

ОХОРОНА ІНФОРМАЦІЙНИХ ВІДНОСИН ЗАСОБАМИ КРИМІНАЛЬНОГО ПРАВА ЯК СКЛADOVA ПІДТРИМАННЯ БЕЗПЕКИ ЦИВІЛЬНОЇ АВІАЦІЇ

Інститут повітряного і космічного права НАУ

У статті висвітлено формування системи знань щодо охорони інформаційних відносин засобами кримінального права.

Місце повітряного транспорту в транспортній системі важко переоцінити, зважаючи на його високу продуктивність, швидкість і якість пасажирських і вантажних перевезень, відсутність потреб у побудові магістральних споруд, хоч і цей вид транспорту має певні недоліки. І йому, як і всій транспортній системі, властиві проблеми безпеки руху і експлуатації. Проблеми безпеки транспортних операцій займали і займають важливе місце у всьому комплексі транспортних проблем, оскільки несуть потенційну небезпеку руйнувань і загибелі людей. У процесі руху транспортні засоби набувають колосальної кінетичної, а літальні апарати також і потенційної енергії, яка звільнюється у випадку відхилення від нормального функціонування. Давньогрецький історик Плутарх доніс до нас слова видатного римського полководця Помпея, з якими він звернувся до матросів із закликом піднятися на борт судна, яке прямувало по бурхливому морю з вантажем зерна до голодного Риму: «*Navigare necesse est, vivere non est necesse*», що в перекладі означає: «Плавати необхідно, навіть якщо це може коштувати життя». Ці слова залишаються до сьогодні актуальними не лише стосовно морського, а й інших видів транспорту, в тому числі повітряного.

Водночас серед пріоритетів розвитку авіатранспортних технологій безпека авіації стабільно посідає перше місце, що і обумовлює актуальність теми статті. Так, 1950–1970 рр. черговість пріоритетних чинників розвитку цивільної авіації виглядала так: безпека польотів – швидкість – дальність – комфорт, у 1970–1980 рр. – безпека польотів – економічність – комфорт – ресурси, в 1980–2000 рр. – безпека польотів – охорона довкілля – економічність – ресурси, а після 2000 р. – безпека польотів – охорона довкілля – авіаційна безпека – економічність [1]. Це обумовлювало постійні наукові дослідження щодо безпеки цивільної авіації фахівцями різних наук,

зокрема правових. Так, питання кримінально-правового забезпечення безпеки авіації досліджувались у працях А. І. Коробєєва, Д. І. Трусова, А. А. Нерсесянца, А. І. Чучаєва та ін.

Метою даної статті є формування системи знань, щодо охорони інформаційних відносин, засобами кримінального права як складової підтримання безпеки цивільної авіації.

Своєрідність функціонування повітряного транспорту полягає в тому, що будь-яке посягання (навіть незлочинного характеру) ставить під загрозу суспільну безпеку, за певних умов може стати причиною більш небезпечного порушення правил безпеки, що в свою чергу посягає на безпеку людей, загрожує збереженню власності, може призвести до не відновлюваних втрат.

Найбільш небезпечними правопорушеннями на повітряному транспорті є злочинні відхилення від безпечних умов пілотування і експлуатації повітряних суден. Згідно зі ст. 3 Конвенції про боротьбу з незаконними актами, спрямованими проти безпеки цивільної авіації, ратифікованої Президією Верховної Ради Української РСР 16.01.1973 р. [2], Україна взяла на себе зобов'язання, відповідно, забезпечити кримінально-правову охорону від незаконних актів, що спрямовані проти безпеки цивільної авіації, загрожують безпеці осіб і майна, серйозно порушують повітряне сполучення і підривають віру народів світу в безпеку цивільної авіації, а також застосовувати суворі покарання щодо осіб, що вчиняють відповідні акти.

За роки незалежності в Україні розпочато складну роботу, спрямовану на створення і вдосконалення нормативно-правової бази, що має забезпечити безпеку функціонування повітряного транспорту. Боротьба з транспортними злочинами в сучасних умовах набуває важливого значення, про що свідчить виділення цих злочинів у самостійний розділ Особливої частини Кримі-

пального кодексу [3]. Більшість злочинів, що посягають на безпеку функціонування повітряного транспорту, законодавець відніс власне до цього розділу. Інформаційні відносини можуть бути додатковим об'єктом злочинів, передбачених статтями 277 «Пошкодження шляхів сполучення і транспортних засобів», 279 «Блокування транспортних комунікацій, а також захоплення транспортного підприємства», 281 «Порушення правил повітряних польотів», 282 «Порушення правил використання повітряного простору». Інформація і інформаційні технології можуть виступати предметом, знаряддям і засобом злочинів, що посягають на безпеку експлуатації і функціонування повітряного транспорту. Зокрема, пошкодження шляхів сполучення і транспортних засобів, між іншим, передбачає умисне руйнування або пошкодження засобів зв'язку чи сигналізації, а також інші дії, спрямовані на приведення зазначених предметів у непридатний для експлуатації стан, якщо це спричинило чи могло спричинити аварію повітряного судна або порушило нормальну роботу транспорту, або створило небезпеку для життя людей чи настання інших тяжких наслідків. Приведення засобів зв'язку і сигналізації у непридатність можливе не лише шляхом їх фізичного руйнування, а й шляхом втручання в роботу систем, що забезпечують їх належне функціонування, отже, пов'язане з інформаційними технологіями. У наступній нормі, що аналізується (ст. 279 «Блокування транспортних комунікацій, а також захоплення транспортного підприємства»), предметом злочину названо транспортні комунікації, і більшість науковців класично вбачають в цьому шляхи сполучення, споруди на них, засоби сигналізації та зв'язку [4]. Однак специфіка технічної ергатичної системи «повітряне судно – екіпаж – середовище» полягає в таких її характеристиках, як широкий діапазон можливостей, здатність до самоорганізації, значною свободою поведінки, тривалим життєвим процесом, а також і великими обсягами інформації, що забезпечують її ефективне і безпечне функціонування. Тобто, слід зважати, що насиченість інформаційними процесами функціонування повітряного транспорту дозволяє заблокувати транспортні комунікації шляхом, наприклад, втручання в діяльність інформаційних систем. Щодо норм, передбачених статтями 276, 281 та 282 Кримінального кодексу України, слід зазначити, що вони мають бланкетний характер і правила, до яких вони звернені охоплюють широкий діапазон відносин, що виникають у зв'язку з експлуатацією та використанням пові-

тряного транспорту. Зокрема, Повітряний кодекс України передбачає, що до авіаційних правил, які визначають і регулюють порядок діяльності авіації України з метою забезпечення безпеки польотів належать норми, що регулюють придатність до експлуатації систем регулювання використання повітряного простору і обслуговування повітряного руху, норми, що регулюють порядок використання повітряного простору, забезпечення аеронавігаційною інформацією та інші, які безпосередньо стосуються інформаційних відносин у сфері цивільної авіації. Аналізуючи охорону інформаційних відносин в цивільній авіації, необхідно зазначити, що інформація, пов'язана з функціонуванням цивільної авіації може мати різний режим доступу – відкрита інформація (наприклад, про розклад авіарейсів, порядок використання повітряних суден тощо), інформація з обмеженим доступом. Відповідно, забезпечення режиму доступу також охороняється кримінальним законом, зокрема, порушення режиму доступу до інформації, що є таємною або конфіденційною тягне за собою кримінальну відповідальність для службової особи, через недбалість якої було заподіяно істотну шкоду охоронюваному законом суспільним відносинам. Авіаційна безпека стимулює розробку захищених баз даних про пасажирів та авіаслужбовців з метою прискорення процедур профалінгу пасажиропотоку. Пасажир, зареєстрований в Нью-Йорку, повинен швидко проходити процедури контролю в Києві чи Москві. Тому постає також питання про захист персональних даних, які становлять об'єкт правової охорони.

Обов'язковою умовою безпеки авіації є ефективність інформаційних процесів, який передбачає передачу таких видів інформації, як-от: усна, письмова, символна, наочна або безсловесна. Інформаційні потоки, що циркулюють у структурі системи підтримання безпеки цивільної авіації умовно становлять п'ять груп: 1) інформація, що добре формалізується (як правило, це характеристики, які можна точно подати в числовій формі); 2) текстова або вербальна інформація, яку можна подати у вигляді лінгвістичних змінних; 3) інформація, що поєднує і числову, і лінгвістичну форму вираження даних; 4) інформація з нечітким числовим відтворенням (наприклад, експертні оцінки); інформація, яку не можна формалізувати (наприклад, через високий ступінь невизначеності).

Інтенсивний розвиток засобів та систем передачі інформації в авіації вимагає забезпечення інформаційної безпеки, одним із напрямів якої є

охорона та захист інформації. Втрата інформації в авіаційній галузі може призвести не тільки до економічних збитків авіакомпаній, Аеропортів та інших авіапідприємств, а й до зниження безпеки польотів та людських жертв.

Останнім часом у дослідженнях фахівців з кримінального права цим проблемам приділялась значна увага, зокрема Д. С. Азарова, А. А. Музики, С. О. Орлова, М. В. Карчевського, Н. А. Резенфельд, П. Д. Біленчука, Б. В. Романюка, В. С. Цимбалюка, В. Д. Гавловського, В. С. Гуцалюка та ін.

Правова охорона інформаційних відносин у цивільній авіації здійснюється через встановлення нормативно-правовими актами України та міжнародним правовими актами (наприклад, вимогами ICAO – International Civil Aviation Organization (Міжнародна організація цивільної авіації)) правил використання, обробки та передачі інформації та встановлення відповідальності за порушення цих правил. Встановлення кримінальної відповідальності за злочини, що посягають на всі види суспільних відносин, у тому числі інформаційні, є прерогативою Української держави.

Ефективна боротьба зі злочинами в цій сфері припускає оптимальне використання репресивних та профілактичних заходів. Найбільш суворим та ефективним заходом є кримінально-правова репресія з боку держави у відповідь на такого роду соціально-негативні явища.

Тенденції криміналізації відповідальності за здійснення злочинів у інформаційній сфері у світовій практиці зводяться до двох варіантів:

- а) застосування традиційних кримінально-правових норм за допомогою інкримінування винним «за аналогією» (як у Великобританії);
- б) внесення в КК нових статей, що встановлюють спеціальну кримінальну відповідальність [5].

Український законодавець скористався другим шляхом. В одній із перших держав СНД, в Україні в 1994 р. було доповнено КК 1960 р. статтею 198¹ «Порушення роботи автоматизованих систем», що встановила кримінальну відповідальність за викривлення чи знищення інформації в автоматизованих системах. Чинний КК України містить розд. XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [3]. Цей розділ містить шість статей, що передбачають відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем,

комп'ютерних мереж чи мереж електрозв'язку (ст. 361), створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361¹), несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361²), несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362), порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363), перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363¹). Цей розділ є одним з найбільш динамічних у чинному КК – за 5 років його існування тричі змінювалась назва цього розділу, а сам розділ було доповнено трьома новими статтями і одну з існуючих викладено у новій редакції. Науковці відзначають, що всім цим змінам кримінального кодексу притаманна спільна властивість: з одного боку, вони спрямовані на усунення певних законодавчих вад, а з другого – породжують нові теоретичні та прикладні проблеми [6].

Аналіз кримінального законодавства та наукових праць дозволяє говорити про наявність наступних недоліків кримінально-правових норм, що передбачають відповідальність у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: неточність формулювань, що особливо спостерігається при визначенні об'єктивної сторони складу злочину, відсутність вказівки на форму вини (за винятком ст. 361¹), з якою може бути вчинено відповідний злочин і відповідної диференціації відповідальності, що породжує труднощі в застосуванні цих норм.

Сфера високих технологій дозволяє не лише вчиняти нові види злочинів, про які було згадано вище, а й вдосконалювати традиційні. Так, світовий досвід показує, що використання інформаційних технологій терористичними угруповуваннями призвів до виникнення кібертерори-

зму – спланованого, вчиненого чи скоординованого в кіберпросторі, тобто з використанням новітніх досягнень в галузі інформаційних технологій. Використання повітряного транспорту вдругій половині ХХ ст. перетворилося на «класичний» спосіб дій терористів. Кібератакам зазвичай піддаються системи управління польотами літаків, а навіть супутників, як це відбулось в Великобританії. І неможна не згадати про трагічні події 11 вересня 2001 р., коли оператори авіарейсів та протиповітряної оборони не змогли вчасно зреагувати на небезпеку.

В основі вищевикладеного можна зробити такі **Висновки:**

1. Оскільки можливість зловживання інформацією, яка передається каналами телекомунікацій, розвивається не менш інтенсивно, ніж засоби їх попередження, тому проблема захисту інформації в галузі цивільної авіації вимагає комплексного підходу, в тому числі засобами кримінального права.
2. Безпека авіації безпосередньо охороняється нормами Кримінального кодексу, що містяться в розд. ХІ «Злочини проти безпеки руху та експлуатації транспорту».

Література

1. *Безпека авіації* / В. П. Бабак, В. П. Марченко, В. О. Максимов та ін. – К.: Техніка, 2004. – С. 16.
2. *Конвенція про боротьбу з незаконними актами, спрямованими проти безпеки цивільної авіації* // Україна в міжнародно-правових відносинах. – К.: Юрінком, 1996.
3. *Кримінальний кодекс України від 5 квітня 2001 р.* // Відомості Верховної Ради України. – 2001. – № 25-26. – Ст. 131.
4. *Науково-практичний коментар Кримінально-*

О. А. Золотар

Охрана информационных отношений способами

В статье рассматривается формирование системы

плуатації транспорту». Водночас функціонування інформації в технічній ергатичній системі «повітряне судно – екіпаж – середовище» опосередковується інформаційно-комунікаційними технологіями, отже відповідні відносини становлять об'єкт злочинів, що передбачені розд. ХІ «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

3. Значну загрозу для безпечного функціонування цивільної авіації становить кібертероризм, тобто спланований, вчинений чи скоординований в кіберпросторі, з використанням новітніх досягнень у галузі інформаційних технологій.

4. І, насамкінець зауважимо, що викладені міркування не вичерпують сутності проблеми кримінально-правової охорони інформаційних відносин у галузі цивільної авіації. Інформаційні процеси в цивільній авіації характеризуються високим рівнем ентропії, що обумовлює динамічність інформаційних відносин і необхідність подальших досліджень у цьому напрямі.

го кодексу України / За ред. М. І. Мельника, М. І. Хавронюка. – К.: Атіка, 2003. – С. 724.

5. *Черных А. В.* Некоторые вопросы квалификации компьютерного саботажа за рубежом // Советское государство и право. – 1988. – № 8. – С. 72.

6. *Музыка А. А., Азаров Д. С.* Законодавство України про кримінальну відповідальність за комп'ютерні злочини: науково-практичний коментар та шляхи вдосконалення. – К.: Вид-во ПАЛИВОДА А. В., 2005. – С. 6.

уголовного права как составная поддержка безо-

знаний относительно охраны информационных от-