopasnost v Ukraine (metodologiya otsenki i mekhanizmy obespecheniya)* [Financial security in Ukraine (assessment methodology and security mechanisms)]. KNTEU, Kiev, Ukraine.
13. Belkov, O. A. (2004), "Conceptual and categorical apparatus of the national security concept", *Informatsionnyy sbornik "Bezopasnost"*, vol. 3, pp. 91-94.
14. Bochurov, A.A., Kurbanov, A.Kh., & Litvinenko, A.N. (2018). "Comparative analysis of domestic and foreign experience in ensuring the economic security of the military-industrial complex". *Izvestiya Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta*, vol. 3, no. 111, pp. 99-106.
15. Zagrebelnaya, A.V. (2015), "Classification of threats to economic security", *Tomskiy politekhnicheskiiy universitet*, vol. 1, no. 8., p. 35.
16. Rudenko, M.N., & Dolganova, Ya.A. (2018), "Research and assessment of factors influencing the functioning of the regional mechanism of economic security", *Natsionalnyye interesy: priority i bezopasnost*, vol. 14, no. 3(360), pp. 465-479.
17. Chizhikov, E.N., Bardulin, Ye.N., & Babenkov, V.I. (2017), "Analysis of threats to economic security in emergency situations", *Izvestiya RARAN*, vol. 2, no. 97, pp. 31-37.
18. Bodrunov, S.D., Demidenko, D.S., & Plotnikov, V.A. (2018), "Reindustrialization and the formation of a "digital economy": harmonization of trends through the process of innovative development", *Upravlencheskoye konsultirovaniye*, vol. 2, no. 10, pp. 43-57.
19. Panchenko, O.A. & Banchuk, M.V. (2012), "Information security of a person in a modern information society", *Ukrayinskyy zhurnal teledytsyny ta medychnoyi telematyky*, vol. 10, no. 1, pp. 106-107.
20. Shastitko, A.Ye. (2002), *Novaya institutsionalnaya ekonomicheskaya teoriya* [New institutional economics], Theis, Moscow, Russia.
21. Kharlamov, A.V., & Adamenko, K.V. (2016), "New competitiveness of business entities and the problem of ensuring economic security", *Izvestiya Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta*, vol. 2, no. 98, pp. 13-16.
22. The official site of Hewlett Packard, Available at: <http://www.hp.com/country/us/en/welcome.html>. (Accessed 28.06.2019)
23. The official site of Risk Based Security, (2017) "Data Breach QuickView. 2017 Report", Available at: <https://pages.riskbasedsecurity.com/2017-ye-breach-quickview-report>. (Accessed 28.06.2019)

Стаття надійшла до редакції 20.07.2019 р.