

Олена Сидорович

доктор економічних наук, професор,
Західноукраїнський національний університет,
м. Тернопіль, Україна
o.sydorovych@wuni.edu.ua
ORCID ID: 0000-0002-4605-3533

Антон Шевчук

кандидат економічних наук, доцент,
Західноукраїнський національний університет,
м. Тернопіль, Україна
Shevchukanton@ukr.net
ORCID ID: 0000-0002-1681-1153

СТРАТЕГІЧНІ ВЕКТОРИ ПОДАТКОВОГО МЕНЕДЖМЕНТУ В УМОВАХ ЦИФРОВИХ ТРАНСГРЕСІЙ ТА ГІБРИДНИХ ЗАГРОЗ

Olena Sydorovych

Dr. Sc. (Economics), Professor,
West Ukrainian National University,
Ternopil, Ukraine

Anton Shevchuk

PhD in Economics, Associate Professor,
West Ukrainian National University,
Ternopil, Ukraine

STRATEGIC VECTORS OF TAX MANAGEMENT IN THE CONTEXT OF DIGITAL TRANSGRESSIONS AND HYBRID THREATS

Анотація. Функціонування людства в сучасних умовах характеризується масштабним впливом тенденцій глобального масштабу, серед яких найбільш значимими є стрімка експансія інформаційних технологій, що, по-перше призводить до глибоких цифрових трансгресій в економіці, суспільстві і процесах державотворення; та, по-друге, зростання гібридних викликів і загроз, які виступають симбіозом військових, економічних, інформаційних, та політичних методів впливу. В цих умовах традиційні підходи до реалізації податкового менеджменту стають недостатніми, а розробка та впровадження нових, адаптивних стратегій набуває критичного значення для забезпечення фінансової стабільності держави, підтримки економічного розвитку та протидії зовнішнім загрозам. Дослідження присвячене окресленню стратегічних векторів реалізації податкового менеджменту в умовах сучасних цифрових трансгресій а також гібридних викликів і загроз.

Ключові слова: податковий менеджмент, гібридні виклики і загрози, цифрова трансгресія, кібербезпека, податкова інфраструктура.

Abstract. *The functioning of humanity in modern conditions is characterized by the large-scale impact of a number of global trends, among which the most significant are the rapid expansion of information technologies, leading to profound digital transgressions in the economy, society, and state-building processes; and, secondly, the growth of hybrid challenges and threats, which act as a symbiosis of military, economic, informational, and political methods of influence. In these circumstances, traditional approaches to the implementation of tax management are becoming insufficient, and the development and implementation of new, adaptive strategies is of critical importance for ensuring the financial stability of the state, supporting economic development, and countering external threats. The study is dedicated to outlining the strategic vectors of tax management under modern digital transgressions and hybrid threats. The goal of formulating tax management strategies at the state level will be to manage taxation processes at the national level by ensuring budget revenues, regulating economic development, and achieving social goals; at the enterprise level – to optimize tax liabilities, minimize risks, and maximize profit; and at the individual level – to utilize tax benefits and methods for minimizing tax liabilities.*

At the state level, key priorities include strengthening digital control over financial flows, active international cooperation in the taxation of the digital economy, and the establishment of robust cybersecurity systems to protect critical tax infrastructure. Corporate tax management facilitates adaptation to new taxation models associated with digital activities, while simultaneously enhancing cybersecurity systems to protect commercial and financial information. At the level of households or individual entrepreneurs, digital transgression necessitates an increase in their level of tax literacy regarding income from digital sources and an awareness of online fraud risks.

Keywords: tax management, hybrid challenges and threats, digital transgression, cybersecurity, tax infrastructure.

Вступ. Сучасний етап розвитку людства позначений безпрецедентно складними та глибокими трансформаціями, зумовленими екзогенними та ендегенними факторами впливу на кшталт стрімкого технологічного та інформаційного прогресу, глобальних екологічних, пандемічних, військових, соціальних викликів, міжнародної нерівності та геополітичної нестабільності, нейтралізація та превенція яких визначили якісно новий контекст існування людської цивілізації, актуалізуючи гостру необхідність переосмислення усталених парадигм розвитку держав та узгодження процесів державотворення.

Управління державними фінансами в умовах динамічних змін та зростаючих загроз в означених координатах розвитку опиняється під значним тиском, оскільки завдання забезпечення макроекономічної стабільності, сталого економічного розвитку, фінансування суспільно значущих програм та виконання соціальних зобов'язань вимагає застосування інноваційних інструментів та підходів, ефективність використання яких ускладнюється функціонуванням держави в умовах військової агресії рф, економічної, соціальної, екологічної, демографічної

криз нею зумовлених. Разом з тим, дієвість фінансових механізмів державотворення без перебільшення є визначальною умовою забезпечення національної безпеки, соціально-економічної стійкості держави, та її існування загалом.

В умовах такої складної та динамічної реальності, ефективне управління державними фінансами, значною мірою залежить від їх ключової складової в частині управління процесами оподаткування, що традиційно у фаховій літературі зводиться до сфери податкового менеджменту.

Окреслення сутності та практичного застосування податкового менеджменту є усталеною темою в фахових дослідженнях і публікаціях вітчизняних вчених, зокрема В. Андрущенко, З. Варналія, О. Данілова, О. Десятнюк, Ю. Іванова, М. Карліна, А. Кізими, А. Крисоватого, М. Крупки, В. Мельника, С. Онишко, А. Соколовської, К. Швабія та ін.

Автори також неодноразово здійснювали наукові розвідки в царині функціонування податкового менеджменту на різних рівнях загалом та аналізу синергійних елементів та ефектів зокрема [1]. Однак, сучасний етап досліджень характеризується значно ширшим охопленням та глибшим розумінням податкового менеджменту як складного та багатовимірного явища, порівняно з ранніми спробами його осмислення в період становлення незалежності України. Це проявляється у масштабнішому пізнанні його сутності та розширених можливостях практичної реалізації відповідно до сучасних економічних і соціальних цілей, пріоритетів розвитку та актуальних викликів. Якщо, на початковому етапі податковий менеджмент трактувався переважно з позицій теоретичного обґрунтування процесів управління обліком платників, податковими зобов'язаннями та своєчасністю їх сплати, то нинішнє трактування зводиться до розуміння його як комплексної системи управління податковими відносинами, що базується на сукупності методів та прийомів їх організації для забезпечення доходів державного бюджету та оптимізації податкових платежів платників з одночасною мінімізацією податкових ризиків.

Виділення невирішених раніше частин загальної проблеми. Не дивлячись на достатньо велику кількість наукових праць, які присвячені розгляду теоретичних, методичних та практичних аспектів податкового менеджменту, функціонування податкової системи України в сучасних умовах зумовлюється новими, не повною мірою дослідженими проблемами, пов'язаними з впливом цифрових трансформацій та гібридних викликів і загроз на сферу управління процесами оподаткування. Саме тому, виникає потреба в детальному дослідженні, всебічному аналізі та комплексній оцінці викликів, які постають перед державою в частині реалізації заходів управлінського впливу в сфері оподаткування, та, безпосередньо, фахівцями, які забезпечують стабільне виконання фіскальних функцій.

Формулювання цілей дослідження зумовлене завданнями обґрунтування стратегічних напрямів розвитку податкового менеджменту в контексті впливу цифровізації та гібридних загроз, зі здійсненням комплексної оцінки можливостей і ризиків, які супроводжують ці процеси для забезпечення фінансової стабільності держави та її економічного розвитку.

Виклад основної частини дослідження. Сучасний глобалізований світ є ареною складних геополітичних процесів, що характеризуються зростанням напруженості між

окремими країнами та регіонами, поширенням гібридних форм конфліктів, боротьбою за ресурси та вплив. Впродовж багатьох століть війни між суверенними державами здійснювались з метою силового підпорядкування противника шляхом використання організованих військових угруповань від початку до завершення військової агресії і були традиційними для військових конфліктів до середини XX століття.

Повномаштабне вторгнення та відкриті військові дії 24.02.2022 року стали максимально «гарячою» фазою реалізації гібридної військової, політичної, інформаційної, ідеологічної та економічної стратегії росії, що реалізовувалась нею впродовж багатьох років з метою повернення України в її поле впливу та контролю. Військові дії на значній території України зумовили глибоку соціально-економічну кризу та значні зміни в структурі доходів і видатків Державного бюджету України. За підсумками 2022 року, не дивлячись на те, що дохідна частина державного бюджету була виконана з приростом (+15,1%), однак її ключову частину становили надходження від фінансової та грантової допомоги. Внаслідок військової агресії відбулася значна втрата податкової бази, зокрема податкові надходження до Державного бюджету України склали 949,8 млрд грн, що на 157,3 млрд грн, або на 14,2% було менше ніж у довоєнному 2021 році [2]. В результаті, мало місце скорочення питомої ваги податкових надходжень на 32,2%, з 85,4% – у 2021 р. до 53,1% від загального обсягу доходів – у 2022 р. Найбільші втрати припали на митні платежі: ПДВ (-33,5% у 2022 р. порівняно з 2021 р.) та акцизний податок (-47,7% у 2022 р. порівняно з 2021 р.) із ввезених товарів, ввізного мита (-36,7% у 2022 р. порівняно з 2021 р.).

Здійснювані проти нашої держави заходи були типовим прикладом війни нового типу, в основу якої покладено принципово інший тип організованої загарбницької стратегії з поєднанням гібридних важелів насильницького впливу на основі використання суміші військової агресії, організованої злочинності, терористичних атак, проведення інформаційних та дезінформаційних кампаній з метою нівелювання ролі державних інституцій та масованого впливу інформаційно-комунікаційних технологій.

Глобалізаційні трансформації посилили взаємозалежності національних економік, культур та політичних систем, одночасно спровокувавши появу значних суперечностей, зумовлених розривом між багатими та бідними країнами, руйнуванням усталених принципів міжнародної безпеки, формуванням нових форм союзів та групувань, що, в підсумку, лише посилює транснаціональні ризики, загрози міжнародного тероризму та кіберзлочинності. Остання, охоплює широкий спектр незаконних дій, що реалізуються за допомогою інформаційно-комунікаційних систем та мереж, включаючи фінансове шахрайство, крадіжки інтелектуальної власності, розповсюдження шкідливого програмного забезпечення, кібершпигунство, які здійснюються з метою завдання економічних збитків, або ж атаки на критичну інфраструктуру з ціллю завдання шкоди національній безпеці в системі заходів так званої «мякої» війни.

На думку колишнього генерального секретаря НАТО Є. Столтенберга, «існує морський, сухопутний і повітряний простір, тепер до них додався ще кіберпростір, який ми визначаємо як простір військових дій» [3]. Внаслідок

глобалізації та масового поширення інформаційних технологій, кіберпростір став досить специфічним середовищем, який здійснює масштабний вплив на розвиток економіки, політичне життя, культуру, технічну, військову та оборонну сферу, державне управління.

Анонімність та транскордонний характер кіберпростору визначають завданням підвищеної складності виявлення та притягнення до відповідальності кіберзлочинців, джерела загрози та ймовірних «кібератак», ідентифікації форми небезпеки та суб'єкта агресії. Якщо попередньо, джерело агресії ідентифікувалось задовго до початку активної фази ворожнечі, то в сучасних умовах досить важко встановити початок здійснення підливних дій та сформувавши прогнози їх подальшого розгортання та алгоритми придушення. Таким чином, лавиноподібний ріст цифрових тенологій, швидкісні темпи розвитку кіберпростору та поширення його використання окрім значних переваг стали каталізатором нового спектру загроз та підвищення рівня вразливості як держави так і її суб'єктів.

До прикладу, одна з наймасштабніших кібератак відбулась 19 грудня 2024 року, завдавши значної шкоди мережевій інфраструктурі державних органів, яка здійснювала обслуговування державних реєстрів. В результаті її здійснення було паралізовано роботу понад 60 з них, окремі з яких перебували в компетенції Міністерства юстиції, у тому числі реєстр актів цивільного стану громадян, реєстри довіреностей та боржників, Єдиний державний реєстр юридичних осіб та ФОП. При цьому, на відновлення роботи усіх реєстрів знадобилося більше місяця, такі реєстри як спадковий, реєстр довіреностей та спеціальних бланків нотаріальних документів вдалося запустити 30 грудня, 5 січня було відновлено роботу реєстру актів цивільного стану, а 20 січня 2025 року офіційно повідомлено про відновлення роботи інфраструктури державних реєстрів після кібератаки.

Окрім колапсу в системі державних органів, отриманого внаслідок кібератаки, значну шкоду було завдано і суб'єктам підприємництва, оскільки у застосунку Дія стали недоступними такі інформаційні модулі як реєстрація, внесення змін до ФОП чи ТОВ, отримання витягів з Єдиного державного реєстру юридичних осіб та ФОП, бронювання працівників тощо. Окрім цього, підприємці зіткнулися з неможливістю подання податкової звітності у звичний спосіб, що могло зумовити порушення податкових та юридичних зобов'язань.

Відповідальність за кібератаку взяла на себе група російських хакерів HakNet Team, на основі публічної заяви оприлюдненої ними у Telegram, хоча за даними СБУ за цим хакерським угрупованням стоять спецпідрозділи російського ГРУ.

Відмітимо, що минулого, 2024 року кількість кібератак на вітчизняну мережеву інфраструктуру, зокрема енергетичний сектор, урядові установи, органи безпеки тощо зросла майже на 70%, було зафіксовано 4315 таких випадків проти 2541 у 2023 році. За визначенням фахівців Державної служби спеціального зв'язку та захисту інформації України [4], основними інструментами за допомогою яких здійснюються кібератаки є масові розсилки небезпечного програмного забезпечення та фішингові листи. Для нейтралізації таких кіберінцидентів функціонує урядова команда реагування на їх появу та попередження CERT-UA, яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України [5].

Від початку повномасштабного вторгнення, фахівцями CERT-UA було зафіксовано більш ніж 10 тис кіберінцидентів, кількість яких збільшується щороку, див. рис.1.



Рис.1. Кількість зафіксованих кіберінцидентів фахівцями CERT-UA впродовж 2021- 2024 років

Джерело: складено авторами за даними CERT-UA

Як видно з даних рисунку, кількість кібератак у 2022 році, з початком повномасштабної війни зросла на 62,5% та становила 2194 випадки. За підсумками 2023 та 2024 років зростання становило 15% і 70% відповідно. Від початку 2025 року, станом на 19.03 кількість кіберінцидентів перевищило на 50% аналогічний показник 2024 року.

Окрім кібератаки здійсненої 19 грудня 2025 року, урядові інформаційні мережі та об'єкти критичної інфраструктури не раз зазнавали заходів кібервпливу, до прикладу:

14.01.2022 року хакери завдали кібератаки більш ніж 70 державним сайтам, а саме: «Дії», сайтам Кабінету Міністрів України, Міністерству охорони здоров'я, Міністерства закордонних справ, Державної служби з надзвичайних ситуацій, Міністерства освіти, Міністерства спорту, Міністерства аграрної політики, Міністерства енергетики, Міноборони, Державної казначейської служби та інших органів;

15.02.2022 року було атаковано засобами інформаційного впливу близько 15 банків, у тому числі ПриватБанк та Ощадбанк, та зазнали втручання сайти Міноборони, Міністерства з питань реінтеграції тимчасово окупованих територій.

23-24.02.2022 було здійснено кібератаку на сайти Кабміну, Верховної Ради, Міністерства закордонних справ, Служби безпеки України та інших органів влади;

12.12.2023 року була здійснена хакерська кібератака, відповідальність за яку взяло на себе хакерське угруповання «Сонцепьок» на найбільшого мобільного оператора зв'язку «Київстар», в результаті якої на основі проникнення в ІТ-структуру та часткове її руйнування стали недоступними послуги мобільного зв'язку та Інтернету. На відновлення роботи мереж знадобилося більше тижня, а сам мобільний оператор «Київстар» зазнав збитків на більш ніж 3,6 млрд. грн;

25.01. 2024 року кібервтручання зазнали дата-центр «Парковий», сервіси «Нафтогазу», Укрзалізниці, Укрпошти та системи «Шлях».

Особливою сферою «інтересу» хакерських угруповань в контексті здійснення кібератак проти України є втручання в інформаційні мережі фіскальних органів держави, використання фішингових листів, спроби зламу інформаційно-мережевої інфраструктури податкових та митних органів. Зокрема, 28.10.2024 року фахівцями CERT-UA були виявлені факти кібервтручання шляхом розповсюдження електронних листів з темами податкової тематики та вкладеннями у вигляді PDF-документів, що імітували запити Державної податкової служби України. Означені файли містили посилання на файловий сервіс (qaz.im, qaz.is, qaz.su), у випадку переходу за якими на комп'ютер завантажувався архів «dps_tax_gov_ua_0739220983.rar», у якому, з кількома рівнями вкладеності, знаходиться захищений паролем архів «Електронний запит документів податкової служби.pdf.rar», який, у свою чергу, містився SFX-файл «Електронний запит документів податкової служби.pdf.exe». Відкриття цього файлу зумовлював відображення користувачеві документу-приманки та запуску на комп'ютері MSI-паketу програми для віддаленого управління LITEMANAGER, що створював технічні передумови для несанкціонованого прихованого віддаленого доступу до комп'ютера користувача [5].

Такий кібервплив, за визначенням фахівців CERT-UA здійснюється хакерським угрупованням UAC-0050. В зоні їх інтересів є комп'ютерні мережі підприємств, на яких здійснюється робота з системами дистанційного банківського обслуговування. Про особливу небезпеку цього типу втручання свідчить той факт, що часто, від моменту первинного ураження до моменту викрадення грошових коштів з банківських рахунків суб'єктів господарювання проходило не більше години.

Заходи кібервпливу є одними з ключових інструментів, що здійснюються спецслужбами рф для дестабілізації ситуації в нашій державі і є новітніми інструментами кібервійни сучасності. З метою їх нейтралізації задіюються плани імплементації новітніх практик у сфері кіберзахисту, спрямованих для забезпечення надійного захисту державних реєстрів та інших критично важливих інформаційних систем України таких як системи виявлення та запобігання вторгнень, багатофакторна автентифікація та шифрування даних.

Гібридна війна, що поєднує військові, економічні, інформаційні та кібернетичні методи впливу, безпосередньо впливає на функціонування податкової системи, діяльність фіскальних інституцій та суб'єктів підприємництва. Кібератаки на фінансову інфраструктуру, використання економічних інструментів як зброї, інформаційні кампанії, спрямовані на підриг довіри до державних інституцій, – усе це дестабілізує економічне середовище та ускладнює виконання фіскальними органами своїх функцій.

Стрімка цифрова трансгресія кардинально трансформує економічні системи, відносини, що формуються між учасниками, створюючи нові форми бізнесу, транзакційного обміну та різновидів активів, які часто не охоплюються традиційними механізмами оподаткування. Експансія цифрових технологій, включаючи розвиток віртуальної економіки, криптовалют, транскордонної електронної комерції, використання штучного інтелекту та великих даних впливають на структуру

національних податкових баз, ускладнюють ідентифікацію платників податків та відкривають широкі можливості для ухилення від сплати податкових платежів. Недостатнє розуміння та неадекватне реагування на ці процеси створює низку загроз для податкових систем, впливає на зменшення податкових надходжень, ускладнення податкового адміністрування, загрожує суттєвими втратами для державних бюджетів та підриває фінансову стабільність держави.

В епоху безпрецедентної цифрової трансгресії та зростаючої кількості та рівня впливу гібридних загроз, ефективність податкового менеджменту на державному, корпоративному та персональному рівнях набуває критичного значення для забезпечення фінансової стійкості, економічної безпеки та соціальної стабільності держави і її учасників. Традиційні підходи до управління податковими зобов'язаннями виявляються недостатніми перед новими викликами, що вимагає розробки та впровадження інноваційних стратегій, які враховують специфіку цифрового простору та багатогранність сучасних загроз.

На державному рівні ключовими стають посилення цифрового контролю за фінансовими потоками, активна міжнародна співпраця у сфері оподаткування цифрової економіки, а також створення надійних систем кібербезпеки для захисту критичної податкової інфраструктури. Протидія фінансуванню незаконних дій та боротьба з дезінформацією, що може підривати довіру до податкової системи, стають невід'ємними елементами державної податкової політики в умовах гібридних загроз.

Корпоративний податковий менеджмент сприяє адаптації до нових моделей оподаткування, пов'язаних з цифровою діяльністю, з одночасним посиленням систем кібербезпеки для захисту комерційної та фінансової інформації. Використання цифрових інструментів для автоматизації податкових процесів та аналізу даних стає не просто перевагою, а необхідною умовою для управління репутаційними ризиками та забезпечення безперервності бізнесу в умовах потенційних кібератак або економічної нестабільності.

На рівні домогосподарств або фізичних осіб-суб'єктів підприємництва, цифрова трансгресія актуалізує підвищення рівня податкової грамотності щодо доходів, у тому числі з цифрових джерел та усвідомлення ризиків онлайн-шахрайства. Спільними для всіх рівнів податкового менеджменту є нагальна потреба у підвищенні кібербезпеки, розвитку цифрової грамотності, здатності до швидкої адаптації до змін та прагненні до більшої прозорості у фіскальних операціях, див. таб. 1.

Водночас, кожен рівень має свої унікальні цілі, інструменти впливу та сфери відповідальності, до прикладу, держава формує правила гри та забезпечує системну протидію загрозам, суб'єкти бізнесу оптимізують свої податкові зобов'язання в рамках закону, а фізичні особи прагнуть мінімізувати свій податковий тягар, дотримуючись законодавства.

Таблиця 1

Спільні та відмінні риси стратегій податкового менеджменту на рівні держави, суб'єктів господарювання та домогосподарств

Масштаб та цілі: Державні стратегії мають макроекономічний та соціальний масштаб, корпоративні – спрямовані на інтереси компанії, персональні – на фінансове благополуччя фізичної особи.	Відмінні ознаки	Стратегії державного податкового менеджменту	Спільні ознаки	Кібербезпека: Захист даних та систем від кібератак є критично важливим для всіх рівнів податкового менеджменту.
Інструменти впливу: Держава використовує законодавство та адміністративні механізми, корпорації – фінансові інструменти та бізнес-стратегії, фізичні особи – особисте фінансове планування та знання законодавства.		Стратегії корпоративного податкового менеджменту		Цифрова грамотність: Розуміння особливостей цифрової економіки та цифрових інструментів стає необхідним для ефективного управління податками.
Рівень відповідальності: Держава несе відповідальність за функціонування всієї податкової системи, корпорації – за свої податкові зобов’язання, фізичні особи – за власну сплату податків.		Стратегії персонального податкового менеджменту		Адаптивність: Необхідність постійно адаптувати стратегії до змін у законодавстві, технологіях та геополітичній ситуації.
Вплив гібридних загроз: Держава протидіє гібридним загрозам на системному рівні, корпорації та фізичні особи – переважно на рівні захисту своїх даних та фінансів.				Прозорість: Прагнення до більшої прозорості у податкових операціях для уникнення ризиків та підвищення довіри.
				Використання технологій: Активне впровадження цифрових інструментів для оптимізації процесів та підвищення ефективності.

Джерело: складено авторами

В цьому контексті, ціллю формування стратегій податкового управління на рівні держави буде управління процесами оподаткування на державному рівні за забезпечення бюджетних надходжень, регулювання розвитку економіки та досягнення соціальних цілей; на рівні підприємств – оптимізація податкових зобов'язань, мінімізація ризиків та максимізація прибутку; на рівні фізичних осіб – використання податкових пільг та способів мінімізації податкових зобов'язань. Загалом, стратегії державного податкового менеджменту – це комплекс цілеспрямованих дій, принципів та методів, які здійснює держава в особі уповноважених органів для ефективного управління національною податковою системою для виконання певних цілей:

фіскальної: забезпечення достатнього обсягу податкових надходжень для фінансування державних видатків, включаючи оборону, освіту, охорону здоров'я, соціальний захист та інші суспільно важливі сфери;

регулюючої: використання податкових інструментів для стимулювання або стримування певних видів економічної діяльності, інвестицій, споживання, а також

для досягнення соціальних цілей (наприклад, через пільги для екологічно чистих виробництв або соціально незахищених верств населення);

контрольної: забезпечення належного обліку та сплати податків, запобігання ухиленню від оподаткування та боротьба з податковими правопорушеннями;

стимулюючої: створення сприятливого податкового клімату для розвитку підприємництва, залучення інвестицій, інновацій та економічного зростання;

соціальної: перерозподіл доходів через систему оподаткування та надання податкових пільг соціально вразливим групам населення тощо.

Основні елементи стратегій податкового менеджменту на рівні держави можуть включати:

– розробку та вдосконалення податкового законодавства: встановлення чітких, справедливих та ефективних правил оподаткування, адаптованих до економічних реалій та міжнародних стандартів;

– оптимізацію системи податкового адміністрування: забезпечення ефективної роботи податкових органів, спрощення процедур сплати податків та подання звітності, впровадження сучасних інформаційних технологій;

– управління податковими ризиками на державному рівні: виявлення та мінімізація ризиків недоотримання податків, ухилення від оподаткування та неефективного використання податкових пільг;

– міжнародне податкове співробітництво: прийняття участі у міжнародних ініціативах щодо боротьби з транскордонним ухиленням від сплати податків та обмін інформацією з іншими країнами;

– підвищення податкової культури та свідомості платників податків: проведення інформаційно-роз'яснювальної роботи щодо податкових обов'язків та переваг сплати податків.

Отже, дієвий державний податковий менеджмент в умовах різноманітних ризиків та загроз, особливо військового характеру, стає критично важливим для: забезпечення фінансової та інституційної стійкості України; фінансування оборонних потреб через мобілізацію достатніх обсягів фінансових ресурсів, необхідних для уможливлення функціонування держави; виконання її соціальних зобов'язань та зміцнення обороноздатності в умовах гібридної агресії; підтримки малого та середнього бізнесу шляхом мінімізації бюрократії та спрощення податкових процедур; запобігання корупційним ризикам та підвищення прозорості діяльності контролюючих органів; захисту прав платників податків тощо.

На рівні суб'єктів господарювання, ефективний податковий менеджмент сприяє оптимізації податків, підвищенню прибутковості, мінімізації ризиків, покращенню фінансового управління, виконанню податкових обов'язків та уникненню санкцій.

Корпоративний податковий менеджмент є складним та багатогранним процесом, що вимагає глибоких знань податкового законодавства, розуміння бізнес-процесів компанії та здатності приймати стратегічні рішення. Ефективна податкова стратегія повинна бути інтегрована в загальну бізнес-стратегію компанії та спрямована на досягнення її фінансових цілей з урахуванням прийнятного рівня податкових ризиків. Постійний моніторинг податкового середовища, адаптація

до змін та використання сучасних інструментів податкового менеджменту є запорукою успішного управління податковими зобов'язаннями та підвищення конкурентоздатності компанії.

Умови цифрових трансгресій та гібридних загроз вимагають від компаній кардинального перегляду своїх стратегій податкового менеджменту. Традиційні підходи стають недостатніми для ефективного управління податковими зобов'язаннями та мінімізації нових видів ризиків. Успішний податковий менеджмент в цьому складному середовищі вимагає посилення цифрової грамотності, впровадження передових технологій контролю та аналізу, активної співпраці, розробки комплексних стратегій управління ризиками та адаптації організаційних процесів. Компанії, які зможуть ефективно інтегрувати ці нові підходи у свою діяльність, зможуть не лише забезпечити свою фінансову стабільність та дотримання законодавства, але й отримати конкурентні переваги в умовах цифрової економіки.

Персональний податковий менеджмент є важливим інструментом для покращення фінансового добробуту фізичних осіб та фізичних осіб-суб'єктів підприємницької діяльності. Ретельне планування та використання доступних законних методів оптимізації оподаткування дозволяє заощадити кошти та спрямувати їх на досягнення особистих фінансових цілей. Регулярний перегляд фінансової ситуації сприяють підтримці ефективної стратегії податкового менеджменту впродовж усього життя.

Підвищення цифрової грамотності громадян є ключовим елементом у запобіганні багатьом формам цифрових трансгресій, таким як фішинг, онлайн-шахрайство та поширення дезінформації. Люди, які володіють необхідними знаннями та навичками, є менш вразливими до маніпуляцій та можуть більш відповідально поводитися в цифровому середовищі.

Висновки та перспективи подальших розвідок. Цифрові трансгресії та гібридні загрози являють собою якісно нові феномени, що суттєво змінюють природу економічних, соціальних та політичних процесів. Загалом, концепт трансгресивного еволюційного процесу визначається ознаками амбівалентності та невизначеності, зумовлюючи перехід соціальної дійсності до нового типу, в результаті усвідомлення чого теоретики «схиляються до думки, що майбутнє суспільства нерозривно пов'язане з подальшою плюралізацією, гібридизацією, зростаючою амбівалентністю та невизначеністю соціального порядку» [6, с. 9].

Іншими словами, з часом лише посилюватимуться: нелінійність та неоднозначність розвитку суспільних, економічних та політичних процесів (так як традиційні лінійні моделі еволюції суспільства не ефективні для опису сучасних процесів, які відбуваються не поступово та передбачувано, а через якісні стрибки, порушення існуючих порядків і виникнення несподіваних комбінацій); внутрішня суперечливість та амбівалентність змін (що супроводжуватиметься внутрішніми напруженнями, конфліктами та непередбачуваними наслідками); зростанням складності та невизначеності (очевидним є те, що у майбутньому матиме місце подальше розмивання кордонів, поєднання різних ідентичностей, ідеологій та практик (гібридизація), що призведе до зростання невизначеності і складності соціального порядку); та усвідомлення того, що суспільне життя характеризуватиметься постійною динамікою, мінливістю та необхідністю

адаптації до нових умов. Це вимагає переосмислення існуючих теоретичних підходів до податкового менеджменту, розробки нових концептуальних рамок, які б враховували специфіку впливу цих чинників на формування, адміністрування та контроль податкових зобов'язань.

Список використаних джерел:

1. Безгубенко Л.М., Безгубенко О.Ю. Синергійні елементи й ефекти податкового менеджменту. *Фінанси України*. 2001. № 10. С. 97–101.
2. Офіційний веб-сайт Міністерства фінансів України. Підсумки 2022 року. URL: https://mof.gov.ua/uk/news/key_results_of_2022_of_the_ministry_of_finance-3788
3. Stoltenberg J. The Three Ages of NATO: An Evolving Alliance. Speech by NATO Secretary General Jens Stoltenberg at the Harvard Kennedy School –23 Se p. 2016- URL: http://www.nato.int/cps/en/natohq/opinions_135317.htm?selectedLocale=en
4. Офіційний веб-сайт Державної служби спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/ua>
5. Офіційний веб-сайт Урядової команди реагування на комп'ютерні надзвичайні події України. URL: CERT-UA <https://cert.gov.ua>
6. Bataille G. (1990). Hegel, Death and Sacrifice. *Yale French Studies*, № 78, pp. 9-28. URL: <https://www.jstor.org/stable/2930112>

References:

1. Bezkhubenko, L. M., & Bezkhubenko, O. Yu. (2001). Synerhiini elementy i efekty podatkovoho menedzhmentu [Synergistic elements and effects of tax management]. *Finansy Ukrainy*, 10, 97–101.
2. Ministry of Finance of Ukraine Official website (2023). Pidsumky 2022 roku [2022 Results]. Available at: https://mof.gov.ua/uk/news/key_results_of_2022_of_the_ministry_of_finance-3788
3. Stoltenberg, J. (2016). *The Three Ages of NATO: An Evolving Alliance* [Promova]. Harvard Kennedy School. Available at: http://www.nato.int/cps/en/natohq/opinions_135317.htm?selectedLocale=en
4. State Service for Special Communications and Information Protection of Ukraine Official website. Available at: <https://cip.gov.ua/ua>
5. Ukrainian Government's Computer Emergency Response Team Official website. CERT-UA. Available at: <https://cert.gov.ua>
6. Bataille, G. (1990). Hegel, Death and Sacrifice. *Yale French Studies*, 78, 9–28.