doi: https://doi.org/10.33763/finukr2021.08.113

УДК 004.9:657:005.93

І. І. Криштопа
доктор економічних наук, професор, професор кафедри податкового менеджменту та фінансового моніторингу Київського національного економічного університету імені Вадима Гетьмана, Київ, Україна, ikryshtopa@kneu.edu.ua
ORCID ID: https://orcid.org/0000-0003-1759-6472

Л. А. Ніколенко
кандидат економічних наук, доцент, доцент кафедри інформатики та системології Київського національного економічного університету імені Вадима Гетьмана, Київ, Україна, larisa_nikolenko@ukr.net
ORCID ID: https://orcid.org/0000-0003-2721-9646

ЗВІТУВАННЯ В РОЗРІЗІ КРАЇН: ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ТА ЗАХИСТУ ІНФОРМАЦІЇ МІЖНАРОДНИХ ГРУП КОМПАНІЙ

Анотація. Забезпечення конфіденційності та захисту інформації, що міститься у звітах у розрізі країн міжнародної групи компаній (Country-by-Country Reports), є одним із найважливіших аспектів реалізації Кроку 13 Плану протидії розмиванню бази оподаткування та виведенню прибутку з-під оподаткування (Плану дій BEPS) у законодавстві країн світу. Враховуючи взяті Україною зобов'язання перед ОЕСР у частині боротьби з ухиленням міжнародних груп компаній від оподаткування, особливої актуальності набуває дослідження модельного законодавства з питань забезпечення конфіденційності й захисту інформації, яка виступає предметом добровільного автоматичного обміну між країнами, та підходів до його імплементації в національне законодавство. Мета дослідження – комплементарний аналіз інституціонального підґрунтя забезпечення конфіденційності й захисту інформації, котра є предметом обміну між країнами – учасницями ОЕСР у межах реалізації заходів Плану дій BEPS. Дослідження базується на поєднанні загальнонаукових методів, методів порівняння та емпіричного підходу. За його результатами доведено необхідність подальшого вдосконалення інституціонального забезпечення захисту й конфіденційності податкової інформації, включаючи ту, якою обмінюються відповідно до міжнародних угод.

Ключові слова: BEPS, захист інформації, конфіденційна інформація, обмін податковою інформацією, звіти в розрізі країн (Country-by-Country Reports).

Табл. 1. **Літ.** 11.

Iryna Kryshtopa
Dr. Sc. (Economics), Professor, Kyiv National Economic University named after Vadym Hetman, Kyiv, Ukraine, ikryshtopa@kneu.edu.ua
ORCID ID: https://orcid.org/0000-0003-1759-6472

Larysa Nikolenko
Ph. D. (Economics), Associate Professor, Kyiv National Economic University named after Vadym Hetman, Kyiv, Ukraine, larisa_nikolenko@ukr.net
ORCID ID: https://orcid.org/0000-0003-2721-9646

COUNTRY-BY-COUNTRY REPORTING: ENSURING CONFIDENTIALITY AND PROTECTION OF INFORMATION OF MULTINATIONAL GROUPS OF COMPANIES

Abstract. *Introduction.* Confidentiality and protection of information contained in Country-by-Country Reports is one of the most important aspects of implementation of provisions of Action 13 of the Base erosion and Profit Shifting Action Plan (BEPS Action Plan) into national legislation of countries around the world. *Problem statement.* Considering Ukraine`s commitments to Organization for Economic Cooperation and Development (OECD) in frames of combating against tax evasion by multinational groups of companies, a particular relevance receives the study of model legislation on confidentiality and protection of information, which is the subject of voluntary automatic exchange between countries, and approaches to its implementation into national legislation. *Purpose.* Complementary analysis of institutional basis for ensuring confidentiality and protection of information that is the subject of exchange between OECD member countries in frames of the BEPS Action Plan. *Materials and methods.* The research is based on a combination of general scientific methods, methods of comparison and empirical approach. *Results.* The need for harmonization of domestic legislation with OECD regulatory requirements that regulate confidentiality of information on taxpayers (including information exchanged in accordance with international agreements) has been substantiated. *Conclusions.* Based on the results of the conducted research it has been proved that there is the need for further improvement of institutional provision of protection and confidentiality of tax information, including information exchanged in accordance with international agreements.

Keywords: BEPS, protection of information, confidential information, exchange of tax information, Country-by-Country Reports.

JEL classification: H29.

И. И. Криштопа
доктор экономических наук, профессор, профессор кафедры налогового менеджмента и финансового мониторинга Киевского национального экономического университета имени Вадима Гетьмана, Киев, Украина

Л. А. Николенко
кандидат экономических наук, доцент, доцент кафедры информатики и системологии Киевского национального экономического университета имени Вадима Гетьмана, Киев, Украина

ОТЧЕТНОСТЬ В РАЗРЕЗЕ СТРАН: ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ МЕЖДУНАРОДНЫХ ГРУПП КОМПАНИЙ

Аннотация. Обеспечение конфиденциальности и защиты информации, которая содержится в отчетах в разрезе стран международной группы компаний (Country-by-Country Reports), является одним из наиболее важных аспектов реализации Шага 13 Плана противодействия размыванию базы налогообложения и выведению прибыли из-под налогообложения (Плана действий BEPS) в законодательстве стран мира. Учитывая взятые Украиной обязательства перед ОЭСР в части борьбы с уклонением международных групп компаний от налогообложения, особую актуальность приобретает исследование модельного законодательства по вопросам обеспечения конфиденциальности и защиты информации, которая выступает предметом добровольного автоматического обмена между странами, и подходов к его имплементации в национальное законодательство. Цель исследования – комплементарный анализ институ-

циональной основы обеспечения конфиденциальности и защиты информации, являющейся предметом обмена между странами – участницами ОЭСР в рамках реализации мероприятий Плана действий BEPS. Исследование базируется на сочетании общенаучных методов, методов сравнения и эмпирического подхода. По его результатам доказана необходимость дальнейшего совершенствования институционального обеспечения защиты и конфиденциальности налоговой информации, включая ту, которой обмениваются в соответствии с международными соглашениями.

Ключевые слова: BEPS, защита информации, конфиденциальная информация, обмен налоговой информацией, отчеты в разрезе стран (Country-by-Country Reports).

Конфіденційна інформація є комерційною, державною або службовою таємницею. Доступ до неї надається залежно від службового становища, використання обмежується договорами про нерозголошення конфіденційних даних.

Питання доступу до інформації вирішує її власник, котрий встановлює її правовий режим відповідно до закону. Модель регулювання ступеня її конфіденційності залежить від сфери суспільного чи економічного життя, національної специфіки. Всі форми обміну інформацією (за запитом, автоматичний, спонтанний) істотно вдосконалено завдяки спільним зусиллям міжнародних організацій, зокрема ОЕСР і урядів країн світу, які усвідомлюють важливість такої діяльності. Під час податкового інформаційного співробітництва особлива увага приділяється автоматичному обміну даними про фінансові рахунки нерезидентів у рамках Закону США "Про податкові вимоги до іноземних рахунків" (Foreign Account Tax Compliance Act – FATCA) й Загального стандарту звітності (Common Reporting Standard – CRS) відповідно до стандартів звітності, розроблених ОЕСР.

У межах заходів протидії розмиванню податкової бази та виведенню прибутку з-під оподаткування згідно з Планом дій BEPS (Base Erosion and Profit Shifting) одним із головних завдань урядів країн світу, зокрема їхніх податкових органів, є забезпечення конфіденційності інформації, що є предметом обміну.

Проблема захисту та конфіденційності інформації є нагальною й для України, що вимагає від вітчизняних науковців вивчення досвіду та розроблення уніфікованих підходів до зобов'язань юрисдикцій з нерозголошення інформації, отриманої від ділового партнера (учасника), захисту її від несанкціонованого доступу, а також передання її учасникам міжнародних угод (підписантам Плану дій BEPS) і звітування в розрізі країн (Country-by-Country Reports) [1].

Конфіденційність – це обмеження доступу до даних певного статусу. Цей термін походить від латинського слова "confidentia", котре перекладається як довіра. Отже, отримати доступ до конфіденційної інформації можуть тільки довірені співробітники. Рішення стосовно контролю доступу реалізуються на організаційному й програмному рівнях.

Попри численні напрацювання в галузі захисту конфіденційної інформації, чіткої, єдиної класифікації її видів поки що не розроблено, хоча різни-

ми дослідниками виявлено понад 30 її різновидів. Наприклад, А. І. Алексенцев пропонував поділити інформацію за видами таємниці; за власниками інформації; за особами, на яких покладено інформаційний захист, і за сферою діяльності, де присутня такого роду інформація. При цьому вчений зауважив про можливий частковий збіг вказаних компонентів [2]. К. Н. Шудрова розподіляє інформацію за рівнями конфіденційності, визначає класи останньої й вимоги щодо захисту до кожного класу, водночас називаючи саме визначення правил автоматичної системи перевірки цілісності та достовірності інформації, її засобів безпеки, побудову надійних схем зберігання й передання даних проблемою [3]. У свою чергу, А. А. Фатьянов класифікував інформацію, що підлягає захисту, за трьома ознаками: належністю, змістом, ступенем конфіденційності (обмеження доступу). На його думку, власниками такої інформації є органи державної влади, юридичні та фізичні особи. За змістом вона може бути поділена на політичну, економічну, військову, наукову, технологічну, особисту, комерційну. [4] О. С. Іванов розглядає окремі положення Плану дій BEPS щодо автоматичного обміну податковою інформацією і складання міжнародної документації з трансфертного ціноутворення. Ним запропоновано низку заходів, які закладають новий фундамент для розвитку міжнародних податкових відносин та виводять їх на новий рівень [5].

Зазначені аспекти потребують подальшого дослідження з метою розроблення уніфікованих правил правової й технічної безпеки міжнародних податкових відносин у напрямі використання та захисту конфіденційної інформації, що є предметом обміну між країнами – учасницями ОЕСР, у рамках Плану дій BEPS.

Метою статті є комплементарний аналіз інституціонального підґрунтя забезпечення конфіденційності та захисту інформації, яка є предметом обміну між країнами – учасницями ОЕСР, у межах реалізації заходів Плану дій BEPS. Для досягнення поставленої мети слід виконати такі наукові завдання: розкрити сутність конфіденційної інформації, проблеми організації інформаційного співробітництва в напрямі обміну інформацією між податковими органами та її ефективного захисту зі збереженням конфіденційності, від яких залежить "справедливе" оподаткування учасників міжнародних економічних відносин.

Вимоги щодо конфіденційності податкової інформації відображено в чинних конвенціях про уникнення подвійного оподаткування й угодах про обмін податковою інформацією, багатосторонній Конвенції про взаємну адміністративну допомогу в податкових справах Ради Європи [6]. Конвенцією передбачено, що країни повинні надавати дані відповідно до їхніх національних правових норм, з огляду на необхідність захисту конфіденційної інформації та міжнародні документи.

Отримана інформація розкривається тільки особам чи органам, причетним до оцінки, збору або стягнення податків, здійснення виконавчих заходів чи кримінального переслідування щодо податків, належних до сплати,

або до прийняття рішень по апеляціях щодо таких податків. Ця інформація може використовуватися виключно особами або органами, про котрі йдеться в укладеному міжнародному договорі, та лише для податкових цілей.

Конфіденційність інформації про платника податків завжди виступає наріжним каменем при побудові податкових систем. І платники податків, і податкові адміністрації вправі очікувати, що дані, якими обмінюються, залишаться конфіденційними. Щоби бути впевненими в діях податкових органів і дотримуватися своїх законних зобов'язань, платники податків повинні знати, що важлива фінансова інформація не буде розголошена спеціально, через необачність або інші прикрі випадки.

Оцінюючи потенційні ризики, підприємства й уряди мають довіряти даним міжнародного обміну інформацією. А розкриття останньої повинне відбуватися за допомогою правового інструментарію, на базі якого здійснюється обмін. Це стосується не тільки правової бази, а й усього спектра процесів інформаційної безпеки та достовірності даних.

Виокремлюють такі основні блоки, що мають важливе значення для забезпечення належних гарантій захисту інформації, яка є предметом обміну:

– правова база;
– менеджмент інформаційної безпеки: практики та процедури;
– контроль за дотриманням конфіденційності;
– санкції при порушенні конфіденційності.

Першим блоком виступає правова (нормативна) база. Інструменти обміну інформацією загалом передбачають, що вона не повинна надаватись іншій юрисдикції, якщо її розголошення суперечитиме правовим нормам юрисдикції, котра надає інформацію.

Забезпечення конфіденційності даних, отриманих відповідно до застосованої правової бази, є надзвичайно важливим. У разі будь-якого порушення конфіденційності або невиконання гарантій (включаючи додаткові гарантії за їх наявності, зазначені компетентним органом, що надає інформацію) компетентний орган має негайно повідомити інші компетентні органи про таке порушення чи невиконання, в т. ч. будь-які санкції або заходи з виправлення становища. Зміст кожного такого повідомлення повинен відповідати правилам конфіденційності та законодавству юрисдикції, де відбулося порушення чи невиконання. Недотримання гарантій конфіденційності й захисту даних може вважатися серйозним порушенням договірних умов і бути підставою для негайного припинення дії міжнародного договору.

Наразі саме податкові органи зацікавлені в інформації про фінансовий і майновий стан підприємства, сплату податків. Тож вони виступають основними користувачами конфіденційної інформації, що є предметом міжнародного обміну.

У рамках приєднання України до заходів протидії розмиванню податкової бази та виведенню прибутку з-під оподаткування Плану дій BEPS звіти в розрізі країн мають подаватися до податкової юрисдикції та розповсюджу-

ватися між юрисдикціями шляхом автоматичного обміну даними. Тож із метою забезпечення захисту й конфіденційності податкової інформації при добровільному обміні між країнами (CbCR), відповідно до Кроку 13 Плану дій BEPS, розглянемо, як поняття конфіденційності та захисту інформації врегульовані в національному законодавстві.

Питання сутності, доступу до інформації про фізичних і юридичних осіб, упровадження інформаційних систем та систем управління інформаційною безпекою регулюються на нормативному рівні одразу кількома законами. У таблиці наведено основні положення національного законодавства, котрі стосуються захисту та конфіденційності інформації.

Основним нормативним актом виступає Закон України "Про інформацію" від 02.10.1992 № 2657-XII (далі – Закон № 2657), яким визначено основні принципи інформаційних відносин, напрями державної інформаційної політики, права та гарантії суб'єктів інформаційних відносин, права захисту й доступ до інформації. За порядком доступу вона поділяється на відкриту та з обмеженим доступом. Згідно із Законом № 2657, інформацією з обмеженим доступом є:

- конфіденційна інформація (тобто про фізичну особу, а також така, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень);
- таємна інформація (котра містить державну, професійну, банківську таємницю, таємницю досудового розслідування тощо);
- службова інформація (що міститься в документах суб'єктів владних повноважень, які становлять внутрішньовідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень).

Утім, на сьогодні в українському законодавстві чіткого визначення поняття "конфіденційна інформація" немає. Закон № 2657 не містить такого терміна, він лише описує узагальнене поняття конфіденційної інформації. Тобто властивість інформації бути недоступною та закритою чи мати обмеження визначає її власник, котрий також встановлює правовий режим для неї відповідно до закону.

У рамках реалізації другого блоку забезпечення належних гарантій захисту інформації, що є предметом обміну, дотримання зобов'язань з конфіденційності й безпеки таких даних податкові органи мають:

1) оцінювати потенційний ризик несанкціонованого доступу до інформації про платників податків, розмір збитків від несанкціонованого використання, розголошення, порушення, модифікації або знищення отриманої чи наданої інформації про платників податків, яка надійшла в ході обміну податковою інформацією;

2) належним чином захищати наявну інформацію в друкованій формі або в цифрових інформаційних засобах, обмежувати доступ до неї автори-

Таблиця. **Нормативне забезпечення захисту інформації та конфіденційності в Україні**

№ з/п	Назва документа	Основні положення щодо захисту інформації	Основні положення стосовно конфіденційності
1	Закон України "Про інформацію" (зі змінами та доповненнями) від 02.10.1992 № 2657-XII [7]	Визначено основні принципи інформаційних відносин і порядок правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують захист інформації	Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом
2	Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 № 80/94-ВР [8]	Встановлено, що об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, призначене для обробки цієї інформації. Застосування комплексної системи захисту інформації з підтвердженою відповідністю та врахуванням галузевих вимог і норм інформаційної безпеки	Конфіденційна інформація – це інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом
3	Закон України "Про доступ до публічної інформації" від 13.01.2011 № 2939-V [9]	Визначено, яка інформація може вільно поширюватися та є відкритою відповідно до законодавства. Стосується також інформації, що раніше була правомірно оприлюднена. Дії закону спрямовані на захист персональних даних: розповсюдження, реалізацію, передачу, знеособлення та знищення персональних даних у інформаційних (автоматизованих) системах	Конфіденційною є інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватись у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. Поширюватися може конфіденційна інформація про особу – її персональні дані, якщо ця особа надала свою згоду
4	Постанова Кабінету Міністрів України "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних системах" від 29.03.2006 № 373 [10]	Захист інформації на всіх етапах створення та експлуатації системи здійснюється відповідно до плану захисту інформації в системі. Визначено, що доступ до службової інформації надається тільки ідентифікованим користувачам	Захисту в системі підлягає конфіденційна інформація, яка перебуває у володінні розпорядників інформації, службова інформація, інформація, яка становить державну таємницю

Складено авторами.

зованих користувачів та очищати цифрові ЗМІ перед утилізацією чи повторним використанням, приділяти особливу увагу користуванню авторизованим програмним забезпеченням і обізнаності співробітників щодо вимог конфіденційності;

3) здійснювати моніторинг політики дотримання конфіденційності та виявляти будь-який несанкціонований доступ і розголошення.

В міру розвитку інформаційних технологій проблема захисту та конфіденційності даних набуває дедалі більшої значущості. Постає потреба в забезпеченні їх конфіденційності, виходячи з державної політики інформаційної безпеки. Інформація визнається конфіденційною саме тому, що вона є об'єктом виключного володіння, користування й розпорядження конкретної особи, організації, комерційної спільноти або державної установи, що зумовлює її доступність тільки адресату.

Третім базовим блоком, який має велике значення для забезпечення належних гарантій захисту інформації, що є предметом обміну, виступає контроль за дотриманням конфіденційності. Порушення конфіденційності є однією з найсерйозніших, із точки зору шкоди, загроз інформаційній безпеці. Тому слід зупинитися на її захисті.

Саме захист конфіденційної інформації сьогодні належить до найважливіших чинників створення та забезпечення передумов, необхідних для стабільності й розвитку інформаційного суспільства. Він спрямований на забезпечення інтересів суб'єктів інформаційних відносин. На цьому наголошують норми Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (зі змінами та доповненнями) від 05.07.1994 № 80/94 (далі – Закон № 80/94). У цьому нормативному акті йдеться про обов'язкове дотримання конфіденційності інформації, а обмеження доступу до таких даних визначено законодавством з метою захисту підвалин конституційного ладу, моральності, здоров'я, прав і законних інтересів інших осіб, забезпечення оборони країни та безпеки держави.

Зміни до Закону № 80/94 стосуються підтвердження відповідності інформаційної системи вимогам захисту інформації ЄС. Мінцифри України впроваджує стандарти системи управління інформаційною безпекою (далі – СУІБ) для окремих категорій інформації. Схваленими змінами вводиться альтернативний спосіб підтвердження відповідності інформаційної системи вимогам щодо захисту даних (подібна практика вже застосовується в Україні у сфері публічних закупівель). Слід підкреслити, що ці вимоги діють для забезпечення інформаційної й кібербезпеки в ЄС і наближують Україну до європейських стандартів.

Комплексна система захисту інформації (далі – КСЗІ) в Україні діє відповідно до нормативного документа технічного захисту інформації "Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" на підставі технічного завдання, підготовленого згідно з Методичними вказівками щодо розробки технічного завдання на створення комплексної системи

захисту інформації в автоматизованій системі. До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від:

– витоку технічними каналами, до котрих належать канали побічних електромагнітних випромінювань і наведень, акустоелектричні та ін.;

– несанкціонованих дій і несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів тощо;

– спеціального впливу на інформацію, зокрема шляхом формування полів і сигналів, для порушення її цілісності або руйнування системи захисту.

За підсумками детального вивчення об'єкта, на якому створюється КСЗІ, уточнення моделі загроз та моделі порушника, результатів аналізу можливості керування ризиками здійснюється вибір основних рішень із протидії всім істотним загрозам, формування загальних вимог, правил, обмежень, що регламентують використання захищених технологій обробки інформації в інформаційно-технічних системах (далі – ІТС), окремих заходів і засобів захисту інформації, діяльність користувачів усіх категорій та документальне оформлення політики безпеки.

Під час розроблення КСЗІ обґрунтовуються й приймаються проєктні рішення, котрі дають змогу реалізувати вимоги технічного завдання, забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також заходів та способів захисту інформації. В результаті створюється комплект робочої й експлуатаційної документації, необхідної для забезпечення тестування, проведення пусконалагоджувальних робіт, випробувань та управління КСЗІ.

Уведення КСЗІ в дію включає складання розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІТС, створення служби захисту інформації, розроблення й затвердження Плану захисту інформації, навчання користувачів ІТС усіх категорій (технічного персоналу, звичайних користувачів та адміністраторів), комплектування КСЗІ засобами захисту інформації, матеріалами, обладнанням, проведення будівельно-монтажних і пусконалагоджувальних робіт, попередніх випробувань та дослідної експлуатації КСЗІ. В ході попередніх випробувань перевіряються працездатність КСЗІ й відповідність її вимогам.

При розробленні системи захисту конфіденційної інформації слід враховувати, що сучасні бізнес-процеси будуються на використанні середовища віртуалізації, хмарних технологій, тож певні рішення повинні застосовуватися при захисті даних у власних інформаційних мережах, інші – при їх розміщенні у хмарі. Обробляючи дані в локальних мережах, найбільшу увагу потрібно приділяти їх структурованості. Адміністрація організації повинна чітко розуміти, які саме інформаційні масиви є конфіденційними, в яких файлах і папках вони містяться, як забезпечується диференціація доступу до них.

Станом на серпень 2021 р. до створення КСЗІ висуваються певні вимоги. Ліцензується діяльність щодо оцінювання захищеності інформації. Тобто ліцензія потрібна у двох випадках: проведення державної експертизи та створення КСЗІ для обробки інформації, що становить державну таємницю (включає обов'язкові роботи із захисту від витоку інформації технічними каналами).

Під час створення КСЗІ й дослідної експлуатації:

- відпрацьовуються технології обробки інформації, обігу її машинних носіїв, керування засобами захисту, розмежування доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів;
- співробітники служби захисту інформації й користувачі ІТС набувають практичних навичок із використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних і розпорядчих документів із питань розмежування доступу до технічних засобів та інформаційних ресурсів;
- здійснюється (за потреби) доопрацювання програмного забезпечення, додаткове налагоджування й конфігурування комплексу засобів захисту інформації від несанкціонованого доступу;
- проводиться (за потреби) коригування робочої та експлуатаційної документації.

За результатами дослідної експлуатації оцінюється готовність КСЗІ в ІТС до представлення на державну експертизу. Державна служба спеціального зв'язку та захисту інформації України приймає рішення щодо можливості й доцільності проведення та організації експертизи, визначає її організатора, реєструє результати та надає Експертний висновок і Атестат відповідності, які засвідчують, що система захисту інформації відповідає вимогам нормативних документів. Варто зауважити, що в Експертному висновку вказується рівень гарантій, який відповідно до нормативного документа "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" встановлює такі критерії, а саме: функціональні, що дають змогу оцінити наявність послуг безпеки, та критерії гарантій, які допомагають оцінити коректність надання послуг безпеки.

Стосовно захисту податкової інформації[1], то ПКУ визначає нерозголошення інформації з обмеженим доступом, яка одержується, використовується, зберігається при реалізації функцій, покладених на контролюючі органи, та вноситься до інформаційних баз даних з урахуванням обмежень, передбачених для податкової інформації з обмеженим доступом. Платник податків має право на нерозголошення контролюючим органом (посадови-

[1] Згідно зі ст. 16 Закону № 2657, податкова інформація – це сукупність відомостей і даних, що створені або отримані суб'єктами інформаційних відносин у процесі поточної діяльності та необхідні для реалізації покладених на контролюючі органи завдань і функцій у порядку, встановленому Податковим кодексом України.

ми особами) відомостей про такого платника без його письмової згоди та відомостей, що становлять конфіденційну інформацію, державну, комерційну чи банківську таємницю (п. 17.1.9 ст. 17 і п. 21.1.6 ст. 21 ПКУ) [11].

На підставі викладеного доходимо таких висновків. Україна зобов'язана брати до уваги вимоги Конвенції про взаємну адміністративну допомогу в податкових справах щодо захисту конфіденційної інформації, де наведено набір інструментів з конфіденційності та організації систем управління інформаційною безпекою. Так, у нашій державі на законодавчому рівні наявна правова база, якою врегульовано питання сутності конфіденційності податкової інформації. Що ж стосується податкової інформації, котра є предметом обміну, то в Податковому кодексі України не передбачено окремих вимог до конфіденційності й захисту інформації для міжнародних груп компаній, які повинні надавати звіти в розрізі країн (Country-by-Country Reports) до відповідних податкових юрисдикцій і розповсюджувати їх між юрисдикціями шляхом автоматичного обміну даними. Тому до такої інформації застосовуються ті самі правила та вимоги, що й до податкової. Отже, подальша робота повинна бути спрямована на створення інституціонального забезпечення дотримання правил адміністрування (відповідно до законодавства України) органами державної влади та місцевого самоврядування, що гарантують конфіденційність інформації про платників податків, включаючи дані, котрими обмінюються за міжнародними угодами.

Список використаних джерел

1. Action 13 Country-by-Country Reporting / OECD. 2021. URL: https://www.oecd.org/tax/beps/beps-actions/action13/.

2. *Алексенцев А. И.* Конфиденциальное делопроизводство. 2003. URL: https://altairbook.com/books/1490428-konfidencialnoe-deloproizvodstvo.html.

3. *Шудрова К.* Об уровнях конфиденциальной информации. *Директор по безопасности*. 2012. С. 24–29. URL: https://euroasia-science.ru/tehnicheskie-nauki.

4. *Фатьянов А. А.* Проблемы защиты конфиденциальной информации, не составляющей государственную тайну. 1997. URL: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/18443727c1ac086ec32575be002e62c3.

5. *Иванов О. С.* Международная координация стран в отношении проблемы размытия налогооблагаемой базы и перемещения прибыли. 2018. URL: https://cy URL: cyberleninka.ru/article/n/mezhdunarodnaya-koordinatsiya-stran-v-otnoshenii-problemy-razmytiya-nalogooblagaemoy-bazy-i-peremescheniya-pribyli.

6. Конвенція про взаємну адміністративну допомогу в податкових справах (ETS 127) від 25.01.1988. URL: https://zakon.rada.gov.ua/laws/show/994_325.

7. Про інформацію : закон України від 02.10.1992 № 2658-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

8. Про захист інформації в інформаційно-телекомунікаційних системах : закон України від05.07.1994№80/94-ВР.URL:https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

9. Про доступ до публічної інформації : закон України від 13.01.2011 № 2939-V. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

10. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних системах : постанова Кабінету Міністрів України від 29.03.2006 № 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text.

11. Вісник. Офіційно про податки / Державна фіскальна служба України. 2021. URL: http://www.visnuk.com.ua/.

References

1. OECD. (2021). *Action 13 Country-by-Country Reporting*. Retrieved from https://www.oecd.org/tax/beps/beps-actions/action13/.

2. Aleksentsev, A. I. (2003). *Confidential proceedings*. Retrieved from https://altairbook.com/books/1490428-konfidencialnoe-deloproizvodstvo.html [in Russian].

3. Shudrova, K. (2012). On the levels of confidential information. *Security Director*, pp. 24–29. Retrieved from https://euroasia-science.ru/tehnicheskie-nauki [in Russian].

4. Fatyanov, A. A. (1997). *Problems of protection of confidential information that does not constitute a state secret*. Retrieved from http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/18443727c1ac086ec32575be002e62c3 [in Russian].

5. Ivanov, O. S. (2018). *International coordination of countries in relation to the problem of erosion of the taxable base and profit transfer*. Retrieved from https://cyberleninka.ru/article/n/mezhdunarodnaya-koordinatsiya-stran-v-otnoshenii-problemy-razmytiya-nalogooblagaemoy-bazy-i-peremescheniya-pribyli [in Russian].

6. OECD. (1998, January 25). *Convention on Mutual Administrative Assistance in Tax Matters* (ETS 127). Retrieved from https://zakon.rada.gov.ua/laws/show/994_325 [in Ukrainian].

7. Verkhovna Rada of Ukraine. (1992). *About information* (Act No. 2658-XII, October 2). Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12#Text [in Ukrainian].

8. Verkhovna Rada of Ukraine. (1994). *On information protection in information and telecommunication systems* (Act No. 81/94-VR, July 5). Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text [in Ukrainian].

9. Verkhovna Rada of Ukraine. (2011). About access to public information (Act No. 2939-V, January 13). Retrieved from https://zakon.rada.gov.ua/laws/show/2939-17#Text [in Ukrainian].

10. Cabinet of Ministers of Ukraine. (2006). About approval Rules for ensuring protection information in information, telecommunication systems (Decree No. 373, March 29). Retrieved from https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text [in Ukrainian].

11. State Fiscal Service of Ukraine. (2021). *Bulletin. Officially about taxes*. Retrieved from http://www.visnuk.com.ua/ [in Ukrainian].