УДК 341.123(045)

Любохинець Л.С.,
кандидат економічних наук, доцент,
доцент кафедри економічної теорії,
Хмельницький національний університет
Поплавська О.В.,
викладач кафедри економічної теорії,
Хмельницький національний університет

СВІТОВА ПРАКТИКА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНОМУ ГЛОБАЛІЗОВАНОМУ СЕРЕДОВИЩІ

Любохинець Л.С., Поплавська О.В. Світова практика забезпечення інформаційної безпеки в сучасному глобалізованому середовищі. У статті проаналізовано особливості формування безпеки інформаційного середовища. Визначено критерії оцінки, форми та методи забезпечення інформаційної безпеки. Висвітлено вплив інформаційних загроз на стан економіки в умовах інтенсивності розвитку глобалізаційних процесів у світовій економіці. Охарактеризовано специфіку впливу інформаційних загроз на зниження рівня економічної безпеки національної економіки.

Ключові слова: інформаційна безпека, інформаційне середовище, інформаційні загрози, модель тріади CIA, інформаційний патронат, інформаційна кооперація, інформаційне протиборство.

Любохинец Л.С., Поплавская О.В. Мировая практика обеспечения информационной безопасности в современной глобализированной среде. В статье проанализированы особенности формирования безопасности информационной среды. Определены критерии оценки, формы и методы обеспечения информационной безопасности. Освещено влияние информационных угроз на состояние экономики в условиях интенсивности развития глобализационных процессов в мировой экономике. Охарактеризована специфика влияния информационных угроз на снижение уровня экономической безопасности национальной экономики.

Ключевые слова: информационная безопасность, информационная среда, информационные угрозы, модель триады CIA, информационный патронат, информационная кооперация, информационное противостояние.

Liubokhynets L.S., Poplavska O.V. Worldwide practice for providing information security in the modern globalized environment. In the article the features of the security information environment analyzed. The evaluation criteria, forms and methods of information security defined. The influence of information threats on the state of the economy in the conditions of the intensity of globalization processes' development in the world economies highlighted. The specificity of information threats' influence to reduce the level of economic security of the national economy characterized.

Key words: information security, information environment, information threats, CIA triad model, information patronage, information co-operation, information confrontation.

Постановка проблеми. Інтенсивність перебігу глобалізаційних процесів у світовій економіці, зміцнення влади транснаціональних компаній, політичних та інформаційних транснаціональних систем вимагають від України відповіді на низку важливих економічних та політичних викликів, визначальними серед яких є необхідність формування єдиного інформаційного простору, здатність до своєчасного й ефективного впровадження передових досягнень у галузях науки, техніки і новітніх технологій, уніфікація інформаційних та телекомунікаційних технологій, створення розвиненого і захищеного інформаційного середовища.

З розвитком інформаційних технологій відбувається і розвиток кіберзлочинності, яка використовує у своїх протизаконних діях вразливі сторони інформаційних систем. Останні три роки для України були особливо насичені інцидентами з порушення роботи елементів інформаційних та телекомунікаційних систем, що є елементами критичної інфраструктури. Тільки за 2016 рік Службою безпеки України зафіксовано 247 кібератак на інформаційно-телекомунікаційні системи дипломатичних установ, правоохоронних структур, енергетичних ресурсів та ресурсів залізної дороги тощо [1, с. 64].

Нині актуальною стає проблема захисту власної інформації та інформації національного рівня. Через незахищеність нашої інформаційної безпеки ми піддаємось кібератакам з боку різних країн, організацій та «хакерів». Всі вони спрямовані на дезорієнтацію населення та на вчинення збитків в соціальній, економічній та політичній сферах держави. Тому актуальним є питання формування сучасної системи інформаційної безпеки, що дає можливість проаналізувати стан захищеності національних інтересів в інформаційному середовищі від зовнішніх та внутрішніх загроз.

Аналіз останніх досліджень і публікацій. Розгляду питань інформаційної безпеки приділяють увагу в своїх дослідженнях В. Артемов, З. Бжезинський, Л. Браун, Г. Кіссінджер, Б. Кормич, В. Ліпкан,

В. Мунтіян, В. Сідак, О. Соснін, О. Степко, Ч. Флавін, Х. Френч, В. Харченко та інші науковці. Проблеми забезпечення інформаційної безпеки аналізують Є. Архипова, І. Березовська, І. Залєвська, Ю. Грицюк, О. Тихомиров. Дослідження сучасних загроз інформаційній безпеці держави ґрунтується на наукових дослідженнях В. Горбуліна, Є. Скулиша, І. Івченко, Р. Калюжного, В. Ліпкана, А. Марущака, Г. Новицького, М. Стрельбицького. Проте, загрози інформаційній безпеці держави в сучасних умовах є динамічними та постійно змінюються, тому питання визначення механізму забезпечення інформаційної безпеки держави залишається нині актуальним.

Формулювання цілей статті. Метою статті є аналіз методів, форм та способів забезпечення інформаційної безпеки, визначених практикою зарубіжних країн, та формування національних інтересів в інформаційному середовищі для виявлення загроз інформаційній системі країни.

Виклад основного матеріалу. Проникнення інформаційних технологій в різні сфери суспільного розвитку приводить до швидкого зростання інформації, яку необхідно захищати з метою збереження її конфіденційності. Якщо в системі захисту інформації є недоліки, то базам даних можуть бути нанесені збитки, які будуть виражатись в порушенні цілісності, втраті необхідної інформації, передачі важливих даних стороннім особам. Кожне порушення роботи механізму захисту бази даних може паралізувати роботу цілих корпорацій, призвести до значних матеріальних втрат. В 2017 році випадкові втрати даних в результаті необережності досягли найвищого рівня. Хоча вони є причиною лише 18% інцидентів у сфері інформаційної безпеки, вони призвели до втрати 1,6 млрд. записів з баз даних, зокрема компанії "Rivers City Media", що склало 86% від всієї кількості викрадених даних. В першому півріччі 2017 року було зареєстровано 918 порушень безпеки в рамках проекту "Gemalto's Bresch Level Index", що призвело до втрати майже 2 мільярдів записів, що на 164% більше, ніж за весь 2016 рік [2].

Дефініція інформаційної безпеки розглядається вченими в аспектах аналізу інформаційного середовища, концепцій та стратегій інформаційної безпеки особи, держави та підприємства, видів, принципів, форм та способів забезпечення інформаційної безпеки, визначення її загроз. В загальному визначенні інформаційна безпека розглядається як стан захищеності інформаційного середовища суспільства від внутрішніх та зовнішніх інформаційних загроз, який забезпечує його формування, використання й прогресивний розвиток в інтересах особистості, суспільства, суб'єктів господарювання та держави. При цьому під інформаційним середовищем розуміють певну сферу діяльності суб'єктів економічної системи зі створення, перетворення та використання інформації.

Інформаційна безпека є важливим фактором з боку маніпуляторів, хто хоче так чи інакше захопити вплив над людиною, групою людей, корпорацією чи країною. Якщо раніше для того, щоб захистити країну, потрібна була сильна, вміла та численна армія з різними видами озброєння, то в нинішній час потрібно декілька вмілих людей, які вміють керувати інформацією, вміють подати її так, як потрібно, вміють спрямувати її туди, куди потрібно, з тією чи іншою метою.

Інформаційна безпека посідає особливе місце в системі національної безпеки, тому загрози інформаційного характеру можуть спрямовуватись до будь-яких структурних складових національної безпеки, однак їх негативний вплив завжди опосередковуватиметься завданням шкоди інформаційній безпеці держави. Зокрема, економічна безпека в сучасних умовах інформаційно-мережевої економіки безпосередньо залежить від безпеки інформаційної, адже головним ресурсом розвитку виробництва стає інформаційний продукт [3, с. 162]. Під впливом інформаційних атак можуть змінюватися світогляд і мораль як окремих осіб, так і суспільства загалом, нав'язуються чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності й форм виявів сучасних методів прихованого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які суперечать інтересам національної безпеки [4]. Отже, система загроз інформаційній безпеці має комплексний характер і в загальному вигляді включає в себе загрози безпеці інформації та інформаційної інфраструктури; загрози безпеці суб'єктів інформаційної сфери й соціальних зв'язків між ними від інформаційних впливів; загрози належному порядку реалізації прав та інтересів суб'єктів інформаційної сфери. Таким чином, загрози інформаційній безпеці держави виступають сукупністю умов і факторів, які становлять небезпеку життєво важливих інтересів держави, суспільства й особи у зв'язку з можливістю негативного інформаційного впливу на свідомість і поведінку громадян, а також інформаційні ресурси та інформаційно-технічну інфраструктуру [5, с. 183].

Специфіка впливу інформаційних загроз на зниження рівня економічної безпеки виявляється на державному, корпоративному й особистісному рівнях. Серед загроз на державному рівні виділяють кібершпіонаж і маніпулювання унікальною інформацією, що веде до порушення стійкого розвитку економіки, ослаблення валюти, нереалізації намічених програм, підриву інвестиційних проектів; ведення інформаційних війн, що веде до відставання ВВП, викликаному зростанням непродуктивних витрат, формування нового сегменту тіньової економіки «чорного» кіберринку, порушення ринкових механізмів і принципів конкуренції, монополізації економіки; інформаційне домінування розвинених країн веде до вилучення технологічної ренти цими країнами, посилення економічної залежності від розвинених країн, витіснення країн, що розвиваються, зі світового інформаційного ринку; інформаційна нерівність всередині країни посилює економічну диференціацію суспільства. Так, внаслідок кібератаки 6 грудня 2016 року було виведено з ладу мережу Державної казначейської служби та Міністерства фінансів України, що призвело до порушення казначейського обслуговування розпорядників та одержувачів бюджетних коштів, тобто трапилася надзвичайна подія в системі, де зазвичай здійснюється близько ста п'ятдесяти тисяч електронних транзакцій за добу. На початку 2017 року, як зазначалось у звіті за 2 квартал 2017 року компанії "Panda Security", маркетингові компанії, які були найняті Республіканською партією США, порушили конфіденційність інформації і відкрили публічний доступ до особистих даних 198 млн. виборців з майже 200 млн. виборців США [6, с. 14].

На корпоративному рівні навмисні і ненавмисні ушкодження інформаційних систем та інфраструктури завдають прямих фінансових збитків і вимагають додаткових витрат на відновлення пошкодженого обладнання; зовнішній і внутрішній кібершпіонаж, а також недбалість персоналу призводять до втрати конкурентних переваг, зниження довіри до фірми, втрати частки ринку і доходів; безконтрольний доступ співробітників до мережі Інтернет знижує продуктивність праці і збільшує втрати робочого часу. Так, в першій половині 2017 року були проведені дві найбільші кібератаки "WannaCry" та "GoldenEye/Petya", від яких постраждали майже всі країни світу і велика кількість компаній, більше 230 000 комп'ютерів. Згідно з різними оцінками експертів втрати від цих атак склали від 1 до 4 млрд. дол. США, тобто від 4 300 до 17 000 дол. в розрахунку на кожний комп'ютер. В цей же період був атакований веб-хостінг "Nayana" в Південній Кореї, в результаті чого було зашифровано даних на 153 серверах "Linux". Злочинці вимагали викуп в розмірі 1,62 млн. дол. США, але після перемовин компанія виплатила їм 1 млн. дол. США [6, с. 11–12].

На особистісному рівні кібершпіонаж з використанням банківських карт призводить до втрати грошових коштів власниками кредитних і депозитних банківських карт; кібершахрайство в мережі Інтернет, SMS-шахрайство призводять до прямих втрат коштів абонентів; атаки на системи, які масово використовуються в повсякденному житті, знижують рівень задоволення поточних потреб людей; інтернет-залежність, інформаційні хвороби призводять до скорочення робочого часу, втрати професійних характеристик, непродуктивних витрат часу і нераціонального витрачання грошових коштів. В червні 2017 року "WannaCry" в Австралії заразив 55 камер, які контролювали швидкість на дорозі і були розташовані на світлофорах, після чого поліція була вимушена відмінити 8 000 штрафів, виписаних за перевищення швидкості [6, с. 16].

Для визначення вимог захисту інформації від несанкціонованого доступу, створення захисних систем та оцінки ступеня захищеності використовують систему критеріїв оцінки інформаційної безпеки, за допомогою яких можна порівняти різні механізми захисту інформаційних систем та визначити напрями вдосконалення мережевої та інформаційної безпеки. Для характеристики основних критеріїв інформаційної безпеки досить часто застосовують модель тріади CIA [7], а саме конфіденційності, цілісності та доступності (рис. 1).

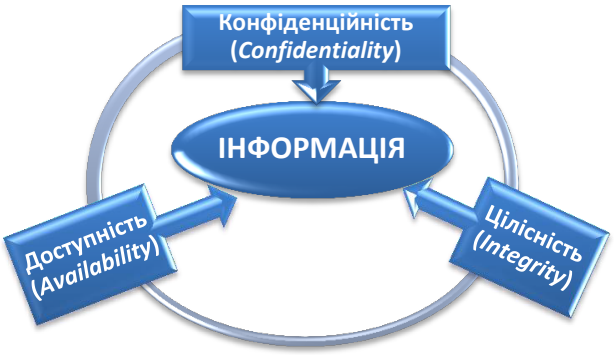

Рис. 1. Модель інформаційної безпеки тріади CIA

При цьому конфіденційність (англ. *confidentiality*) – це захист від несанкціонованого ознайомлення з інформацією, тобто інформація не може бути отримана неавторизованим користувачем; цілісність (англ. *integrity*) – це неможливість модифікації інформації неавторизованим користувачем, захист від руйнування і несанкціонованих змін; доступність (англ. *availability*) – це можливість отримати будь-яку інформацію за наявності у суб'єкта відповідних повноважень в необхідний для нього час.

Забезпечення доступності, цілісності та конфіденційності кіберпростору стало однією з глобальних проблем XXI століття та метою ефективного функціонування держави, економіки та суспільства загалом.

Аналогічно до моделі тріади CIA в Україні департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України було розроблено та застосовано низку нормативних документів для визначення критеріїв оцінки безпеки інформаційних технологій та систем. До них відносять, наприклад, нормативний документ технічного захисту інформації 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». Для забезпечення інформаційної безпеки підприємства також використовуються міжнародні стандарти ISO (ISO/IEC 17799:2005, ISO/IEC 27001:2013 тощо) для підтримки рішень на основі ITIL та COBIT і виконання вимог акта Сербайнза-Оклі про відповідальність акціонерів за обізнаність про стан своїх активів.

Разом з моделлю CIA для характеристики критеріїв інформаційної безпеки використовують такі властивості, як апелювання (можливість доведення авторства конкретної особи), підзвітність (можливість фіксації діяльності користувачів інформаційної системи), достовірність (ступінь об'єктивного, точного відображення подій та фактів, що мали місце у визначений період часу), автентичність (гарантування ідентичності заявленим суб'єктам або ресурсам).

Існують різні методи та способи забезпечення інформаційної безпеки. Завдання забезпечити інформаційну безпеку в країні означає задіяння всіх доступних методів та заходів задля захисту потреб суспільства, окремих особистостей та самої держави в інформації. Державним забезпеченням інформаційної безпеки займаються організаційні об'єднання державних органів на основі правових та нормативних актів. Таким чином, найважливіша вимога до обґрунтування способів, форм і механізмів їхньої реалізації полягає в абсолютному верховенстві права в будь-якій, зокрема політичній, діяльності. Кожний суб'єкт інформаційного процесу повинен мати відповідну правову свідомість, бути законослухняним, добре уявляти наслідки своїх дій для інших суб'єктів та ступінь відповідальності в разі порушення їхніх життєво важливих інтересів. Це є принциповим, оскільки застосування тих чи інших форм і способів залежить від того, чи є інформаційні загрози наслідком ненавмисних або навмисних дій суб'єктів інформаційного процесу. У першому випадку забезпечення інформаційної безпеки здійснюється у формах інформаційного патронату та інформаційної кооперації, у другому – інформаційного протиборства [8, с. 100].

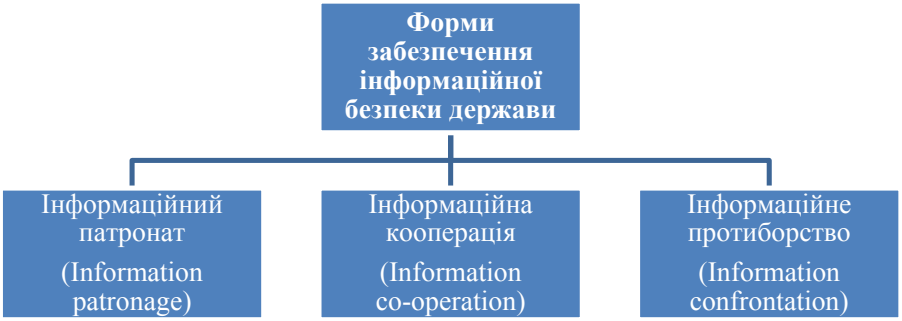

Рис. 2. Основні форми забезпечення інформаційної безпеки держави [8, с. 100]

Інформаційним патронатом називається форма забезпечення інформаційної безпеки з боку держави фізичних та юридичних осіб. Інформаційне забезпечення безпеки включає добування різноманітних відомостей про дестабілізуючі фактори та інформаційні загрози, обмін інформацією між органами управління та засобами системи інформаційної безпеки. Інформаційний захист здійснюється різними шляхами, а саме від прийняття законопроектів до вжиття оперативних заходів силами інформаційної безпеки в процесі розвідувальної, контррозвідувальної, оперативно-розшукової та оперативно-інформаційної діяльності.

Інформаційною кооперацією є форма забезпечення інформаційної безпеки між рівноправними суб'єктами інформаційного процесу, що включає сукупність взаємоузгоджених дій, спрямованих на отримання відомостей про дестабілізацію інформаційної безпеки в країні, інформаційні загрози та методи боротьби з ними. Україна активно співпрацює зі світовими організаціями безпеки та охорони інформації. Так, Державна служба спеціального зв'язку та захисту інформації України і компанія "Microsoft" у грудні 2014 року уклали Угоду про співробітництво з питань безпеки (Government Security Program), в рамках якої держава отримує доступ до інформації, що збирається в центрі Безпекового реагування компанії "Microsoft" про нові кіберзагрози, джерела мережевих атак. При цьому окремим елементом Угоди є Програма безпекової кооперації, за якою урядові організації спільно з "Microsoft" мають змогу реагувати на комп'ютерні інциденти та запобігати наслідкам кібератак.

Інформаційне протиборство – форма суперництва соціальних систем в інформаційній сфері щодо впливу на різні сфери соціальних відносин і встановлення контролю над джерелами стратегічних ресурсів, в результаті якого одна з груп отримає переваги, які потрібні їм задля подальшого розвитку. Інформаційне протиборство відбувається між різними видами соціальних суб'єктів, але цілі ряди таких взаємодій утворюють окремі форми протиборства (інформаційні війни, злочинність, тероризм).

Інформаційна війна – це явище, за якого здійснюється сильний вплив на інформаційну сферу противника, яке створює підґрунтя для початку «бойових дій» (інформаційних). Під час ведення інформаційної війни використовується широкий спектр різноманітних засобів, за допомогою яких вживається заходів щодо деструктивного впливу на інформаційну сферу ворога. Під час інформаційних війн проводяться інформаційні операції, завданням яких є вплив на аудиторію задля побудови її свідомості. Якщо така операція виявиться вдалою, ворог зможе безперешкодно управляти аудиторією. Такі операції найчастіше проводяться іноземними спецслужбами в межах таємних місій з метою підриву та зміни суспільної думки суспільства на негативну та протиправну, що полегшить послаблення суспільного ладу.

Серед методів інформаційних операцій досить часто виділяють дезінформування, пропаганду, психологічний тиск, поширення чуток. При цьому дезінформування визначають як психологічний вплив на суспільство, метою якого є подання такої інформації, яка введе об'єкт в оману щодо справжнього стану справ; пропаганду розглядають у формі чуток та суспільних комунікацій, які здійснюються з метою зміни суспільної думки на користь тієї чи іншої громадської позиції; психологічний тиск – це маніпулювання однієї людини іншою з метою контролювання чужої поведінки; поширення чуток – форма умисного поширення помилкової інформації певними особами чи групами осіб з метою підриву чиєїсь громадської позиції, а також уведення суспільства у стан плутанини.

Висновки. Таким чином, інформаційна безпека є складним, системним, багаторівневим явищем, на стан якого впливають зовнішні і внутрішні чинники, зокрема політичний стан у світі; внутрішньополітичний стан в державі; стан і рівень інформаційно-комунікаційного розвитку країни. Загрози інформаційній безпеці здебільшого супроводжують виникненням та реалізацією загроз в економічний і політичній сферах, у сфері виконання функцій держави, тому заподіяння шкоди в інформаційні сфері є передусім засобом досягнення інших цілей зловмисників. Але традиційні рішення безпеки, хоча і є ефективними під час захисту від відомих загроз, все ж не здатні захищати від атак, які використовують нешкідливі інструменти та інші вдосконалені техніки. Виникнення професійних кіберзлочинних груп, злом виборчих систем в різних країнах світу, витік інструментів шпигунства, а також масовані атаки з державною підтримкою – всі ці фактори перевели кібервійну на найвищий рівень, змінюючи основи інформаційної безпеки в усьому світі. Тому інформаційна безпека все частіше розглядається як стратегічний напрям політики держави, спрямованої на посилення безпеки та надійності національних інформаційних систем.

Список використаних джерел:

1. Залєвська І. Інформаційна безпека України в сучасних умовах: політичний аспект : дис. … канд. політ. наук / І. Залєвська. – О., 2012 – 177 с.
2. Количество инцидентов с кражей данных продолжает расти [Електронний ресурс]. – Режим доступу : https://www.securitylab.ru/blog/company/PandaSecurityRus/342992.php.
3. Цивілізаційний вибір України: парадигма осмислення і стратегія дії : національна доповідь / [ред. кол.: С. Пирожков, О. Майборода, Ю. Шайгородський та ін.]. – К. : НАН України, 2016. – 284 с.
4. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки / Г. Сащук [Електронний ресурс]. – Режим доступу : http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php/
5. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз / Т. Ткачук // Підприємництво, господарство і право. – 2017. – № 10. – С. 182–186.
6. Pandalabs – Отчет за 2 квартал 2017 года [Електронний ресурс]. – Режим доступу : https://pandasecurity.bitrix24.ru/docs/pub/1c3e16b44b7eced067ca1ceb9ae381ce/default/?&.
7. Thor Olavsrud. 4 information security threats that will dominate 2017. CIO (December 29, 2016) [Електронний ресурс]. – Режим доступу : https://www.cio.com/article/3153706/security/4-information-security-threats-that-will-dominate-2017.html.
8. Лук'янова В. Інформаційна безпека в умовах розвитку інформаційних систем / В. Лук'янова, А. Лаутар // Вісник Хмельницького національного університету. Серія: Економічні науки. – 2013. – № 2. – Т. 3. – С. 97–101.
9. Аналіз механізмів реалізації мережевих атак прикладного рівня в інтересах проведення криміналістичних розслідувань кіберзлочинів / [А. Снігуров, В. Балашов, А. Сердюк] // Збірник наукових праць Харківського національного університету повітряних сил. – 2017. – Вип. 2 (51). – С. 64–68.

УДК 352.07:336.1

Манойленко М.В.,
аспірант,
Міжнародний університет бізнесу та права

ФІНАНСОВА ДЕЦЕНТРАЛІЗАЦІЯ ЯК ОСНОВА РОЗВИТКУ МІСЦЕВИХ БЮДЖЕТІВ

Манойленко М.В. Фінансова децентралізація як основа розвитку місцевих бюджетів. У статті наводяться результати дослідження фінансової децентралізації як основи формування самодостатніх територіальних громад, умови реалізації її основних принципів на сучасному етапі розвитку України.

Ключові слова: фінансова децентралізація, місцеві бюджети, державна політика.

Манойленко М.В. Финансовая децентрализация как основа развития местных бюджетов. В статье приводятся результаты исследования финансовой децентрализации как основы формирования самодостаточных территориальных общин, условия реализации ее основных принципов на современном этапе развития Украины.

Ключевые слова: финансовая децентрализация, местные бюджеты, государственная политика.

Manoylenko M.V. Financial decentralization as the basis for the development of local budgets. In the article the research results of fiscal decentralization as the basis for the formation of communities self-sufficient, conditions for the implementation of the basic principles at the present stage of development of the Ukrainian state.

Key words: fiscal decentralization, local governments, public policy.

Постановка проблеми. Чинна система місцевого самоврядування в Україні навіть за існування законодавчо-правового підґрунтя (в Конституції України закладено засади місцевого самоврядування, ратифіковано Європейську хартію місцевого самоврядування, прийнято низку базових нормативно-правових актів щодо діяльності органів місцевого самоврядування) [1] вирізняється неефективністю та нездатністю задовольнити потреби суспільства в наданні високоякісних і доступних адміністративних, соціальних та інших послуг. Із сформованих близько 12 тисяч територіальних громад більшість через надмірну подрібненість та надзвичайно слабку матеріально-фінансову базу неспроможні виконувати всі повноваження органів місцевого самоврядування, а необхідність в їх фінансовій підтримці шляхом дотацій вирівнювання несе додаткове навантаження для державного бюджету, стримує розвиток як держави загалом, так і більш фінансово спроможних територіальних одиниць зокрема.

Аналіз останніх досліджень і публікацій. Дослідженням цієї проблеми займалися українські та зарубіжні вчені, такі як В.А. Лебедєв, Д.П. Боголепов, В. Оутс, В.Л. Андрущенко, О.П. Кириленко, О.С. Дрезденська, Ч. Тібо, Р. Масгрейв, Л.І. Якобсон, О.О. Сунцова, Д.В. Полозенко, Ю.А. Глущенко.

Проведення масштабної реформи державного управління з перерозподілом функцій, повноважень і