

РОЗДІЛ 3

БЕЗПЕКОВА ДІЯЛЬНІСТЬ В АВІАЦІЙНІЙ СФЕРІ

УДК 34:004.056.53(043.2)

Адаменко О.М., здобувач вищої освіти
третього (освітньо-наукового) рівня,
Національний авіаційний університет, м. Київ, Україна

ЗНАЧЕННЯ КІБЕРБЕЗПЕКИ ДЛЯ АВІАЦІЙНИХ СИСТЕМ

Кібербезпека стала ключовим аспектом сучасної технологічної інфраструктури, і це особливо важливо для авіаційних систем. У теперішньому світі авіація відіграє важливу роль у глобальному сполученні та господарському розвитку. Збої в авіаційних системах можуть призвести до серйозних наслідків, включаючи аварії, загрози для життя пасажирів і персоналу, а також економічні збитки. У цьому контексті кібербезпека стає дуже важливою для забезпечення надійності та безпеки авіаційних систем. Більш детально розглянемо значення кібербезпеки для авіаційних систем, а також способи захисту цих систем від кіберзагроз.

Авіаційні системи – це складні технічні системи, які включають в себе літаки, аеропорти, системи керування повітряним рухом, системи навігації та багато іншого. Завдання авіаційних систем охоплюють забезпечення безпеки і ефективності повітряного руху, пасажирського комфорту і швидкості перевезення, а також мінімізацію впливу авіації на довкілля.

Забезпечення безпеки авіації – це одне з найважливіших завдань авіаційних систем. Система безпеки України слідкує за збоями в цих системах, адже вони можуть призвести до аварій, які загрожують життю пасажирів і членів екіпажу. Крім того, авіаційна безпека також стосується захисту від терористичних загроз і забезпечення цілісності авіаційної інфраструктури.

Ефективність авіаційних систем визначається їхнього здатністю обробляти великий потік даних і керувати повітряним рухом, щоб забезпечити оптимальний розклад рейсів та мінімізувати затримки. Це також включає в себе забезпечення надійності та доступності авіаційних систем.

Однією з основних загроз є можливість вторгнення в системи керування повітряним рухом, що може призвести до неконтрольованого руху повітряних суден і авіаційних аварій. Такий

сценарій може стати катастрофічним і призвести до значних втрат життів та руйнувань. Наприклад, зміна маршруту літака без належного контролю може призвести до небезпеки для життя пасажирів і персоналу.

Злам конфіденційної інформації, такої як пасажирські дані, може призвести до втрати довіри пасажирів до авіакомпаній і авіаційних систем загалом. Це може мати серйозний вплив на бізнес авіакомпаній і галузь в цілому.

Збої в авіаційних системах також можуть призвести до значних економічних збитків. Наприклад, затримки в рейсах і втрата даних можуть коштувати авіакомпаніям мільйони доларів. Такі збитки можуть мати далекосяжні наслідки для галузі авіації та здатні вплинути на господарську стабільність.

Таким чином, кібербезпека в авіації стала критично важливою для забезпечення надійності і безпеки авіаційних систем. Ризики, пов'язані з кіберзагрозами, несуть серйозні наслідки для авіаційної безпеки, і ці ризики ростуть з кожним днем.

У сучасному світі існують різноманітні типи кіберзагроз, які можуть вплинути на авіаційні системи. Найпоширеніші з них розкриємо більш детально. Віруси та малвари – це програми, які можуть інфікувати комп'ютерні системи і поширювати збої. У відомостях існують приклади вірусів, які були спрямовані на авіаційні системи та завдали шкоди їхньому функціонуванню. Фішинг і соціальна інженерія – це методи, які використовуються зловмисниками для отримання доступу до конфіденційної інформації шляхом маніпулювання людьми. Наприклад, атакувачі можуть виманювати важливі паролі або іншу конфіденційну інформацію від працівників авіакомпаній або аеропортів. Дистриб'ютивні атаки на відмову в обслуговуванні (ДДОС) можуть призвести до відмови в роботі серверів і мереж, що використовуються в авіаційних системах. Це може викликати затримки в рейсах і перерви у зв'язку. Зловмисники можуть вторгнутися в комп'ютерні мережі авіаційних систем і отримати доступ до даних та систем керування. Це може зумовити неконтрольований рух літаків та інші авіаційні аварії. Деякі кіберзагрози можуть бути спрямовані на шпигунство і викрадення конфіденційної інформації. Наприклад, іноземні держави або конкуренти можуть намагатися отримати доступ до важливих даних про авіаційні системи. Це лише деякі приклади типів кіберзагроз, з якими стикаються авіаційні системи. Зростання кількості та складності цих загроз робить кібербезпеку більш актуальною і важливою для галузі авіації.

Надважливим кроком до активізації міжнародного співробітництва у боротьбі з кіберзагрозами у цивільній авіації стало прийняття у 2019 р. в ході 40-ї сесії Асамблеї ІКАО низки документів, в тому числі резолюції А40-10 «Вирішення проблем кібербезпеки в цивільній авіації». Цей документ визначає план протидії держав-членів ІКАО кіберзагрозам у сфері цивільної авіації, в якому можна виділити основні завдання: 1) здійснювати стратегію кібербезпеки; 2) визначити створювані можливими кіберінцидентами загрози і чинники ризику для польотів і критично важливих систем цивільної авіації, а також серйозні наслідки, до яких можуть призвести такі інциденти; 3) визначити коло обов'язків національних органів і зацікавлених сторін галузі стосовно кібербезпеки в цивільній авіації; 4) заохочувати вироблення загального розуміння державами-членами кіберзагроз та факторів ризику, а також загальних критеріїв для визначення ступеня важливості об'єктів і систем, що вимагають захисту; 6) створювати державно-галузеві партнерства і механізми на національному та міжнародному рівнях і брати участь в їх діяльності щодо систематичного Актуальні проблеми держави і права 41 обміну інформацією в області кіберзагроз, інцидентів, тенденцій і заходів протидії; 8) заохочувати розвиток в національних органах і в авіаційній галузі життєздатної культури кібербезпеки на всіх рівнях; 10) розробити принципи і, за необхідності, виділяти ресурси для забезпечення таких вимог до критично важливих авіаційних систем; повинна бути забезпечена структурна безпека систем; системи повинні бути стійкими; способи передачі даних повинні бути безпечними і забезпечувати цілісність і конфіденційність даних; повинні бути впроваджені методи моніторингу систем і виявлення інцидентів та подання повідомлень про них; необхідно проводити судовокриміналістичний аналіз кіберінцидентів; 11) співпрацювати в розробці програми ІКАО у сфері кібербезпеки згідно з єдиним, комплексним і функціональним підходом, що включає області аеронавігації, зв'язку, спостереження, експлуатації повітряних суден, льотної придатності та інші відповідні дисципліни.

Національний центр кібербезпеки Сполученого Королівства Великої Британії авіаційних систем прогнозує появу значними викликів, які включатимуть в себе ряд загроз. Зловмисники можуть використовувати штучний інтелект і машинне навчання для створення більш скоординованих та складних кібератак. Науковці та фахівці з кібербезпеки також використовують ці технології для захисту від кіберзагроз. Зловмисники можуть діяти з будь-якої точки світу і направляти свої атаки на авіаційні системи в інших країнах.

Це ускладнює завдання виявлення та розслідування кіберзагроз. Цифрова трансформація авіації передбачає збільшення використання цифрових технологій і збільшення автоматизації в авіаційних системах. Це створює нові можливості для кіберзагроз та потребу в збільшенні захисту.

Забезпечення кібербезпеки в авіації вимагає співробітництва між країнами, авіаційними компаніями та міжнародними організаціями. Загрози в мережі надграничні, і спільні зусилля є необхідними для їх ефективного управління. Кібербезпека має величезне значення для авіаційних систем, оскільки ці системи відіграють ключову роль у глобальному сполученні та господарському розвитку. Кіберзагрози можуть призвести до серйозних наслідків, включаючи аварії, втрати життів і економічні збитки. Забезпечення кібербезпеки в авіації вимагає використання різних засобів та практик, включаючи шифрування даних, віддалений моніторинг і виявлення загроз, фізичний захист і тренування персоналу.

Література

1. Розв'язання проблем кібербезпеки в цивільній авіації. Резолюції Асамблеї. Асамблея – 40-та сесія, Монреаль, 24 вересня – 4 жовтня 2019 р. А40-10. С. 50–53. ICAO: web-site. URL: https://www.icao.int/Meetings/a40/Documents/Resolutions/a40_res_prov_ru.pdf.

УДК 343.98(043.2)

Гольдберг Н.О., к.ю.н.,
Національний авіаційний університет, м. Київ, Україна

ВЗАЄМОДІЯ СЛІДЧОГО З ІНШИМИ СЛУЖБАМИ ПРИ ПРОВЕДЕННІ ОГЛЯДУ МІСЦЯ АВІАЦІЙНОЇ ПОДІЇ

Однією з найважливіших слідчих (розшукових) дій при розслідуванні кримінальних правопорушень, що пов'язані з авіаційними подіями, є грамотний і своєчасний огляд місця події. Проте підготовка та проведення такого огляду мають свою специфіку, зумовлену низкою чинників, а саме: необхідністю в більшості випадків зміни обстановки місця події до початку його огляду, великими розмірами території, що підлягає огляду, значною кількістю потерпілих і загиблих, часто важкодоступністю місця події, одночасним проведенням огляду комісією, що проводить службове розслідування, тощо.