УДК 65.011.05: 004.056.53

Д. О. Стажкова, Л. В. Костюченко
(Національний авіаційний університет, Україна)

Дослідження засобів безпеки управління інформаційними потоками у повітряному просторі цивільної авіації

Економіко-політична нестабільність держави посилює увагу до безпеки управління інформаційними потоками у повітряному просторі цивільної авіації. Досліджені сучасні розробки в області безпеки передачі критично важливої інформації в відповідних системах авіоніки повітряних суден, зокрема шифрування повідомлень засобом приватних ключів.

В умовах економіко-політичної нестабільності в державі, ведення гібридної війни сусідньою країною, постійної загрози фізичного знищення внаслідок повномасштабних воєнних дій тощо, питання безпеки управління інформаційними потоками у повітряному просторі цивільної авіації є особливо актуальним. Адже бортові провідні та бездротові пристрої авіоніки повітряних суден мають змогу доступу до системи побудови маршрутів повітряних трас та програмувати алгоритми виконання польоту по маршруту за допомогою органів керування. Несанкціоноване перепрограмування маршруту, включно з хакерськими методами впливу, може спричинити навмисне або ненавмисне пошкодження даних чи загалом систем, що мають критичне значення для безпечної експлуатації повітряних суден (далі – ПС). Загрози існують також для функціонування всіх автоматизованих функціональних систем та комплексів авіоніки ПС. Зазвичай критичними місцями потрапляння загроз є точки доступу через мережу Інтернет. Отже питання забезпечення кібербезпеки авіаційної галузі є дуже актуальною на сьогодні, оскільки обставини в Україні та світі про це яскраво свідчать. Україна вперше зазнала кібернетичної атаки на комп'ютерні системи та центральний сервер аеропортів Борисполю та Харкова у червні 2017 році, що призвело до відмов в обслуговування ПС та затримки вильотів. Через декілька місяців у жовтні 2017 р. – затримка вильотів ПС з аеропорту Одеси в результаті взлому комп'ютерної мережі аеропорту, що призвело до втрати конфіденційності інформації. За оцінкою фахівців Європейського агентства з безпеки польотів (EASA), протягом 2019 року авіаційні системи світу щомісяця піддавалися кібератакам до 1000 разів. Дослідження показали, що проведення кібернетичних атак в авіаційні галузі у світі спричиняють збій у роботі всієї системи. Так, наприклад [1]:

- у 2019 р. – втручання в комп'ютерну систему внутрішніх авіаліній США, що призвело до вимушеної посадки ПС та збоїв в роботі Авіаційної бортової системи адресації і передачі повідомлень (ACARS);
- у 2020 р. – збої в комп'ютерній системі організації Eurocontrol , що призвело до порушення цілісності системи обміні даних та затримки більш 15000 рейсів в Європі.

Таким чином, підходи щодо протидії кібернетичним атакам повинні бути системними, надійними та комплексними, авіаційна галузь відноситься до об'єктів критичної транспортної інфраструктури України. Програма безпеки

передачі критично важливої інформації в відповідних системах авіоніки повітряних суден повинна розроблятись для захисту, надійності, цілісності та безпеки мережі та даних. Ефективна безпека передачі критично важливої інформації в комп'ютерно-інтегрованих авіаційних системах націлена на боротьбу з різними загрозами та не дозволяє їм потрапляти або розповсюджуватися в системах авіоніки ПС. До найпоширеніших загроз належать: віруси, троянські коні; хакерські атаки; провокування псевдовідмов під час роботи різних функціональних систем та комплексів ПС коли насправді системи знаходяться в працездатному стані; перехоплення та крадіжка даних; діяльність та вплив вороже налаштованих агентурних розвідкок, тощо. Успішна атака може призвести до ускладнень в роботі функціональних систем ПС розвитку ускладнень умов польоту, а в випадку наростання неправдивих даних про умови польоту – до аварійних та катастрофічних ситуацій. Загрози можуть спричинити найрізноманітніші збої та відмови, адже авіоніка ПС дуже складна та насичена складними комп'ютерними мережами. В результаті проведеного аналізу спеціалізованих літературних та онлайн-джерел [2–5, 6] визначено сучасні види кіберзагроз саме в розрізі діяльності сучасної цивільної авіації. Ґрунтуючись на результатах дослідження визначимо класифікацію базових загроз та відмов сучасних авіаційних каналів зв'язку (див. табл. 1).

Таблиця 1

Види та наслідки загроз безпеці цивільній авіації

Загальний ідентифікатор загрози	Загрози мережі даних ПС	Наслідки впливу під час експлуатації
Пасивна атака	Прослуховування або підслуховування, що загрожує безпеці, недоліки в політиці безпеки	Несанкціонована корупція або втрата даних, що спричиняють небезпечні умови польоту
Зовнішні завади	Зовнішні завади можуть порушити прийом управляючих інформаційних повідомлень	Відмова в обслуговуванні
Хибні спрацювання індикації та сигналізації	Безпечний стан роботи функціональних систем може бути порушений у разі проникнення небезпеки Спонукання екіпажу до неправильних дій.	Хибне спрацювання сигналізації (пожежа, відмови, не спрацювання аварійних режимів)

Джерело: розроблено авторами на основі [2- 5, 6].

Отже, на сьогодні використання надійних та ефективних методів захисту інформації, яка передається в системі взаємодії «земля-повітря» потребує глибоких досліджень, адже дані канали є незахищеними. Дослідження сучасноного забезпечення безпеки та стану передачі даних в системах авіоніки літаків показали, що нові типи ПС використовують технологію TCP / IP для систем, що з'єднують як доменні повітряні судна, так і кабінні інтерфейси, що практично робить ПС мережним доменом-сервером. Архітектура цієї повітряної мережі (див. рис.1) [6] дозволяє підключатися до зовнішніх систем і мереж, наприклад, бездротові системи передачі та системи обслуговування, супутникової комунікації (SATCOM), електронної пошти, мережі Інтернет тощо.

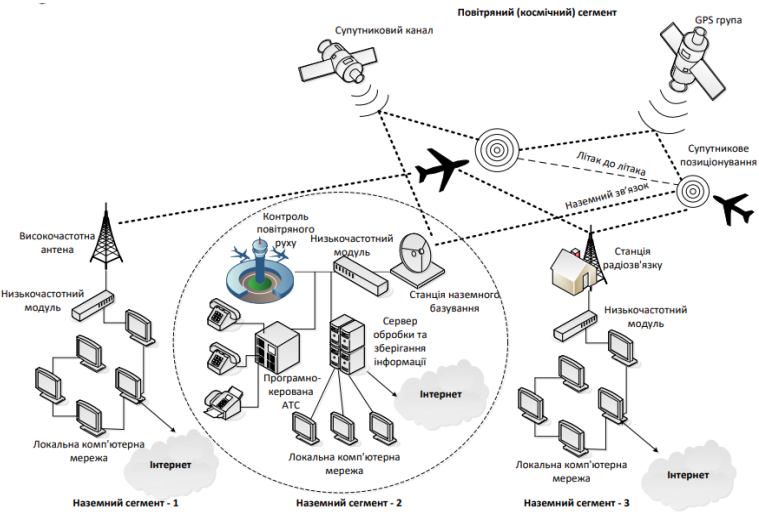

Рис. 1. Архітектура сучасної повітряної мережі
Джерело: [6].

Основна перевага використання протоколу TCP / IP – це можливість передачі інформації до ПС без використання носіїв інформації. Використання того підходу призводить до появи вразливих місць та зовнішніх загроз, що може призвести до отримання несанкціонованого доступу та вплинути на роботу функціональних систем авіоніки ПС [5, 6]. Несанціонований доступ до режимів функціонування авіоніки ПС на будь-якому етапі функціонування сучасної повітряної мережі призведе до порушення конфіденційності, цілісністності та доступності даних, що з великою долею ймовірності створить екстремальні умови експлуатації ПС, обґрунтує застосування кібернетичної безпеки та захищеності ведення конкурентного бізнесу авіакомпаній в цілому. Під час розповсюдження програмного забезпечення для функціональних систем авіоніки ПС хакери можуть робити спроби маніпулювання та пошкодження критичного програмного забезпечення, призначеного для оновлення програмного забезпечення ПС. Під поняттям маніпуляцій та пошкодження критичного програмного забезпечення розуміються навмисні несанкціоновані маніпуляції з оригінальним програмним забезпеченням або введення підробленого програмного забезпечення. Несвоєчасне виявлення маніпулювання програмним забезпеченням, підробка адміністративних повідомлень ПС може спричинити посилання помилкових сигналів тривоги та загальної відмови у послугах. Наслідком можуть бути необґрунтовані затримки польотів ПС, тобто загроза безпеки авіації загалом. Таким чином, передача критичних даних зумовлює необхідність розробки чіткої програми безпеки експлуатації ПС для забезпечення належного контролю під час керування програмним забезпеченням та безпекою інформаційної мережі на борту ПС [6]. Дослідження показали, що сучасний інженерний науково-

дослідницький підхід доводить необхідність відповідних важливих експлуатаційних впроваджень у роботу авіаційних систем відповідних приватних ключів. Кожне ПС та центр контролю повітряного руху під час обміну інформацією повинні використовувати приватні ключі з обов'язковим доступом до свого відкритого ключа. Це дозволить зашифрувати повідомлення за допомогою своїх приватних ключів, а всі інші учасники обміну інформацією матимуть змогу розшифрувати відповідний відкритий ключ [5]. Такий підхід, на думку авторів [6], забезпечить процедуру взаємної автентифікації та ідентифікації. Зокрема, використання такої автентифікації попередить зв'язок із неавторизованими компонентами або зовнішніми несанкціонованими пристроями і направлена на усунення широкого набору атак. На думку авторів [6], саме подвійний шлях інфаструктури відкритих ключів впроваджує сучасну технологію цифрового підпису, яка дозволяє ПС автентифікувати та цілісно захищати кожне інформаційне повідомлення, яке вони транслюють. Широкого науково-методичного дослідження потребують комп'ютерно-інтегровані авіаційні системи, які функціонують безпосередньо на борту ПС [6].

Висновки

Таким чином, у дослідженні висвітлено сучасний стан забезпечення кібернетичної безпеки повітряних суден вітчизняних авіакомпаній, а також нові підходи щодо сучасний засобів передачі даних каналів «земля-повітря» та «повітря-повітря». Такі засоби дозволять попередити факти виникнення ризиків та загроз ефективного управління інформаційними потоками у повітряному просторі цивільної авіації різного рівня залежно від етапу виконання. А отже це уможливлює швидко реагувати на різного роду загрози.

Список літератури

1. Fatigue risk management system implementation guide for operators [URL: https://www.researchgate.net/publication/312971231_Fatigue_Risk_Management_System_in_Aviation
2. Safety Management Manual URL: https://www.skybrary.aero/bookshelf/books/644.pdf
3. DPP: Dual Path PKI for Secure Aircraft Data Communication URL: https://vtechworks.lib.vt.edu/bitstream/handle/10919/20373/Buchholz_AK_T_2013.pdf?sequence=1
4. The Boeing Company Boeing Commercial Airline PKI Basic Assurance CERTIFICATE POLICY URL: http://www.boeing.com/crl/Boeing_BCA_PKI_CP_1.4.pdf
5. Mohamed-Slim Ben Mahmoud, Nicolas Larrieu, Alain Pirovano. A performance-aware Public Key Infrastructure for next generation connected aircrafts. DASC 2010, 29th IEEE/AIAA Digital Avionics Systems Conference, Oct 2010, Salt Lake City, United States. pp 3.C.3-1 - 3.C.3-16, 2010. https://doi.org/10.1109/DASC.2010.5655369 [22 березня 2020].
6. Robinson, Richard V., Mingyan Li, Scott A. Lintelman, Krishna Sampigethaya, Radha Poovendran, David von Oheimb, Jens-Uwe Buber, Jorge Cuellar, 2008, Electronic Distribution of Airplane Software and the Impact of Information Security on Airplane Safety, 4680 Springer Berlin / Heidelberg 28-39. https://doi.org/10.1007/978-3-540-75101-4_3