Міністерство юстиції України
Науково-дослідний центр судової експертизи
з питань інтелектуальної власності

ПРОБЛЕМИ ТЕОРІЇ ТА ПРАКТИКИ СУДОВОЇ ЕКСПЕРТИЗИ З ПИТАНЬ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

(«КРАЙНЄВСЬКІ ЧИТАННЯ»)

Матеріали VI Міжнародної науково-практичної конференції
(23 грудня 2022 р., м. Київ)

МІНІСТЕРСТВО ЮСТИЦІЇ УКРАЇНИ
Науково-дослідний центр судової експертизи
з питань інтелектуальної власності

ПРОБЛЕМИ ТЕОРІЇ ТА ПРАКТИКИ СУДОВОЇ ЕКСПЕРТИЗИ З ПИТАНЬ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ («Крайнєвські читання»)

Матеріали VI Міжнародної науково-практичної конференції
(23 грудня 2022 р., м. Київ)

Київ
Видавництво Ліра-К
2022

УДК 347
П78

Рекомендовано до друку
Вченою радою Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України
(протоколи № 1 від 22.12.2022; № 2 від 11.01.2023)

Рецензенти:

Барабаш О. В. – доктор технічних наук, професор, професор кафедри автоматизації проектування енергетичних процесів і систем Навчально-наукового інституту атомної та теплової енергетики Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»;

Кучук Н. Г. – доктор технічних наук, професор, професор кафедри електронних обчислювальних машин Національного технічного університету України «Харківський політехнічний інститут».

П78 **Проблеми теорії та практики судової експертизи з питань інтелектуальної власності («Крайнєвські читання»):** Матер. VI Міжнар. наук.-практ. конф. (23 грудня 2022 р. м. Київ); за ред. д.т.н. М.О. Можаєва / НДЦСЕ з питань інтелектуальної власності Мін'юсту. Київ: Видавництво Ліра-К, 2022. – 112 с.
ISBN 978-617-520-433-7

Матеріали VI Міжнародної науково-практичної конференції «Проблеми теорії та практики судової експертизи з питань інтелектуальної власності» («Крайнєвські читання») присвячені актуальним проблемам теорії та практики судової експертизи з питань інтелектуальної власності. Поряд із питаннями теорії та методології судової експертизи у сфері інтелектуальної власності й питаннями щодо захисту права інтелектуальної власності значна увага приділяється об'єдиним з ними судово-економічним, товарознавчим дослідженням, а також дослідженням у сфері інформаційних технологій у контексті повномасштабної збройної агресії РФ проти України.

Запропоновані матеріали науково-практичної конференції розраховані на судових експертів, суддів і представників органів досудового розслідування, оцінювачів, науковців і представників громадськості, які цікавляться захистом права на об'єкти інтелектуальної власності.

Організатори конференції не в усіх випадках поділяють погляди, висловлені в наведених матеріалах, але з повагою ставляться до цінностей наукового плюралізму та свободи академічних досліджень.

УДК 347

ISBN 978-617-520-433-7

ЗМІСТ

4. ЕКСПЕРТИЗА КОМП'ЮТЕРНИХ ПРОГРАМ, БАЗ ДАНИХ І ТЕЛЕКОМУНІКАЦІЙ ПІД ЧАС ВИРІШЕННЯ ЕКСПЕРТНИХ ЗАВДАНЬ У СФЕРІ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Тюлєнєв Сергій Анатолійович,
кандидат економічних наук, директор Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України, судовий експерт

ПРО VI МІЖНАРОДНУ НАУКОВО-ПРАКТИЧНУ КОНФЕРЕНЦІЮ «ПРОБЛЕМИ ТЕОРІЇ ТА ПРАКТИКИ СУДОВОЇ ЕКСПЕРТИЗИ З ПИТАНЬ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ» («КРАЙНЄВСЬКІ ЧИТАННЯ»)

Ми живемо у складний і водночас дуже цікавий час, що ставить перед нами багато викликів і стимулює до розвитку.

Якщо проаналізувати, міжособистісна комунікація зазнала значних трансформацій, починаючи з 2019 року, коли пандемія «Ковід-19» змусила людство переглянути звички свого пересування і спілкування й перейти в онлайн-режим. А сьогодні так званому «живому» спілкуванню між людьми заважає значно гірша від «корона-вірусу» навала – повномасштабна війна, яку веде російська федерація проти України. Та попри це, ми залишаємось незламними і продовжуємо працювати, розвиватися і проводити міжнародні конференції.

23 грудня 2022 на базі Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України відбулася VI Міжнародна науково-практична конференція «Проблеми теорії та практики судової експертизи з питань інтелектуальної власності» («Крайнєвські читання»), присвячена, зважаючи на вимоги часу, аналізові розвитку й формування теоретичних і методичних основ судово-експертної діяльності з питань інтелектуальної власності та інформаційних технологій в умовах повномасштабної збройної агресії російської федерації проти України.

На розгляд учасників конференції були винесені такі питання:

− Теорія, історія та методологія судової експертизи з питань інтелектуальної власності в Україні та за кордоном.

− Наукова спадщина засновника НДЦСЕ з питань інтелектуальної власності, судового експерта і вченого П.П. Крайнєва (1952-2014 рр.).

– Судова експертиза у сфері авторського права та суміжних прав.

– Судова експертиза у сфері технічної творчості комерційних (фірмових) найменувань і торгівельних марок.

– Економічні дослідження та експертизи у сфері інтелектуальної власності.

– Експертиза комп'ютерних програм, баз даних і телекомунікацій під час вирішення експертних завдань у сфері інтелектуальної власності.

– Перспективи і шляхи розвитку та вдосконалення науки й освіти у сфері захисту інтелектуальної власності.

З огляду на особливості сучасних українських реалій, конференція відбувалася як в онлайн-режимі, так і очно. Попри всі означені перепони, на відеоконференції була присутня значна кількість осіба.

Відкрила конференцію директор Департаменту експертного забезпечення правосуддя Міністерства юстиції України, кандидат юридичних наук, заслужений юрист України Наталія Миколаївна Ткаченко, яка особисто завітала до Центру.

У режимі відеозв'язку із словами привітання до присутніх звернувся заступник Міністра юстиції України, кандидат юридичних наук Андрій Віталійович Гайченко.

Із вітальними промовами виступили директор Київського науково-дослідного інституту судових експертиз Міністерства юстиції України, доктор юридичних наук, заслужений юрист України Олександр Григорович Рувін і директор Одеського науково-дослідного інституту судових експертиз Міністерства юстиції України Дмитро Іванович Кішко.

Від Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» слово взяв заступник директора – завідувач Київського відділення ННЦ ІСЕ, вчений секретар Науково-консультативної ради при Голові Верховної Ради України, доктор юридичних наук, професор, заслужений юрист України Владислав Леонідович Федоренко. Львівський науково-дослідний інститут судових експертиз представив вельмишановний заступник директора з наукової роботи Богдан Мар'янович Лозинський.

Особливо приємно, що до конференції також долучилися зарубіжні колеги з Латвії, Грузії та Вірменії. Зокрема перед присутніми виступив заступник декана юридичного факультету Ризького університету імені Пауля Страдиня, доктор права, доцент, професор Вищої банківської школи Латвії Яніс Грасіс, який висловив підтримку й солідарність з українським народом у боротьбі з російськими агресорами й особисто, й від імені наукової спільноти Латвії.

Заступник директора Михайло Олександрович Можаєв розповів про діяльність Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України й основні перспективи розвитку установи.

Необхідно зауважити, що за період з січня по жовтень 2022 року до Центру надійшло на виконання 167 судових експертиз та експертних досліджень, з яких було виконано 133. З листопада надійшло на виконання 378 судових експертиз та експертних досліджень, станом на 22.12.2022 виконання складає 75 експертиз.

Водночас на виконанні фахівців Центру за зверненнями Служби безпеки України, Державного бюро розслідувань, Національної поліції та інших правоохоронних органів перебуває 47 судових експертиз щодо встановлення збитків, завданих військовою агресією російської федерації проти України.

А також за останні два місяці проведені платні експертизи на суму 903 тис. гривень, що становить 60 % від усіх зароблених протягом звітного періоду коштів.

Збільшення кількості експертиз і підвищення інших значущих показників експертної й наукової діяльності Науково-дослідного центру судової експертизи з питань інтелектуальної власності вимагає урізноманітнення видів експертних досліджень, що проводяться в установі. У зв'язку з повномасштабною збройною агресією Росії проти України виникає нагальна необхідність у проведенні різноманітних видів судових експертиз як у сфері досліджень руйнівного впливу дій агресорів на споруди й інфраструктуру країни, так і в галузі досліджень інформаційного простору, пов'язаних з ІТ-технологіями та з аналізом технологій комунікативного (пропагандистського) впливу, що застосовуються в інформаційній війні, яку

веде РФ проти української держави. На сьогоднішній день у НДЦСЕ з питань інтелектуальної власності наявні фахівці у галузі дослідження вибухотехніки, пожежної безпеки, електротехніки й інших технологічних досліджень, пов'язаних з руйнівними наслідками російського збройного вторгнення, а також спеціалісти з досліджень інформаційних і комунікативних технологій.

Розширення кола експертних досліджень вимагає, відповідно, внесення коректив у назву експертної установи, що повинна відображати загальні напрямки своєї діяльності. Також у січні 2023 планується відкриття нових лабораторій і нового приміщення Центру.

Інші доповідачі ознайомили аудиторію з основними напрямками й тенденціями розвитку теорії, історії і методології судової експертизи з питань інтелектуальної власності в Україні та закордоном, а також експертних досліджень у галузі інформаційних технологій.

Владислав Леонідович Федоренко ознайомив слухачів з основними віхами українського законотворення, що стосуються судової експертизи з питань інтелектуальної власності в контексті набуття Україною членства в Європейському Союзі. Наталія Валеріївна Кісіль розповіла про особливості підготовки судових експертів у сфері інтелектуальної власності та визначення їх професійних компетентностей.

Присутні могли почути цікаві й змістовні доповіді як експертів (співробітників Центру й працівників інших експертних установ України), так і науковців. Зокрема, професор кафедри кібербезпеки та інформаційних технологій Харківського національного економічного університету імені С. Кузнеця, доктор технічних наук, професор Сергій Геннадійович Семенов виступив із доповіддю, присвяченою дуже актуальній за нинішніх обставин темі: «Аналіз і порівняльні дослідження загроз кібербезпеки безпілотних літальних апаратів».

У всіх виступах розглянуті теми, що репрезентують найважливіші проблеми в галузі сучасного розвитку судово-експертної діяльності в умовах російської збройної агресії проти України. Більшість доповідей були наочно проілюстровані.

Таким чином, VI Міжнародна науково-практична конференція «Проблеми теорії та практики судової експертизи з питань інтелектуальної власності» («Крайнєвські читання») стала звітним заходом Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України щодо підсумків наукової роботи за 2022 рік в умовах російської агресії.

Учасники конференції за результатами усіх виступів прийняли Резолюцію, якою визначені перспективні напрямки науково-дослідної, організаційної й експертної діяльності Центру у 2023 році, а саме:

– необхідність подальшого розвитку науково-методичного експертного інструментарію, від технічних спеціальностей (у сфері військових, будівельно-технічних, земельно-технічних досліджень) до економічної оцінки ризиків, завданих підприємствам унаслідок повномасштабної збройної агресії РФ проти України;

– поглиблене експертне вивчення і впровадження інформаційних технологій для боротьби з російським агресором;

– актуалізація судово-експертної діяльності з питань інтелектуальної власності із чинними нормативно-процесуальними актами, що з'являються внаслідок інтеграційних процесів в українському законодавстві у контексті набуття Україною членства в Європейському Союзі.

1. СУДОВА ЕКСПЕРТИЗА У СФЕРІ АВТОРСЬКОГО ПРАВА ТА СУМІЖНИХ ПРА

Мотузка Катерина Андріївна,
магістр з інтелектуальної власності, судовий експерт сектору авторського права та суміжних прав лабораторії авторського права та інформаційних технологій, Науково-дослідний центр судової експертизи з питань інтелектуальної власності Міністерства юстиції України

ДОСЛІДЖЕННЯ ДИСЕРТАЦІЇ ЯК ОБ'ЄКТА АВТОРСЬКОГО ПРАВА

На сьогодні виникає багато питань у сфері дослідження та захисту об'єктів авторського права. Основним об'єктом дослідження в авторському праві є твір. Відповідно до ст. 8 Закону України «Про авторське право і суміжні права», об'єктами авторського права, зокрема, є літературні письмові твори белетристичного, публіцистичного, наукового, технічного або іншого характеру (книги, брошури, статті тощо), виступи, лекції, промови, проповіді та інші усні твори, драматичні, музично-драматичні твори, пантоміми, хореографічні та інші твори, створені для сценічного показу, та їх постановки, похідні твори, збірники творів, збірники обробок фольклору, енциклопедії та антології, збірники звичайних даних, інші складені твори за умови, що вони є результатом творчої праці за добором, координацією або упорядкуванням змісту без порушення авторських прав на твори, що входять до них як складові частини. Також варто окремо визначити таке поняття як твір. Закон України «Про авторське право і суміжні права» визначає твір як сукупність ідей, думок, міркувань, образів, наукових положень, оцінок, висновків, пропозицій тощо, які виникли в процесі творчої діяльності автора і знайшли свої відображення у певній об'єктивній формі. [3]

Коли йдеться про літературний твір наукового характеру, як об'єкт авторського права, то «Методика проведення експертних досліджень літературних творів наукового характеру», а також спеціальна наукова література визначають, що науковий твір:

«а) є результатом наукової творчості, а тому являє собою певний науковий результат;

б) цей результат має бути виражений у певній об'єктивній формі, а саме: втілений у літературний твір наукового характеру» [6, С. 19; 24,].

Одним із різновидів наукового твору є дисертація. Науковий твір – дисертація – готується й публічно захищається для здобуття наукового ступеню. В наш час наявність наукового ступеня надає певні преваги у підвищенні соціального статусу в суспільстві, визначає пріоритетність на ринку праці та сприяє просуванню на службі (кар'єрний зріст).

Дисертація має певну структуру твору, через яку розкривається результат творчої діяльності автора, а саме: актуальність вибраної теми, зв'язок роботи з науковими програмами, мету і завдання, об'єкт і предмет дослідження, а також наукову новизну та практичне значення. Отже, твори наукового характеру мають свою специфіку і певний підхід у дослідженні.

Враховуючи попит на отримання наукового ступеня, зріс ризик неправомірного використання у дисертації інших наукових творів, а також інших порушень прав автора.

Для розуміння випадків неправомірного використання творів потрібно розуміти, коли використання є дозволеним. Так, Цивільним кодексом України у ст. 444 визначено випадки правомірного використання твору без згоди автора, а саме: «Твір може бути вільно, без згоди автора та інших осіб, та безоплатно використаний будь-якою особою: 1) як цитата з правомірно опублікованого твору або як ілюстрація у виданнях, радіо- і телепередачах, фонограмах та відеограмах, призначених для навчання, за умови дотримання звичаїв, зазначення джерела запозичення та імені автора, якщо воно вказане в такому джерелі, та в обсязі, виправданому поставленою метою». При цьому,

особа, яка використовує твір, зобов'язана зазначити ім'я автора твору та джерело запозичення [2].

Водночас, законодавство не дає чіткого визначення обсягу твору, який може використовуватися іншим автором у своєму творі, та виправдовує поставлену мету. Це унеможливлює чітке, однозначне й об'єктивне встановлення обсягу припустимого цитування, оскільки оцінювання цього обсягу як допустимого/ не допустимого залежить від виду та характеру наукового твору, його обсягу та форми.

Отже, перед експертом найчастіше постає питання: «Чи використано у творі інший твір, в обсязі, що не перевищує такий, що відповідає зазначеній меті?» З метою виявлення збігів у зовнішній формі вираження досліджуваних творів проводиться порівняльний аналіз цих творів.

Інструкцією про призначення та проведення судових експертиз та експертних досліджень (п. 1.4.) визначено, що під час проведення експертиз (експертних досліджень) судові експерти, застосовують відповідні методи дослідження, методики проведення судових експертиз, а також нормативно-правові акти та нормативні документи (міжнародні, національні та галузеві стандарти, технічні умови, правила, норми, положення, інструкції, рекомендації, переліки, настановчі документи Держспоживстандарту України), а також чинні республіканські стандарти колишньої УРСР та державні класифікатори, галузеві стандарти й технічні умови колишнього СРСР, науково-технічну, довідкову літературу, програмні продукти тощо [5].

Вибір методів проведення судової експертизи чи експертного дослідження належить до компетенції судового експерта.

Таким чином експертом проводиться порівняльний аналіз текстів. Під час дослідження використовуються різні методики, методи для пошуку запозичень (ознак плагіату) у творах, зокрема у творах наукового характеру. Для виявлення збігів у творах, у тому числі у творах наукового характеру, проводитися порівняння двома можливими шляхами. Перший шлях – це ручний пошук, який здійснюється підчас дослідження експертом. Зрозуміло, що такий спосіб є досить трудомістким і значно розтягнутим у часі, окрім того, не може охопити весь масив

даних, які необхідно було б дослідити. Зі зростанням прогресу та появою різноманітних інновацій з'явився другий спосіб дослідження, а саме автоматизований пошук ознак використання одного твору в іншому, що здійснюється за допомогою спеціалізованого програмного забезпечення.

Програмне забезпечення значною мірою полегшує дослідницький процес експерта. Але програма має і свої недоліки: використання програмного забезпечення можливе тільки в тому випадку, коли об'єкти дослідження надані в електронному вигляді. Варто зазначити, що з появою таких програм з'явилися способи їх обходу.

Таким чином, під час проведенні дослідження дисертації варто покладатись не тільки на програмне забезпечення, а й на вже випробуванні часом методи дослідження.

Список використаних джерел:

1. Конституція України від 28.06.1996 № 254к/96-ВР (зі змінами № 742-VII від 21.02.2014).
2. Цивільний кодекс України від 16.01.2003 №435-IV (із змінами від 30.09.2015)
3. Закон України "Про авторське право та суміжні права" від 23.12.1993 року №3792-XII (зі змінами№ 927-19 від 13.01.2016).
4. Про наукову і науково-технічну діяльність: Закон України від 26 листопада 2015 р. Відомості Верховної Ради України. 2016. № 3. Ст. 25.
5. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень: Наказ Міністерства юстиції України від 08 жовтня 1998 року. *Офіційний вісник України*. 1998. № 46, С. 172, код акту 6348/1998
6. Методика проведення експертних досліджень літературних творів наукового характеру / В.Л. Федоренко (кер.), О.В. Голікова, Н.В. Кісіль, Н.Б. Климова, Н.Є. Яркіна та ін.: за наук. ред. акад. НАПрН України О.В. Скрипнюка. Київ: НДЦСЕ з питань інтелектуальної власності, 2019. 85 с.

2. СУДОВА ЕКСПЕРТИЗА У СФЕРІ ТЕХНІЧНОЇ ТВОРЧОСТІ КОМЕРЦІЙНИХ (ФІРМОВИХ) НАЙМЕНУВАНЬ І ТОРГОВЕЛЬНИХ МАРОК

Фоя Оксана Анатоліївна,
судовий експерт сектору засобів індивідуалізації лабораторії права промислової власності Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України

Ковальова Наталія Миколаївна,
в.о. завідувачки лабораторії права промислової власності Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України

МЕТОДИКА ЕКСПЕРТНОГО ДОСЛІДЖЕННЯ ПРОМИСЛОВИХ ЗРАЗКІВ

Основними напрямками діяльності Науково-дослідного центру судової експертизи з питань інтелектуальної власності (далі – Центр) є проведення прикладних науково-дослідних робіт у галузі судової експертизи з питань інтелектуальної власності, впровадження їх результатів в експертну, слідчу та судову практику; проведення судових експертиз й експертних досліджень із застосуванням засобів і методів судової експертизи; надання консультацій з питань, вирішення яких потребує спеціальних знань у сфері інтелектуальної власності.

Одним із провідних напрямків діяльності Центру є дослідження за спеціальністю 13.4 «Дослідження, пов'язані з промисловими зразками».

Промисловий зразок – результат інтелектуальної, творчої діяльності людини в галузі художнього конструювання [1].

Предметом судової експертизи промислових зразків є фактичні дані й обставини справи про властивості, ознаки, закономірності створення й використання промислових зразків, які встановлюються шляхом застосування спеціальних знань, з

метою надання висновку з питань, що є або будуть предметом судового розгляду.

Основним завданням досліджень, пов'язаних з промисловими зразками є надання висновку судового експерта про властивості, сутності ознаки, закономірності створення й використання промислових зразків, а також вирішення питання про дійсність / недійсність свідоцтва на відповідний промисловий зразок [2].

З метою підвищення якості висновків судового експерта у сфері інтелектуальної власності Центром було започатковано Науково-дослідну роботу (НДР) «Методика експертного дослідження промислових зразків» (далі – Методика) за спеціальністю 13.4 – «Дослідження, пов'язані з промисловими зразками». Керівником наукової роботи призначено Ковальову Наталію Миколаївну, яка на теперішній час виконує обов'язки завідувачки лабораторією права промислової власності Центру і є судовим експертом вищого кваліфікаційного класу. Робота з розробки Методики проводилася протягом 2021 – 2022 років.

Метою роботи є розроблення методичних рекомендацій щодо особливостей проведення експертних досліджень, пов'язаних із промисловими зразками.

На сьогоднішній день в Україні відсутня методика проведення судових експертиз, пов'язаних із промисловими зразками, яка б була внесена в установленому порядку до Реєстру методик проведення судових експертиз Мін'юсту України.

Разом з тим, експертами проводиться значна кількість судових експертиз та експертних досліджень, пов'язаних із промисловими зразками. У практиці судової експертизи на розгляд експерта досить часто ставляться питання, що викликані порушенням прав власника на промисловий зразок, визнанням свідоцтва (до 2020р. – патенту) на промисловий зразок недійсним у зв'язку із порушенням прав третіх осіб, визнанням свідоцтва на промисловий зразок недійсним у зв'язку із невідповідністю заявленого умовам надання правової охорони. Відсутність єдиної методики проведення судових експертиз, пов'язаних з промисловими зразками, призводить до використання експертами різних підходів і методів під час проведення судових експертиз й експертних досліджень, що в свою чергу є підставою

для судів призначати повторні судові експертизи і призводить до затягування строків вирішення спорів у судових інстанціях.

Дана методика має використовуватися експертами в галузі інтелектуальної власності науково-дослідних установ судових експертиз Міністерства юстиції України під час проведення судових експертиз у сфері інтелектуальної власності з дослідження промислових зразків.

Створення «Методики проведення експертного дослідження промислових зразків» є актуальним також, зважаючи на оновлення чинного законодавства про охорону права на промислові зразки. Закон України «Про охорону прав на промислові зразки» було змінено з метою покращення механізму охорони прав на промислові зразки та гармонізації законодавства України із законодавством ЄС. Методика створена з урахуванням змін до означеного Закону.

Так, у 2020 році були внесені зміни до Закону України «Про охорону прав на промислові зразки», що призвели до змін в категоріально-термінологічному апараті. Було оновлено механізми правової охорони промислових зразків, права й обов'язки суб'єктів прав на промислові зразки, порядок визнання Апеляційною палатою прав на промислові зразки недійними.

У новій редакції Закону України «Про охорону прав на промислові зразки» від 14.10.2020 року, порівняно з редакцією Закону України «Про охорону прав на промислові зразки» від 05.10.2012 року, змінено саме визначення об'єкту охорони. Відповідно до Закону, промисловим зразком може бути зовнішній вигляд виробу або його частини, що визначається, зокрема, лініями, контурами, кольором, формою, текстурою та/або матеріалом виробу, та/або його оздобленням [1]. Також зазнав уточнень перелік об'єктів, що не можуть отримати правову охорону як промислові зразки.

У новій редакції Закону додано ще один критерій охороноздатності, окрім новизни, – індивідуальний характер.

Відповідно до Закону промисловий зразок визнається таким, що має індивідуальний характер, якщо загальне враження, яке він справляє на інформованого користувача, відрізняється від загального враження, яке справляє на такого користувача будь-який інший промисловий зразок, доведений до загального відома.

Для оцінки індивідуального характеру береться до уваги ступінь свободи автора під час створення промислового зразка [1].

Чи відповідає промисловий зразок критеріям охороноздатності, новизни й індивідуального характеру встановлюється, для зареєстрованого промислового зразка, до дати подання заявки до НОІВ або, якщо заявлено пріоритет, до дати її пріоритету, для незареєстрованого промислового зразка, – до дати, на яку промисловий зразок, вперше був доведений до загального відома.

Зареєстрований промисловий зразок вважається доведеним до загального відома, якщо був опублікований у результаті здійснення державної реєстрації або з інших підстав, або був експонований на виставці, використаний у торгівлі або іншим чином оприлюднений, крім випадків, коли такі події не могли стати відомими під час звичайного провадження господарської діяльності у колах, що спеціалізуються у відповідній галузі і провадять свою діяльність на території України, до дати подання заявки до НОІВ або, якщо заявлено пріоритет, до дати пріоритету. Незареєстрований промисловий зразок вважається доведеним до загального відома, якщо він був опублікований, експонований на виставці, використаний у торгівлі або в інший спосіб оприлюднений таким чином, що під час звичайного провадження господарської діяльності такі заходи з об'єктивних причин могли стати відомими у колах, що спеціалізуються у відповідній галузі і провадять свою діяльність на території України. Не вважається доведеним до загального відома промисловий зразок, розкритий третій особі за явної чи неявної умови збереження конфіденційності [1].

Уведено таке поняття як незареєстрований промисловий зразок, якому запроваджена правова охорона.

В редакції Закону України «Про охорону прав на промислові зразки» від 05.10.2012 року не застосовувались такі поняття як «індивідуальний характер», «загальне враження», «інформований користувач» і «ступінь свободи автора», які були введені в нову редакцію Закону.

Збільшено обсяг прав власника промислового зразка – сукупність суттєвих ознак замінили враженням, яке промисловий зразок справляє на поінформованого користувача; запроваджено можливість скасування реєстрації промислового зразка в

позасудовому порядку в Апеляційній палаті; збільшено термін охорони з 15 до 25 років; змінення вигляду охоронного документа з «патенту» на «свідоцтво». Ці та інші положення оновленого Закону України «Про охорону прав на промислові зразки» зумовлюють нагальну потребу в розробленні єдиних методичних підходів щодо дослідження такого об'єкта інтелектуальної власності, як промисловий зразок.

Підсумовуючи зазначене вище, слід визнати, що Методика є актуальною у зв'язку із внесенням змін до Закону України «Про охорону прав на промислові зразки», та створить єдиний підхід до проведення судових експертиз й експертних досліджень за спеціальністю 13.4 «Дослідження, пов'язані з промисловими зразками».

НДР «Методика проведення експертного дослідження промислових зразків» призначена для безпосереднього використання атестованими судовими експертами під час проведення судових експертиз за спеціальністю 13.4 «Дослідження, пов'язані з промисловими зразками», а також для підготовки і підвищення кваліфікації судових експертів за цією спеціальністю.

Ця Методика також може використовуватись судами і органами досудового розслідування для призначення експертизи, а також фізичними і юридичними особами під час замовлення експертних досліджень промислових зразків як об'єктів права інтелектуальної власності. Матеріали НДР «Методика проведення експертного дослідження промислових зразків» може бути використана як основа для подальшого написання методик і методичних рекомендацій зі спорідненої проблематики.

Список використаних джерел:

1. Про охорону прав на промислові зразки: Закон України № 3688-XII від 15 грудня 1993 р. Відомості Верховної Ради України. 1994. № 7. Ст. 34.

2. Судова експертиза об'єктів права інтелектуальної власності в Україні: навч.-метод. вид.; В.Л. Федоренко (кер.), О.Г. Адлер, Л.П. Тимощик, Н.М.Ковальова, О.В. Голікова, Т.М. Чабанець та ін.; за ред. проф. В.Л. Федоренка, вид. 2-ге, розшир. і доп. / НДЦСЕ судової експертизи з питань інтелектуальної власності Мін'юсту. Київ : Видавництво Ліра-К, 2022, 196 с.

Заніна Тетяна Анатоліївна,
старший науковий співробітник лабораторії товарознавчих досліджень та досліджень об'єктів інтелектуальної власності Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М.С. Бокаріуса»

Копитько Алла Петрівна,
старший науковий співробітник лабораторії товарознавчих досліджень та досліджень об'єктів інтелектуальної власності Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М.С. Бокаріуса»

Мануленко Олександра Володимирівна,
старший науковий співробітник лабораторії товарознавчих досліджень та досліджень об'єктів інтелектуальної власності Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М.С. Бокаріуса»

ПРАВОВИЙ ЗАХИСТ ЕТИКЕТОК ТА УПАКОВОК, ЯК ОСОБЛИВИХ ОБ'ЄКТІВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

У роботі судових експертів з питань інтелектуальної власності нерідко виникають ситуації, коли досліджуваний об'єкт одночасно відноситься до сфер дії декількох спеціальних законів. Зокрема, це стосується таких специфічних об'єктів правової охорони, як етикетка та упаковка.

Упаковка і етикетка являють собою ключові елементи в боротьбі за споживача. Як показують багато маркетингових досліджень при первинній покупці 75% мотивації припадає на упаковку або на етикетку, саме тому цим елементам виробники приділяють особливо пильну увагу.

З точки зору цивільного права засоби індивідуалізації продукції або компанії (яскрава етикетка, упаковка, що запам'ятовується) є об'єктами інтелектуальної власності. Об'єкти інтелектуальної власності – це результати інтелектуальної діяльності, тобто діяльності дизайнерів і художників. Конкретні об'єкти інтелектуальної власності названі в різних законах і, відповідно, ними і охороняються, закріплюючи за правовласниками виключні права на

використання даних об'єктів. Таким чином, упаковка та етикетка – це особливі результати інтелектуальної діяльності, які можуть охоронятися в якості різних об'єктів інтелектуальної власності.

Ідентифікація товарів за зовнішнім виглядом та інформацією на упаковці свідчить про наявність у цій категорії розрізнювальних особливостей, отже, упаковка може служити засобом для індивідуалізації товарів. Такі ж особливості притаманні іншим маркетинговим засобам – етикеткам, биркам, ярликам тощо, тому різні види упаковок або етикеток можуть бути зареєстровані як торговельні марки.

Розробка макетів для упаковок і оформлення етикеток часто виконується дизайнерами і художниками, тому є результатом творчості. Створювані предмети володіють новизною, оригінальністю, мають вигляд готового виробу і можуть охоронятися як промислові зразки.

Дизайн упаковки та етикетки може також охоронятися нормами авторського права як твір, якщо носить творчий характер і є результатом творчої роботи художника або дизайнера.

Вибір виду захисту залишається за виробником. Цей вибір залежить від особливостей упаковки й етикетки, а також від того, в чому полягає творчість їх створення і їх цінність.

Поняття «етикетка» розкривається Законом України «Про інформацію для споживачів щодо харчових продуктів»: «етикетка (стікер) – бирка, напис, позначка, графічне або інше зображення, написане, надруковане, нанесене з використанням трафарету, марковане, витиснене або відбите на упаковці чи додане до упаковки або тари, в якій знаходиться харчовий продукт».

Етике́тка (відповідно до ДСТУ 3321-96. Система конструкторської документації) – експлуатаційний документ, який містить основні показники якості і технічні характеристики виробу, ґарантовані підприємством-виробником.

Тобто, виходячи з наведеного, етикетка – засіб інформування та ідентифікації, що містить, як правило, зображення, текстовий і рекламний матеріал про упаковану продукцію та її виробника, яке розміщується безпосередньо на упаковці.

Метою етикетки є здійснення маркетингової функції з просування товару за допомогою використання на етикетці привабливих графічних і описових елементів.

Упаковка – результат проведення комплексу заходів, що забезпечують захист продукції від пошкоджень і втрат, від негативних факторів навколишнього середовища і полегшує процес оберту продукції під час транспортування, складування, реалізації тощо.

Останнім часом роль упаковки значно підвищилася. Зараз основне її завдання полягає в залученні уваги до товару і наданні інформації про нього. Це стимулює покупку товару, а також виділяє його серед багатьох аналогічних товарним знаком, текстом, формою або кольоровим оформленням. Упаковка, таким чином, набула значення рекламного засобу, розрахованого на широке коло споживачів і довгостроковий вплив.

Варіантом охорони упаковки або етикетки в якості торговельної марки може бути реєстрація комбінованого позначення.

У відповідності до ст. 1 Закону України «Про охорону прав на знаки для товарів і послуг»: «Торговельна марка – позначення, за яким товари і послуги одних осіб відрізняються від товарів і послуг інших осіб».

За класичним визначенням, упаковка та етикетка є різновидом комбінованих товарних знаків. Дійсно, одне з її призначень – це основна функція торговельної марки взагалі: відрізняти товари одного виробника від однорідних товарів інших виробників. Так чи інакше, етикетка (упаковка) використовується для позначення (а отже, відмінності) товару конкретного виробника, і в цьому полягає її суть як об'єкта, що підлягає охороні згідно із Законом «Про охорону прав на знаки для товарів і послуг».

Закон України «Про охорону прав на знаки для товарів і послуг» передбачає досить дієві засоби захисту прав власників торговельних марок.

Згідно з пунктом 2 статті 20 зазначеного Закону: «власник свідоцтва може також вимагати усунення з товару, його упаковки незаконно використаної торговельної марки або позначення, схожого з нею настільки, що їх можна сплутати, або знищення виготовлених зображень торговельної марки або позначення, схожого з нею настільки, що їх можна сплутати».

Відповідно до пункту 4 статті 16 Закону України «Про охорону прав на знаки для товарів і послуг»:

«Використанням торговельної марки визнається:

– нанесення її на будь-який товар, для якого торговельну марку зареєстровано, упаковку, в якій міститься такий товар, вивіску, пов'язану з ним, етикетку, нашивку, бирку чи інший прикріплений до товару предмет, зберігання такого товару із зазначеним нанесенням торговельної марки з метою пропонування для продажу, пропонування його для продажу, продаж, імпорт (ввезення) та експорт (вивезення);

– застосування її під час пропонування та надання будь-якої послуги, для якої торговельну марку зареєстровано;

– застосування її в діловій документації чи в рекламі та в мережі Інтернет.

Торговельна марка визнається використаною, якщо її застосовано у формі зареєстрованої торговельної марки, а також у формі, що відрізняється від зареєстрованої торговельної марки лише окремими елементами, якщо це не змінює в цілому відмітності торговельної марки».

Звідси зрозуміло, чому найпоширеніше питання, що стоїть перед судовим експертом під час розгляду справ про порушення прав власника свідоцтва, має стандартний зміст: чи є позначення, застосоване на упаковці товару виробника А (етикетка), схожим настільки, що його можна сплутати із зображенням знака для товарів і послуг (торговельної марки) за свідоцтвом №..., що належить виробнику Б?

Упаковки та етикетки у якості торговельної марки можуть бути зареєстровані як комбіновані.

Комбіновані торговельні марки – позначення, які складаються з декількох різновидів елементів: словесних, візуальних або голографічних. Наприклад, торговельна марка включає найменування і візуальний елемент, пов'язаний з діючою хімічною речовиною або інформує споживача про те, для яких цілей може бути використаний препарат (зображення хворого горла, голови тощо).

Комбіновані позначення можуть порівнюватися із комбінованими позначеннями та з тими видами позначень, які входять до його складу як елементи.

Під час дослідження схожості комбінованих позначень визначається як схожість усього позначення в цілому, так і його

складових елементів із урахуванням значущості розташування тотожних або схожих елементів.

При порівнянні комбінованих позначень в першу чергу виділяється домінуючі елементи, які визначають загальне враження від позначення. Як правило, домінуючим елементом позначення, яке складається зі слова та зображення, є словесний елемент, тому що його називають під час замовлення товарів і послуг.

Торговельна марка й упаковка (етикетка) призначені для виконання різних функцій і до них відповідно ставляться різні вимоги.

Торговельна марка індивідуалізує товар, вироблений певною юридичною особою або індивідуальним підприємцем.

Торговельна марка не може складатися тільки з описових елементів, необхідність використання яких в цивільному обороті може виникнути у будь-якої особи, яка виробляє такий саме або однорідний товар (при встановленні однорідності товарів визначається принципова можливість виникнення у споживача уявлення про приналежність цих товарів одному виробнику).

Упаковка (етикетка) слугує джерелом інформації про товар. На відміну від торговельної марки упаковка (етикетка) повинна містити, в залежності від встановлених вимог до маркування товару, в першу чергу, описові елементи: зазначення виду товару, його характеристики, найменування виробника і його місцезнаходження тощо. Етикетка може містити товарний знак виробника товару.

Оскільки обсяг правової охорони, що надається зареєстрованим торговельним маркам, визначається зображенням позначення та переліком товарів і послуг, установлення ступеня схожості торговельних марок є комплексним дослідженням, яке складається з двох взаємопов'язаних стадій:

1) порівняння між собою зображень позначень щодо визначення ступеня їх схожості;

2) порівняння між собою товарів і/або послуг, на які поширюється правова охорона досліджуваних позначень, і визначення їх спорідненості (однорідності).

Оригінальна компоновка всіх елементів упаковки, яка грає найважливішу роль в просуванні товарів, дизайнерські розробки

і нові художні рішення у виробі (промисловий дизайн) можуть отримати охорону в якості промислового зразка. Умовами надання правової охорони упаковок як промислових зразків є наявність новизни та оригінальності у об'єктів.

Пункт 2 статті 5 Закону України «Про охорону прав на промислові зразки» визначає, що «промисловим зразком може бути зовнішній вигляд виробу або його частини, що визначається, зокрема, лініями, контурами, кольором, формою, текстурою та/або матеріалом виробу, та/або його оздобленням».

Правову охорону в якості промислового зразка отримують етикетки, упаковки, тара, створені на основі художньо-конструкторських рішень, що визначають зовнішнє виконання виробів. Захист дизайнерських рішень в якості промислових зразків більш надійна і дозволяє доводити авторство в суді.

Істотними ознаками упаковки як промислового зразка є ознаки, що характеризують естетичні особливості зовнішнього вигляду виробу, а саме – конфігурацію, форму, орнаменти, кольорову гаму, лінії, контури виробу.

Відповідно до пункту 2 статті 20 Закону України «Про охорону прав на промислові зразки»:

«Використанням зареєстрованого промислового зразка визнається виготовлення виробу із застосуванням зареєстрованого промислового зразка, застосування такого виробу, пропонування для продажу, в тому числі через Інтернет, продаж, імпорт (ввезення), експорт (вивезення) та інше введення його в цивільний оборот або зберігання такого виробу в зазначених цілях.

Виріб визнається виготовленим із застосуванням зареєстрованого промислового зразка, якщо зовнішній вигляд такого виробу або його частини справляє на поінформованого користувача таке саме загальне враження, як і промисловий зразок, що охороняється.»

Умови надання правової охорони для торговельної марки і промислового зразка абсолютно різні, тому такі об'єкти інтелектуальної власності розрізняються за багатьма критеріями:

1. Елемент захисту.

Торговельна марка являє собою деяке позначення (словесне, образотворче, комбіноване або об'ємне), що слугує для

індивідуалізації товарів і послуг. Охороняється в тому вигляді, в якому вона представлена для реєстрації, забезпечує захист для зазначених у переліку товарів по МКТП.

Промисловий зразок охороняє рішення зовнішнього вигляду виробу промислового або кустарно-ремісничого виробництва. Тобто, промисловий зразок, зокрема, може використовуватися для захисту дизайну товару, його форми, зовнішнього вигляду і використовуваної для нього упаковки.

2. Правовласники.

Правовласником торговельної марки може бути тільки юридична особа або фізична особа, яка має статус індивідуального підприємця, а ось фізична особа, яка не має статусу індивідуального підприємця, правовласником торгової марки бути не може. Законодавством не передбачено жодних обмежень на територію реєстрації юридичної особи (або громадянство фізичної особи).

Правовласником свідоцтва на промисловий зразок може бути як фізична (зокрема й та, яка має статус індивідуального підприємця), так і юридична особа, знову ж таки без обмежень в частині громадянства.

3. Термін дії та умови захисту прав.

Термін дії торгівельної марки 10 років і можливе його продовження без обмежень на такий же термін. Термін дії свідоцтва на промисловий зразок 5 років, можливе продовження, але дія свідоцтва не перевищує 25 років

Власник торговельної марки зобов'язаний використовувати позначення, а власник промислового зразка таким обов'язком не наділений, свідоцтво не може бути анульованим, навіть якщо він (промисловий зразок) не використовується.

Одночасне використання охорони оригінальної упаковки, яскравої етикетки в якості торговельної марки і промислового зразка дозволяє створити максимальний правовий захист, а у випадках припинення охорони по одному з об'єктів (наприклад, визнання товарного знака загальновідомим) заявник зможе мати захист на іншій підставі, за свідоцтвом на промисловий зразок.

Враховуючи найбільш яскраві приклади експертної практики при проведенні досліджень у справах, що стосуються спорів щодо оригінальної упаковки або яскравої етикетки, слід

зазначити, що ці справи є дуже різними за своїми обставинами та змістом позовних вимог. Проте, їх поєднує те, що у ході розгляду цих справ було наочно доведено: упаковки (етикетки), зареєстровані як торговельні марки або як промислові зразки, мають певну специфіку, тому їх правова охорона і захист вимагають адекватного розширеного підходу.

Список використаних джерел:

1. Про охорону прав на знаки для товарів і послуг: Закон України від 15 грудня 1993 року № 3689-XII. URL: https://zakon.rada.gov.ua/laws/show/3689-12#Text (дата звернення: 18.11.2022).

2. Про охорону прав на промислові зразки: Закон України від 15 грудня 1993 року № 3688-XII. URL: https://zakon.rada.gov.ua/laws/show/3688-12#Text (дата звернення: 18.11.2022).

3. Методичні рекомендації щодо особливостей проведення експертних досліджень, пов'язаних з етикетками: звіт НДР (заключ.) / МІОУ, Науково-дослідний центр судової експертизи з питань інтелектуальної власності; кер. Н. М. Ковальова; викон.: Т. М. Чабанець, О. А Фоя, Н. Б. Климова, А. П. Копитько, Т. А. Заніна.- 0119U001355.- НДЦСЕ, 2020, – 98 с.

3. ЕКОНОМІЧНІ ДОСЛІДЖЕННЯ ТА ЕКСПЕРТИЗИ У СФЕРІ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Тюлєнєв Сергій Анатолійович,
кандидат економічних наук, директор Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України, судовий експерт

Тимощик Лілія Павлівна,
кандидат економічних наук, учений секретар Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України, судовий експерт, оцінювач

ШЛЯХИ ОЦІНКИ ШКОДИ ДЛЯ НЕМАТЕРІАЛЬНИХ АКТИВІВ В КОНТЕСТІ РОСІЙСЬКОЇ ЗБРОЙНОЇ АГРЕСІЇ

Вступ. Гібридизм збройної агресії РФ веде до асиметричних дій російського уряду в заподіянні шкоди Україні, зокрема і для компаній. Одним з таких інструментів гібридної збройної агресії РФ є зумисне руйнування бізнесу на території України. Причому така заподіяна шкода орієнтується не тільки на руйнування виробничих майданчиків і логістичних систем, але й на винищення нематеріальних активів компаній в Україні, що є іншим ключовим драйвером їхньої конкурентоспроможності як на коротко-, так і довгостроковому горизонтах поряд із більш традиційними для фокусу дослідників і практиків матеріальними активами. Відповідно це зумовлює значну актуальність проблематики оцінки шкоди для нематеріальних активів, а також пошуку інструментарію збереження цих активів як критично важливого драйверу для підтримання функціонування бізнесу на короткостроковому горизонті в контексті воєнного часу та на довгостроковому горизонті на етапі повоєнної відбудови.

Постановка завдання. Метою цього дослідження є ідентифікація особливостей оцінки шкоди для нематеріальних

активів з урахуванням сучасного контексту збройної агресії РФ. В межах цього дослідження сформовано ряд завдань:

− визначити сутність нематеріальних активів і їхню роль у конкурентоспроможності бізнесу з особливим фокусом на сучасні умови гібридної збройної агресії РФ;

− здійснити аналіз підходів до оцінки завданої шкоди, нематеріальним активам під час російської збройної агресії;

− сформувати пропозиції зі збереження нематеріальних активів в умовах сучасних викликів бізнес-середовища.

Результати. Міжнародний стандарт фінансової звітності *IAS* 38 [1] визначає нематеріальні активи як ідентифікований негрошовий актив, що не має фізичної форми. Зауважимо, що нематеріальні активи не є фізичними активами (як, наприклад, обладнання, сировина або товарні запаси), але в сучасних умовах ведення бізнесу складають суттєву цінність для компанії або в розрізі її іміджу на ринку, або здатності вести бізнес в сучасних умовах діджиталізованої постіндустріальної економіки [2-3]. Відповідно нематеріальні активи є ключовим драйвером забезпечення конкурентоспроможності бізнесу на ринку – особливо у сучасних турбулентних умовах бізнес-середовища, що були спричинені збройною агресією РФ.

Найбільш поширені типи нематеріальних активів такі:

− торгові марки;

− патенти;

− інтелектуальна власність;

− ділова репутація.

Відповідно, виходячи з природи та характеристик нематеріальних активів, постає складне завдання оцінки шкоди, що була заподіяна цим активам компаній в умовах збройної агресії РФ. Розглянемо детальніше можливий підхід до означеної проблематики.

Збройна агресія РФ, накладення санкцій, контрзаходи з боку російського уряду, вихід компаній з російського ринку вплинули на компанії та нематеріальні активи, які перебувають в їхній власності. Відповідно вказані активи можуть потенційно бути знеціненими внаслідок комплексу описаних вище подій [4-5]. Отже, ключовими факторами, що можуть спричинити знецінення нематеріальних активів є:

– наявність значних активів або провадження бізнес-діяльності та російській або білоруській території;

– часткове або повне ведення бізнесу в Україні;

– перебування бізнесу в списку компаній або галузей економіки, що підпадають під санкції або контрзаходи російського уряду;

– залежність від постраждалих ланцюжків постачання;

– руйнування бізнес-майданчику (часткове або повне).

Відповідно в межах кращих галузевих практик знецінення нематеріальних активів внаслідок заподіяної шкоди має відбуватися в рамках підходу оцінки грошових потоків від даного нематеріального активу. Відповідно по факту події, яка спричинила вибуття нематеріального активу, необхідно визначити суму відшкодування – вартість у використанні (*Value in Use, VIU*) і справедливу вартість за вирахуванням витрат на вибуття (*Fair Value Less Costs of Disposal, FVLCD*) – активу, який генерує грошові кошти (*Cash-Generating Unit, CGU*), оскільки це необхідно для прогнозування майбутніх грошових потоків [2-5]. Зауважимо, що прогнози грошових потоків і прогнозний бюджет компанії зазвичай слугують відправною точкою для аналітичної процедури дисконтування грошових потоків, які використовуються для розрахунку суми відшкодування. Згідно з міжнародними стандартами фінансової звітності *IAS* 36 [6] і *IFRS* 13 [7]. Значні припущення, такі як прогноз продажів, темпи зростання й темпи інфляції, маржинальність, капітальні витрати і ставки дисконтування потребуватимуть переоцінки та оновлення відповідно до значних змін в економічних і ринкових умовах. Грошові потоки, що використовуються для підрахунку *FVLCD*, мають бути оновлені. Це дозволить відобразити припущення, які використовували б учасники ринку на основі ринкових умов та інформації, доступної на звітну дату.

Підчас оцінки шкоди для нематеріальних активів у сучасних умовах в межах виділеної вище аналітичної процедури дисконтування грошових потоків від нематеріального активу, що знецінився, важливо відобразити ризик у ставці дисконтування. Зауважимо, що ставка дисконтування, яка використовується для дисконтування прогнозованих грошових за обома підходами, може бути значного змінена внаслідок зростання ризиків [8-9].

Зокрема, ставка дисконту повинна відображати вплив змін процентних ставок і ризикового середовища на звітну дату. Звертаємо увагу на те, що в разі застосування методу очікуваного грошового потоку під час оцінки нематеріальних активів, ставка дисконтування має виключати ризики, які були відображені в грошових потоках, з метою уникнення ситуації подвійного врахування цього показника.

За оцінки майбутніх грошових потоків від оцінюваних нематеріальних активів важливо враховувати вплив санкцій, зміни цін на товари й сировину, зміни бізнес-середовища, в якому компанії здійснюють свою бізнес-діяльність. Така оцінка є складним завданням унаслідок впливу ефекту невизначеності в розрізі короткострокових подій і довгострокових наслідків на повоєнному етапі розвитку. Відповідно в межах аналізу *VIU* прогнози грошових потоків мають базуватися на обґрунтованих припущеннях, що являють найбільш якісну можливу оцінку стану бізнес-середовища на період корисного використання оцінюваного нематеріального активу.

Зауважимо, що під час здійснення означеної аналітичної процедури варто базувати прогнози у впливу збройної агресії РФ на національну економіку України на зовнішніх надійних джерелах. Поміж таких джерел можемо в першу чергу виділити економічні прогнози центральних банків і міжнародних фінансових інститутів. Додатково можливо використати прогнози знаних незалежних дослідницьких центрів, що мають надійну репутацію [10-11].

Відображення ризику в ставці дисконтування в межах здійснюваної аналітичної процедури з оцінки нематеріальних активів в умовах збройної агресії може мати певні особливості. Зокрема, турбулентність може мати значний вплив на премії за ризик, притаманні для компаній (ризик фінансування; ризик, притаманний країні; ризик у розрізі прогнозування), які використовуються для визначення відповідної ставки дисконтування для майбутніх грошових потоків. Розкриємо вказані ризики більш детально. Ризик фінансування являє собою премію, яка враховує потенційні ускладнення фінансування капітальних інвестицій компанії або її операційних витрат як у коротко-, так довгостроковій перспективі. Ризик, притаманний

країні є премією, що враховує додатковий ризик, пов'язаний із здійсненням бізнес-діяльності у відповідній країні. Ризик в розрізі прогнозування являє собою премію, що враховує вищий рівень невизначеності під час розрахунку фінансово-економічних прогнозів на найближчу перспективу, що зумовлено складністю адекватного прогнозування масштабу впливу збройної агресії у різних її виявах.

У межах прогнозування грошових потоків можна використовувати два підходи, а саме, традиційний підхід, що використовує єдиний прогноз грошових потоків, або підхід очікуваного грошового потоку (*Expected Cash Flow, ECF*), що в свою чергу застосовує кілька зважених за ймовірністю прогнозів грошових потоків [2-5]. Відповідно підхід *ECF* може бути більш адекватним сучасній ситуації для визначення й моделювання різних потенційних результатів – наприклад, моделювання різних сценаріїв санкційних заходів.

Зауважимо, що існує кілька основних ризиків для нематеріальних активів компанії. Подамо зазначених перелік на рис. 1.

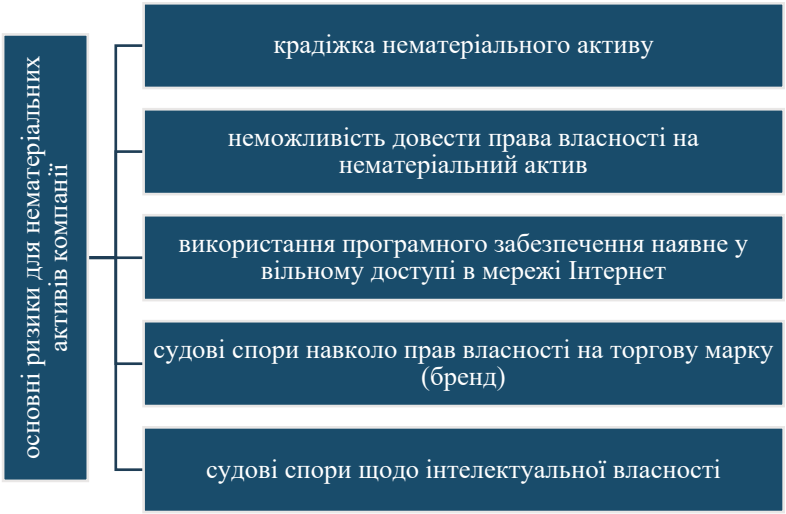

Рис. 1. Основні ризики для нематеріальних активів компанії
Джерело: складено автором.

Зауважимо, що в сучасній економіці, яка перебуває на постіндустріальному етапі розвитку, нематеріальні активи є ключовим драйвером розвитку та створення вартості для різноманітних груп стейкхолдерів. Відповідно завдання збереження нематеріальних активів і оцінка шкоди, що заподіяна даним активам в умовах турбулентного середовища (зокрема, російської збройної агресії), є ключовою проблематикою як для компаній, так і для інших зацікавлених сторін на мікро- та макрорівнях [12-13].

Відповідно компаніям необхідно впроваджувати систему обов'язкового перманентного моніторингу стану нематеріальних активів, а також розробити та впровадити ряд засобів контролю, що є невід'ємною складовою частиною надійного комплексу з управління ризиками компанії. До того ж, структура моніторингу й контролю за нематеріальними активами вимагають вмонтованості проблематики якісного та цілісного функціонування комплексу нематеріальних активів компанії у ключові бізнес-процеси компанії, які створюють основу для вартості її нематеріальних активів [14-15]. В межах цього завдання необхідно здійснити низку кроків:

Крок 1. Сформувати розуміння топ-менеджерів компанії щодо важливості нематеріальних активів у системі створення вартості для стейкхолдерів, а також системи ризиків, що пов'язані з нематеріальними активами.

Крок 2. Впровадити узгоджені бізнес-практики й бізнес-процеси на рівні компанії, що забезпечують збереження нематеріальних активів і ділової репутації компанії;

Крок 3. Розширення системи моніторингу й контролю стану нематеріальних активів, зокрема, на рівні наглядової ради компанії.

Розкриємо більш детально виділені вище кроки в контексті забезпечення збереження нематеріальних активів компанії в умовах збройної агресії РФ.

Відповідно в межах Кроку 1 топ-менеджмент компанії має розуміти, які ключові бізнес-процеси впливають на нематеріальні активи і стан ділової репутації компанії в умовах турбулентності бізнес-середовища. В розрізі даних бізнес-процесів топ-менеджери мають фокусуватися на тому, якими є ключові

показники ефективності для цих бізнес-процесів в контексті збереження нематеріальних активів, а також які сигнали з раннього попередження загроз в площині нематеріальних активів.

Можемо рекомендувати розробити та впровадити систему раннього попередження в напрямку збереження нематеріальних активів, а також адекватних для даної проблематики засобів контролю й моніторингу стану нематеріальних активів компанії. Наголосимо, що дана система засобів контролю та моніторингу може бути використана в практичній площині як для виявлення та усунення загроз для нематеріальних активів, так посилення поточного стану та розширення нематеріальних активів і відповідно їх ринкової вартості [16-17].

Запропонована система заходів контролю й моніторингу в площині стану нематеріальних активів може бути реалізована за допомогою таких інструментів:

– *бенчмаркінг системи збереження нематеріальних активів*: цей інструмент являє собою порівняння цільового і поточного стану нематеріальних активів, а також порівняння стану різних груп активів за цільовими й фокусними групами активів як всередині компанії, так і поза її межами;

– *аналіз розриву в контексті збереження нематеріальних активів*: цей інструмент сприяє подоланню розбіжностей між цільовим і поточним станом нематеріальних активів з точки зору існуючої бізнес-практики всередині компанії та зразковою передовою бізнес-практикою в площині проблематики збереження нематеріальних активів у турбулентному середовищі. Також він слугує підґрунтям для розробки та імплементації стратегічного плану стосовно мінімізації ризиків в площині нематеріальних активів, що сприятиме усуненню ідентифікованого розриву та приведення стану бізнес-практик компанії у відповідність до кращих галузевих стандартів;

– *економіко-математичне моделювання ризиків для нематеріальних активів*: в межах цього інструменту регресійного аналізу здійснюється робота з виявлення ключових драйверів для ризиків в площині нематеріальних активів, визначення характеру впливу цих ризиків на стан нематеріальних активів у коротко- й довгостроковому періодах, сценарне

прогнозування різноманітних кризових ситуацій стосовно стану нематеріальних активів, оцінка потенційної шкоди для нематеріальних активів в розрізі різноманітних сценаріїв кризових ситуацій;

– *стрес-тестування стану нематеріальних активів*: означений інструмент вивчає поточний стан і потенційну заподіяну шкоду для нематеріальних активів унаслідок розгортання різноманітних кризових ситуацій. Цей інструмент також аналізує готовність бізнес-процесів і бізнес-практик компанії до реалізації різноманітних ризиків та потенційні наслідки для стану нематеріальних активів, що стануть результатом роботи таких бізнес-процесів і бізнес-практик у кризовій ситуації. Результатом стрес-тестування стану нематеріальних активів є формування рекомендацій з усунення недоліків існуючих бізнес-процесів і бізнес-практик, а також запровадження ряду покращень для даного комплексу, що сприятиме кращій підготовленості компанії до потенційної кризової ситуації – та відповідно вищої спроможності бізнесу до захисту нематеріальних активів, мінімізації заподіяної шкоди та швидшого відновлення;

– *моніторинг управлінської звітності компанії в площині стану нематеріальних активів*: цей інструмент представляє систему моніторингу внутрішніх даних управлінської звітності компанії, що отримані в рамках роботи системи *ERP* на предмет трендів, динаміки, структури та ключових індикаторів стану нематеріальних активів. Така система моніторингу, що заснована на внутрішніх управлінських даних компанії, має у своєму складі окремий блок вибіркового точкового моніторингу й окремий блок перманентного моніторингу – в площині стану нематеріальних активів. Така конфігурація системи моніторингу сприяє максимальному ефекту від роботи вказаного аналітичного інструменту. До того ж, зазначена система забезпечує адекватний комплекс бізнес-аналітики, яку топ-менеджмент і наглядові ради можуть використовувати під час планування та реагування на ключові сигнали на рівні компанії до того етапу кризової ситуації, коли ці ризики реалізуються або вийдуть з-під контролю;

– *розбудова системи контролінгу поведінки в рамках роботи з ризиками в площині нематеріальних активів*: такий

інструмент узгоджує системи контролю й моніторингу з комплексом мотивацій і стимулів основних стейкхолдерів всередині та ззовні компанії – таким чином, сприяючи дотриманню бажаних найкращих практик і зниженню ризиків для нематеріальних активів. За ситуації коли поведінка чітко і транспарентно пов'язана з бажаними бізнес-практиками в розрізі збереження нематеріальних активів, існує більша ймовірність адекватної роботи зазначеної системи та вчасного реагування компанії на виклики в площині заподіяння потенційної шкоди для нематеріальних активів.

– *розвиток комплексу комунікації зі стейкхолдерами в напрямку збереження нематеріальних активів:* цей інструмент має сприяти, по-перше, більшій узгодженості дій компанії (як на рівні топ-менеджменту, так і виконавців) і різноманітних груп стейкхолдерів в площині збереження нематеріальних активів; по-друге, кращим результатам оцінки заподіяної шкоди для нематеріальних активів компанії в результаті збройної агресії РФ; по-третє, розбудові проактивної системи роботи з ризиками для нематеріальних активів і встановлення системи раннього реагування на рівні компанії.

Узагальнено пропонована система заходів контролю й моніторингу в площині стану нематеріальних активів має забезпечити адекватну систему їхнього збереження на рівні компанії в різноманітних аспектах бізнес-практик і бізнес-процесів. Особливо важливо інтегрувати сучасні тенденції науки про бізнес-управління – з урахуванням поведінкового аспекту різноманітних груп стейкхолдерів всередині та ззовні компанії [18-19]. Зокрема, особливий фокус у процесі збереження нематеріальних активів в умовах російської збройної агресіє має бути приділений інституту наглядової ради та її інноваційного потенціалу в розрізі даної проблематики. Так, наглядова рада визначається як «експертний орган, що підтримує зміни на підприємстві, формує конкурентні переваги, сприяє залученню фінансування й мінімізації ризиків та зрештою забезпечує створення доданої вартості для стейкхолдерів» [20, с. 81]. Відповідно функціонала а інструментарій, що доступний наглядовій раді є критично важливим у сучасному контексті

вирішення досліджуваної проблематики й суттєво доповнює вже існуючий напрацьований інструментарій в означеній царині.

Висновки. В підсумку, досліджено проблематику оцінки шкоди для нематеріальних активів компаній в умовах російської збройної агресії. Окремий фокус даного дослідження направлений на визначення особливостей впливу турбулентного бізнес-середовища на особливості оцінки шкоди для нематеріальних активів. Як результат, це зумовлює необхідність комплексного вивчення ситуації та її потенційного впливу як на мікро-, так і макрорівнях рівнях в аспекті різноманітних факторів.

Зауважимо, що оцінка шкоди для нематеріальних активів в умовах значної турбулентності – зокрема, збройної агресії – є складним завданням, що потребує врахування широкого спектру факторів впливу. Додаткову складність і для цього завдання складає фактор невизначеності, що притаманний для турбулентного бізнес-середовища під час воєнного часу. Відповідаючи на вказану нагальну проблематику, пропонуємо сформувати та запровадити систему раннього попередження в напрямку збереження нематеріальних активів, а також адекватних для цієї проблематики засобів контролю й моніторингу стану нематеріальних активів компанії. Пропонована система складається з низки інструментів: 1) бенчмаркінг; 2) аналіз розриву; 3) економіко-математичне моделювання ризиків для нематеріальних активів; 4) стрес-тестування стану нематеріальних активів; 5) моніторинг управлінської звітності компанії в площині стану нематеріальних активів; 6) розбудова системи контролінгу поведінки в рамках роботи з ризиками в площині нематеріальних активів; 7) розвиток комплексу комунікації зі стейкхолдерами в напрямку збереження нематеріальних активів.

Перспективами майбутніх досліджень в означеній царині є розширення аналізу проблематики оцінки шкоди нематеріальним активам в розрізі кількісних і якісних факторів впливу, а також поширення цього дослідження на розробку й імплементацію цілісної системи контролю та моніторингу на рівні компанії, що покликана підтримати збереження нематеріальних активів в умовах російської збройної агресії.

Список використаних джерел:

1. Міжнародний стандарт фінансової звітності IAS 38 Intangible Assets. 2022. URL: https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/ (Дата доступу: 01.12.2022).

2. Osinsk M., Selig P., Matos F., Roman D. Methods of evaluation of intangible assets and intellectual capital. *Journal of Intellectual Capital*. 2017. №18(3). С. 470–485.

3. Abdifatah A., Nazli A. The role of intangible assets and liabilities in firm performance: empirical evidence. *Journal of Applied Accounting* Research. 2018. №19(1). P. 42–59.

4. Alexandr S., Mihaela P. Main approaches in measuring intangible assets. *International Journal of Education and Research*. 2014. №1(7). P. 1–6.

5. Kao L.-F., Yu-Chun C. The Determinants and Market Reaction of Goodwill Impairment Losses. *Sun Yat-sen Management Review*. 2017. №25(4). С. 935–965.

6. Міжнародний стандарт фінансової звітності IAS 36 Impairment of Assets. 2022. URL: https://www.ifrs.org/issued-standards/list-of-standards/ias-36-impairment-of-assets/ (Дата доступу: 01.12.2022).

7. Міжнародний стандарт фінансової звітності IFRS 13. URL:https://www.ifrs.org/content/dam/ifrs/publications/pdfstandards/english/2022/issued/part-a/ifrs-13-fair-value-measurement.pdf?bypass=on (Дата доступу: 01.12.2022).

8. Chen W.-T., Li-Peng H. Assets Impairment and Systematic Risk. *Journal of Contemporary Accounting*. 2014. №15(2). P. 139–158.

9. Tseng Y.-J., Pin-Feng W. The Relationship between Patterns of Asset Impairment Recognition and Macroeconomic Factors. *Fu Jen Management Review*. 2016. №23(2). P. 1–34.

10. Ясишена В., Головай Н. Класифікаційні й амортизаційні аспекти обліку нематеріальних активів. *Економіка та держава*. 2022. №3/2022. С. 4–10.

11. Куцик П., Дрогобицький І., Плиса З., Скоп Х. Облікова концепція управління вартістю нематеріальних активів підприємства: монографія. Львів: Растр-7. 2016. 268 с.

12. Suliman A. Countries urged to protect property in war to save culture, identity. *Thomson Reuters Foundation*. 2019. URL: https://www.reuters.com/article/global-property-war-idUSL5N25V40H (Дата доступу: 01.12.2022).

13. International armed conflict in Ukraine. *Geneva Academy of International Humanitarian Law and Human Right. RULAC*. 2022. URL:

https://www.rulac.org/browse/conflicts/international-armed-conflict-in-ukraine (Дата доступу: 01.12.2022).

14. Полосьмак О. Зміни у сфері інтелектуальної власності у зв'язку з війною. *UZ.LIGAZAKON*. 2022. URL: https://uz.ligazakon.ua/ua/magazine_article/EA015934 (Дата доступу: 01.12.2022).

15. Доронцева Є. Дієві рецепти підтримки бізнесу: як західні області України заохочують підприємців до релокації. *Vox Ukraine*. 2022. URL: https://voxukraine.org/diyevi-retsepty-pidtrymky-biznesu-yak-zahidni-oblasti-ukrayiny-zaohochuyut-pidpryyemtsiv-do-relokatsiyi/ (Дата доступу: 01.12.2022).

16. Наливайко А. Теорія стратегії підприємства. Сучасний стан та напрямки розвитку: підруч. для студ. вищ. навч. закл. Київ: КНЕУ. 2010. 228 с.

17. Козловський В., Дончак Л. Внутрішній економічний механізм виробничих підприємств: монографія. Тернопіль: Крок. 2013. 204 с.

18. Кашуба Я. Вибір методів та підходів стратегічного управління розвитком підприємництва. *Економіка та держава*. 2011. № 9. С. 16–18.

19. Дикань В., Зубенко В., Маковоз О., Токмакова І., Шраменко О. В. Стратегічне управління: навч. посіб. Київ: Центр учбової літератури. 2013. 272 с.

20. Терещенко О., Алексін Г. Роль інститутів наглядової ради та незалежного директора в максимізації вартості компанії. *Фінанси України*. 2019. №9. С. 81–93.

Тимощик Лілія Павлівна,
кандидат економічних наук, учений секретар Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України, судовий експерт, оцінювач

Голець Ірина Василівна,
магістр з фінансового ринку, завідувач сектором лабораторії економічних досліджень Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України, судовий експерт, оцінювач

РИЗИКИ ДЛЯ ДІЛОВОЇ РЕПУТАЦІЇ КОМПАНІЇ ВНАСЛІДОК ЗБРОЙНОЇ АГРЕСІЇ РФ

Вступ. Російська збройна агресія зумовила суттєві атипові виклики для України як на мікро-, так і на макрорівні. Ці ризики реалізуються поміж різними економічними агентами – зокрема й на рівні компаній. Одним з таких ключових викликів є зростаючі ризики в площині ділової репутації компаній в контексті російської збройної агресії. Особливої важливості ця проблематика набуває через гібридизм збройної агресії РФ, що веде до атипових і асиметричних шкідницьких ефектів для економічних агентів в Україні. Додатково це зумовлюється прагненням російського уряду заподіяти Україні максимально можливу шкоду – усіма доступними способами. Відповідно це веде до утворення нестандартної ситуації, за якої для українських компаній виникають ускладнення, пов'язані з таким ключовим нематеріальним активом як репутація, що є особливо актуальним у сучасних ускладнених умовах соціально-економічної турбулентності.

Постановка завдання. Метою цього дослідження є визначення особливостей роботи з ризиками в площині ділової репутації компаній з особливими фокусом на дотримання прав людини як основний драйвер забезпечення належного рівня ділової репутації бізнесу в сучасних умовах збройної агресії РФ. В межах цього дослідження сформовано такі завдання:

– визначити сутність ділової репутації компанії та чинники впливу на цю категорію;

– здійснити аналіз контексту збройної агресії в площині збереження ділової репутації компанії з особливим фокусом на дотримання прав людини;

– сформувати пропозиції з забезпечення збереження ділової репутації бізнесу на належному рівні в умовах збройної агресії.

Результати. Ділова репутація є ключовим нематеріальним активом для бізнесу в сучасних складних умовах екзогенного та ендогенного середовища діяльності компаній. Ділова репутація визначається Словником Оксфордського університету (*Oxford Dictionary*) як система думок спільноти щодо суб'єкта бізнесу, що заснована на минулих подіях і досвіді [1] . Таке тлумачення можемо доповнити думкою Pires і Trez [2], які зазначають необхідність визначення ділової репутації в 3 площинах: 1.) соціальних очікувань; 2.) бізнес-іміджу; 3.) суспільної довіри.

Відповідно в межах виділених вище площин:

– *соціальних очікувань*: ділова репутація визначається як узагальнення очікувань широкої спільноти та окремих вузьких груп стейкхолдерів, що засновані на минулих подіях і усталених релевантних практиках;

– *бізнес-іміджу*: ділова репутація є комплексом особистісних ознак і характеристик т.зв. корпоративної ідентичності, що приписується спільнотою окремій компанії;

– *суспільної довіри*: ділова репутація ідентифікується як система думок стейкхолдерів у межах концепції довіри, що фокусується на чесності й надійності компанії [3-4].

В умовах сьогодення, коли важливість горизонтальних зв'язків і взаємної довіри суттєво зросли в своїй важливості, шкода діловій репутації компанії може стати критичною для компанії і в коротко-, і в довгострокових перспективах її діяльності [3, 5].

Зауважимо, що збройна агресія створює суттєві ризики для бізнесу – як загального характеру, так і більш специфічні. Відмітимо, що контекст значного ризику є складним середовищем для діяльності компанії. Наразі українські компанії стикнулися із складним високоризиковим середовищем ведення бізнесу внаслідок російської збройної агресії [6-7]. Це

зумовлюється тим, що компанії – особливо малий і середній бізнес – не мають достатніх важелів впливу на ухвалення важливих рішень на рівні державної або місцевої влади. Зокрема, до означеного напрямку обмежень для бізнесу в умовах збройної агресії можемо віднести:

- брак достатньої інформації для прийняття управлінських рішень на рівні компанії;
- відсутність важелів впливу на державні установи різних рівнів для захисту інтересів бізнесу;
- неможливість забезпечення адекватного рівня безпеки для власних співробітників;
- звужені можливості для виконання ділових зобов'язань під тиском обмежень, запроваджених органами державної влади [8-9].

Додатково зауважимо, що хоча компанії можуть зустрітися з недоліками національної законодавчої бази, які обмежують їх з деяких питань, компанії часто діють у нормативно-правовому середовищі, що суперечить міжнародним стандартам з прав людини та забезпечує недостатні гарантії для запобігання порушенням прав людини [8, 10-11]. Додатковим фактором, що ускладнює цю проблематику є корупція. Зауважимо, високий рівень корупції збільшує ймовірність того, що бізнес може сам бути залученим до корупції. Це також негативно впливає на репутацію компанії. За турбулентних умов соціально-економічного та соціально-політичного середовища – зокрема, збройної агресії – такий ризик суттєво зростає. Країна зі слабким верховенством права також може мати погано функціонуючу або корумповану судову систему, що підриває ефективність механізмів розгляду скарг і блокує постраждалим сторонам доступ до адекватного правового захисту [11, 13]. Ці виклики наражають компанії на репутаційні ризики. Означена проблематика ускладнюється тим, що за такого розвитку ситуації суттєво росте ймовірність причетності бізнесу до порушень прав людини, які негативно впливають на ділову репутацію компаній, що в свою чергу веде до руйнації цінності, котра створюється компанією для суспільства, акціонерів, інвесторів і інших груп стейкхолдерів.

Зауважимо, що бізнес у середовищі високого ризику – зокрема, у воюючій країні – з більшою ймовірністю або прямо

спричинить, або опосередковано сприятиме порушенням прав людини. Також імовірним є завдання шкоди окремим громадянам і спільноті внаслідок підтримання певних ділових зв'язків. Порушення компаніями прав людини в таких ситуаціях можуть містити такі проблеми:

- захоплення землі;
- забруднення навколишнього середовища;
- позбавлення роботи та засобів до існування;
- обмеження свободи слова;
- використання персональних даних громадян;
- порушення таємниці листування [14-15].

Зауважимо, що збройний конфлікт і права людини тісно пов'язані – конфлікт створює ризики для додаткових порушень прав людини. Бізнес-діяльність може загострити існуючі конфлікти та соціально-політичну нестабільність різними шляхами, наприклад: управлінські рішення щодо роботи на ринку, практика найму та закупівель, партнерство з місцевими організаціями. Корупція в бізнесі також може призвести до порушення прав людини, послаблюючи стан верховенства права, що суттєво ускладнює соціально-економічний розвиток в країні [16-18].

Незважаючи на ці виклики, ефективна робота бізнесу в умовах високого ризику є ключовим драйвером подолання наслідків збройної агресії, підтримки рівня життя громадян, забезпечення підтримки адекватного стану людського капіталу. Зауважимо, що ключовим в даному контексті є врахування компаніями місцевої соціально-економічної, соціально-культурної, соціально-політичної ситуації та повага до міжнародних стандартів в царині прав людини [19-20]. Відповідно компанії, які інтегрують комплекс дотримання права людини в процес прийняття стратегічних і тактичних управлінських бізнес-рішень, будуть більш стійкими до сучасних викликів збройної агресії та соціально-економічної кризи [21-22].

Унаслідок цього, ризик для ділової репутації таких компаній – навіть в умовах гібридизму російської збройної агресії – буде знижуватися, забезпечуючи стійкі позиції бізнесу як на поточному проміжку часу, так і в перспективі повоєнного періоду в Україні. Відповідно виробничі, маркетингові,

інвестиційні, фінансові рішення бізнесу, які прямо чи опосередковано зміцнюють інституції та структури громадянського суспільства на різних рівнях, сприятимуть запобіганню розвитку негативних наслідків в різноманітних соціально-економічних, соціально-культурних, соціально-політичних площинах і на коротко-, і на довгостроковому горизонтах. Додатково зазначений вище підхід бізнесу сприятиме створенню середовища, що підтримуватиме як комерційну успішність компаній, так і захист прав людини.

У контексті пошуку способів збереження ділової репутації компаній в умовах гібридної агресії РФ зауважимо, що бізнесу необхідно здійснювати належну перевірку дотримання прав людини під час ухвалення своїх стратегічних і тактичних рішень. Такий підхід з боку компаній уможливить виявлення та запобігання потенційно небезпечних бізнес-практик в контексті порушення прав людини в умовах російської збройної агресії значної соціально-економічної турбулентності. Відповідно це посилить позиції компанії з точки зору її корпоративної соціальної відповідальності, що позитивно впливатиме на здатність бізнесу забезпечувати збереження ділової репутації в умовах збройної агресії РФ [23-24].

Така відповідальність бізнесу посилюється в ситуаціях високого ризику, коли ризик порушення прав людини об'єктивно суттєво зростає, а діяльність бізнесу може або поглибити стан соціально-економічної турбулентності, або навпаки полегшити кризовий стан в площині різноманітних економічних агентів і груп стейкхолдерів – в першу чергу, найбільш вразливих соціально-демографічних груп громадян. Відповідно бізнес-практики прямо або опосередковано впливають на можливість досягнення позитивного стану на фоні збройної агресії не тільки на мікро-рівні (в розрізі збереження ділової репутації компанії), але і на макрорівні (часткове або повне зняття напруги на рівні громади, регіону, держави та забезпечення формування адекватних для сучасної ситуації соціально-економічних, соціально-культурних, соціально-політичних процесів у країні).

Як наслідок, компанії в цьому контексті мають провадити своєрідний автономний контроль і моніторинг у царині дотримання прав людини у сфері своєї бізнес-діяльності. Такий

автономний контроль і моніторинг на рівні бізнесу в галузі прав людини відповідно до *UNGP* [25] поєднує такі аспекти:

- розвиток чутливості до конфліктів;
- запобігання жорстокості;
- підтримка правосуддя перехідного періоду.

В практичному вияві забезпечення вищезазначених стандартів в царині бізнесу вимагає провадження такої роботи на систематичній та узгодженій основі, враховуючи контекст на макро- та мікро-рівнях.

Важливим аспектом у цій роботі на рівні бізнесу є вивчення та дотримання інтересів ключових груп стейкхолдерів, що забезпечує досягнення максимально можливого результату в розрізі виконанні завдання. Отже необхідно здійснювати додатковий аналіз, що сфокусований на поглиблення розуміння локальної специфіки в розрізі соціальних, демографічних, політичних, культурних, екологічних аспектів. Зауважимо, що за неналежного аналізу та подальшої імплементації сформованих рішень у бізнес-практиках кризова ситуація та соціальна напруженість на локальному, регіональному або національному рівні може погіршитися. Тому підкреслюється важливість дотримання зважених бізнес-практик в забезпеченні як збереження ділової репутації бізнесу, так і відносної стабільності інших економічних агентів, що узгоджені поміж собою через прагнення дотримання прав людини в турбулентних умовах.

В однозначному контексті високо ризикового середовища, що було спричинено російською збройною агресією та, як наслідок, соціально-економічною кризою, компанії необхідно вживати практичні кроки для визначення потенційно небезпечних драйверів, що можуть вести до зростання ризиків для її ділової репутації. Як визначено вище, в межах цього даного підходу компанії першочергово необхідно здійснити оцінку за допомогою автономного моніторингу заходів з підтримання прав людини в умовах збройної агресії.

Отже, для реалізації наведеного компанії необхідно здійснити оцінку, що підтримується системою заходів. Опишемо пропоновану систему заходів більших деталях нижче.

Захід 1: Постановка системи аналітики в розрізі ділової репутації компанії та дотримання прав людини в умовах

збройної агресії. В межах цього заходу компанія має виробити ряд аналітичних інструментів., що сприяють відслідковуванню потенційно ризикових зон в контексті її ділової репутації, зважаючи на динаміку розвитку збройної агресії та кризи в державі в різноманітних аспектах соціально-економічної, соціально-культурної, соціально-політичної природи. Наголосимо, що методологія означених аналітичних заходів може відрізнятися залежно від контексту локалізованих ризиків, що є специфічними для окремих груп стейкхолдерів, але така система має поєднувати запланований моніторинг вже відомих ризиків із встановленням системи для виявлення й отримання інформації про непередбачені динамічні ризики. Механізм пропонованої системи може включати регулярний моніторинг ЗМІ та кабінетне дослідження; спільний обмін інформацією з місцевими й регіональними осередками громадянського суспільства; активне залучення локальних груп стейкхолдерів. Зауважимо, що пропонована система перманентного моніторингу вимагатиме встановлення механізмів постійного, децентралізованого та локалізованого збору й аналізу інформації.

Захід 2. Оцінка контексту потенційних ризиків для ділової репутації в умовах збройної агресії. Цей захід поєднує оцінку ситуації в царині дотримання прав людини (законодавча база, вплив на вразливі верстви населення, доведені факти порушення прав людини, інше), а також оцінку динаміки збройної агресії, включаючи основні причини та потенційні сценарії розвитку збройної агресії і турбулентності в розрізі соціально-економічної, соціально-культурної, соціально-політичної проблематики. Наголосимо на важливості корегування цього аналізу на дії й мотивації ключових груп стейкхолдерів. Підкреслюємо, що результати аналізу можливі для застосування тільки в контексті дій усіх груп економічних агентів, не обмежуючись виключно поглядом компанії (тобто її топ-менеджерів і акціонерів). Зауважимо, що здійснений в межах цього заходу аналіз закладає основу для конфліктологічної оцінки фактичного та потенційного впливу бізнес-діяльності компанії на права людини.

Захід 3. Оцінка ризиків для прав людини з урахуванням сучасної ситуації збройної агресії. Компанія має визначити, як її

бізнес-практики, продукти, ланцюжки поставок, операційна робота впливає на актуальний стан прав людини на рівні громади, регіону, держави, зокрема, способи, якими бізнес-діяльність компанії впливає на сучасний стан напруженості.

Захід 4. Аналіз ключових ризиків з точки зору як прав людини, так і динаміки кризи в державі на фоні збройної агресії. У конфліктних ситуаціях пріоритизація ризиків для ділової репутації вимагає від компанії здійснення аналізу ймовірності настання ключових наслідків, що спричинені збройною агресією та кризою в державі – в контексті ймовірності загострення окремих загальних і специфічних проблем унаслідок, по-перше, управлінських рішень компанії та, по-друге, підтримання її звичайних бізнес-практик.

Захід 5. Постановка системи регулярної та широкої комунікації з ключовими локальними стейкхолдерами. Залучення стейкхолдерів відіграє ключове значення в рамках моніторингу ситуації в реальному часі, а також визначення рівня фактичної і потенційної шкоди в царині прав людини внаслідок бізнес-діяльності, а також розробки та реалізації результативних заходів із запобігання та пом'якшення таких ризиків. Зауважимо, що в контексті високого ризику для ділової репутації – особливо сучасної збройної агресії РФ –залучення стейкхолдерів має відбуватися на більш ранніх етапах та в розширеному форматі. Це сприятиме зниженню інформаційної асиметрії, а також підтримає розбудову довіри й доброзичливості в означеній площині між бізнесом і ключовими групами стейкхолдерів. Наголосимо, що такий формат взаємодії має бути перманентним, а також обов'язково поєднувати регулярні точки взаємодії між компанією та ключовими групами стейкхолдерів на різних рівнях. Це, в свою чергу, забезпечить змогу компанії відстежувати ключові зміни в контексті збройної агресії, загрози для прав людини та ділової репутації компанії. Зауважимо, що під час здійснення даного заходу необхідно створити безпеку для стейкхолдерів в різноманітних аспектах на коротко- та довгостроковому горизонтах.

Захід 6. Розвиток взаємодії компанії в сучасному контексті з іншим бізнесом, громадянським суспільством, інституціями. Зауважимо, що найбільш серйозні та стійкі проблеми в царині

прав людини, що в свою чергу чинять вплив на стан ділової репутації компанії, як правило, є системними та пов'язані з масштабними проблемами, що, переважно, є надто об'ємними і складними, для того щоб одна окрема компанія була спроможна їх вирішити самостійно. Відповідно до *UNGP* [25] уряди мають підтримувати компанії у виявленні та реагуванні на підвищені ризики в царині прав людини в умовах високого ризику – такого як збройна агресія. Відповідно компаніям у контексті забезпечення дотримання прав людини та збереження своєї ділової репутації необхідно співпрацювати з органами державної влади різного рівня, іншими компаніями, бізнес-асоціаціями, професійними об'єднаннями, громадськими організаціями, дипломатичним корпусом, інституціями громадянського суспільства з метою, по-перше, обміну інформацією та аналізу мінливості конфліктного середовища, його впливу на бізнес й інших стейкхолдерів, формування відповідних заходів реагування; по-друге, провадження спільного моніторингу дотримання прав людини, зокрема прозорості постачальників, поведінки бізнес-партнерів з високим ризиком (наприклад, в царині військових поставок або державних закупівель); по-третє, розроблення та запровадження мінімальних стандартів у спільній з партнерами проблематиці (наприклад, в площині ринкової інфраструктури); по-четверте, вжиття колективних дій у випадках, коли впливу однієї окремої компанії недостатньо для запобігання або зниження рівня шкоди у сфері дотримання прав людини (наприклад, колективна боротьба з корупцією).

Захід 7. Посилення системи реагування на кризи в надзвичайних ситуаціях. Зауважимо, що ризик збройної агресії є нестандартним, відповідно бізнес може суттєво постраждати в результаті реалізації цього ризику. Зокрема, внаслідок збройної агресії компанія може стати об'єктом насильства або стати співучасником порушень прав людини. Відповідно компанія має реалізовувати заходи з планування сценаріїв, а також розробити внутрішні нормативні документи з реагування на такі ризики, зокрема, в площині збереження своєї ділової репутації.

Захід 8. Пріоритезація безпеки співробітників і бізнес-партнерів. Означений захід поєднує в собі включає створення планів евакуації для переміщення персоналу з небезпечних зон,

забезпечення належного захисту робочих місць, а також забезпечення доступу працівників до постійної медичної допомоги. З огляду на бізнес-партнерів компанії необхідно створити такі бізнес-процеси, що максимально знижують ризики для життя та здоров'я співробітників бізнес-партнерів, які задіяні в бізнес-діяльності компанії (в першу чергу, підрядників з логістичних і виробничих процесів). Це забезпечить збереження позитивного іміджу компанії на фоні збройної агресії та відповідно підтримуватиме її ділову репутацію на належному рівні.

Висновки. Підсумовуючи наведене, досліджено проблематику збереження ділової репутації компаній в умовах збройної агресії РФ. Особливий фокус спрямовано на дотримання прав людини в контексті даної проблематики як основний драйвер забезпечення ділової репутації на належному рівні в турбулентних умовах, що зумовлені російською збройною агресією. Відповідно це спричинює необхідність застосування системи заходів для вирішення цього завдання, що узгоджені між собою та спрямовані на широкі групи стейкхолдерів як на коротко-, так і на довгостроковому горизонтах.

Відповідно компаніям, які націлені на довгострокове зростання і збереження своєї ділової репутації, необхідно виробити певну систему підходів з автономного контролю й моніторингу дотримання прав людини – в першу чергу, для реалізації своїх бізнес-практик, формування та імплементації стратегічних і тактичних рішень.

Наголосимо, що така система заходів з автономного контролю й моніторингу дотримання прав людини в контексті підтримки ділової репутації на належному рівні має реалізовуватися не тільки на мікро-рівні, але і на макрорівні. Відповідно компанії в цьому контексті необхідно залучати широкі групи стейкхолдерів, а також інші бізнеси з метою забезпечення довготривалого результату у цій сфері.

У відповідь на таку потребу пропонуємо реалізувати систему заходів, що покликана забезпечити підтримку на належному рівні ділової репутації компанії в умовах російської збройної агресії, в основі якої дотримання прав людини як головний драйвер позитивної репутації бізнесу. В межах цієї пропозиції сформовано систему з восьми заході, а саме: 1) постановка системи аналітики в

розрізі ділової репутації компанії та дотримання прав людини в умовах збройної агресії; 2) оцінка контексту потенційних ризиків для ділової репутації в умовах збройної агресії; 3) оцінка ризиків для прав людини з урахуванням сучасної ситуації збройної агресії; 4) аналіз ключових ризиків з точки зору як прав людини, так і динаміки кризи в державі на фоні збройної агресії; 5) постановка системи регулярної та широкої комунікації з ключовими локальними стейкхолдерами; 6) розвиток взаємодії компанії в сучасному контексті з іншим бізнесом, громадянським суспільством, інституціями; 7) посилення системи реагування на кризи в надзвичайних ситуаціях; 8) пріоритезація безпеки співробітників і бізнес-партнерів.

Перспективами майбутніх досліджень означеної проблематики є поглиблення аналізу драйверів ділової репутації бізнесу в умовах збройної агресії, а також розширити таке дослідження на іноземні компанії, що прямо або опосередковано можуть перебувати під впливом збройної агресії РФ в Україні.

Список використаних джерел:

1. Словник Оксфордського університету. 2022. URL: https://www.oxfordlearnersdictionaries.com/ (Дата доступу: 30.11.2022).
2. Pires V., Trez, G. Corporate reputation: A discussion on construct definition and measurement and its relation to performance. *Revista de Gestão*. 2018. №25(1). С. 47−64.
3. Iff A., Sguaitamatti D., Alluri R., Kohler D. Money Makers as Peace Makers? Business Actors in Mediation Processes. *SwissPeace Working Paper Series*. 2010. №2. С. 1–37.
4. Slim H. Business actors in armed conflict: towards a new humanitarian agenda. *International Review of the Red Cross*. 2012. №94(887). С. 903–918.
5. Tripathi S. Business in armed conflict zones: how to avoid complicity and comply with international standards. *Politorbis*. 2010. №50(3). С. 131–142.
6. Rettberg A., Leiteritz R., Nasi C. Entrepreneurial Activity in the Context of Violent Conflict: Business and Organized Violence in Colombia. *Journal of Small Business and Entrepreneurship*. 2011. №24(2). С. 179–196.
7. Stewart F. Horizontal Inequalities in Kenya and the Political Disturbances of 2008: Some Implications for Aid Policy. *Conflict, Security & Development*. 2010. №10(1). С. 133–159.

8. Ramadhan S.W. The Concepts and Practice of Peace, Peacebuilding and Religious Peacebuilding. *Journal for Peace and Justice Studies.* 2011. №20(2). С. 10–31.

9. Lundan S.M., Muchlinski P. Human Rights Due Diligence in Global Value Chains. *Progress In International Business Research*. 2012. №7. С. 181–201.

10. Jamali D., Mirshak R. Business-conflict Linkages: Revisiting MNCs, CSR, and Conflict. *Journal of Business Ethics*. 2010. №93(3). С. 443–464.

11. Chesterman S. Lawyers, Guns, and Money: The Governance of Business Activities in Conflict Zones. *Chicago Journal of International Law*. 2010. №11. С. 321.

12. Besley T., Torsten P. Fragile States and Development Policy. *Journal of the European Economic Association*. 2011. №9(3). С. 371–398.

13. Gómez del Prado J.L. UN Convention to Regulate PMSCs. *Criminal Justice Ethics*. 2012. №31(3). С. 263–264.

14. Патлах І. Управління репутаційними ризиками в діяльності підприємства. *Вісник Нац. техн. ун-ту "ХПІ" : зб. наук. пр. Темат. вип. : Актуальні проблеми управління та фінансово-господарської діяльності підприємства*. 2015. № 23(1132). С. 140–143.

15. Кісіль Б. Методи визначення та оцінки репутаційних ризиків підприємства. *Молодий вчений*. 2016. №12(40). С. 782–786.

16. Грабчак В. Сутність поняття «репутація підприємства» та її складових. *Глобальні та національні проблеми економіки*. 2016. №10. С. 313–318.

17. Помянська Н. Управління діловою репутацією на синергетичних засадах. *Науковий вісник Херсонського державного університету*. 2014. №9(4). С. 57–61.

18. Швіндіна Г., Кошевець В. Ділова репутація як показник ефективності функціонування організації. *Вісник СумДУ. Серія Економіка*. 2011. №2. С. 75–79.

19. Нестеренко О., Сердюков К. Методологія формування обліковозвітної інформації про соціально-репутаційний капітал фінансових установ. *Економічна стратегія і перспективи розвитку сфери торгівлі та послуг*. 2019. №1. С. 15–25.

20. Дерев'янко О. Проблема відсутності системного репутаційного менеджменту на підприємствах України. *Інноваційне підприємництво: стан та перспективи розвитку*: зб. матеріалів І Всеукр. наук.-практ. конф., 29-30 берез. 2016 р., ДВНЗ «Київ. нац. екон. ун-т ім. В. Гетьмана». Київ: КНЕУ. 2016. С. 121–123.

21. Пушак Я., Завербний А. Корпоративна репутація як ключовий вектор підвищення рівня економічної безпеки. *Соціально-правові студії*. 2020. №2(8). С. 130–136.

22. Дерев'янко О. Механізми впливу репутаційного менеджменту на бізнес-результати. *Стратегія економічного розвитку України*. 2018. №42. С. 5–18.

23. Завербний А., Шпак Ю., Побурко О. Проблеми та перспективи застосування репутаційного менеджменту українськими підприємствами за умов зовнішньоекономічної діяльності. *Інфраструктура ринку*. 2020. №4. 1С. 80–86.

24. Фурман А. Управління репутацією у воєнний час. Legal Alliance. 2022. URL: https://www.legalalliance.com.ua/publikacii/upravlinna-reputacieu-u-voennij-cas/ (Дата доступу: 30.11.2022).

25. Стандарти UNGP. 2022. URL: https://www.ungpreporting.org/ (Дата доступу: 30.11.2022).

Бутнік-Сіверський Олександр Борисович,
головний науковий співробітник економіко-правового відділу Науково-дослідного інституту інтелектуальної власності Національної академії правових наук України, доктор економічних наук, професор, академік Академії технологічних наук України та академік Української академії наук, судовий експерт

Климова Наталія Борисівна,
головний судовий експерт Київського науково-дослідного інституту судових експертиз Міністерства юстиції України

Доровських Анатолій Васильович,
головний судовий експерт Київського науково-дослідного інституту судових експертиз Міністерства юстиції України, доктор технічних наук, професор, академік Академії інженерних наук України

ПИТАННЯ СУДОВОЇ ЕКСПЕРТИЗИ, ЯКІ ПОТРЕБУЮТЬ ЗАСТЕРЕЖЛИВОСТІ ПРИ ЇХ ВИРІШЕННІ В МЕЖАХ ЧИННОГО ЗАКОНОДАВСТВА

Вступ. У середовищі судових експертів виникла пропозиція замінити питання «Чи правильно визначено суму роялті за використання об'єкта?», яке входить до переліку питань, що розглядаються у рамках економічного дослідження об'єктів інтелектуальної власності, затвердженого наказом Міністерства юстиції України від 08 жовтня 1998 року № 53/5, шляхом доповнення його такими питаннями:

1. «*Яка ринкова ставка ліцензійного платежу (роялті, авторської винагороди, паушального платежу) в процентному виразі від (зазначити базу роялті: обсягу виробництва, або обсягу реалізації продукції (товарів, робіт, послуг) з використанням об'єкта права інтелектуальної власності, або прибутку тощо) станом на (зазначити дату) (з урахуванням наданої експерту інформації щодо ставок роялті щодо аналогічних об'єктів)?*»

2. «*Чи підтверджується документально розрахунок ставки роялті в процентному виразі, визначений в (зазначається документ, на підставі якого були відображені в бухгалтерському обліку відповідні господарські операції, або акт перевірки контролюючого органу, або у позовних вимогах)?*»

3. «*Чи підтверджується документально розмір необґрунтованого завищення ліцензійного платежу (роялті, авторської винагороди, паушального платежу) (найменування організації) у сумі (зазначається сума) за період (зазначається період), визначений в акті перевірки контролюючого органу або у позовних вимогах? Якщо так, – у якій сумі?*».

Мета дослідження. На наш погляд, з формулюванням запропонованих питань не можна погодитись, оскільки їх вирішення виходить за межі компетенції судового експерта за спеціальністю 13.9 «Економічні дослідження у сфері інтелектуальної власності» та потребує отримання додаткових підтверджуючих документів, про залучення яких чинним положенням судовий експерт за спеціальністю 13.9 клопотати не може та що потребує застережливості при їх прийнятті в межах чинного законодавства України.

Результати дослідження. Виходячи зі змісту цих питань, виникає потреба встановити: чи правомірно відносити господарські операції з роялті, авторської винагороди, паушального платежу до компетенції експертної спеціальності 13.9?

Зазначимо, що Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень (затверджених наказом Міністерства юстиції України від 08 жовтня 1998 року № 53/5, зареєстрованих у Міністерстві юстиції України 03 листопада 1998 року за № 705/3145 (у редакції наказу Міністерства юстиції України від 26 грудня 2012 року № 1950/5) у розділі V «Експертиза об'єктів інтелектуальної власності», містять орієнтовний перелік питань за кожною експертною спеціальністю. Основним завданням експертизи об'єктів інтелектуальної власності є визначення властивостей цих об'єктів, до яких належать об'єкти промислової власності, об'єкти авторського права і суміжних прав. Відповідно до п. 5.4, окрему групу становлять економічні дослідження об'єктів інтелектуальної власності, зокрема визначення вартості перелічених вище об'єктів інтелектуальної власності та розрахунок збитків, завданих у результаті порушення прав на них.

Звернемо увагу на те, що за своєю суттю *роялті – це будь-який платіж*, отриманий як винагорода за користування або за надання права на користування будь-яким об'єктом права

інтелектуальної власності (об'єктами промислової власності, нетрадиційними об'єктами інтелектуальної власності, об'єктами авторського права і суміжних прав), а саме: літературними творами, творами мистецтва або науки, включаючи комп'ютерні програми, інші записи на носіях інформації, відео- або аудіокасети, кінематографічні фільми або плівки для радіо- чи телевізійного мовлення, будь-яким патентом, зареєстрованим знаком для товарів і послуг чи торговельною маркою, дизайном, секретним кресленням, моделлю, формулою, процесом, правом на інформацію щодо промислового, комерційного або наукового досвіду (ноу-хау).

Отже, економічна суть та процедури *визначення вартості роялті* (права використання об'єкта інтелектуальної власності) є відмінними від процедур та методик визначення вартості самого об'єкта права інтелектуальної власності (ОПІВ), мають похідний характер від вартості об'єкта інтелектуальної власності та умов ліцензійного договору. Отже, вирішення питань щодо визначення ринкової вартості роялті та правильності розрахунку його розміру на підставі умов ліцензійного договору не потребує спеціальних знань експерта у галузі інтелектуальної власності, а є предметом здійснення оцінки оцінювачем та предметом економічної експертизи. Справедливу величину ставки роялті (діапазону) відповідно до вимог інструкції Фонду державного майна України може визначити лише оцінювач за напрямком оцінки 2.2. «Оцінка прав на об'єкти інтелектуальної власності», а не судовим експертом за спеціальністю 13.9.

Сертифікований оцінювач після здійснення розрахунку вартості права використання об'єкта інтелектуальної власності на свій розсуд та у межах компетенції, використовуючи відомі методики, з урахуванням особливості використання або надання права на використання ОПІВ, визначає, відповідно на свій суб'єктивний розсуд, частку роялті або ставку роялті в процентному виразі до прийнятої ним бази розрахунку. Результат розрахунку узгоджується з контрагентами ліцензійного договору. Тому підстав для перевірки розміру ринкової вартості ОПІВ та прийнятої частки / ставки роялті в процентному виразі не має сенсу, так як присутні ринкові відносини контрагентів ліцензійного договору, а розрахунки можна отримати у

сертифікованого оцінювача за погодженням замовника оцінки, відповідно до умов договору щодо комерційної таємниці.

Щодо змісту першого питання, то воно передбачає здійснення експертом дослідження зі встановлення відповідності величини роялті, встановленого ліцензійним договором права користування певним об'єктом інтелектуальної власності, ринковим цінам на право користування подібними правами користування. При цьому зазначене питання безпосередньо не стосується суті експертизи інтелектуальної власності та дослідження вартості самого об'єкта інтелектуальної власності.

Ринкова вартість права користування об'єктом інтелектуальної власності безпосередньо залежить від умов ліцензійного договору; відповідно при дослідження слід обирати ліцензійні договори з ідентичними умовами (щодо способу оплати, щодо можливості надання субліцензії, щодо регіону поширення, щодо функціонального використання ліцензіатом набутих прав користування тощо). Відповідно, зазначене дослідження може здійснюватись виключно з урахуванням вимог ст. 39 Податкового кодексу України (далі – ПК України) [1] в частині порядку визначення ціни, що відповідає принципу «витягнутої руки» та із використанням даних, розміщених у спеціалізованих базах даних, де розміщена інформація, що могла б використовуватись як порівняльна при визначенні ринкової вартості роялті та встановлення відповідності розміру роялті, встановленого у конкретному ліцензійному договорі ринковому розміру роялті.

Відповідно до пп. 39.2.2, при визначенні відповідності ціни операції (розміру плати за користування об'єктом інтелектуальної власності) звичайним (ринковим) цінам, слід досліджувати ідентичні операції, за якими виконуються всі нижче наведені умови зіставності.

Комерційні та фінансові умови операцій (підп.39.2.2 ст.39 ПК України) визнаються зіставними з неконтрольованими, якщо:

− немає значних відмінностей між ними, що можуть істотно вплинути на фінансовий результат під час застосування відповідного методу трансфертного ціноутворення;

− такі відмінності можуть бути усунені шляхом коригування умов та фінансових результатів контрольованої або

неконтрольованої операції для уникнення впливу таких відмінностей на зіставність.

Під час визначення зіставності операцій аналізуються такі елементи контрольованих та зіставних операцій:

– характеристика товарів (робіт, послуг), які є предметом операції;

– функції, які виконуються сторонами операції, активи, що ними використовуються, умови розподілу між сторонами операції ризиків та вигід, розподіл відповідальності між сторонами операції та інші умови операції (далі – функціональний аналіз);

– стала практика відносин та умови договорів, укладених між сторонами операції, які істотно впливають на ціни товарів (робіт, послуг);

– економічні умови діяльності сторін операції, включаючи аналіз відповідних ринків товарів (робіт, послуг), які істотно впливають на ціни товарів (робіт, послуг);

– бізнес-стратегії сторін операції (за наявності), які істотно впливають на ціни товарів (робіт, послуг).

У разі відсутності або недостатності інформації про окремі неконтрольовані операції для визначення показників рентабельності може використовуватися фінансова інформація юридичних осіб, які здійснюють діяльність, зіставну із контрольованою операцією, за умови наявності інформації про те, що зазначені юридичні особи не здійснюють операції з пов'язаними особами.

Визначення зіставності юридичних осіб здійснюється з урахуванням їх галузевої специфіки та відповідних видів діяльності, що здійснюються ними в зіставних з контрольованою операцією економічних (комерційних) умовах.

Визначення зіставності комерційних та/або фінансових умов операцій з умовами контрольованої операції може здійснюватися, зокрема, але не виключно, за результатами аналізу:

– кількості товарів, обсягу виконаних робіт (наданих послуг);

– строків виконання господарських зобов'язань;

– умов проведення платежів під час здійснення операції;

– офіційного курсу гривні до іноземної валюти, встановленого Національним банком України, у разі використання такої валюти у розрахунках під час здійснення операції, зміни такого курсу;

– розміру звичайних надбавок чи знижок до ціни товарів (робіт, послуг), зокрема знижок, зумовлених сезонними та іншими коливаннями споживчого попиту на товари (роботи, послуги), втратою товарами споживчих якостей, закінченням (наближенням дати закінчення) строку зберігання (придатності, реалізації), збутом неліквідних або низьколіквідних товарів;

– розподілу прав та обов'язків між сторонами операції, визначених за результатами функціонального аналізу.

Аналіз функцій, які виконуються сторонами операції, під час визначення зіставності комерційних та/або фінансових умов операцій з умовами контрольованої та неконтрольованих операцій може проводитися з урахуванням матеріальних та нематеріальних активів, що перебувають у розпорядженні сторін операції та використовуються в цілях отримання доходу.

Визначення та аналіз функцій, які виконуються сторонами операції, здійснюються на підставі укладених договорів, даних бухгалтерського обліку, фактичних дій сторін операції та фактичних обставин її проведення відповідно до суті операції.

Під час визначення зіставності комерційних та/або фінансових умов зіставних операцій з умовами контрольованої операції також можуть враховуватися ризики сторін операції, пов'язані з провадженням господарської діяльності, що впливають на умови операції.

Враховуючи те, що відповідно до п. 2.3 Інструкції про призначення та проведення судових експертиз та експертних досліджень №53/5 експерту заборонено самостійно збирати матеріали, які підлягають дослідженню, а також вибирати вихідні дані для проведення експертизи, якщо вони відображені в наданих йому матеріалах неоднозначно, при вирішення питання щодо встановлення розміру ринкової вартості роялті *експерт ризикує отримати упереджену, однобоку та необ'єктивну інформацію, а результати експертизи – будуть об'єктом маніпулювання.*

При застосуванні підходу до визначення ринкової ставки роялті за допомогою визначення діапазону рентабельності,

звертаємо увагу на наступне. Відповідно до п. 39.3.2.2 ст. 39 ПК України, якщо під час застосування методів трансфертного ціноутворення порівняння ціни або рентабельності в контрольованій операції проводиться з цінами або показниками рентабельності кількох зіставних неконтрольованих операцій або юридичних осіб, які не здійснюють операції з пов'язаними особами, обов'язково використовується діапазон цін (рентабельності). Якщо ціна в контрольованій операції або відповідний показник рентабельності контрольованої операції перебуває:

- в межах діапазону, вважається, що умови контрольованої операції відповідають принципу «витягнутої руки»;
- поза межами діапазону цін (рентабельності), розрахунок податкових зобов'язань платника податків у контрольованій операції проводиться відповідно до ціни (показника рентабельності), яка (який) дорівнює значенню медіани такого діапазону.

Порядок розрахунку діапазону цін (рентабельності) та медіани діапазону цін (рентабельності) затверджується Кабінетом Міністрів України. (Постанова Кабінету Міністрів України від 4 червня 2015 року № 381).

Згідно з підп. 39.3.2.4 ст. 39 ПК України передбачено, що вибір показника рентабельності може здійснюватися з урахуванням, зокрема, але не виключно, таких факторів:

- виду діяльності сторони контрольованої операції;
- розподілу функцій, ризиків, активів сторін;
- економічної обґрунтованості обраного показника;
- незалежності показника від доходів та/або витрат, визнаних в операціях між пов'язаними сторонами, та/або в контрольованих операціях.

Під час визначення рівня рентабельності контрольованих операцій можуть бути використані фінансові показники, які забезпечують встановлення відповідності умов контрольованої операції принципу «витягнутої руки», зокрема, але не виключно:

а) валова рентабельність, що визначається як відношення валового прибутку до чистого доходу (виручки) від реалізації товарів (робіт, послуг), розрахованого без урахування акцизного

податку, мита, податку на додану вартість, інших податків та зборів;

б) валова рентабельність собівартості, що визначається як відношення валового прибутку до собівартості реалізованих товарів (робіт, послуг);

в) чиста рентабельність, що визначається як відношення прибутку від операційної діяльності до чистого доходу (виручки) від реалізації товарів (робіт, послуг), розрахованого без урахування акцизного податку, мита, податку на додану вартість, інших податків та зборів;

г) чиста рентабельність витрат, що визначається як відношення прибутку від операційної діяльності до суми собівартості реалізованих товарів (робіт, послуг) та операційних витрат (адміністративних витрат, витрат на збут та інших), пов'язаних з реалізацією товарів (робіт, послуг);

ґ) рентабельність операційних витрат, що визначається як відношення валового прибутку до операційних витрат (адміністративних витрат, витрат на збут та інших), пов'язаних з реалізацією товарів (робіт, послуг);

д) рентабельність активів, що визначається як відношення прибутку від операційної діяльності до поточної ринкової вартості необоротних та оборотних активів (крім поточних фінансових інвестицій і грошових коштів та їх еквівалентів), що прямо або опосередковано використовуються у контрольованій операції. У разі відсутності необхідної інформації про поточну ринкову вартість активів, рентабельність активів може визначатися на основі даних бухгалтерської звітності;

е) рентабельність капіталу, що визначається як відношення прибутку від операційної діяльності до капіталу (сума необоротних та оборотних активів, крім поточних фінансових інвестицій і грошових коштів та їх еквівалентів, крім поточних зобов'язань).

Підпункт 39.3.2.6 ст. 39 ПК України визначає, що показники рентабельності для цілей цієї статті визначаються на підставі даних бухгалтерського обліку та фінансової звітності, відображених за національними положеннями (стандартами) бухгалтерського обліку або міжнародними стандартами відповідно до стандартів бухгалтерського обліку та фінансової

звітності, що використовуються в Україні, з відповідним коригуванням для забезпечення зіставності показників.

Отже, для розрахунку діапазону цін (рентабельності) та медіани діапазону цін (рентабельності), також необхідно провести юридичний аналіз багаточисельних ліцензійних угод по суті (порівняння ціни або рентабельності в контрольованій операції з цінами або показниками рентабельності кількох зіставних неконтрольованих операцій або юридичних осіб, які не здійснюють операції з пов'язаними особами) з комерційних баз даних, створених особами, які збирають та узагальнюють інформацію, що надсилається компаніями до відповідних адміністративних органів, та надають платний доступ до неї в електронному форматі, зручному для проведення пошуків та статистичного аналізу (прикладом таких баз даних є: RoyaltyStat (https://www .royaltystat.com/), RoyaltyRange (https:// www.royaltyrange.com/), Royaltysource (https://www.royaltysource.com/) та інші.

Отже, для отримання величини ставки роялті, яка, зазвичай, відсутня в наданих на дослідження матеріалах, експерт має звернутися до органу, який призначив експертизу, з метою отримання платного «Звіту про надання консультації щодо ліцензійних угод та ставок ліцензійної винагороди (ставок роялті)» у сфері та за параметрами об'єкту потенційної угоди, що складається оцінювачем за напрямком оцінки 2.2. «Оцінка прав на об'єкти інтелектуальної власності», а не судовим експертом.

Частіше ставки роялті в процентному виразі встановлюють з використанням відповідних відомих джерел, як середні за галузями діяльності (нормативний відсоток розміру роялті), а розмір роялті за ліцензійними договорами використання або надання права на використання об'єктів авторського права та суміжних прав встановлюється з використанням відповідних відомих джерел або в процентному виразі до прибутку (доходу) за згодою сторін ліцензійного договору.

При цьому зазначимо, що згідно з п. 2.3 Інструкції № 53/5 судовому експерту заборонено:

− самостійно збирати матеріали, які підлягають дослідженню, а також вибирати вихідні дані для проведення експертизи, якщо вони відображені в наданих йому матеріалах неоднозначно;

– вирішувати питання, які виходять за межі спеціальних знань експерта, та з'ясування питань права і надавати оцінку законності проведення процедур, регламентованих нормативно-правовими актами.

Додатково слід звернути увагу, що визначення справедливої величини ставки роялті (діапазону) може визначити лише оцінювач за напрямком оцінки 2.2. «Оцінка прав на об'єкти інтелектуальної власності», а не судовий експерт.

Щодо змісту другого питання, то звертаємо увагу на те, що це питання за своєю суттю та способом дослідження є виключно економічним (передбачає дослідження документів бухгалтерського та податкового обліку, що є компетенцією судових експертів за спеціальністю 11.1) і не потребує спеціальних знань у сфері інтелектуальної власності.

Щодо змісту третього питання, то воно є правовим, оскільки містить елементи правової оцінки – необґрунтованості завищення ліцензійного платежу, здійснення якої належить до компетенції органів слідства, державного фінансового та податкового контролю. Частіше ставки роялті в процентному виразі встановлюють з використанням відповідних відомих джерел, як середні за галузями діяльності (нормативний відсоток розміру роялті), а розмір роялті за ліцензійними договорами використання або надання права на використання об'єктів авторського права та суміжних прав встановлюється з використанням відповідних відомих джерел або в процентному виразі до прибутку (доходу) за згодою сторін ліцензійного договору.

Отже, з урахуванням вимог п. 2.3 Інструкції № 53/5 вказане питання в такій редакції не може вирішуватись судовим експертом через його правовий характер.

Крім того, згідно з п. 1.1 Розділу ІІІ Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень: «*Вирішення питань, що належать до компетенції органів державного фінансового та податкового контролю (здійснення експертами-економістами перевірки певного комплексу або окремих питань фінансово-господарської діяльності установ, організацій, підприємств з метою виявлення наявних фактів порушення законодавства,*

фактів порушення податкового законодавства, встановлення винних у їх допущенні посадових і матеріально відповідальних осіб), не належить до завдань економічної експертизи».

У бухгалтерському обліку та фінансовій звітності сплату роялті фіксують як платежі з використанням відповідних банківських документів у встановленому порядку. Підставою є ліцензійний договір, акти сплати роялті за відповідний період, податкова звітність.

Більш детально, ці питання стосуються *ліцензійного платежу (роялті, авторської винагороди, паушального платежу),* який є *винагородою* за згодою контрагентів ліцензійного договору, що не протирічить ст. 1109 ЦК України [2], або *платіж за використання або за надання права на використання об'єкта права інтелектуальної власності*, а також як *роялті є доход з джерелом його походження з України*, тобто доход, отриманий резидентами або нерезидентами від будь-яких видів їхньої діяльності на території України (підп. 14.1.225 п. 14.1 ст. 14 ПК України).

Підтвердженням доцільності нашої позиції, є зміст положень ПК України, в якому в залежності від правового статусу фізичної особи, з якою укладений ліцензійний договір про використання об'єкта права інтелектуальної власності, кардинально змінюється підхід до оподаткування роялті. Підпунктом 162.1.1 п. 162.1 ст. 16 ПК України передбачено, що фізична особа – резидент, яка отримує доходи як з джерела їх походження в Україні, так і іноземні доходи, є платником податку на доходи фізичних осіб, а відповідно до підп. 164.2.3 п. 164.2 ст. 16 ПК України доходи від продажу, користування, розпорядження та отримання у спадщину ОПІВ, є базою оподаткування ПДФО (прибутковий податок). Особливості оподаткування роялті встановлено для фізичних осіб п. 170.3 ПК України, в якому зазначено, що роялті оподатковуються за правилами, визначеними для оподаткування дивідендів (п. 170.5 ПК України), тобто 18 %.

Юридична особа, яка нараховує роялті, включаючи суб'єктів спрощеної системи оподаткування або звільнених від сплати податків з будь-яких підстав, є податковим агентом під час нарахування роялті (підп. 170.5.2 п. 170.5 ПК України) та зобов'язана нарахувати ПДФО та сплатити його у відповідні строки до державного бюджету України.

Щодо авторської винагороди або гонорару, то це винагорода, яка виплачується авторам за використання творів науки, літератури або мистецтва. Вибір ставки авторського гонорару провадиться на основі угоди автора з організацією, що використовує його твір, і фіксується в самому договорі. Можлива виплата авторові авансу, якщо це обумовлено в договорі. За кожний вид використання твору, незалежно від виплати винагороди за інші види використання, виплачується особливий авторський гонорар. Між співавторами авторський гонорар розподіляється за їхньою угодою. Якщо такої угоди не досягнуто, то суперечки співавторів розглядаються в суді.

Зазвичай авторська винагорода визначається у договорі у вигляді відсотків від доходу, отриманого від використання твору. Деякі автори, посилаючись на ч. 2 ст. 33 Закону України «Про авторське право і суміжні права» [3], вимагають застосовування мінімальних ставок авторської винагороди, затверджених Кабінетом Міністрів України (Постанова Кабінету Міністрів України №72 від 18 січня 2003 р.), оскільки в деяких випадках розмір винагороди може бути більшим ніж запропонований видавцем відсоток від доходу, отриманого від використання твору.

Висновки. Судовий експерт за експертною спеціальністю 13.9 «Економічні дослідження у сфері інтелектуальної власності» до змісту трьох запропонованих питань щодо роялті стосунку не має, оскільки питання виходять за межі компетенції цієї спеціальності. Вирішення питань щодо визначення ринкової вартості роялті та правильності розрахунку його розміру на підставі умов ліцензійного договору не потребує спеціальних знань експерта у галузі інтелектуальної власності, а є предметом здійснення оцінки оцінювачем та предметом економічної експертизи.

Список використаних джерел:

1. Податковий кодекс України: Закон України від 2 грудня 2010 року № 2755-VI. Дата оновлення: 25.11.2022. URL: https://zakon.-rada.gov.ua/laws /show/2755-17#Text (дата звернення 28.11.2022).

2. Цивільний кодекс України: Закон України від 16 січня 2003 року № 435-IV. Дата оновлення: 10.10.2022. URL: https://zakon.rada.gov.ua/laws/show /435-15#Text (дата звернення 28.11.2022).

3. Про авторське право і суміжні права: Закон України від 23 грудня 1993 року № 3792-XII. Дата оновлення: 05.01.2022. URL: https://zakon.rada.gov. ua/laws/show/3792-12#Text (дата звернення 28.11.2022).

КОМЕНТАР ФАХІВЦЯ

Рішенням весняного засідання секції судової експертизи об'єктів інтелектуальної власності від 15.04.2022, за пропозицією представника КНДІСЕ Н. Климової, розглянуто та підтримано наступну пропозицію.

«Звернутися до Департаменту експертного забезпечення правосуддя та Директорату правосуддя та кримінальної юстиції Міністерства юстиції України щодо внесення змін до розділі V. «Експертиза об'єктів інтелектуальної власності» Науково-методичних рекомендацій із питань підготовки та призначення судових експертиз та експертних досліджень, затверджених Наказом Міністерства юстиції України від 08.10.1998 №53/5 в частині уточнення питання: «*Чи правильно визначено суму роялті за використання об'єкта?*» й викладу його в наступній редакції: «*Яким є розмір суми роялті за використання об'єкта права інтелектуальної власності?*»».

Роялті – це будь-яка винагорода за використання об'єктів права інтелектуальної власності. Ставка та база роялті встановлюється ліцензійним договором. Якщо під сумнів ставиться ставка чи база роялті, їх відповідність ринковим ставкам і базам (істотне завищення, заниження), то необхідні спеціальні знання щодо об'єктивності їх встановлення за первинною документацією бухобліку. Судовий експерт підтверджує вірність арифметичного розрахунку платежів, отриманих як роялті за використання ОПІВ.

Вбачаємо, що питання можна викласти у редакції: «*Яким є розмір роялті за використання об'єкта права інтелектуальної власності?*», без слова «*сума*». Оскільки «сума», по-суті, є показником «розміру» роялті. Відповідно, запропонована редакція питання не звужує його зміст.

Судовому експерту ставиться питання «*Яким є розмір роялті за використання об'єкта права інтелектуальної власності?*», коли необхідно:

– визначити матеріальних збитків за використання об'єктів інтелектуальної власності без укладення з правовласником жодного ліцензійного договору. У цьому випадку, судовий експерт, за відсутності ставки і бази роялті, як власне і самого ліцензійного договору, встановлює їх розмір, ґрунтуючись на аналізі ринку надання права користування об'єктами інтелектуальної власності, а також на основі вартості інтелектуальної власності, помноженої на коефіцієнт капіталізації;

– визначити відповідність ставки і бази роялті, встановленій у ліцензійному договорі, до ставки і бази роялті, властивій конкретній галузі народного господарства на дату оцінки. Поширеною на сьогодні стала практика виведення грошових коштів за кордон в офшорні зони через такий «показник як роялті», яка перевіряється БЕБ;

– дослідити питання трансфертного ціноутворення саме ставок роялті для проведення міжнародного аудиту та ін.

28 жовтня 2022 року відбулося осіннє засідання секції судової експертизи об'єктів інтелектуальної власності, на якому обговорювалось питання про внесення змін до орієнтовного переліку питань, які містяться у Науково-методичних рекомендаціях з питань підготовки і призначення судових експертиз та експертних досліджень, затверджених наказом Міністерства юстиції України від 08 жовтня 1998 року № 53/5, зареєстрованих у Міністерстві юстиції України 03 листопада 1998 року за № 705/3145 (у редакції наказу Міністерства юстиції України від 26 грудня 2012 року № 1950/5) за експертною спеціальністю 13.9:

«Яка ринкова ставка ліцензійного платежу (роялті, авторської винагороди, паушального платежу) в процентному виразі від (зазначити базу роялті: обсягу виробництва, або обсягу реалізації продукції (товарів, робіт, послуг) з використанням об'єкта права інтелектуальної власності, або прибутку тощо) станом на (зазначити дату) (з урахуванням

наданої експерту інформації щодо ставок роялті щодо аналогічних об'єктів)?

Чи підтверджується документально розрахунок ставки роялті в процентному виразі, визначений в (зазначається документ, на підставі якого були відображені в бухгалтерському обліку відповідні господарські операції, або акт перевірки контролюючого органу, або у позовних вимогах)?

Чи підтверджується документально розмір необґрунтованого завищення ліцензійного платежу (роялті, авторської винагороди, паушального платежу) (найменування організації) у сумі (зазначається сума) за період (зазначається період), визначений в акті перевірки контролюючого органу або у позовних вимогах? Якщо так, – у якій сумі?».

Під час палкої дискусії було висвітлено дві позиції :

Позиція Климової Н. Б.: «Орієнтовний перелік питань для спеціальності 13.9 є схожим переліку питань для економічної експертизи і ці питання є такими що дублюють їх. Якщо виникає таке складне питання для вирішення якого потрібні консолідовані знання, можна зробити комплексну експертизу, залучити економіста, проявити ініціативу і зробити це питання до конкретного випадку, до конкретного дослідження. А не потрібно міняти так докорінно питання в Орієнтовному переліку питань судової експертизи з дослідження об'єктів інтелектуальної власності, саме 13.9. Климова Н. Б. запропонувала із питання «Чи правильно визначено суму роялті за використання об'єкта?», викладеного в абзаці сорок четвертому пункту 5.5 розділу V. Експертиза об'єктів інтелектуальної власності Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень, затверджених наказом Міністерства юстиції України 08.10.1998 № 53/5 (у редакції наказу Міністерства юстиції України 26.12.2012 № 1950/5), забрати слова «Чи правильно».

Позиція Тимощик Л. П.: Питання «Чи правильно визначено суму роялті за використання об'єкта?», викладеного в абзаці сорок четвертому пункту 5.5 розділу V. Експертиза об'єктів інтелектуальної власності Науково-методичних рекомендацій з

питань підготовки та призначення судових експертиз та експертних досліджень, затверджених наказом Міністерства юстиції України 08.10.1998 № 53/5 (у редакції наказу Міністерства юстиції України 26.12.2012 № 1950/5) замінити такими питаннями:

«Яка ринкова ставка ліцензійного платежу (роялті, авторської винагороди, паушального платежу) в процентному виразі від (зазначити базу роялті: обсягу виробництва, або обсягу реалізації продукції (товарів, робіт, послуг) з використанням об'єкта права інтелектуальної власності, або прибутку тощо) станом на (зазначити дату) (з урахуванням наданої експерту інформації щодо ставок роялті щодо аналогічних об'єктів)?

Чи підтверджується документально розрахунок ставки роялті в процентному виразі, визначений в (зазначається документ, на підставі якого були відображені в бухгалтерському обліку відповідні господарські операції, або акт перевірки контролюючого органу, або у позовних вимогах)?

Чи підтверджується документально розмір необґрунтованого завищення ліцензійного платежу (роялті, авторської винагороди, паушального платежу) (найменування організації) у сумі (зазначається сума) за період (зазначається період), визначений в акті перевірки контролюючого органу або у позовних вимогах? Якщо так, – у якій сумі?».

За результатами голосування члени секції (11 голосів із 13) підтримали позицію Тимощик Л. П.

З протоколом осіннього засідання секції судової експертизи об'єктів інтелектуальної власності науково-консультативної та методичної ради з проблем судової експертизи об'єктів інтелектуальної власності при Міністерстві юстиції України, що відбулося 28.10.2022 можна ознайомитися за посиланням: https://minjust.gov.ua/files/general/2022/12/30/20221230145347-91.pdf.

Тимощик Лілія Павлівна,
кандидат економічних наук, учений секретар Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України, судовий експерт, оцінювач

Рак Віра Михайлівна,
науковий співробітник Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України, судовий експерт, оцінювач

ОСОБЛИВОСТІ ВИЗНАЧЕННЯ РОЗМІРУ МАТЕРІАЛЬНОЇ ШКОДИ ПРИ ПОРУШЕННЯХ ПРАВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ НА ОБ'ЄКТИ ПРОМИСЛОВОЇ ВЛАСНОСТІ

Під час проведення економічних досліджень у сфері інтелектуальної власності (спеціальність 13.9) використовуються методи аналізу, синтезу, абстрагування, порівняння й узагальнення, а також спеціальні методи економічного аналізу, математичного моделювання, підходи та методи незалежної оцінки майна і майнових прав.

Перед розрахунком матеріальної шкоди, що завдається внаслідок порушення прав інтелектуальної власності на об'єкти промислової власності, необхідно враховувати наявність підстав порушення права без згоди власника прав. Іншими словами, необхідно встановити, чи використано винахід відповідно до положень ч. 2 ст. 28 Закону України «Про охорону прав на винаходи та корисні моделі». Встановлення зазначених обставин є обов'язковою умовою наявності матеріальної шкоди, що підлягає визначенню.

Використання прав, наданих патентом, здійснюється в межах, передбачених законодавством. Відповідно до Закону України № 2174-IX «Про захист інтересів осіб у сфері інтелектуальної власності під час дії воєнного стану, введеного у зв'язку із збройною агресією Російської Федерації проти України» з дня введення в Україні воєнного стану зупиняється перебіг строків для вчинення дій, пов'язаних з охороною прав інтелектуальної власності, а також строків щодо процедур набуття цих прав (визначених законами України «Про охорону прав на промислові зразки», «Про охорону прав на знаки для товарів і послуг», «Про охорону прав на компонування напівпровідникових виробів», «Про охорону прав на винаходи і корисні моделі», «Про правову охорону географічних зазначень», «Про авторське право і суміжні права», «Про охорону прав на сорти рослин»).

З дня, наступного за днем припинення чи скасування воєнного стану, перебіг цих строків продовжується з урахуванням часу, що минув до їхнього зупинення.

Будь-яка особа не може використовувати запатентований винахід без згоди власника патенту. Але, як правило, не визнається незаконним використання його без комерційної мети, з науковою метою або в порядку експерименту, а також у деяких інших випадках. Загалом питання про те, законним чи незаконним є таке використання, належить до компетенції суду, а отже розрахунок матеріальної шкоди проводиться за умови, якщо такий факт буде встановлено в суді.

Матеріальна шкода включає як пряму дійсну шкоду, так і втрачену (упущену) вигоду.

Пряма дійсна шкода – це безпосереднє зменшення активів підприємства – його майна й майнових прав, які відображаються в балансі. До її складу входять втрати (яких особа зазнала зі знищенням або пошкодженням речі – недостачі, розкрадання, природний убуток) та витрати (які особа зробила або мусить зробити для відновлення свого порушеного права). Вказане вище підтверджується нормами п. 1 ч. 2 ст. 22 ЦКУ, а саме: «втрати, яких особа зазнала у зв'язку зі знищенням або пошкодженням речі, а також витрати, які особа зробила або мусить зробити для відновлення свого порушеного права (реальні збитки)».

Втрачена (упущена) вигода відповідно до п. 2 ч. 2 ст. 22 ЦКУ визначається як «доходи, які особа могла б реально одержати за звичайних обставин, якби її право не було порушене».

Особливістю складових матеріальної шкоди при порушенні прав на об'єкти інтелектуальної власності є те, що вона фактично не включає пряму дійсну шкоду, оскільки при порушенні прав інтелектуальної власності об'єкт інтелектуальної власності у дійсності не зникає, на відміну від матеріальних об'єктів, які можуть бути знищені або пошкоджені.

У процесі визначення розміру упущеної вигоди визначається розмір прибутку, який власник винаходу міг би отримати на законних підставах, а саме на основі ліцензії (ліцензійного договору).

Під час використання винаходу без дозволу матеріальна шкода власнику заподіюється внаслідок зменшення обсягу товарів, що ним реалізуються, та попиту на них, тому втрачена

вигода полягає в розмірі прибутку, який власник міг би отримати, але не отримав унаслідок появи на ринку фальсифікованого товару, або в розмірі ліцензійної винагороди, що є прибутком (доходом), який недоотримав власник винаходу, якби особа використовувала винахід на законних підставах.

Відповідно до п. 26 Національного стандарту №4 «Оцінка майнових прав інтелектуальної власності» розмір збитків за неправомірне використання об'єкта права інтелектуальної власності визначається станом на дату оцінки із застосуванням оціночної процедури накопичення прибутку (доходу), який не отримав суб'єкт права інтелектуальної власності та/або ліцензіат унаслідок неправомірного використання об'єкта права інтелектуальної власності, виходячи з обсягів виробництва та/або реалізації контрафактної продукції.

Відповідно до Національного стандарту №1 «Загальні засади оцінки майна і майнових прав» оціночна процедура – це дії (етапи), виконання яких у певній послідовності дає можливість провести оцінку [*6*]. За таких умов, оціночна процедура накопичення прибутку (доходу) належить до методів дохідного підходу, а відповідно до п. 10 Національного стандарту №4 – це метод непрямої капіталізації (дисконтування грошового потоку) та метод прямої капіталізації доходу [*7*]. Згідно з п. 11 Національного стандарту №4 застосування методів непрямої капіталізації (дисконтування грошового потоку) та прямої капіталізації доходу передбачає визначення розміру тієї частини доходу, що отримана у зв'язку з наявністю у юридичної або фізичної особи майнових прав інтелектуальної власності [*7*]. Водночас грошовим потоком чи доходом може бути:

– для методів переваги у прибутку і розподілу прибутків – різниця між прибутком суб'єкта права інтелектуальної власності, отриманого внаслідок використання об'єкта права інтелектуальної власності, та прибутком, отриманим без використання такого об'єкта;

– для методу додаткового прибутку – додатковий прибуток, який отримано суб'єктом права інтелектуальної власності унаслідок використання об'єкта права інтелектуальної власності;

– для методу роялті – ліцензійний платіж за надання прав на використання об'єкта права інтелектуальної власності.

Відповідно до п. 15 Національного стандарту №4 метод роялті застосовується за умови, що майнові права інтелектуальної власності надані або можуть бути надані за ліцензійним договором іншій фізичній або юридичній особі [*7*].

Таким чином, з урахуванням наведених вище особливостей та в залежності від наявних матеріалів, наданих на дослідження, можливо визначити розмір матеріальної шкоди, спричинений порушеннями прав інтелектуальної власності на об'єкти промислової власності.

Список використаних джерел:

1. Цивільний кодекс України : Закон України від 16.01.2003 р. № 435-IV. Голос України.12.03.2003. № 45.
2. Про охорону прав на винаходи та корисні моделі : Закон України від 15.12.1993 р. № 3687 – XII. Відомості Верховної Ради України. 1994. № 7, ст. 32.
3. Про захист інтересів осіб у сфері інтелектуальної власності під час дії воєнного стану, введеного у зв'язку із збройною агресією Російської Федерації проти України: Закон України від 01.04.2022 р. № 2174-IX. Офіційний вісник України. 29.04.2022. № 33, стор. 100, стаття 1749, код акта 110972/2022.
4. Про авторське право і суміжні права : Закон України від 23.12.1993 р. № 3792-XII. Голос України. 23.02.1994.
5. Про оцінку майна, майнових прав та професійну оціночну діяльність в Україні : Закон України від 12.07.2001№ 2658-Ш. Офіційний вісник України. 07.09.2001. № 34, стор. 1, стаття 1577, код акта 19803/2001.
6. Національний стандарт № 1 «Загальні засади оцінки майна і майнових прав» : Постанова Кабінету Міністрів України від 10.09.2003 р. № 1440. Офіційний вісник України. 26.09.2003. № 37, стор. 64, стаття 1995, код акта 26384/2003.
7. Національний стандарт № 4 «Оцінка майнових прав інтелектуальної власності» : Постанова Кабінету Міністрів України від 03.10.2007 р. № 1185. Офіційний вісник України. 15.10.2007. № 75, стор. 24, стаття 2792, код акта 41131/2007.
8. Методика оцінки майнових прав інтелектуальної власності : затверджено наказом Фонду державного майна України від 25.06.2008 р. № 740. Офіційний вісник України. 22.08.2008. № 60, стор. 33, стаття 2042, код акта 43963/2008.

Германюк Ірина Володимирівна,
науковий співробітник лабораторії економічних досліджень Науково-дослідного центру судових експертиз з питань інтелектуальної власності Міністерства юстиції України

ПРОБЛЕМИ ВИЗНАЧЕННЯ НЕМАТЕРІАЛЬНИХ АКТИВІВ У БУХГАЛТЕРСЬКОМУ ОБЛІКУ ПІДПРИЄМСТВ

Анотація: Розвиток правової держави супроводжується багатогранним розвитком інтелектуальної власності. У господарській діяльності виникає чимало питань з бухгалтерського обліку нематеріальних активів та відповідно відображення інформації про нематеріальні активи у фінансовій звітності. Одним з ключових питань є визначення і класифікація нематеріального активу й відповідно подальший облік нематеріальних активів і не відображення у фінансовій звітності. Неоднозначність нормативних документів та методологічних розробок щодо обліку нематеріальних активів потребує додаткових роз'яснень для їх практичного застосування Тому розглянуто основні проблеми визначення та класифікацію нематеріального активу.

Ключові слова: нематеріальний актив, ідентифікація, класифікація, немонетарність.

Бухгалтерський облік нематеріальних активів (НМА) регулюється Положенням (стандартом) бухгалтерського обліку 8 «Нематеріальні активи» (далі- П(с)БО 8) та Міжнародним стандартом бухгалтерського обліку 38 (далі- МСБО 38).

Нематеріальний актив – немонетарний актив, який не має матеріальної форми та може бути ідентифікований. [1, п.4].

Згідно з МСБО 38, **нематеріальний актив –** немонетарний актив, який не має фізичної субстанції та може бути ідентифікований. [2, п.8].

Отже, нематеріальність і немонетарність дозволяє відокремити нематеріальні активи від фінансових та матеріальних активів.

Слід зазначити, що механізм ідентифікації нематеріальних активів не визначений ані в П(с)БО8, ані в нормативних

документах і методичних рекомендаціях, що викликає багато питань щодо визнання в бухгалтерському обліку нематеріальних активів і їх подальшого обліку. У ПСБО8 не передбачено визначення ідентифікації або ідентифікованих активів.

Певний механізм ідентифікації нематеріальних активів передбачено МСБО 38.

За визначенням нематеріального активу, його необхідно ідентифікувати так, щоб відокремлювати від гудвілу. [2, п.11].

Відповідно до п.12. МСБО 38 [2], актив є ідентифікованим, якщо він:

а) може бути відокремлений, тобто його можна відокремити або відділити від суб'єкта господарювання і продати, передати, ліцензувати, здати в оренду або обміняти індивідуально або разом із пов'язаним з ним контрактом, ідентифікованим активом чи зобов'язанням, незалежно від того, чи має суб'єкт господарювання намір зробити це, або

б) виникає внаслідок договірних або інших юридичних прав, незалежно від того, чи можуть вони бути передані або відокремлені від суб'єкта господарювання або ж від інших прав та зобов'язань.

Бухгалтерський облік нематеріальних активів ведеться щодо кожного об'єкта за такими групами [1, п.5]:

− права користування природними ресурсами (право користування надрами, іншими ресурсами природного середовища, геологічною та іншою інформацією про природне середовище тощо);

− права користування майном (право користування земельною ділянкою відповідно до земельного законодавства, право користування будівлею, право на оренду приміщень тощо);

− права на комерційні позначення (права на торговельні марки (знаки для товарів і послуг), комерційні (фірмові) найменування тощо), крім тих, витрати на придбання яких визнаються роялті;

− права на об'єкти промислової власності (право на винаходи, корисні моделі, промислові зразки, сорти рослин, породи тварин, компонування (топографії) інтегральних мікросхем, комерційні таємниці, у тому числі ноу-хау, захист від

недобросовісної конкуренції тощо), крім тих, витрати на придбання яких визнаються роялті;

– авторське право та суміжні з ним права (право на літературні, художні, музичні твори, комп'ютерні програми, програми для електронно-обчислювальних машин, компіляції даних (бази даних), виконання, фонограми, відеограми, передачі (програми) організацій мовлення тощо), крім тих, витрати на придбання яких визнаються роялті;

– інші нематеріальні активи (право на провадження діяльності, використання економічних та інших привілеїв тощо).

Група нематеріальних активів – сукупність однотипних за призначенням та умовами використання нематеріальних активів [1, п.4].

Для обліку й узагальнення інформації про наявність і рух нематеріальних активів призначений рахунок 12 «Нематеріальні активи» [3].

Рахунок 12 "Нематеріальні активи" має такі субрахунки:

121 «Права користування природними ресурсами»

122 «Права користування майном»

123 «Права на комерційні позначення»

124 «Права на об'єкти промислової власності»

125 «Авторське право та суміжні з ним права»

127 «Інші нематеріальні активи».

Придбаний або отриманий нематеріальний актив відображається в балансі, якщо існує імовірність одержання майбутніх економічних вигод, пов'язаних з його використанням, та його вартість може бути достовірно визначена [1, п.6]:

Нематеріальний актив, отриманий в результаті розробки, слід відображати в балансі за умов, якщо підприємство має [1, п.7]:

– намір, технічну можливість та ресурси для доведення нематеріального активу до стану, у якому він придатний для реалізації або використання;

– можливість отримання майбутніх економічних вигод від реалізації або використання нематеріального активу;

– інформацію для достовірного визначення витрат, пов'язаних з розробкою нематеріального активу.

Відповідно до п.12. МСБО 38 [2, п.119], клас нематеріальних активів є групою активів, подібних за характером і

використанням у діяльності суб'єкта господарювання. Окремі класи можуть, наприклад, включати:

а) назви брендів;

б) заголовки та назви видань;

в) комп'ютерне програмне забезпечення;

г) ліцензії та привілеї;

ґ) авторські права, патенти та інші права на промислову власність, права на обслуговування та експлуатацію;

д) рецепти, формули, моделі, проекти та прототипи;

е) нематеріальні активи на етапі розробки.

Зазначені класи поділяються на (об'єднуються у) менші (більші) класи, якщо це призводить до доречнішої інформації для користувачів фінансової звітності.

Отже, П(с)БО8 містить такі групи нематеріальних активів, що не передбачені МСБО 38, а саме: права користування природними ресурсами та права користування майном. Проте групи будь-яких об'єктів інтелектуальної власності (як комп'ютерні програми, товарні знаки) не зазначені в П(с)БО8, наявні лише права.

Статтею 420 Цивільного кодексу України передбачено, що до об'єктів права інтелектуальної власності, зокрема, належать [4, ч.1 ст.420]:

- літературні та художні твори;
- комп'ютерні програми;
- компіляції даних (бази даних);
- виконання;
- фонограми, відеограми, передачі (програми) організацій мовлення;
- наукові відкриття;
- винаходи, корисні моделі, промислові зразки;
- компонування напівпровідникових виробів;
- раціоналізаторські пропозиції;
- сорти рослин, породи тварин;
- комерційні (фірмові) найменування, торговельні марки (знаки для товарів і послуг), географічні зазначення;
- комерційні таємниці.

Відповідно до ч.1 ст.433 Цивільного кодексу України [4], об'єктами авторського права є твори, а саме:

1) літературні та художні твори, зокрема:

- романи, поеми, статті та інші письмові твори;
- лекції, промови, проповіді та інші усні твори;
- драматичні, музично-драматичні твори, пантоміми, хореографічні, інші сценічні твори;
- музичні твори (з текстом або без тексту);
- аудіовізуальні твори;
- твори живопису, архітектури, скульптури та графіки;
- фотографічні твори;
- твори ужиткового мистецтва;
- ілюстрації, карти, плани, ескізи і пластичні твори, що стосуються географії, топографії, архітектури або науки;
- переклади, адаптації, аранжування та інші переробки літературних або художніх творів;
- збірники творів, якщо вони за добором або упорядкуванням їх складових частин є результатом інтелектуальної діяльності;

2) комп'ютерні програми;

3) компіляції даних (бази даних), якщо вони за добором або упорядкуванням їх складових частин є результатом інтелектуальної діяльності;

4) інші твори.

Відповідно до ч.1 ст.155 Цивільного кодексу України [5], об'єктами прав інтелектуальної власності у сфері господарювання визнаються:

- винаходи та корисні моделі;
- промислові зразки;
- сорти рослин та породи тварин;
- торговельні марки (знаки для товарів і послуг);
- комерційне (фірмове) найменування;
- географічне зазначення;
- комерційна таємниця;
- комп'ютерні програми;
- інші об'єкти, передбачені законом.

Тобто, в ПСБО8 зазначено, що бухгалтерський облік нематеріальних активів ведеться щодо кожного об'єкта за відповідними групами. Водночас наведено визначення групи нематеріальних активів, але не наведено визначення об'єкта

нематеріальних активів. У ст. 420 Цивільного кодексу України та у ст.155 Господарського кодексу України наведено переліки об'єктів прав інтелектуальної власності, проте відсутнє визначення поняття «об'єкта нематеріальних активів». Отже, в ПСБО8, Цивільному кодексі України та в Господарському кодексі України відсутнє визначення категорії «об'єкт» нематеріальних активів.

Таким чином, аналіз питань, пов'язаних з визначенням і класифікацією нематеріальних активів, свідчить про необхідність удосконалення класифікації нематеріальних активів за певними класифікаційними ознаками, які дозволять полегшити ідентифікацію об'єктів нематеріальних активів.

Висновки. На практиці виникає чимало проблем, пов'язаних із визначенням і класифікацією нематеріального активу та відповідно подальший облік нематеріальних активів і їх відображення у фінансовій звітності. Існує необхідність удосконалення класифікації нематеріальних активів за певними класифікаційними ознаками, які дозволять полегшити ідентифікацію об'єктів нематеріальних активів. Також необхідно визначити механізм ідентифікації нематеріальних активів або визначити категорію «ідентифіковані активи».

Список використаних джерел:

1. Про затвердження Національного положення (стандарту) бухгалтерського обліку : Наказ; Мінфін України від 18.10.1999 № 242 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/z0750-99 (дата звернення: 02.12.2022).
2. Міжнародний стандарт бухгалтерського обліку 38 (МСБО 38). Нематеріальні активи : Стандарт; IASB від 01.01.2012 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/929_050 (дата звернення: 02.12.2022).
3. Інструкція про застосування Плану рахунків бухгалтерського обліку активів, капіталу, зобов'язань і господарських операцій підприємств і організацій : Інструкція; Мінфін України від 30.11.1999 № 291 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/z0893-99 (дата звернення: 02.12.2022).
4. Цивільний кодекс України : Кодекс України; Закон, Кодекс від 16.01.2003 № 435-IV // База даних «Законодавство України» / Верховна

Рада України. URL: https://zakon.rada.gov.ua/go/435-15 (дата звернення: 02.12.2022).

5. Господарський кодекс України : Кодекс України; Закон, Кодекс від 16.01.2003 № 436-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/436-15 (дата звернення: 07.12.2022).

4. ЕКСПЕРТИЗА КОМП'ЮТЕРНИХ ПРОГРАМ, БАЗ ДАНИХ І ТЕЛЕКОМУНІКАЦІЙ ПІД ЧАС ВИРІШЕННЯ ЕКСПЕРТНИХ ЗАВДАНЬ У СФЕРІ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Можаєв Михайло Олександрович,
д.т.н., заступник директора Науково-дослідного центру судових експертиз з питань інтелектуальної власності Міністерства юстиції України, судовий експерт

Гомон Володимир Олексійович,
судовий експерт лабораторії авторського права та інформаційних технологій Науково-дослідного центру судових експертиз з питань інтелектуальної власності Міністерства юстиції України

Бикова Тетяна Максимівна,
завідувач сектору інформаційних технологій лабораторії авторського права та інформаційних технологій Науково-дослідного центру судових експертиз з питань інтелектуальної власності Міністерства юстиції України, судовий експерт

СИСТЕМА МАРШРУТИЗАЦІЇ ТРАФІКУ ТА АНАЛІЗ ОСНОВНИХ ЗАГРОЗ

Анотація. Проведено аналіз системи маршрутизації трафіку для термінації голосового трафіку. Дослідження порушення порядку маршрутизації телекомунікаційного трафіку дозволить фахівцям значно підвищити обґрунтованість управлінських рішень з організації діяльності в сферах критичного застосування, виробити практичні рекомендації щодо впровадження нових інформаційних технологій, досліджувати шляхи побудови маршрутизації телекомунікаційного трафіку захищених комп'ютерних систем і мереж.

Ключові слова: маршрутизація, термінація, трафік, рефайл.

Постановка проблеми. Великі вимоги до своєчасності, достовірності та надійності інформаційних процесів у різних

галузях діяльності сучасного суспільства, а також розширення можливостей обчислювальної техніки привели до удосконалення і впровадження методів розподіленої обробки даних за рахунок реалізації мережевого доступу до комп'ютерних систем. Найбільш широкого застосування такі системи й мережі набули в так званих сферах критичного застосування, до яких належить діяльність операторів мобільного зв'язку. Не зважаючи на очевидну різнорідність сфер критичного застосування, їх об'єднує одна дуже важлива обставина – значний збиток від порушення порядку маршрутизації голосового трафіку.

Аналіз останніх досліджень й публікацій. Актуальність полягає в тому, що на сьогоднішній день відсутні методики або методичні рекомендації у судово-експертній системі України щодо дослідження апаратних й програмних засобів, призначених для порушення порядку маршрутизації голосового трафіку.

Додатковим фактором актуальності роботи є аналіз методів призначених для порушення порядку маршрутизації, а також особливостей їхньої реалізації на різних рівнях моделі взаємодії відкритих систем, розгляд основних концептуальних питань створення, функціонування, розвитку і використання національної системи конфіденційного зв'язку.

Ефективність систем телекомунікаційної взаємодії безпосередньо залежить від ефективності різних інформаційних технологій, що забезпечують підтримку бізнес-процесів операторів і провайдерів телекомунікаційних послуг. Для якісного надання послуг і підтримки конкурентоспроможності оператори телекомунікацій повинні ефективно використовувати наявні телекомунікаційні ресурси, не допускаючи або зводячи до мінімуму нелегальний пропуск трафіку. Шахрайське або недобросовісне використання каналів зв'язку може призвести не тільки до зниження якості послуг, що надаються абонентам, але і до значних фінансових втрат і серйозних боргових зобов'язань при взаєморозрахунках операторів фіксованого зв'язку.

Для підвищення ефективності діяльності операторів телекомунікацій створюються і впроваджуються різні системи управління, які здійснюють автоматизацію управління підприємством оператора і технологічним обладнанням телекомунікаційних мереж. Прагнення операторів мінімізувати

нелегальне використання каналів зв'язку, своєчасно виявляти і припиняти різноманітні способи шахрайства і хакерські дії, змушує їх шукати або самостійно розробляти різні спеціалізовані рішення.

З огляду на різноманіття телекомунікаційних технологій, широкий спектр методів шахрайства та способів нелегального використання ресурсів операторів, неможливо створити універсальну систему, здатну виявляти всі існуючі й потенційно можливі методи шахрайства і способи зловживання. Тому виникає необхідність розробки моделей, методів і алгоритмів аналізу використання комунікаційних ресурсів. У цій роботі розглянуті і запропоновані алгоритми аналізу й контролю голосового трафіку для виявлення випадків нелегального використання обладнання і каналів зв'язку.

Метою цієї статті є отримання доступу до функціональних здібностей, дослідження голосового трафіку, аналіз отриманої інформації у відповідності до певних критеріїв.

Дослідження голосового трафіку дозволить фахівцям значно підвищити обґрунтованість управлінських рішень з організації діяльності в сферах критичного застосування, виробити практичні рекомендації щодо впровадження нових інформаційних технологій, досліджувати шляхи побудови найбільш захищених комп'ютерних систем і мереж. Крім того, аналізована тема буде корисною фахівцям з інформаційної безпеки, до кола завдань яких надежить виявлення і припинення злочинних посягань на трафік.

Виклад основного матеріалу.

На глобальному рівні справа поставлена «на широку ногу» – в світі є цілі телекомунікаційні біржі, що продають послуги подібних фірм. Оператори, які направляють дзвінки в Україну, самі вирішують – використовувати дешевий і часто неякісний рефайл, або ж офіційно купувати послуги українських колег. В Україні дуже багато компаній, які займаються транзитом міжнародного трафіку. Вони працюють на території Української держави, але зареєстровані в інших юрисдикціях. Відповідно, дохід від їхньої діяльності також «осідає» в інших юрисдикціях.

Багато міжнародних операторів самі докуповують такий трафік, щоб менше платити за міжнародними договорами, але якість цього трафіку дуже погана.

Всередині України мова йде про сотні фірм різного масштабу, які обслуговують такий бізнес. На них припадає від 20% усіх доходів, що повинні були б осісти на рахунках мобільних операторів за обслуговування міжнародних дзвінків. Податки з таких доходів ці фірми, зрозуміло, не платять.

Рефайл – сумний приклад міжнародного шахрайства з метою заробити на продажу міжнародного трафіку, знаходячи незаконні маршрути його пересування від ініціатора дзвінка до одержувача. Водночас, в залежності від того, де саме в ланцюжку відбувається шахрайство, може відбуватися підміна номера, з якого зроблений вихідний дзвінок. Причини цього явища носять економічний характер: низькі ставки термінації міжнародного і національного трафіку, відсутність ідентифікації припейд-клієнтів.

Сам рефайл є кримінально караним діянням, яке потрапляє під ст. 361 Кримінального кодексу України – несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку. У Реєстрі судових рішень є сотні справ, пов'язаних з цією статтею.

А оператори, в свою чергу, постійно виявляють тисячі випадків втручання в роботу своїх мереж. «У 2016 році зафіксовано понад 12 000 випадків шахрайства з голосовим трафіком проти «Укртелекому»». Під шахрайством мається на увазі підміна міжнародних дзвінків псевдо-національними, тобто рефайл. Такі дзвінки надходять з мереж мобільних операторів. Відбувається відстеження подібних випадків, про які повідомляється операторам зв'язку, унаслідок чого застосовується блокування номерів шахраїв. З огляду на той факт, що мобільні картки продаються без ідентифікації абонента (припейд), то відстежити таких шахраїв стає вкрай складно.

Проблема такого роду шахрайства є загальносвітовою, тому випадки порушення маршрутизації виявляються з різних напрямків.

У зв'язку з девальвацією національної валюти з 2013 року рефайл став одним з основних видів шахрайства. У боротьбі з ним компанії на постійній основі співпрацюють з правоохоронними органами. За останні роки неодноразово припинялася незаконна маршрутизація трафіку. Першочергове

завдання в боротьбі з рефайлом – навчання співробітників новим технологіям, а також закупівля і впровадження сучасних систем з виявлення шахраїв.

У зв'язку із запуском мережі нового покоління й великою популярністю смартфонів стали розвиватися нові підвиди мобільних махінацій. Один з яскравих прикладів – термінація МН-трафіку за схемою GSM to Viber. Від такого виду шахрайства зараз страждають оператори усього світу.

На сьогодні нелегальна термінація трафіку стала однією з основних бід будь-якого телекомунікаційного оператора. Найбільше страждають оператори в тих країнах, де міжнародний зв'язок коштує значно дорожче за локальний трафік. У топ держав, які більше інших страждають від цього виду шахрайства, входять країни Африки, Балканського півострова, Азії та східної Європи.

Як відомо, суть цього виду шахрайства полягає в напрямку міжнародного голосового або SMS трафіку в обхід належного комутаційного обладнання. Унаслідок чого виникає низка проблем. По-перше, оператор втрачає гроші на взаємні розрахунки – інтерконект. По-друге, страждає якість зв'язку, з'являються сторонні шуми, затримки, часті обриви. По-третє, відбувається підміна номера абонента.

Якщо кілька років тому цим видом фроду (шахрайства) могли займатися тільки люди з відповідною технічною освітою, то сьогодні «бізнес» такого роду можна купити під ключ. В інтернеті безліч пропозицій від організацій, готових за прийнятну плату продати і налаштувати необхідне обладнання, встановити спеціалізоване програмне забезпечення для імітації людської активності, звести з оригінатора трафіку, надавати цілодобову технічну підтримку. І, звичайно ж, вони навчать, де розмістити обладнання і як здійснити налаштування, щоб операторам було складніше виявляти і блокувати SIM-карти шахрая [3].

У світовій практиці застосовуються два основних різновиди систем виявлення цього виду шахрайства:

1. Активні системи – це системи, що виявляють фродові номера, здійснюючи сесії тестових викликів (продзвонів) з різних частин світу на номери оператора.

2. Пасивні системи – це системи, які здійснюють аналіз активності абонентів на предмет «людяності».

Якщо з активними системами все більш-менш ясно, то для налаштування пасивних систем потрібен глибокий аналіз з метою виявлення основних критеріїв, що відрізняють фродові карти від живих абонентів. Це не таке просте завдання, як може здатися на перший погляд.

Завдяки сучасним системам, SIM-карти в шлюзах дозволяють:

- відправляти і приймати повідомлення із заздалегідь підготовленим текстом;
- здійснювати дзвінки і відповідати на них з переданням запису реальної розмови в голосовий канал;
- створювати групи, імітуючи спілкування з постійними контактами (друзями);
- імітувати різне переміщення між локаціями, в залежності від часу та дня тижня;
- відправляти USSD запити для перевірки балансу та підключення бонусів. Зчитувати необхідну інформацію з відповідей;
- стежити за балансами і бонусами;
- задавати розклад для розподілу обсягів трафіку протягом доби і в різні дні тижня.

Ми пропонуємо звернути увагу на деякі особливості роботи систем імітації людської діяльності, які можна спробувати використовувати для додаткового виявлення SIM-карт шахраїв, або для того щоб ускладнити шахраям життя.

Термінатору необхідно контролювати баланси і бонуси на своїх SIM-картах. Це потрібно для того, щоб номер несподівано не замовк (адже вони теж повинні підтримувати репутацію в очах своїх клієнтів.) Системи, керуючі термінацією трафіку, вміють відправляти USSD команди для перевірки балансів та підключення бонусів. Також вони можуть зчитувати потрібну інформацію з одержуваних відповідей. У разі якщо відповідь прочитати не вдалося, після декількох спроб, система часто вивантажує SIM-картку зі шлюзу. Якщо періодично вносити невеликі зміни в USSD відповідь, щоб ускладнити парсинг тексту за маскою, теоретично можна добитися збою в роботі парсеру і, як наслідок, ускладнити життя шахраєві.

Під час імітації людської активності система здійснює передзвін між номерами в шлюзі. Таким чином, у процесі виявлення номера термінатора, необхідно проаналізувати зв'язок з іншими SIM-картами [4].

Система, яка керує термінацією, дозволяє створювати кілька локацій і налаштовувати переміщення між ними. Водночас, через те, що миттєве переміщення на велику відстань буде виглядати підозрілим, задається затримка між відходом з однієї локації і появою в інший. На час затримки SIM-карта відключається. Виходячи з цієї особливості, пропонується проаналізувати географію переміщення абонентів. Переміщуються вони поступово чи перескакують між локаціями, минаючи проміжні базові станції. Також є сенс подивитися на інші номери, список локацій яких збігається з локаціями виявлених номерів.

Звичайно малоймовірно, що описані вище методи, застосовні для всіх операторів і всіх термінаторів. Але є сенс проаналізувати трафік термінаторів через призму цих особливостей.

Якщо ж потрібен універсальний метод, яким можна доповнити систему виявлення нелегальної термінації, то найкращий результат дасть порівняння вихідних дзвінків у роумінгу, одержуваних з TAP файлів і NRTRDE, з вхідними дзвінками у власних телефонах.

Загалом логіка контролю наступна: абонент А знаходиться в роумінгу і телефонує абоненту В. Абоненти А і В є абонентами оператора. Якщо абоненту В у цей час прийшов вхідний дзвінок аналогічної тривалості з номера С, то через номер здійснюється термінація трафіку. Звичайно подібний контроль не може зрівнятися з продзвоном, але, як показала практика, може бути приємним доповненням до нього, з високим відсотком точності.

Боротьба з нелегальною термінацією трафіку – важке й дороге завдання. Але якщо ситуацію пустити на самоплив, одного разу настане день, коли прибуток за інтерконект стане для оператора історією.

Висновки. Було проведено дослідження технології VoIP-телефонії, технології SIP-телефонії та передачі телекомунікаційного трафіку на фізичному і канальному рівнях.

У статті було наведено рекомендації з дослідження апаратних і програмних засобів, що використовуються для термінації

голосового трафіку. Дослідження порушення порядку маршрутизації телекомунікаційного трафіку дозволить фахівцям значно підвищити обґрунтованість управлінських рішень з організації діяльності у сферах критичного застосування, виробити практичні рекомендації щодо впровадження нових інформаційних технологій, досліджувати шляхи побудови маршрутизації телекомунікаційного трафіку захищених комп'ютерних систем і мереж.

Список використаних джерел:

1. Попков Д. Транзит-шахрайство, або Шахрайство у великих розмірах // ІнформКур'єр-Зв'язок. 2005. № 2. С. 55–56.
2. Правила приєднання телекомунікаційних мереж та їх взаємодії: «Про затвердження Правил приєднання телекомунікаційних мереж та їх взаємодії» від 28.03.05 № 161.
3. Правила надання послуг місцевого, внутрішньозонового, міжміського та міжнародного телефонного зв'язку: Постанова від 18.05.05 № 310.
4. Вимоги до будівництва ТМЗК: Наказ Міністерства інформаційних технологій та зв'язку «Про затвердження вимог до будівництва телефонної мережі загального користування» від 08.08.05 № 97.
5. Вимоги до порядку пропуску трафіку в телефонній мережі загального користування: Наказ Міністерства інформаційних технологій та зв'язку «Про затвердження Вимог до порядку пропуску трафіку в телефонній мережі загального користування» від 08.08.05 № 98.
6. Літягіна П. Є. Роль системи моніторингу в інфраструктурі оператора МГ / Мн-зв'язок // Укр. спілкування. 2007. № 9. С. 100–105.

Голікова Олена Валеріївна,
завідувач лабораторії авторського права та інформаційних технологій Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України, судовий експерт

Заікіна Тетяна Василівна,
судовий експерт сектору інформаційних технологій лабораторії авторського права та інформаційних технологій Науково-дослідного центру судових експертиз з питань інтелектуальної власності Міністерства юстиції України

ВИКОРИСТАННЯ СПЕЦІАЛІЗОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ПРИ ДОСЛІДЖЕННІ ВІДОМОСТЕЙ З БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Сучасні технології, які стрімко розвиваються, на сьогоднішній день направлені на створення не лише об'єктів, що спрямовані покращити людське життя, але й на засоби його руйнування. Давно минули ті часи, коли єдиною зброєю людини була загострена палиця або важкий камінь. Сучасний світ вимагає сучасних засобів, нерідко засобів подвійного призначення, таких, що в мирний час можуть бути вірними помічниками людини, а у час збройних агресій стати однією із найстрашніших загроз. До таких засобів можна віднести і БПЛА – безпілотні літальні апарати, що в мирний час допомагають нам досліджувати світ з висоти, а під час воєнної агресії – займаються розвідкою і наносять нищівні удари по об'єктах інфраструктури і цивільних об'єктах.

Розглянемо детальніше, що являє собою БПЛА та яким чином його можна дослідити, з метою отримання інформації, яку він може у собі мати.

Безпілотний літальний апарат (дрон, БПЛА) – повітряне судно, призначене для виконання польоту без пілота на борту, керування польотом якого і контроль за яким здійснюється відповідною програмою або людиною за допомогою станції керування по каналах зв'язку [1]. БПЛА/комплекс БПЛА складається з безпосередньо безпілотного літального апарата, системи керування (зовнішньої), пускової установки. За своїм

призначенням можуть поділятися на БПЛА цивільного – загальногосподарчого / багатофункціонального призначення та БПЛА спеціального призначення, зокрема військового (розвідувальні, ударні). Розміри сучасних дронів, залежно від їх функціональності та обладнання, різняться від декількох сантиметрів (вагою до 20 грамів) до десятків метрів (вагою у декілька тон), які можуть бути застосовані на значних дистанціях від місць їх запуску і тривалий час діяти автономно.

БПЛА, що використовуються під час воєнних дій, умовно можна поділити на розвідувальні та ударні.

Тактичні розвідувальні БПЛА призначені для забезпечення розвідувальною інформацією частин і з'єднань сухопутних військ від корпусної ланки і нижче, а також частин і з'єднань військово-морських сил (ВМС).

Розвідувальні безпілотні літальні апарати (далі – РБПЛА), як військового, так і цивільного призначення, можуть бути носіями даних стосовно потенційних цілей для знищення, мають у собі інформацію щодо маршруту руху РБПЛА, даних «підсвічених» об'єктів інфраструктури, які зафіксовані та збережені у пам'яті РБПЛА. Основна задача такого засобу – пошук і фіксація відомостей про потенційну ціль ураження, а також фото- або відеофіксація інформації щодо розташування, кількості, засобів захисту супротивника тощо.

Ударні безпілотні літальні апарати, здебільше військового призначення (далі – УБПЛА), є носіями даних стосовно запланованих до знищення / знищених об'єктів, мають у собі інформацію щодо маршруту руху УБПЛА, даних стосовно знищених / пошкоджених об'єктів інфраструктури, також можуть виконувати розвідувальну або пошукову функцію. УБПЛА можуть як комплектуватись баражувальними боєприпасами, так і являти собою такий боєприпас (дрон-камікадзе). Так, наприклад, **Баражувальний боєприпас RAM UAV (ТОВ КОРТ),** основним призначенням якого є виявлення у визначеному районі й ураження наземних або надводних броньованих цілей та систем протиповітряної оборони. Безпілотник має електричний двигун, що забезпечує дальність польоту до 30 кілометрів на крейсерській швидкості 70 кілометрів за годину. Запуск здійснюється за допомогою

спеціальної катапульти. На розгортання апарата потрібно лише 10 хвилин, а максимальний час польоту становить 40 хвилин. Завдяки інтегрованому льотному контролеру можна автоматично вести літак заданим маршрутом, переглядати відео в реальному часі та здійснювати прицільне ураження цілі після її виявлення [7]. Схожий принцип дії й у відомого нині БПЛА «Герань 2» (Shahed 136), щоправда дальність польоту у такого «безпілотника» до 1000 км. Та й керованість польоту набагато краща.

До іншої групи можна віднести відомий нині БПЛА Bayraktar TB2. «Байрактар ТБ2 (Тактичний Блок 2)» (*Bayraktar TB2* (Taktik Blok 2) – турецький ударний оперативно-тактичний середньовисотний безпілотний літальний апарат (БПЛА) з великою тривалістю польоту, здатний виконувати дистанційно керовані або автономні польоти. Літаки та їхнє озброєння контролюються екіпажем на наземній станції керування. Такий «безпілотник» може нести на собі протитанкові ракети та авіаційні бомби [5]. Цей БПЛА вже добре зарекомендував себе у нинішній війні.

У пам'яті БПЛА, як ударного, так і розвідувального, можуть міститися наступні типи даних:

- геолокаційні дані;
- польотна інформація;
- інформація щодо виявлених об'єктів, сил (особовий склад, озброєння, військова техніка тощо);
- інформація та метадані щодо уражених об'єктів (місце розташування об'єкта, час і умови використання засобів ураження, точка влучання, дані у вигляді файлів типу фото / відео тощо) [4].

Усі ці відомості можуть мати значення для розслідування фактів атаки на об'єкти інфраструктури й цивільні об'єкти. Однак, виникає питання, як цю інформацію отримати?

Фактично, у будь-якому пристрої міститься носій даних, який і досліджується з метою пошуку й аналізу певної інформації та який можливо дослідити за допомогою стандартних програмних засобів. Однак, зважаючи на специфіку об'єкта, отримана інформація може виявитись розрізненою, не систематизованою, або, навіть, зашифрованою.

З метою повного і ґрунтовного дослідження носія інформації у складі БПЛА пропонується використовувати спеціалізоване програмне забезпечення, призначене саме для таких об'єктів.

Для прикладу розглянемо можливості використання СПЗ «Oxygen Forensics Detective». ***СПЗ «Oxygen Forensics Detective»*** (далі – СПЗ) – спеціалізоване криміналістичне програмне забезпечення для вилучення, декодування, розблокування й аналізу багатоплатформних, мультиформатних даних / файлів з різноманітних цифрових джерел походження, резервних копій, логів, системних файлів, облікових даних ЕОМ на ОС Windows, macOS, Linux, носіїв даних, БПЛА, хмарних сервісів із пошуком інформації (артефактів) за визначеними параметрами.

Також функціональні можливості СПЗ налічують інструментарій обходу (нейтралізації) блокувань паролем (пошук паролів, за наявністю відповідної бази даних / оновлень СПЗ), пошук паролів до зашифрованих даних, обхід блокувань екранів апаратних засобів, виявлення видалених даних тощо [3].

За рахунок інноваційних інструментів СПЗ надає можливість здійснювати багатофакторний аналіз виявлених даних із формуванням зручних звітів, пошуку соціальних зв'язків, створення класифікації зображень із врахуванням часових (хронологічних) атрибутів.

Враховуючи те, що зазначене вище СПЗ «Oxygen Forensics Detective» має вбудовану базу даних драйверів, плагінів, оновлень, велику кількість функціональних можливостей щодо дослідження ІТ устаткувань, засобів і складових інформаційно-телекомунікаційних мереж, складних програмно-апаратних засобів тощо та спеціалізовані, об'єктно орієнтовані засоби роботи з БПЛА, вбачається, що СПЗ "Oxygen Forensics Detective" є ефективним, зручним і гнучким засобом для оперативного та якісного дослідження БПЛА.

До особливостей застосування СПЗ "Oxygen Forensics Detective" під час дослідження БПЛА належить можливість імпорту файлів журналів БПЛА типу *.dat (перевагою, у порівнянні з іншими СПЗ, є одночасна візуалізація мапи, місцезнаходження БПЛА та його руху із одночасною хронологічною прив'язкою усіх метаданих), що дозволяє безпосередню інтеграцію «Oxygen Forensic® Drone» до

інструментарію СПЗ «Oxygen Forensic® Maps» із аналізом GPS, імпортом візуалізацією місцезнаходження/позиціонування, побудовою маршруту руху БПЛА, аналізом даних інших програмних застосунків (стороннього виробника) БПЛА, дозволяє вивантажувати дані з хмарних сервісів БПЛА типу хмара DJI, SkyPixel, Parrot тощо [3].

Особливістю формування підсумкового звіту, за результатом повного дослідження БПЛА (чи його окремих складових) є поєднання зібраних з усіх доступних джерел даних із формуванням розгорнутого звіту, об'єднаних в єдиний набір / масив даних із вивантаженими додатками «Oxygen Forensic®».

Окремо варто зазначити, що інструментарій «Oxygen Forensic®» із модулем «Oxygen Forensic® Maps» та інструментарієм «Oxygen Forensic® Drone» автоматично аналізує розташування GPS, дані маршруту, декодує дані у придатний для перегляду аналітика вигляд, у хронологічному порядку, підкреслюючи важливу / критичну інформацію – фізичну адресу, геокоординати, швидкість, висоту, напрямки руху з автоматичним відтворенням візуального маршруту із зазначенням визначних місць (точки на карті, де БПЛА здійснив фотографування, зняв відео).

Таким чином, можна вважати, що використання СПЗ "Oxygen Forensics Detective" значно підвищує якісні показники проведення дослідження таких об'єктів, як БПЛА, дозволяє отримати й систематизувати виявлені дані, якісно їх візуалізує та об'єднує.

В подальшому планується розглянути питання щодо формування алгоритму дій експерта під час дослідження БПЛА з використанням СПЗ "Oxygen Forensics Detective".

Список використаних джерел:

1. Великий тлумачний словник сучасної української мови (з дод. і допов.) / уклад. і гол. ред. В. Т. Бусел. 5-те вид. К. ; Ірпінь : Перун, 2005.
2. Тлумачний словник з інформатики / Г.Г. Півняк, Б.С. Бусигін, М.М. Дівізінюк та ін. Д., Нац. Гірнич. ун-т, 2010. 600 с.
3. Керівництво користувача "Oxygen Forensics Detective". URL: https:// oxygenforensicsDetective/15.3-1 (дата звернення: 05.12.2022).

4. Системи виявлення та аналізу дронів. URL: https://drone-detection-system.com (дата звернення: 09.12.2022).
5. Вікіпедія. Стаття «Bayraktar_TB2». URL: https://uk.wikipedia.org/wiki/Bayraktar_TB2.
6. Вікіпедія. Стаття «Shahed_136». URL: https://ru.wikipedia.org/wiki/Shahed_136.
7. Армія FM. Топ ударних безпілотників України. URL: https://www.armyfm.com.ua/top-udarnih-bezpilotnikiv-ukraini/.

Старенький Іван Володимирович,
судовий експерт сектору досліджень телекомунікаційних систем та засобів лабораторії досліджень об'єктів інформаційних технологій, телекомунікаційних систем та засобів Одеського науково-дослідного інституту судових експертиз Міністерства юстиції України

ОТРИМАННЯ ДОСТУПУ ДО КОРЕНЕВОЇ СТРУКТУРИ ПОБІТОВОЇ КОПІЇ НОСІЯ ІНФОРМАЦІЇ, НА СИСТЕМНОМУ РОЗДІЛІ ЯКОГО ЗДІЙСНЮВАВСЯ ЗАПУСК BITLOCKER

Анотація. В даній роботі описано порядок дій щодо отримання доступу до кореневої структури файлової системи носія інформації, на системному розділі якого здійснювався запуск шифрування інформації за допомогою програмного забезпечення Bitlocker.

Ключові слова: файлова система, файлова таблиця, операційна система, шифрування інформації, Bitlocker, файловий реєстр, носій інформації.

У відповідності до затверджених Міністерством юстиції України методик [1], дослідження носіїв інформації (жорсткі диски, SSD-накопичувачі, USB-накопичувачі) проводиться в такий спосіб, аби запобігти внесенню будь-яких змін у файлову структуру носія інформації, що досліджується. Так в [2] автором відмічається, що одним з етапів комп'ютерно-технічного дослідження є створення побітової копії цифрового носія інформації, або образу, який в подальшому стає об'єктом дослідження експерта.

Залежно від того, в яких умовах буде проводитися створення побітової копії носія інформації, можна виділити декілька способів створення такої копії. Один з методів передбачає використання дистрибутиву операційної системи (ОС) Linux з встановленим програмним забезпеченням (ПЗ) «Guymager», що дозволяє створювати побітові копії носіїв інформації в форматі RAW-даних [3] з розширенням вихідного файлу «*.dd».

На Рис. 1-4 наведено послідовність дій при створенні побітової копії носія інформації за допомогою ПЗ «Guymager» в середовищі ОС Kali Linux.

Рис. 1. Стартове вікно ПЗ «Guymager»

Рис. 2. Фрагмент вікна ПЗ «Guymager» з вибором дій щодо обраного носія інформації, що викликається правим кліком маніпулятора «мишка»

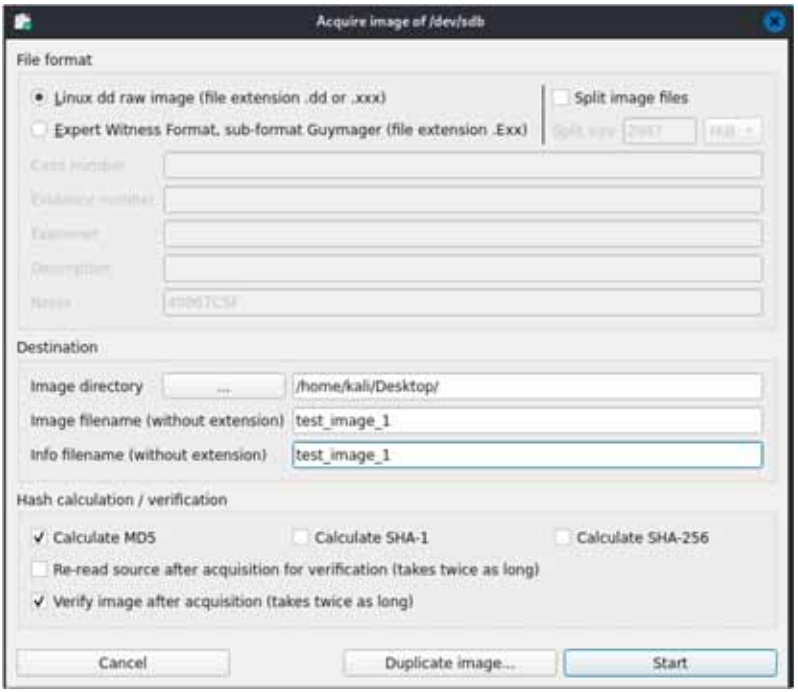

Рис. 3. Менеджер налаштування побітової копії носія інформації

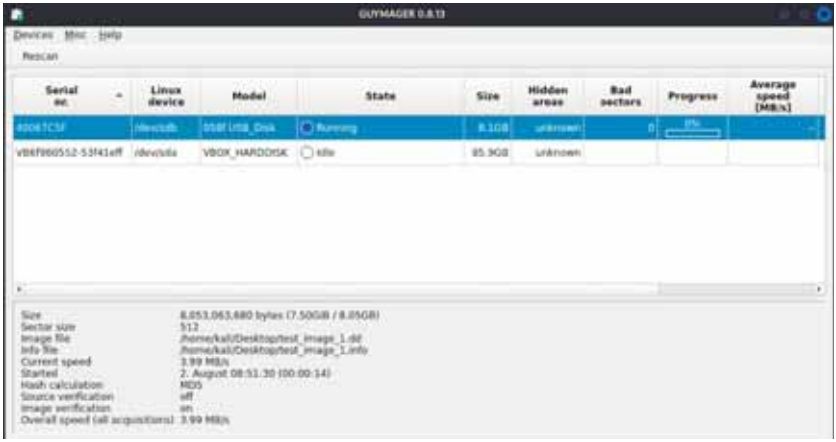

Рис. 4. Вікно ПЗ «Guymager» з відображенням процесу створення побітової копії носія інформації

Після наведених маніпуляцій в зазначеній директорії створюється два файли, це сама побітова копія носія у форматі «*.dd» та файл з розширенням «*.info», в якому містяться дані щодо створеної побітової копії накопичувача, включаючи інформацію про фізичний носій інформації та контрольні суми побітової копії носія.

Інший метод передбачає використання ПЗ «AccessData Forensic Toolkit (FTK) Imager» [4] (далі «FTK Imager»). Оскільки ПЗ «FTK Imager» розроблено для сімейства ОС Windows, то для його використання без апаратного блокатора запису, необхідно внести декілька змін в налаштуваннях ОС Windows, аби носію інформації, що є об’єктом дослідження, не присвоювалася логічна літера розділу операційної системи.

Також ПЗ «FTK Imager» може використовуватися на робочих виїздах на місця скоєння правопорушень, за наявності відповідного дозволу (у разі відсутності апаратного блокатора запису) на увімкненій робочій станції правопорушника, шляхом встановлення ПЗ «FTK Imager» на робочій станції правопорушника з подальшим створенням побітової копії носія інформації на зовнішній накопичувач інформації.

На Рис.5-11 наведено послідовність дій при створенні побітової копії носія інформації за допомогою ПЗ «FTK Imager».

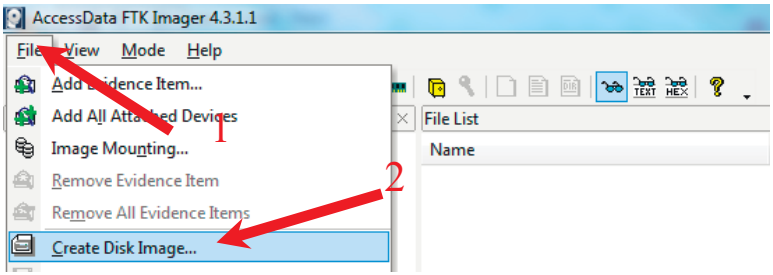

Рис. 5

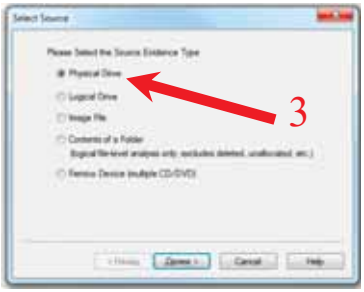

Рис. 6

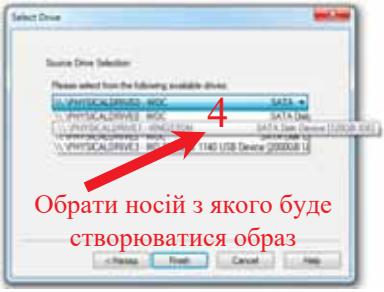

Рис.7

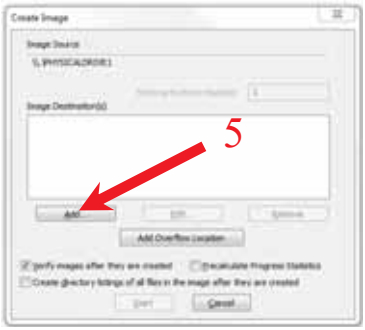

Рис. 8

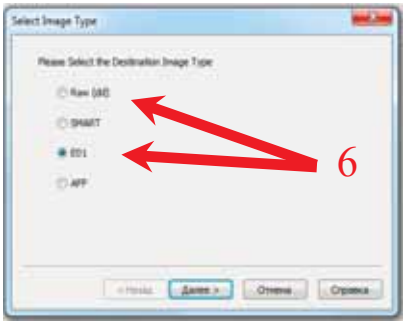

Рис. 9

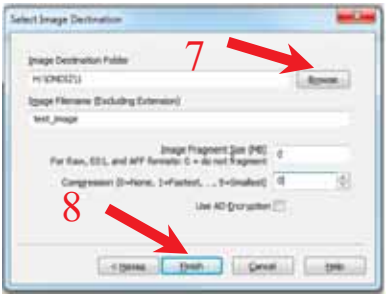

Рис. 10

Рис. 11

Рис. 5-11. Послідовність дій із створення побітової копії

Рис. 12. Результат створення побітової копії носія інформації за допомогою ПЗ «FTK Imager»

В цій роботі розглянуто випадок дослідження побітової копії носія інформації, яка була отримана з використанням ПЗ «FTK Imager» та яка інтерпретується спеціалізованим програмним забезпеченням, як зашифрований за допомогою програмного забезпечення «BitLocker» [5] носій інформації, з розширенням вихідного файлу побітової копії «*.001».

На початку відзначимо, що фізичний носій інформації, з якого було зроблено побітову копію з розширенням «*.001», не перебував в активному стані шифрування інформаційного наповнення за допомогою ПЗ «BitLocker». Однак, ПЗ «Autopsy» [6] вказує на те, що весь системний розділ побітової копії накопичувача інформації зашифровано за допомогою ПЗ «BitLocker» (див. Рис. 13), що відносить цей випадок до «нестандартних», і саме тому він представляє інтерес.

Рис. 13. Результат спроби переглянути файлову структуру побітової копії файлу «img_DESKTOP.001»

З файлами побітових копій з розширенням «*.001», при «нестандартних» ситуаціях, працювати не дуже зручно, оскільки обмежений функціонал маніпулятивних можливостей, які можна застосувати щодо файлу з розширенням «*.001». Тому більш доцільною є конвертація побітової копії носія інформації з розширенням «*.001» в розширення «*.dd», детальний алгоритм конвертації наведено в [2].

Під час спроби змонтувати системний розділ в середовищі ОС Linux, було отримано повідомлення про неможливість успішного виконання команди через «невідомий тип файлової системи 'BitLocker'» (див. Рис. 14).

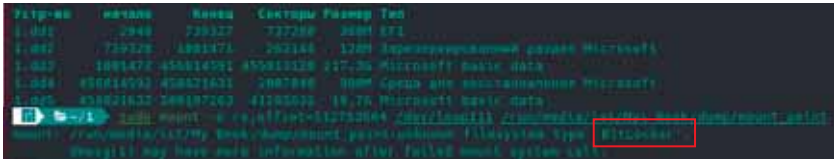

Рис. 14. Результат спроби переглянути файлову структуру побітової копії файлу «img_DESKTOP.001»

Наступним кроком серед інформації побітової копії було здійснено пошук сигнатури BitLocker-шифрування, щоб впевнитися в тому, чи дійсно на системному розділі накопичувача встановлене шифрування за допомогою ПЗ «BitLocker». Результат пошуку BitLocker-сигантури наведено на Рис. 15.

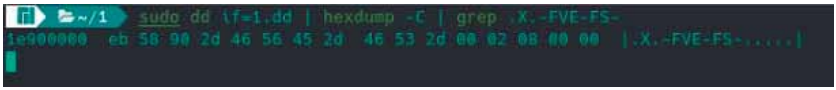

Рис. 15. Команда пошуку та результат пошуку BitLocker-сигантури в терміналі ОС Linux

Оскільки за всіма ознаками на накопичувачі присутнє шифрування за допомогою ПЗ «BitLocker», файл з розширенням «*.dd» було переконвертовано в «*.vmdk» [2], щоб на його основі здійснити запуск віртуальної машини з метою встановлення

факту, чи дійсно встановлено на даному носієві інформації шифрування системного розділу за допомогою ПЗ «BitLocker».

В середовищі запущеної віртуальної машини експертом було встановлено, що користувач для входу до свого облікового запису використовує пароль, див Рис. 16.

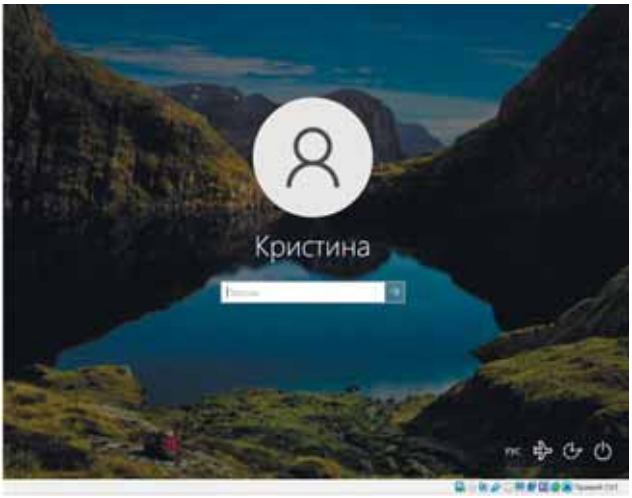

Рис. 16. Вікно введення паролю користувача облікового запису

Під час зміни паролю користувача облікового запису експертом було отримано доступ до файлової структури операційної системи. На Рис. 17 наведено вікно «Мій комп'ютер», на якому видно, що системний диск «(C:)» знаходиться в стані, який називається «Очікування активації BitLocker (pre-provisioning BitLocker)».

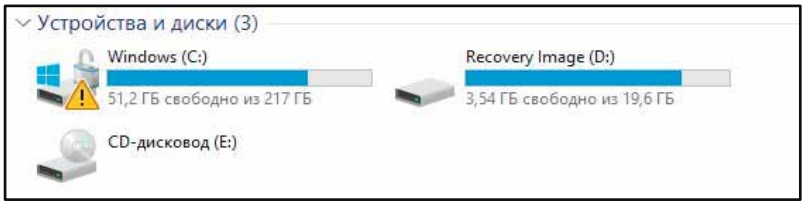

Рис. 17. Тека «Мій комп'ютер» в середовищі віртуальної машини

Саме такий стан системного диску, що пройшов сканування на шифрування, визначався в терміналі ОС Linux та ПЗ «Autopsy», як активне шифрування за допомогою ПЗ «BitLocker», що в свою чергу заважало отримати доступ до файлової структури побітової копії носія інформації.

Виконавши деактивацію шифрування інформаційного вмісту системного диску, експерт отримав доступ до кореневої структури системного розділу побітової копії носія інформації з розширенням файлу «*.vmdk».

Висновок. В наведеній роботі було розглянуто випадок, коли за всіма ознаками можна отримати підтвердження, що системний розділ накопичувача інформації зашифровано за допомогою програмного забезпечення «BitLocker». У випадку, якби системний диск було дійсно зашифровано, то в середовищі віртуальної машини, перед введенням паролю користувача облікового запису, експертові відобразилося вікно для введення паролю шифрування ПЗ «BitLocker».

З великою долею вірогідності, в певний час користувач даної робочої станції мав на меті з тої або іншої причини встановити шифрування на системний розділ носія інформації, з метою чого було здійснено попередню підготовку розділу для здійснення шифрування за допомогою ПЗ «BitLocker».

Розглянутий у цій роботі випадок дозволив встановити послідовність дій експерта при «нетиповій» ситуації, у випадку, коли отримати доступ до перегляду файлової структури носія інформації неможливо.

З проведеного дослідження однозначно можна зробити висновок, що використання розширення «*.001» у якості вихідного розширення для побітової копії фізичного носія інформації може призвести до того, що буде витрачено додатковий час на один-два цикли конвертації побітової копії з метою отримання «більш вигіднішого розширення», а що більший обсяг носія інформації, то більше часу буде затрачено на цикли конвертації. Тому найбільш доцільно створювати побітові копії фізичних носіїв інформації з вихідним розширенням «*.dd», яке більш «привітливе» в роботі з дистрибутивами ОС Linux та спеціалізованим ПЗ.

Список використаних джерел:

1. Методика дослідження інформації на цифрових носіях (№ 10.9.07). *Реєстр методик судових експертиз* / Міністерство юстиції України. 2011.

2. Старенький І.В. Донченко О.І. Дослідження інформаційного наповнення побітової копії носія інформації шляхом утворення його VMDK-посилання. *Одеський науково-дослідний інститут судових експертиз Міністерства юстиції України Вісник ОНДІСЕ Науково-практичне видання* №11 2022 (ст. 82-87).

3. RAW-дані. *Вікіпедія: вільна енциклопедія*. URL: https://ru.wikipedia.org/wiki/RAW_(формат_данных) (дата звернення: 17.11.2022).

4. FTK Imager. *AccessData*. URL: https://accessdata.com/product-download/ftk-imagerversion-4-5 (дата звернення: 17.11.2022).

5. BitLocker. *Вікіпедія: вільна енциклопедія*. URL: https://ru.wikipedia.org/wiki/BitLocker (дата звернення: 17.11.2022).

6. Autopsy. *Вікіпедія: вільна енциклопедія*. URL: https://en.wikipedia.org/wiki/Autopsy_(software) (дата звернення: 17.11.2022).

Semenov Serhii,
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine, doctor of technical sciences, professor, professor department cyber security and information of technologies

Minjian Zhang,
Zhejiang Nova Intelligent Technology Co. Ltd, Zhejiang, China

OVERVIEW OF METHODS FOR IMPROVING THE CYBER SECURITY OF UNMANNED AERIAL VEHICLES WITH THE BUILT-IN ADS-B SYSTEM

Introduction. Air traffic volumes are steadily increasing every year. The desire to reduce the impact of aviation on the environment and more efficient use of airspace and aircraft (AC) necessitates increased operational flexibility while maintaining or improving the level of safety. The safe management of an increasingly large and complex air traffic requires the use of more advanced tools and means. One of such important tools in the process of air traffic management (ATM) is aeronautical surveillance, in particular Automatic Dependent Surveillance Broadcast Type (AZN-B).

The ADS-B system broadcasts data from the aircraft on its location (coordinates: latitude, longitude), absolute altitude, speed, identification index, quality of navigation data and other information received from on-board systems. Data on the location and speed of the aircraft, as a rule, are obtained from the new global navigation satellite system (GNSS). Navigation data quality indicators are determined using the SBAS2 satellite augmentation system . ADS-B messages are broadcast and can be received and processed by any suitable receiver. The ADS-B structure is shown in fig. 1.

Today, ADS-B is considered by the International Civil Aviation Organization (ICAO) as the primary surveillance method. Collaborative surveillance using currently available technologies using the 1030/1090 MHz radio frequency bands (SSR, Mode S, WAM and ADS-B) is an important trend over the coming decades3 . The aviation administrations of the United States and Europe declare in the NextGen4 and SESAR5 programs, respectively, the mandatory equipping of aircraft with the ADS-B system. Measures are also being

taken in the Ukraine for the widest possible introduction of ADS-B6,7. Thus, it should be expected that ADS-B will be everywhere in the near future be introduced, used, improved and modernized, i.e., in general, play one of the key roles in monitoring. However, ADS-B lacks explicit mechanisms to protect confidentiality, the integrity and availability of data transmitted between aircraft and air traffic controllers, which makes such a system vulnerable to cyberterrorist threats, which are especially relevant in connection with the modern development of computer technology and software defined radio (SDR – Software Defined Radio). This topical issue is the subject of this article, which discusses methods that could improve the security of the ADS-B system.

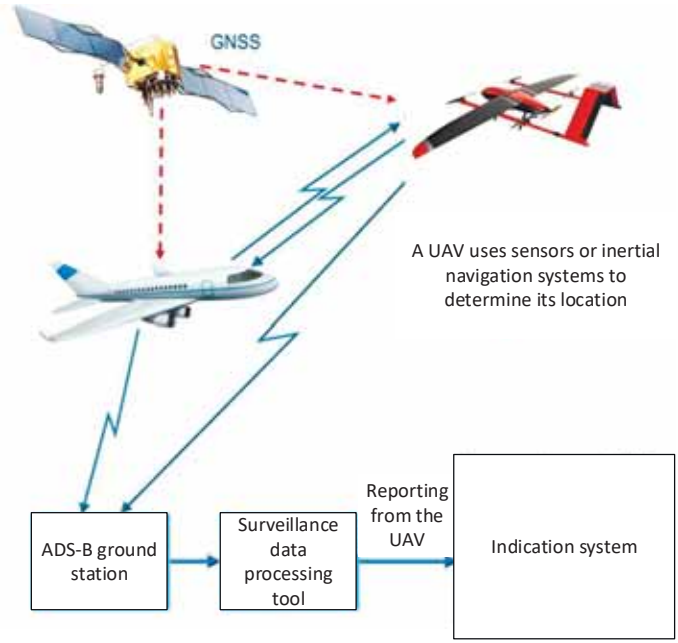

Fig.1. ADS-B system

Problem of low security of ADS-B. The problem of low ADS-B security is not new and is widely covered in technical and popular science literature [1–10]. In this article, the main attention will be paid

to the ADS-B system based on the use of ADS with a 1090-MHz extended squitter (AZN-B 1090 ES), since it is this ADS-B 1090 ES that has been adopted today as the main one for creating a unified system at the state and international levels8,9,10. Among the main reasons for the insecurity of ADS-B, two can be highlighted:

− the system was originally developed on the assumption that each participant must be able to observe everyone else, i.e. the system is open to any participant;

− at the time of development of the system, serious cyberterrorist threats did not exist either they were improbable, or they were erroneously thought to be improbable.

− As a result, the ADS-B system is easily susceptible to spoofing and other types of attacks. This is largely due to the widespread use of low-cost, powerful devices such as software-defined radios (SDRs). Consider the classification of attacks that can threaten ADS-B. The main types of attacks will be given in accordance with the classification of attacks set out in [3].

− Aircraft reconnaissance. It is characterized by an attempt to extract information about the movement of the aircraft. This attack may also be a preparatory stage for a more complex attack.

− Direct jamming of a ground station. Blocking transmission at 1090 MHz using a jammer. It is characterized by a lack of targeting, i.e., it acts on all objects in the suppression zone, limited by the technical characteristics of the jamming transmitter.

− Throw in a decoy at a ground station. Formation and transmission of false messages on the air, which lead to the appearance of a false message on the dispatcher's console. be able to observe everyone else, i.e. the system is open to any participant;

− Direct suppression of the onboard station. Same as direct jamming of a ground station, only the target of the attack is an aircraft. The target aircraft must be equipped with ADS-B In.

− Throwing in a decoy at the onboard station. Same as dropping a decoy on an earth station, only the target of the attack is an aircraft. Target air the ship must be equipped with ADS-B In equipment. The effect of an attack is similar to that of a direct aircraft suppression attack.

− Combinations of one or more of the above types. The presented classification shows that the targets of an attack can be an

aircraft (aircraft) or a ground station (controller); attack methods can be interception, direct jamming, or emitting false signals. The difficulty of such attacks is characterized in [3] from low to medium-high. The most difficult attack to implement is targeting a ground station to drop messages. Harmful impact from attacks can manifest itself in the form of loss of confidentiality, loss of trust in the system, loss of control.

It should be noted that the problem of insecurity or insufficient security is inherent not only in ADS-B, but also in many other equally important aircraft radio systems, for example, GNSS, voice and digital VHF communications (VHF, CPDLC, ACARS), information services (TIS -B, FISB), surveillance and collision avoidance systems (PSR, SSR, MLAT, TCAS), etc. At the same time, the need for a comprehensive solution to the problem of cybersecurity for the entire spectrum of communications, navigation and surveillance becomes obvious. Otherwise, with comprehensive protection of only the ADS-B system, it remains possible to carry out attacks on other systems – GNSS or voice communications. Jamming these systems is not much more difficult than jamming ADS-B, and the result will be approximately the same, and possibly worse. In such a situation, only an integrated approach to solving the problem of ensuring the cybersecurity of an aircraft (aviation system, aviation complex) will provide an effective, reliable and safe result. Returning to the reasons for the vulnerability of such an extensive group of aeronautical telecommunication systems, we can briefly indicate the following [4, 5].

− Long development and certification cycles. The cycles of development and implementation of new technologies in aviation reach twenty or more years. This duration is explained by a large number of tests and certifications to achieve a “no dangerous level” of technology. This often does not take into account the increased malicious potential and the changing threat model brought about by advances in wireless technologies.

− Inheritance and compatibility requirements. Civil aviation retains older technologies, not only as a back-up and for investment reasons, but also because of the greatest possible interoperability for air traffic control worldwide.

− Price pressure. The aviation industry is competitive and under significant price pressure. Changes to fit existing aircraft are costly

and therefore unpopular unless they provide immediate financial or technological benefits to aircraft operators who pay the cost of implementing the new technology.

− Frequency overload. Some ATC frequencies, in particular the 1090 MHz channel, are heavily loaded. The number of aircraft is increasing and they are simultaneously using the same frequencies. The situation is further aggravated by the increase in the number of unmanned aircraft (UA) flights that will be allowed to enter controlled airspace in the foreseeable future.

− Preference for open systems. Air traffic communication protocols are open to every user. Despite existing security and privacy concerns, ICAO plans to create future open access protocols. It is expected that such an approach will meet typical aviation requirements such as ease of communication, compatibility and management of administrative differences between countries and airspace classes.

Review of the main ways to solving the problem. All protection methods for broadcast radio systems can be divided into two large groups. The first group includes methods based on the identification and authentication of subscribers of broadcast radio networks. The second group includes methods based on the verification of data transmitted over broadcast radio networks by unauthenticated subscribers. In addition, protection methods can be divided into those that allow to detect an attack or those that allow to detect and prevent an attack. Methods of the first group implement algorithms of the "identification-authentication" type and can be divided into non-cryptographic and cryptographic, the latter can use symmetric or asymmetric encryption. Non-cryptographic schemes include various methods for authenticating users and identifying radios based on hardware or software imperfections or wireless channel characteristics that are difficult to replicate. The purpose of such schemes is to identify suspicious activity on the network. At present, such methods can hardly be successfully applied in civil aviation, but they are used, for example, in tasks of state identification. Message authentication in broadcast media is more complex than in point-to-point links. The symmetry property is only useful for point-to-point authentication where two parties trust each other. There are many difficulties associated with generating, storing, managing, distributing, and destroying keys. Thus, in essence, an asymmetric mechanism is

required so that receivers can verify messages but cannot generate authentic messages themselves.

Here it is necessary to designate a whole layer of solutions based on the use of ATD with the TDMA access method (for example, VDL mode 4) [6, 7, 11, 12]. For example, it is proposed to use asymmetric encryption at the link level using public and private keys.

In order to be able to send messages to several recipients (broadcast mode), a common session key is generated. Each broadcast message is signed by the sender and encrypted with a shared session key. Recipients decrypt messages with the session key and the sender's public key. Thus, the use of encryption of transmitted data allows you to provide the necessary level of protection. To date, VDL Mode 4 FABR is not used by most states for ADS-B purposes, so this solution may not be acceptable in terms of global application in the short term. Methods of the second group involve the use of various algorithms for verifying data from the ADS-B system with some additional data received through other channels or from other systems. In this case, as a rule, identification of two or more locations or any individual location parameters should be performed. Verification is a very useful tool for enhancing ADS-B security. The updated Air Navigation Surveillance Manual 2 edition11 explicitly indicates the need to compare ADS-B data with other data, such as flight data, flight profiles in the flight data processing system, and observations from other sources such as like radar and multilateration, if any.

Location verification can be performed in various ways [13, 14]. Let us consider the main verification methods that can be used to improve the security of the ADS-B system.

Multilateration (MLAT). The multilateration system is, in fact, a difference-range radio navigation system and is a form of independent cooperative observation. Thus, position determination is based on the calculation of the differences in the time moments of signal arrival at several receivers spaced apart in space. Position surfaces are hyperboloids, which is why this system is also called hyperbolic (the same as the radio engineering long-range navigation system of the LORAN type, RSDN).

Multilateration is the preferred solution for position verification by terrestrial facilities or services. It is used in the USA, in Europe and in the Russian Federation. An important advantage of multilateration

is that it can make use of existing aircraft communications. Thus, no modifications to the current aircraft infrastructure are required, but ground receiving stations and central processing stations must be used. At present, studies on wide-gap multilateration are being actively carried out. Compared to primary radars, wide area multilateration is relatively simple and cost effective to implement and use on the ground. Multilateration systems are not free from disadvantages, the main of which are: susceptibility to multipath propagation, the need for correct signal detection at a relatively large number of receiving stations, the requirement for a separate communication line between the central processing station and receiving The complexity of MLAT attacks is relatively high, especially when compared to spoofing the content of insecure ATC protocols.

– Distance limitation. The idea behind the distance constraint is to establish a cryptographic protocol for having a confirming party, indicating to the verifying party that the confirming party is within a certain physical distance. This makes it possible to calculate the distance, based on the propagation time of the radio signal, between the verifier's request and the corresponding acknowledgment response. In aviation, a certain distance can serve as an upper bound, an additional piece of information that can later be used as a means of verifying and authenticating the aircraft by verifying the truth of claims. The method of limiting the distance by various trusted entities (eg, ground stations) can be used in conjunction with MLAT to discover the actual location of the confirming aircraft. In addition, by accounting for differences in received signal strength, distance-based attacks and baseline attacks on the protocol can be mitigated. This demonstrates the possibility of combining various physical layer methods to increase theoretical protection. However, it is difficult to solve practical problems when using such protocols in ATC.

– Kalman filtering. Kalman filtering methods are widely used in verification problems. Usually, the Kalman filter works iteratively in the "prediction" – "correction" mode, while not only the estimate state vector, but also estimates of the uncertainty of the state vector (correlation matrix of filtering errors). At the prediction stage, the Kalman filter extrapolates the values of the state variables as well as their uncertainties. At the second stage, the measurement data must be processed and the extrapolation result is refined. Thus, at any moment

of time, there is an estimate of the state vector and an estimate of the correlation matrix of filtering errors (extrapolated or refined from the measurement results). These estimates can be used to verify the incoming data, for example, by the method of identification according to the criterion. Kalman filtering allows detection of fictitious maneuvers, speeds, ranges, or other features and greatly increases the complexity of attacks.

– Statistical testing of hypotheses. To solve the verification problem, one can use the methods of statistical testing of hypotheses. In this case, a line of hypotheses is built regarding the intentions to change the location of each observed object. The newly obtained data are used to test hypotheses, the most plausible of which are accepted as true. Data that does not satisfy any of the hypotheses is considered suspicious. Suspicious data can be either real, non-malicious objects that have just come into view, or false data that is an attack on the system. Then the process is repeated. Thus, the trajectories of all observed true objects begin to "knit". In the process of processing subsequent observations, inconsistent data can be eliminated. The use of statistical hypothesis testing makes attacks more difficult, especially when this method is used in conjunction with other methods, such as MLAT.

– Group verification. Group verification is multilateration performed by a group of aircraft. To perform such multilateration, a group consisting of four or more aircraft in mutual radio visibility is required. Each member of the group must be sure that the other members of the group are real non-malicious aircraft. In most cases, authentication will be required to establish mutual trust. Multilateration is carried out by means of mutual radio exchange by the difference-range method or by the method of taking into account differences in the level of the received signal. As a result of multilateration, each aircraft not included in the group will be assigned either to the "fake" or to the trusted one. In the latter case, such an aircraft must be included in the group. Group verification significantly increases the complexity of attacks, although it has a number of disadvantages. The main disadvantages are the need to organize new protocols and noise-proof communication channels, the need to perform authentication, the complexity of the procedure for including a malicious aircraft in a group or excluding it.

– Plausibility check. Checking any parameters for compliance with acceptable behavior. Although not necessary and sufficient, such a check may nevertheless indicate “abnormal” behavior of the subscriber, which should be more carefully analyzed by other methods. The following behaviors or parameter values can be noted to indicate unusualness: sudden appearance, impossible location claim, beyond

– Use of additional data. Sometimes there is a fundamental possibility of using additional data. For example, if mode 4 LAN is used for ADS-B, it becomes possible to measure the mutual distance between subscribers. Such measurements can be used for additional verification. Using the methods of spatial signal processing, one can obtain goniometric measurements, which can also be used for additional verification. Other possibilities may emerge as existing and new ADS-B protocols are modified.

Conclusion. Currently, the ADS-B system is vulnerable to cyberterrorist threats. At the same time, there are many ways to improve the security of ADS-B. The article gives a classification of threats and methods for improving the security of the ADS-B system. It is expected that in the near future the development of surveillance systems will involve the modernization of the existing 1090 ES protocol, not only from the standpoint of increasing throughput, but also for the purpose of serious processing in terms of improving security, especially in the context of the existing and developing level of cyber attacks. In addition, in order to radically increase the level of safety, the ATM system itself, using ADS-B data, should also be modernized.

References:

1. Krishnan, Rahul & Rajendran, Ganesh Babu & Kaviya, S. & Kumar, N. & Rahul, C. & Raman, S. (2017). Software defined radio (SDR) foundations, technology tradeoffs: A survey. 2677-2682. 10.1109/ICPCSI.2017.8392204.

2. 14 CFR Part 91, Automatic Dependent Surveillance Broadcast (ADS-B) Out Performance Requirements to Support Air Traffic Control (ATC) Service; Final Rule. May 28, 2010.

3. Alghamdi, Fatimah & Alshhrani, Amal & Hamza, Nermin. (2018). Effective Security Techniques for Automatic Dependent Surveillance-

Broadcast (ADS-B). International Journal of Computer Applications. 180. 23-28. 10.5120/ijca2018916598.

4. Kacem, Thabet & Wijesekera, Duminda & Costa, Paulo & de Barros Barreto, Alexandre. (2014). Security requirements analysis of ADS-B networks. CEUR Workshop Proceedings. 1304. 40-47.

5. Manesh, Mohsen Riahi & Kaabouch, Naima. (2017). Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system. International Journal of Critical Infrastructure Protection. 19. 10.1016/j.ijcip.2017.10.002.

6. Strohmeier, Martin & Lenders, Vincent & Martinovic, Ivan. (2013). Security of ADS-B: State of the Art and Beyond. IEEE Communications Surveys & Tutorials. 17. 10.1109/COMST.2014.2365951.

7. Purton, Leon & Abbass, Hussein & Alam, Sameer. (2010). Identification of ADS-B System Vulnerabilities and Threats. ATRF 2010: 33rd Australasian Transport Research Forum.

8. John Perkaus ADS-B Cyber Security alert. (2020): Access to an electronic resource https://www.perkausandfarley.com/wp-content/uploads/2022/01/ADSBCyberSecurity.pdf

9. Purvis, A., Morris, B. and McWilliam, R., (2015) 'FlightGear as a Tool for Real Time Fault-injection, Detection and Selfrepair', Procedia CIRP, vol. 38, pp. 283-288

10. "MITRE's Making Security Measurable," MITRE's Making Security Measurable. Available: http://makingsecuritymeasurable.mitre.org/.

11. E. Sirin, B. Parsia, B. C. Grau, A. Kalyanpur, and Y. Katz, "Pellet: A practical OWL-DL reasoner," Web Semantics: Science, Services and Agents on the World Wide Web, vol. 5, no. 2, pp. 51–53, Jun. 2007.

12. E. Cook, "ADS-B, Friend or Foe: ADS-B Message Authentication for NextGen Aircraft," 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems, 2015, pp. 1256-1261, doi: 10.1109/HPCC-CSS-ICESS.2015.201.

13. S. Amin, T. Clark, R. Offutt and K. Serenko, "Design of a cyber security framework for ADS-B based surveillance systems," 2014 Systems and Information Engineering Design Symposium (SIEDS), 2014, pp. 304-309, doi: 10.1109/SIEDS.2014.6829910.

14. E. Hableel, J. Baek, Y. -J. Byon and D. S. Wong, "How to protect ADS-B: Confidentiality framework for future air traffic communication," 2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2015, pp. 155-160, doi: 10.1109/INFCOMW.2015.7179377.

Наукове видання

ПРОБЛЕМИ ТЕОРІЇ ТА ПРАКТИКИ СУДОВОЇ ЕКСПЕРТИЗИ З ПИТАНЬ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ
(«Крайнєвські читання»)

Матеріали VI Міжнародної науково-практичної конференції
(23 грудня 2022 р., м. Київ)

Керівник видавничого проєкту *В.І. Зарицький*
Комп'ютерний дизайн *О.П. Щербина*
Авторська редакція

Підписано до друку 21.12.2022. Формат 60x84 $^{1}/_{16}$.
Папір офсетний. Друк офсетний. Гарнітура Times New Roman.
Умовн. друк. аркушів – 6,51. Обл.-вид. аркушів – 5,11.
Тираж 300

Видавець і виготовлювач: ТОВ «Видавництво Ліра-К»
Свідоцтво № 3981, серія ДК.
03142, м. Київ, вул. В. Стуса, 22/1
тел./факс (044) 247-93-37; (050) 462-95-48
Сайт: lira-k.com.ua, редакція: zv_lira@ukr.net