

Процедури та технології, спрямовані на забезпечення безпеки пасажирів та екіпажу, включають в себе охоронні перевірки, навчання щодо поведінки в надзвичайних ситуаціях та системи аварійного виходу.

– Кібербезпека:

Зростання кількості підключених до мережі систем в авіації створює нові виклики в галузі кібербезпеки. Захист інформаційних систем і мереж дуже важливий для запобігання кібератак та забезпечення безпеки в авіації.

– Глобальні виклики:

Авіаційна безпека також стикається з глобальними викликами, такими як зміни клімату, пандемії, геополітичні конфлікти та інші фактори, які можуть вплинути на безпеку польотів і інфраструктуру.

– Міжнародне співробітництво:

Важливою складовою безпеки в авіації є співробітництво між країнами та авіаційними організаціями для обміну інформацією, координації заходів безпеки та вирішення спільних викликів [1].

Отже, забезпечення безпеки в авіаційній сфері вимагає постійної уваги, інноваційних рішень і співробітництва всіх сторін галузі для забезпечення найвищого рівня безпеки пасажирів і персоналу, а також для захисту навколишнього середовища.

Література

1. Національна бібліотека України. URL: <http://dspace.nbuv.gov.ua/handle/123456789/180429>

2. Державна авіаційна служба України. URL: <https://avia.gov.ua/bezpeka-aviatsiyi/aviatsijna-bezpeka/#>

УДК 341.824:338.47 (043.2)

Карасьова Л.М., здобувач вищої освіти
першого (бакалаврського) рівня,
Національний авіаційний університет, м. Київ, Україна
Науковий керівник: Лихова С.Я., д.ю.н., професор

СТАН КІБЕРБЕЗПЕКИ В СФЕРІ АВІАЦІЇ

В 21 столітті, при розвитку інформаційних технологій в галузі авіації з'явилась нова проблема в суспільстві, а саме правопорушення в інформаційній сфері. В нашому сучасному світі, людина з мінімальними знаннями хакинга та комп'ютером, телефоном чи будь-яким іншим гаджетом може: шахраювати з квитками та резерваціями; вплинути на технічне обладнання

літаків; вкрасти конфіденційну інформацію про пасажирів; здійснити атаку на систему керування рейсами; вплинути на технічне обладнання літаків; можуть намагатися втрутитися в бортові системи літаків, такі як системи управління двигунами або автопілот. Ці, та багато інших прикладів, можуть призвести до небезпеки польоту, стабільності та повної справності літака та використання персональних даних пасажирів.

Щоб чітко та правильно обґрунтувати дане питання, для початку пропоную визначити що ж таке кібербезпека. Хочеться зазначити, що єдиного підходу до визначення даного поняття не існує, тому будемо звертатися до практики та роздумів науковців.

До прикладу, Н.В. Фурашев в своїх працях, визначав кібербезпеку, як стан спроможності людини, суспільства і держави запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу (управління) інформації [1]. Автор наголошує на тому, що кібербезпека є складним та активним процесом, який вимагає від суспільства постійного вдосконалення, навичок та практики для завчасного подолання та попередження кіберзагроз.

Звернувшись до законодавства України, а саме, статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» можна сказати, що закон трактує даний термін, як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, за якого забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [2]. Законодавець тлумачить дане поняття як забезпечення конфіденційності та вживання всіх можливих заходів для запобігання доступу або втрати конфіденційних даних.

Кіберзахист – справа критично важлива. На сьогодні в авіації в середньому по світу 78 % кібератак – вдалі. Через кожну таку атаку процеси в організації можуть зупинитись, в результаті установа зазнає репутаційних та матеріальних збитків, кібератака навіть може призвести до людських втрат.

В той же час, питання кібербезпеки в авіаційній галузі України регулюються такими нормативно-правовими документами: Резолюцією ІКАО А39-19 «Рішення проблем кібербезпеки в цивільній авіації» (від 06.10.2016), Законом України «Про Державну програму авіаційної безпеки цивільної авіації» (від 21.03.2017), Законом України «Про основні засади забезпечення кібербезпеки України» (від 05.10.2017), що зобов'язують установи та організації

вживати заходів для захисту від несанкціонованого доступу і захищати персональні дані клієнтів, а також передбачають відповідальність за недотримання цих вимог [3].

Україна вперше зазнала кібератаки на ІТ-системи та центральні сервери аеропортів «Бориспіль» і «Харків» у червні 2017 року, що призвело до відмов у обслуговуванні літаків і затримок рейсів. Через кілька місяців, у жовтні 2017 року, рейси з Одеського аеропорту були затримані через зламаною комп'ютерну мережу аеропорту, що призвело до втрати інформаційної безпеки.

Варто відзначити, що військова авіація, у порівнянні з цивільною, сьогодні більш захищена, проте дійсно 100-відсоткових дієвих методів щодо забезпечення кібербезпеки не існує і тут. Справа у тому, що сучасні дрони і військовий авіатранспорт – це набір електронних компонентів, які скеровуються не стільки людиною, скільки спеціальною програмою. Відповідно, умілий хакер може зламати її і внести зміни в програмне забезпечення. Таким чином, кібератаки здатні повністю змінити хід ведення бойових дій [4].

За для забезпечення кібербезпеки та попередження кібератак в авіації пропонуємо деякі заходи, які допоможуть посилити кібербезпеку держав:

- Встановлення якісних та надійних антивірусних систем.

- Використання сильних, надійних та унікальних паролів, які захищають персональні дані та конфіденційну інформацію.

- Проведення постійних перевірок безпеки, попередження та виправлення помилок, які можуть призвести до втрати інформації.

- Шифрування даних та інформації, за для кращого їх захисту.

- Постійне вдосконалення та захист систем керування повітряним рухом.

- Постійний моніторинг безпеки систем авіакомпаній.

- Захист бортових систем літаків.

- Постійний зв'язок та обмін досвідом з іншими державами.

- Постійне підвищення освітнього рівня персоналу авіаційної галузі, а також проведення тренінгів та навчань з питань кібербезпеки.

Розглядаючи комп'ютерно-інтегровані авіаційні системами, що забезпечують зв'язок між об'єктами діяльності цивільної авіації в межах каналів «земля-повітря» та «повітря-повітря», дедалі гостріше постає питання безпечної експлуатації таких авіаційних систем з точки зору негативного впливу постійно зростаючих з кожним роком кіберзагроз, та пониження стану забезпечення кібернетичної безпеки авіаційної галузі в цілому. Стан захисту

каналів «земля-повітря» та «повітря-повітря» в таких авіаційних системах знаходиться на різних рівнях та на пряму залежить від діяльності всіх складових авіаційної діяльності (аеропорт, повітряне судно, інформаційна мережа, управління повітряним рухом, тощо). Деякі канали зв'язку на сьогоднішній день взагалі не захищені та знаходяться у відкритому стані, що провокує неминуче зростання кібернетичних атак та вимагає впровадження і застосування сучасних інформаційно-комунікаційних технологій в такі канали зв'язку [5].

Підводячи висновок, хотіла б сказати, що кібербезпека в сфері авіації є складним та дуже відповідальним процесом, від якого залежить не тільки авіація а й персональні дані людей які проходять через системи аеропортів. Стан кібербезпеки в сфері авіації стає все актуальнішою темою в сучасному світі, в якому стають залежні від інформаційних технологій, що призводить до більшого ризику застосування кібератак. Перш за все кібератаки можуть впливати на системи управління повітряним рухом, що може призвести до серйозних наслідків для безпеки польотів, життя та здоров'я пасажирів авіакомпаній.

Загалом, лише комплексний підхід, може гарантувати найвищий рівень кібербезпеки в авіації, забезпечуючи безпеку та стабільність.

Література

1. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. Інформація і право. 2012. № 2. С. 162-169.
2. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовт. 2017 р. № 2163-VIII. URL: <https://ips.ligazakon.net/document/JH1N268B?an=3https://ips.ligazakon.net/document/JH1N268B?an=3>
3. Кібербезпека аеропортів України. URL: <https://www.icu-ng.org/icu-ng/novyny/kiberbezpeka-aeropotivukrayiny/>
4. Філінович В.В. Кібербезпека та загрози в авіаційній сфері: правовий аспект. Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право». Київ: НАУ, 2021. № 3 (60) С. 38-44.
5. Ільєнко А.В., Ільєнко С.С., Кваша Д.С. Сучасний стан забезпечення кібернетичної безпеки цивільної авіації України та світу. URL: https://www.researchgate.net/publication/344385843_SUCASNIJ_STAN_ZABEZPECENNA_KIBERNETICNOI_BEZPEKI_CIVILNOI_AVIACII_UKRAINI_TA_SVITU

Ковригіна О.К., здобувач вищої освіти
першого (бакалаврського) рівня,
Національний авіаційний університет, м. Київ, Україна
Науковий керівник: Грекова Л.Ю., старший викладач

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ ПОРУШЕННЯМИ АВІАЦІЙНОЇ БЕЗПЕКИ

Авіаційні катастрофи часто є результатом злочинних дій, наприклад тероризму, піратства повітряного простору або навмисного знищення літака. У контексті війни з Російською Федерацією питання якісного розслідування авіаційних подій набуває особливої актуальності. Від початку повномасштабного вторгнення відбулись наступні авіаційні катастрофи, які розслідувала українська сторона: авіаційні події з вертольотом та літаком на аеродромі у Малі, авіаційна катастрофа з вертольотом в м. Бровари, Київської області там де загинуло керівництво МВС України. Авіаційна катастрофа з літаком у Грецькій Республіці, авіаційна аварія на аеродромі Ужгорода і у Запорізькій області [6]. Саме тому важливо створити загальне уявлення про розслідування авіаційних подій в Україні, ідентифікувати компетентні органи, які відповідають за ці процедури, та розглянути нормативно-правові аспекти, що регулюють цей процес.

Керуючись Повітряним Кодексом, можемо зазначити, що проведення розслідувань це зібрання та аналіз інформації, формування висновків, визначення причин та/або супутніх чинників, а також розроблення рекомендацій для забезпечення. Відповідно до цього регулятивного документу, проведення розслідувань авіаційних подій та інцидентів, які стосуються цивільних повітряних суден України і іноземних цивільних повітряних суден, а також порушень використання повітряного простору України, покладається на спеціалізовану експертну установу.

Аналіз поточних законодавчих актів виявив, що станом на жовтень 2023 року ми не маємо повноцінного нормативно-правового акту який регулював би питання функціонування цієї експертної установи, про яку йдеться у Повітряному Кодексі України. Дію поточної було припинено 01.01.2022 року [1]. Зовсім нещодавно Кабінет Міністрів погодився із пропозиціями Міністерства розвитку громад, територій та інфраструктури щодо покладення функцій державної спеціалізованої експертної установи з технічного розслідування подій на транспорті на Національне