

Гусар О.А., к.ю.н.,
Мудрик Р.Р., студентка,
Юридичний факультет,
Національний авіаційний університет, м. Київ

ПРОБЛЕМНІ ПИТАННЯ КІБЕРБЕЗПЕКИ В УКРАЇНСЬКІЙ АВІАЦІЇ

Проблема забезпечення кібербезпеки носить глобальний характер і досить гостро постає у сучасному інформаційному суспільстві. Провідні держави світу все більше уваги приділяють кіберзахисту власних критичних інфраструктур. Особливої уваги заслуговує цивільна авіація (ЦА), рівень критичності якої значно підсилюється підвищеним ступенем комунікації та взаємодії між наземними системами і повітряними суднами, а впровадження сучасних інформаційних та комунікаційних технологій (ІКТ) з одного боку підвищує ефективність і спрощує формальності у діяльності ЦА, а з іншого – породжує цілу низку нових уразливостей та потенційних загроз [1].

Сучасна система повітряного транспорту є багатофункціональною й диктує високий темп технологічних та інформаційних процесів. При цьому забезпечення надійності та своєчасності інформаційних потоків є невід'ємною частиною авіаційної безпеки, що й обумовлює актуальність даної теми [2].

Останнім часом посилилась національна і глобальна чутливість до загроз тероризму і інших видів несанкціонованого впливу на авіаційну систему. Сумно відомий приклад – події 11 вересня 2001 р. у США, коли терористи використали літаки цивільної авіації як засоби масового знищення людей. У цьому випадку було зафіксовано незаконне втручання не лише шляхом проникнення на борт літаків, але й у інформаційні навігаційні системи [3].

Хакерські атаки на комп'ютерні авіаційні системи стали серйозною загрозою безпеки польотів. У зоні ризику опинилися сервери авіакомпаній і аеропортів: «зломи систем» уже призводили до затримок і навіть скасування рейсів [4].

Згідно з дослідженням «Глобальний індекс кібербезпеки» (Global Cybersecurity Index), який щорічно проводиться Міжнародним союзом електрозв'язку (ITU), в 2017 році Україна зайняла «почесне» 59 місце в рейтингу з 193 можливих [5].

За словами Віталія Бордунова, експерта ІКАО: «На сьогоднішній день кіберзагрози розглядаються як незаконне втручання в процес управління повітряним рухом, як видача неправдивих вказівок, які

можуть привести до авіакатастрофи. Але якогось спеціального документа ІКАО, який би чітко вказував, як діяти в разі кібернападів, поки немає. Держави, які є членами ІКАО, повинні виробити єдиний підхід до проблеми і виступити єдиним фронтом. Але в даний час немає навіть технологічної єдності в боротьбі з кіберзагрозами» [4].

Пасажиропотік в Україні постійно зростає, на наш ринок приходять нові перевізники – потужні світові лоукостери, відповідно, зростають вимоги до кібербезпеки. З 2018 року почала впроваджуватись національна стратегія кібербезпеки. На даний час розбудовуються 5 національних центрів кібербезпеки, починають створюватися галузеві і регіональні центри. Ryanair, ірландська бюджетна авіакомпанія, планує відкрити в Україні власний ІТ-хаб – четвертий за потужністю після Мадриду, Вроцлава та Дубліна, що дозволить створити самостійну надійну інформаційну систему [6].

Крім того, 5 жовтня 2017 року був прийнятий закон «Про основні засади забезпечення кібербезпеки України», який вступив в силу лише 9 травня 2018 року. Він зараз і є основним документом, що регулює сферу кіберзахисту в країні, що створює державну систему кіберзахисту. Найголовніше, що цей закон розподіляє функції між правоохоронцями і спецслужбами [7].

Президент через очолювану ним Раду національної безпеки і оборони України координує діяльність в сфері кібербезпеки. Робочий орган РНБО – Національний координаційний центр кібербезпеки – здійснює координацію та контроль за діяльністю суб'єктів сектора безпеки і оборони, які забезпечують кібербезпеку. Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Нацполіція, СБУ, Міноборони і Генштаб Збройних Сил, розвідувальні органи, Нацбанк [8].

Але, даний Закон має свої недоліки. Зокрема, через те, що відповідальність за кіберзлочини розподіляється між різними органами, але фактично жоден із органів не відповідає. Немає єдиного органу, який би поніс відповідальність. Крім того, щодо критично важливих об'єктів інфраструктури, то вони повинні забезпечити самі надійну систему захисту і головна роль спрямована саме на ці об'єкти. Але є й інші організації та підприємства, які також знаходяться під загрозою кібератак.

Отже, зрозуміло, що на сьогодні, в Україні система кіберзахисту тільки поетапно будується. Є деякі позитивні зрушення, але їх замало. Кібербезпека – це спільна мета, і її досягнення полягає в об'єднанні зусиль державного та приватного секторів. Потрібно залучати волонтерські організації, сприяти підвищенню цифрової

грамотності громадян і культури безпеки поведінки в кіберпросторі. Загалом, державним органам необхідно мобілізувати свої зусилля для того, щоб допомогти здолати наявні перешкоди і поліпшити регулюючі механізми з метою підвищення ефективності реалізації спільних проектів і програм та вироблення нових.

Література

1. Харченко В., Корченко О., Гнатюк С. Базова модель формування вимог до забезпечення кібербезпеки цивільної авіації. URL: <file:///C:/Users/user/Downloads/10708-27796-1-SM.pdf> (дата звернення: 18.10.2019).

2. Золотар О. Правові основи захисту інформації в галузі цивільної авіації. URL: file:///C:/Users/user/Downloads/Pinform_2008_2_8.pdf (дата звернення: 18.10.2019).

3. Золотар О. Охорона інформації як напрям у інформаційній безпеці в складі безпеки цивільної авіації та її співвідношення із захистом інформації. URL: <http://ela.kpi.ua/bitstream/123456789/9735/3/08.pdf> (дата звернення: 18.10.2019).

4. Ячменникова Н. Секьюрити для неба. URL: <https://rg.ru/2017/07/17/kak-zashchitit-aviatransport-ot-hakerskih-atak.html> (дата звернення: 18.10.2019).

5. Швачка А. Состояние кибербезопасности в Украине: независимая внешняя оценка. URL: <https://delo.ua/special/sostojanie-kiberbezopasnosti-v-ukraine-nezavisimaja-vneshnjaja-o-346292/> (дата звернення: 18.10.2019).

6. Кібербезпека в авіації: чому це вадливо саме зараз? URL: <https://gigacloud.ua/blog/zahodi/kiberbezpeka-v-aviacii-chomu-ce-vazhlivo-same-zaraz> (дата звернення: 18.10.2019).

7. Система киберзащиты Украины: Есть? Нет? Строится? URL: <https://www.ukrinform.ru/rubric-technology/2491869-sistema-kiberzasity-ukrainy-est-net-stroitsa.html> (дата звернення: 18.10.2019).

8. Закон о кибербезопасности вступил в силу. URL: https://jurliga.ligazakon.net/news/170010_zakon-o-kiberbezopasnosti-vstupil-v-silu (дата звернення: 18.10.2019).

УДК 347.682 (043.2)

Кунєв Ю.Д., д.ю.н., професор,
Юридичний факультет,
Національний авіаційний університет, м. Київ

ПУБЛІЧНІ ФОРМАЛЬНОСТІ В ЦИВІЛЬНІЙ АВІАЦІЇ

Оскільки світ змінюється у бік глобалізації, інтеграції, демократизації та спрямованості на реалізацію прав окремої людини/спільноти, незмінним стає процес спрощення умов і