КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (9), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.9.2436
УДК 004.056.53(045)

Ільєнко Анна Вадимівна
кандидат технічних наук, доцент
доцент кафедри комп'ютеризованих систем захисту інформації
Національний авіаційний університет університет, факультет кібербезпеки комп'ютерної та програмної інженерії, Київ, Україна
ORCID: 0000-0001-8565-1117
ilyenko.a.v@nau.edu.ua

Ільєнко Сергій Сергійович
кандидат технічних наук, доцент
доцент кафедри автоматизації та енергоменеджменту
Національний авіаційний університет університет, аерокосмічний факультет, Київ, Україна
ORCID: 0000-0002-0437-0995
ilyenko.a.v@nau.edu.ua

Кваша Діана Сергіївна
бакалавр
студентка кафедри комп'ютеризованих систем захисту інформації
Національний авіаційний університет університет, факультет кібербезпеки комп'ютерної та програмної інженерії, Київ, Україна
ORCID: 0000-0003-2299-2736
diana_kvasha@ukr.net

СУЧАСНИЙ СТАН ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ЦИВІЛЬНОЇ АВІАЦІЇ УКРАЇНИ ТА СВІТУ

Анотація. 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 напряму 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. Зважаючи на постійно зростаючу статистику кібератак на роботу цивільної авіації в світовому масштабі, після глибокого аналізу та опрацювання зазначеної проблематики, автори статті висвітили сучасний стан забезпечення кібернетичної безпеки та організації захисту каналів «земля-повітря» та «повітря-повітря» парку перебуваючих в експлуатації повітряних суден авіакомпаній України, а також детально розглянути світовий досвід. Автори всебічно охопили та дослідили усі складові діяльності авіаційної системи, причому особлива увага приділена повітряним суднам, зпроектованим конструкторським бюро ДП (АНТК) «Антонов» паралельно часовому проміжку еволюційного розвитку шин та мереж даних провідних світових лідерів авіабудування (таких як Airbus та Boeing). Також приділено увагу сучасному стану та механізмам передачі даних каналів «земля-повітря» та «повітря-повітря» та архітектурі сучасної повітряної мережі комп'ютерно-інтегровані авіаційні системи. Авторами планується ряд науково технічних рішень щодо розробки та впровадження ефективних методів та засобів щодо забезпечення вимог, принципів та підходів забезпечення кібернетичної безпеки та організації захисту каналів «земля-повітря» та «повітря-повітря» в дослідних комп'ютерно-інтегрованих авіаційних системах.

Ключові слова: комп'ютерно-інтегрована авіаційна система, кіберзагроза, кібернетична безпека, авіаційна галузь, повітряне судно, методи автентифікації, інфраструктура відкритих ключів.

ISSN 2663 - 4023

1. ВСТУП

Безпечний обмін інформацією в сучасних реаліях викликає все більшу стурбованість у користувачів всього світу. Основні дані, які передаються відкрито, вразливі до різноманітних кібератак, які можуть загрожувати цілісності та доступності будь-якої інформаційної системи, яка направлена на забезпечення передачі критично важливої інформації. Існує занепокоєння, що без застосування досліджень надійних методів кібербезпеки критичні системи, на які покладаються люди, можуть бути схильними до кібернападів. Актуальність кібернетичної безпеки в авіаційній галузі загострилася через всебічне використання мережі «Інтернет» та бездротового зв'язку в системах передачі інформації між способами зв’язку диспетчерських пунктів аеропортів, повітряних суден (ПС) та аеронавігаційних систем забезпечення і контролю повітряного руху по маршруту польоту (авіаційна система на основі інформаційної мережі «Земля-Земля», «Земля-Повітря» та «Повітря-Повітря). Такі системи зазвичай називаються комп’ютерно-інтегрованими авіаційними системами. Україна як частина авіаційного співтовариства з своєю авіаційно-будівною складовою (ДП «Антонов») повинна рухатись в унісон з провідними виробниками та експлуатантами авіаційної техніки. З практики застосування інформаційних технологій провідних світрових фірм-виробників (Boeing, Airbus та ін.) в сучасних ПС за останнє десятиліття почали впроваджуватись ефективні методи захисту та протидії кіберзагрозам при передачі, зберіганні та обробці критично важливих польотних даних. Один із таких прикладів у галузі авіації - надійні методи ідентифікації між ПС та системами забезпечення і контролю повітряного руху. Розглядаючи вищеописані комп’ютерно-інтегровані авіаційні системи можемо переконатись, що вона містить велику кількість критично важливих інформаційних даних, які мають конфіденційний статус, тому, якщо інформація передається відкрито, дані системи стають досить вразливими до кібератак. Загрози та ризики зростатимуть з збільшенням підключених пристроїв передачі інформації як в аеропортових інформаційних мережах, так і в мережах безпосередньо ПС. Це може призвести до наведень та поширень різноманітних кібернетичних атак. Тому кібератаки в авіаційній галузі можуть загрожувати як безпечній експлуатації самого ПС, так і авіаційній системі цілому (в масштабі всередині державного та міждержавного авіасполучення).

З огляду на це, потрібно вводити та використовувати ряд засобів захисту цілісності, конфіденційності інформації в авіаційних системах передачі, збереження та обробки критично важливих даних.

Постановка проблеми. Застосовуючи сучасні технології, авіаційні системи передачі, збереження та обробки критично важливих даних стають все більш автоматизованими та можуть працювати як в парі, та і незалежно від голосових команд диспетчерів управління повітряним рухом. Зараз відповідні системи авіоніки сучасних ПС можуть транслювати та отримувати інформацію про ПС та його місцезнаходження за допомогою транспондерної технології. Це зменшує навантаження на диспетчерських пункти вздовж всього маршруту польоту та дозволяє ПС взяти на себе більше відповідальності за підтримання безпеки польоту. Однак цим авіаційним системам бракує методів автентифікації джерела або можливості перевірити цілісність вмісту інформаційного повідомлення. Це відкриває для хакерів можливість потенційно створювати шахрайські інформаційні повідомлення або маніпулювати вмістом повідомлень, які, в свою чергу, можуть вплинути на органи керування ПС в режимі «автопілот» та відхилити його від заданого курсу польоту. Ретельне дослідження в

галузі передачі авіаційних даних дає змогу чітко розуміти примітиви кібербезпеки задля формування надійного проекту безпеки для захисту ПС від кіберзагроз в цілому. В статтях [1] і [2] висвітлено основні проблеми, та виклики які постають перед авіаційною галуззю в світовому масштабі, а в статтях [3-9] визначено основні напрями захисту каналів зв'язку «земля-повітря». **Метою статті** є дослідження сучасного стану забезпечення захисту інформації в авіаційній галузі України, що дає змогу проаналізувати основні проблеми, та висвітлити основні ідеї авторів щодо їх вирішення.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Характеристика загроз авіаційних каналів зв'язку. Бортові провідні та бездротові пристрої авіоніки ПС мають змогу доступу до системи побудови маршрутів повітряних трас та програмувати алгоритми виконання польоту по маршруту за допомогою органів керування ПС в різних режимах польоту (сучасний бортовий компютер **FMC**-Flight Management Computer який управляється з допомогою дисплея **CDU** – Central Display Unit*).* Несанкціоноване перепрограмування маршруту (в тому числі хакерськими методами впливу) може призвести до навмисного або ненавмисного пошкодження даних та/або систем, що мають важливе (критичне) значення для безпечної експлуатації ПС. Загрози існують також для функціонування всіх автоматизованих функціональних систем (ФС) та комплексів авіоніки ПС. Зазвичай критичними місцями потрапляння загроз є точки доступу через мережу «Інтернет» (за допомогою постачальника програмного забезпечення до свого оператора або його підрядника) та пункти, де запрограмована інформація передається від оператора (аеропорту чи диспетчерського пункту по трасі слідування) до ПС. Питання забезпечення кібербезпеки авіаційної галузі є дуже актуальною на сьогодні, оскільки обставини в Україні та світі про це яскраво свідчать.

Наведемо деякі факти проведення кібернетичних атак в авіаційні галузі у світі:

2006 р. – інтернет атака на центри контролю повітряного руху США;

2008 р. – зараження бортового комп'ютера рейса Spanair 5022 шкідливим програмним забезпеченням, що призвело до катастрофи;

2009 р. – втручання в систему GPS США, що використовується для заходу на посадку ПС;

2013 р. – втручання в інформаційну систему аеропортів Туреччинпи, що призело до призупинення паспортного контролю;

2013 р. – втручання в комп'ютерні мережі 75 аеропортів США;

2014 р. – втрата керування ПС при дистанційному підключенні до автопілоту та зникнення ПС рейсу MH370 Малазійских авіаліній з радарів (одна з ключових версій катастрофи);

2014 р. – масштабні атаки на комп'ютерні авіаційні системи Пакистану, Саудовскої Аравії, Південної Кореї та США;

2015 р. – поширення шкідливого програмного забезпечення в комп'ютерні системи аеропорту США, що призвело до призупинення польотів;

2015 р. – несанкціоноване втручання в комп'ютерну системи аеропорту Польської авіакомпанії LOT, що призвело до сбоїв при обслуговуванні ПС та втраті конфіденційної інформації;

2016 р. – проникнення до комп'ютерної системи та зараження комп'ютерів аеропорту Талліну шкідливим програмним забезпеченням, що призвело до втрати

конфіденційної інформації;

2017 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);

2018 р. – збої в комп'ютерній системі організації Eurocontrol , що призвело до порушення цілісності системи обміні даних та затримки більш 15000 рейсів в Європі.

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. 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 ПС 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 ФС 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 автори згрупували, синтезували та таблично представили сучасні види кіберзагроз саме в розрізі діяльності сучасної цивільної авіації [3-9]. Наведемо запропоновану класифікацію базових загроз та відмов сучасних авіаційних каналів зв'язку (таблиця 1).

Таблиця 1

Види загроз цивільній авіації

Загальний ідентифікатор загрози s	**Загрози мережі даних ПС**	**Приклад впливу під час експлуатації**
Невдача	Безпечний стан роботи ФС (авіоніки вцілому) може бути порушений у разі несанкціонованого доступу	Доступ до контролю польотів сторонніми особами, що впливають на безпеку
Заперечення	Системні ресурси обладнання ПС вичерпані через атаку відмови в обслуговуванні, системні помилки, шкідливі дії	Критичні послуги, порушені перевантаженням системи або перешкоджанням трафіку

ISSN 2663 - 4023

Управління доступом	Особа, яка не є уповноваженим користувачем, може отримати доступ до відповідних ФС авіоніки ПС через несанкціонований контролер, помилку системи підробки або атаку зловмисних цілей	Несанкціонований доступ
Пасивна атака	Прослуховування або підслуховування, що загрожує безпеці, недоліки в політиці безпеки	Несанкціонована корупція або знищення даних, що спричиняють небезпечні умови польоту
Зовнішні завади	Зовнішні завади можуть порушити прийом управляючих інформаційних повідомлень	Відмова в обслуговуванні
Помилкове введення та нав'язування	Підробка повідомлень та трансляція з метою перехоплення управління повітряним рухом та ПС	Помилково вказують, що зіткнення є неминучим; провокувати пілотів на неправильні дії або впливати на наземні станції керування повітряним рухом; перешкоджати законному прийому повідомлень
Помилки навігації	Прослуховування супутникових систем навігації	Нав'язування неправдивої інформація про положення або швидкість ПС; порушення резервного радіолокаційного або голосового зв'язку
Хибні спрацювання індикації та сигналізації	Безпечний стан роботи ФС (авіоніки вцілому) може бути порушений у разі проникнення небезпеки. Спонукання екіпажу до неправильних дій.	Хибне спрацювання сигналізації та індикації про стан ФС (пожежа, відмови, не спрацювання аварійних режимів)

На сьогоднішній день використання надійних та ефективних методів захисту інформації, яка передається в системі взаємодії «земля-повітря» потребує глибоких досліджень, адже дані канали є незахищеними [10,11].

Сучасний стан передачі даних в системах авіоніки ПС, забезпечення безпеки та проблемні місця. Раніше ПС використовували в цивільній (ARINC 429 / ARINC 629) або військовій авіації (MIL-STD-1553) стандартні шини для передачі даних в ФС авіоніки. Процеси передачі інформації з використанням протоколу передачі TCP та / або TCP / IP були фізично та логічно ізольовані від використання в ФС авіоніки ПС.

Розвиток авіаційних технологій в сфері передачі даних про стан ФС: ARINC 429 (100 кбіт/с) - лінійна однонаправлена шина; MIL-STD-1553B, також відома як DEF-STAN-00-18 та STANAG 3838 (1 Мбіт/с) - лінійна двонаправлена шина з централізованим контролем, протокол «команда/відповідь»; ARINC 629 (2 Мбіт/с) - лінійна двонаправлена шина з розподіленим контролем, з розпізнаванням множинного

доступу/зіткнення (CSMA / CD), а також з динамічним розподілом часових інтервалів (DTSA); ARINC 664 (AFDX Ethernet 10/100 Мбіт/с) - двонаправлена мережа зв'язку з розподіленим контролем та протоколом CSMA/CD для забезпечення псевдо-детермінованого часу та керування резервуванням; CANbus (1 Мбіт/с) - лінійна двонаправлена шина з пріоритетним протоколом «виявлення/уникнення» зіткнень.

В табл. 2 зібрано, обґрунтовано та порівняно характеристики та продуктивність основних інформаційних шин в мережах зв'язку ФС, що використовуються в сучасному літакобудуванні [12,13].

Таблиця 2

Порівняння шин передачі даних «Data bus network»

Шини, мережі	**MIL-STD-1553B**	**ARINC 429**	**ARINC A664-P7**	**CANbus**
Макс. довжина повідомлення	32 × 16-bit	18-bit	1518 bytes (1 byte = 8 bits)	8 bytes
Макс. швидкість	1 Mbps	100 kbps	10/100 Mbps	1 Mbps
Тип зв'язку	Двосторонній Напівдуплекс	Одно спрямований	Двосторонній Повний дуплекс	Двосторонній Напівдуплекс
Протокол	Команда /відповідь	Прямий	CSMA/CD + розширення	CSMA/CD
Макс. довжина шини	100 м	65 м	<100 м	40 м
Затримка сигналу	Немає	Незначна	Залежить від навантаження	Залежить від пріоритету
Error containment	Parity bit	Parity bit	Cyclic redundancy check	Extensive cyclic redundancy check
Обробка помилок	Зворотній звязок	Зворотній зв'язок відсутній	Зворотній звязок	Негайна спроба зязку заново
Резервування	Подвійне	Просте	Подвійне	Просте
Фізична реалізація	Подвійна «вита пара»	«Вита пара»	Подвійна «вита пара» або оптоволокно	Вита пара або оптоволокно

Кожна шина, або мережа передачі даних знайшла своє місце в архітектурі ФС авіоніки сучасного ПС. Ключовими вимогами є задоволення вимог до продуктивності, цілісності та доступності (цінова складова). ARINC 664-P7 підходить для високої пропускної спроможності, інформаційної основи для всіх ФС авіоніки ПС, включаючи керування польотом та навігацію, реалізацією сучасного інтерфейсу ергономіки «скляної кабіни».ARINC 429 використовується як засіб для зв'язку та перевірки стану ФС під час діагностування та вбудованого контролю життєво важливих параметрів. CANbus підходить для зв’язку з різними датчиками,а також для передачі даних всередині ФС ПС.

Світові лідери Airbus та Boeing мають різні архітектурні філософії які інтегрують шини CANbus і ARINC 429 з мережею ARINC 664-P7. Шина Avionics Standard Communications Bus була розроблена компанією Honeywell і використовується в ЦА і бізнес-джетах на швидкості 670 кбіт/с. Комерційна стандартна шина даних,

ISSN 2663 - 4023

розроблена компанією Rockwell Collins для використання в ЦА, аналогічна ARINC 429, працює на 12,5 кбіт/с та 50 Кбіт/с. Цифрові шини RS232, RS422 та IEEE 1394 Firewire з швидкістю 800 Мбіт/с також використовуються в передачі цифрового відео.

На прикладі графічного зображення (рис. 1) авторами інтегровано та показано технології шин даних, застосованих в ПС України відповідно до еволюційного використання та впровадження шин та мереж даних лідерів світового літакобудування [12,13].

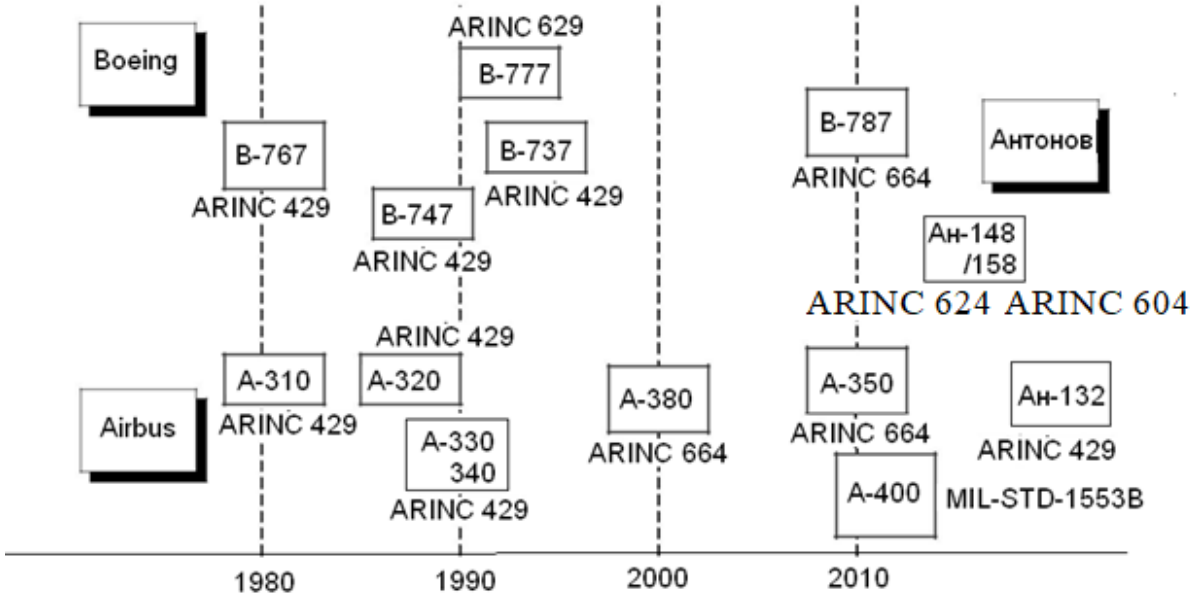

Рис. 1. Еволюційне застосування технологій шин даних

Нові типи ПС використовують технологію TCP / IP для систем , що з'єднують як доменні ПС, так і кабінні інтерфейси таким чином, що практично робить ПС мережним доменом-сервером. Архітектура цієї повітряної мережі дозволяє підключатися до зовнішніх систем і мереж, наприклад, бездротові системи передачі та системи обслуговування, супутникової комунікації (SATCOM), електронної пошти, мережі Інтернет тощо. 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 ФС авіоніки ПС. Несанціонований доступ до режимів функціонування авіоніки ПС на будь-якому етапі функціонування сучасної повітряної мережі (авторське бачення сучасної повітряної мережі показано на рис.2) 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.

ISSN 2663 - 4023

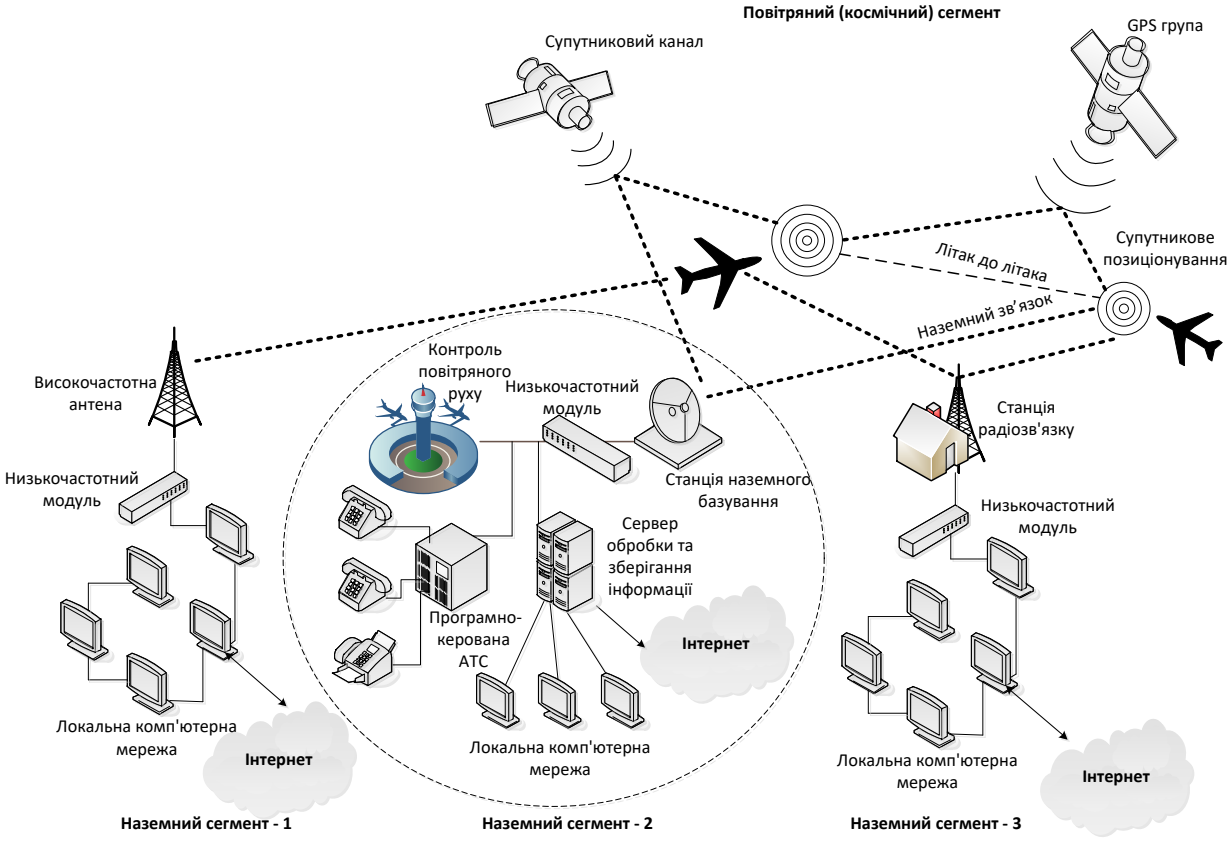

Рис. 2. Архітектура сучасної повітряної мережі

Під час розповсюдження програмного забезпечення (ПЗ) для ФС авіоніки ПС хакери можуть робити спроби маніпулювання та пошкодження критичного програмного забезпечення, призначеного для оновлення ПЗ ПС. Під поняттям маніпуляцій та пошкодження критичного ПЗ будемо розуміти навмисні несанкціоновані маніпуляції з оригінальним програмним забезпеченням або введення підробленого програмного забезпечення. Не своєчасне виявлення маніпулювання програмним забезпеченням, підробка адміністративних повідомлень ПС (тобто команд завантаження, запитів та відповідних відповідей) може призвести, наприклад, до помилкових сигналів тривоги та загальної відмови в послугах. Такий тип атаки на програмне забезпечення може створити необґрунтовані затримки польотів ПС та поставити під загрозу безпеку авіації в цілому. З огляду на все вищезазначене, передача критичних даних зумовлює необхідність розробки чіткої програми безпеки експлуатації ПС для забезпечення належного контролю під час керування / розповсюдження програмного забезпечення та безпеки інформаційної мережі на борту ПС.

3. ПОДАЛЬШІ НАПРЯМИ ДОСЛІДЖЕННЯ

В подальших дослідження авторами роботи планується зосередити увагу на організації захисту каналів «земля-повітря» та «повітря-повітря» в дослідних комп’ютерно-інтегрованих авіаційних системах з використанням криптографічних методів захисту інформації, а саме з використанням асиметричної криптографії та інфраструктури відкритого ключа. Асиметрична криптографія, відома як криптографія

відкритого ключа, використовує сучасну теорію чисел для створення двох ключів, одного відкритого та одного приватного, які працюють разом для досягнення ряду цілей кібернетичної безпеки для проведення процедур ідентифікації та автентифікації джерела інформації [14].

Сучасний інженерний науково–дослідницький підхід спонукає до відповідних важливих експлуатаційних впроваджень в роботу досліджуваних авіаційних систем відповідних приватних ключів. Кожне ПС та центр контролю повітряного руху (КПР) під час обміну інформацією повинні використовувати приватні ключі з обов'язковим доступом до свого відкритого ключа. Таке рішення дозволяє зашифрувати повідомлення за допомогою своїх приватних ключів, а всі інші учасники обміну інформацією мають змогу розшифрувати відповідний відкритий ключ. Такий підхід забезпечить процедуру взаємної автентифікації та ідентифікації.

Розглянемо теоретичні підходи, а саме ідею авторів щодо застосування технології «криптографія відкритого ключа» для авіаційної системи на основі інформаційної мережі «земля-повітря». Ретельне вивчення областей КПР та кібербезпеки виявило потенційну проблему із сучасними методами ідентифікації ПС та моніторингу, а також інструментами, необхідними для усунення цих проблем. Офіційне визначення проблеми та пошук подібних потенційних рішень призвели до розуміння того, що реалізація потужної інфаструктури відкритих ключів є доцільною, що направлена на забезпечення надійної автентифікації та безпечного зв'язку між пристроями ПС так і за його межами . Використання автентифікації на основі PKI попередить зв'язок з неавторизованими компонентами або зовнішніми несанкціонованими пристроями і направлена на усунення широкого набору атак. Подвійний шлях ІВК є однією з перших запропонованих конструкцій для захисту вразливих місць безпеки в комунікаціях даних «ПС - ПС» та «ПС - КПР». Метою впровадження ІВК є захист інформації (активів), що передаються або піддаються впливу зовнішнього середовища, та для захисту обміну інформацією між авіаційними компаніями при організації захисту каналів «земля-повітря» та «повітря-повітря». Надалі під поняттям ІВК в авіаційній галузі будемо розуміти сукупність технологій та політик, що беруть участь в управлінні, зберіганні та скасуванні сертифікатів відкритих ключів кінцевих користувачів при організації захисту авіаційного каналу зв'язку чи при розповсюдженні та / або використанні програмного забезпечення. Запропонована авторами ідейна конструкція вирішує проблему ідентифікації ПС за допомогою надійних методів взаємної автентифікації між ПС та КПР. 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. Автори статті налаштовані всебічно розглянути проблеми та способи реалізації питання кіберзахисту таких ФС в наступних дослідженнях.

4. ВИСНОВКИ

В даній статті висвітлений сучасний стан забезпечення кібернетичної безпеки та організації захисту каналів «земля-повітря» та «повітря-повітря» парку перебуваючих в експлуатації повітряних суден авіакомпаній України, також детально розглянутий світовий досвід в даному напрямку. Проаналізовано основні проблеми дослідження, розглянуто дієві шляхи їх вирішення та протидії кібертероризму. Детально

проаналізовано та наведеноо факти проведення кібернетичних атак в авіаційні галузі в Україні та світі за останнє десятиліття, а також наведено узагальнену характеристику загроз авіаційних каналів зв'язку, що порушують доступність, конфіденційність та цілісність інформації. Звернута особлива увага повітряним суднам, зпроектованим конструкторським бюро ДП (АНТК) «Антонов», проведено аналіз еволюційного розвитку шин та мереж даних сучасних ПС провідних світових лідерів Airbus та Boeing та конструкторські рішення ДП Антонов. Показано, що зростання кібернетичних атак в цивільні авіацій супроводжується впровадженням та застосуванням сучасних інформаційно-комунікаційних технологій, що з одного боку підвищує ефективність діяльності, а з іншого збільшує кількість уразливостей та можливостей здійснення кібернетичного впливу на комп'ютерно-інтегровані авіаційні системи. Висвітлено сучасний стан передачі даних каналів «земля-повітря» та «повітря-повітря», узагальнено представлено архітектуру сучасної повітряної мережі комп'ютерно-інтегровані авіаційні системи. Виходячи з вищезазначеного, запропоновано теоретичні підходи щодо організації кібернетичного захисту авіаційних каналів зв'язку з використанням методів та підходів шифрування, а саме застосування інфраструктури відкритих ключів для проведення процедури автентифікації та контролю цілісності повідомлень щодо забезпечення організації повітряного руху. Колективом авторів заплановано у подальшій науково-технічній діяльності розробити та впровадити ефективні методи та засоби щодо забезпечення сформованих у цій роботі вимог, принципів та підходів забезпечення кібернетичної безпеки та організації захисту каналів «земля-повітря» та «повітря-повітря».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Fatigue risk management system implementation guide for operators [Онлайн]. – Режим доступу: https://www.researchgate.net/publication/312971231_Fatigue_Risk_Management_System_in_Aviation [22 березня 2020].

[2] Aviation security law (2010) Ruwantissa Abeyratne [Онлайн]. – Режим доступу: https://books.google.com.ua/books?id=tw8g6C479vUC&pg=PA116&lpg=PA116&dq=aircraft+pki&source=bl&ots=JcZ_b5z7yL&sig=xlkbmLsRXTO6Y2FPNPrpZnvH52s&hl=ru&sa=X&ved=2ahUKEwjzzsb525reAhVFpYsKHbJcAMo4ChDoATABegQICRAB#v=onepage&q=aircraft%20pki&f=false [22 березня 2020].

[3] Safety Management Manual [Онлайн]. – Режим доступу: https://www.skybrary.aero/bookshelf/books/644.pdf [22 березня 2020].

[4] DPP: Dual Path PKI for Secure Aircraft Data Communication [Онлайн]. – Режим доступу: https://vtechworks.lib.vt.edu/bitstream/handle/10919/20373/Buchholz_AK_T_2013.pdf?sequence=1 [22 березня 2020].

[5] The Boeing Company Boeing Commercial Airline PKI Basic Assurance CERTIFICATE POLICY [Онлайн]. – Режим доступу: http://www.boeing.com/crl/Boeing_BCA_PKI_CP_1.4.pdf [22 березня 2020].

[6] Aircraft Network Security Program [Онлайн]. – Режим доступу: https://www.caas.gov.sg/docs/default-source/pdf/ac121-7-2(rev-0)-aircraft-network-security-progamme-(ansp).pdf [22 березня 2020].

[7] 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].

[8] 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. [22 березня 2020].

[9] Robinson, Richard V., Mingyan Li, Scott A. Lintelman, K.Sampigethaya, Radha Poovendran, David von Oheimb, Jens-Uwe Buber, 2007, Impact of Public Key Enabled Applications on the Operation and

Maintenance of Commercial Airplanes. https://doi.org/10.2514/6.2007-7769. [22 березня 2020].

[10] Приложение 17 к Конвенции о международной гражданской авиации «Безопасность. Защита международной гражданской авиации от актов незаконного вмешательства». [Онлайн]. – Режим доступу: http://www.6pl.ru/asmap/Annexes//an17_cons_ru.pdf [22 березня 2020].

[11] Doc 8973 ICAO «Руководство по авиационной безопасности» (Restricted) [Онлайн]. – Режим доступу: http://dspk.cs.gkovd.ru/library/data/8973_cons_ru_ruk__vo_po_ab_izd_9_e_2014g_.pdf [22 березня 2020].

[12] Ian Moir, Allan Seabridge, Malcolm Jukes. Civil Avionics Systems. [Онлайн]. – Режим доступу: http://dl.booktolearn.com/ebooks2/engineering/aeronautical/9781118341803_civil_avionics_systems_fffd.pdf [22 березня 2020].

[13] Ian Moir, Allan Seabridge. Aircraft Systems Mechanical, electrical, and avionics subsystems integration. [Онлайн]. – Режим доступу: https://soaneemrana.org/onewebmedia/AIRCRAFT%20SYSTEMS%20BY%20IAN%20MOIR%20&%20ALLAN%20SEABRIDGE%20TRIBIKRAM.pdf [22 березня 2020].

[14] Kazmirchuk, S., Anna, I., Sergii, I.: Digital signature authentication scheme with message recovery based on the use of elliptic curves. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds.) ICCSEEA 2019. AISC, vol. 938, pp. 279–288. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-16621-2_26. [22 березня 2020].

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (9), 2020
ISSN 2663 - 4023

Ilyenko Anna
Candidate of Technical Sciences, assistant professor
assistant professor of Information Security Systems Department National Aviation University of Kyiv, Faculty of Cyber Security, Computer and Software Engineering, Ukraine
ORCID: 0000-0001-8565-1117
ilyenko.a.v@nau.edu.ua

Ilyenko Sergii
Candidate of Technical Sciences, assistant professor
assistant professor of Automation and Energy Management Department National Aviation University of Kyiv, Aerospace Faculty, Ukraine
ORCID: 0000-0002-0437-0995
ilyenko.a.v@nau.edu.ua

Kvasha Diana
Student Information Security Systems Department
National Aviation University of Kyiv, Faculty of Cyber Security, Computer and Software Engineering, Ukraine
ORCID: 0000-0003-2299-2736
diana_kvasha@ukr.net

THE CURRENT STATE OF THE CYBERSECURITY OF CIVIL AVIATION OF UKRAINE AND THE WORLD

Abstract. Considering computer-integrated aviation systems that provide a link between civil aviation activities within the ground-to-air and air-to-air channels, the question of the safe operation of such aviation systems from an ever-increasing cyber threats, and the decline in cybersecurity for the aviation industry as a whole. The protection status of ground-to-air and air-to-air channels in such aviation systems is at different levels and depends directly on the activity of all components of aviation activity (airport-aircraft-information network-air traffic management, etc.). To date, some communication channels are not secure at all and are in an open state, which provokes a rapid growth of cyber-attacks and requires the introduction and application of modern information and communication technologies in such communication channels. In view of the ever-increasing cyber statistics on the work of civil aviation worldwide, the authors of the article highlighted the current state of cyber security and protection of ground-to-air and air-to-air channels of the aircraft fleet of Ukrainian airlines, and take a closer look at the world experience. The authors comprehensively covered all components of the aviation system, with particular attention given to aircraft designed by Antonov Design Bureau with the time evolution of tire development and data networks of the world's leading aviation industry leaders (such as Airbus and Boeing). Also, attention is given to the present state and mechanisms of data transmission of the ground-to-air and air-to-air channels and the architecture of the modern air-network of computer-integrated aviation systems. The authors plan a number of scientific and technical solutions for the development and implementation of effective methods and means to ensure the requirements, principles and sub-approaches to ensure cyber security and the organization of protection of ground-to-air and air-to-air channels in experimental computer-integrated aviation systems.

Keywords: computer integrated aviation system; cyber threat; cyber security; aviation; aircraft; authentication methods; public key infrastructure.

REFERENCES

[1] Fatigue risk management system implementation guide for operators [Online]. Available: https://www.researchgate.net/publication/312971231_Fatigue_Risk_Management_System_in_Aviation [Accessed: 22 march 2020] (in English).

[2] Aviation security law (2010) Ruwantissa Abeyratne [Online]. Available: https://books.google.com.ua/books?id=tw8g6C479vUC&pg=PA116&lpg=PA116&dq=aircraft+pki&source=bl&ots=JcZ_b5z7yL&sig=xlkbmLsRXTO6Y2FPNPrpZnvH52s&hl=ru&sa=X&ved=2ahUKEwjzzsb

525reAhVFpYsKHbJcAMo4ChDoATABegQICRAB#v=onepage&q=aircraft%20pki&f=false [Accessed: 22 march 2020] (in English).

[3] Safety Management Manual [Online]. Available: https://www.skybrary.aero/bookshelf/books/644.pdf [Accessed: 22 march 2020] (in English).

[4] DPP: Dual Path PKI for Secure Aircraft Data Communication [Online]. Available: https://vtechworks.lib.vt.edu/bitstream/handle/10919/20373/Buchholz_AK_T_2013.pdf?sequence=1 [Accessed: 22 march 2020] (in English).

[5] The Boeing Company Boeing Commercial Airline PKI Basic Assurance CERTIFICATE POLICY [Online]. Available: http://www.boeing.com/crl/Boeing_BCA_PKI_CP_1.4.pdf [Accessed: 22 march 2020] (in English).

[6] Aircraft Network Security Program [Online]. Available: https://www.caas.gov.sg/docs/default-source/pdf/ac121-7-2(rev-0)-aircraft-network-security-progamme-(ansp).pdf [Accessed: 22 march 2020] (in English).

[7] 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. DOI: 10.1109/DASC.2010.5655369. [Accessed: 22 march 2020] (in English).

[8] 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. DOI: 10.1007/978-3-540-75101-4_3. [Accessed: 22 march 2020] (in English).

[9] Robinson, Richard V., Mingyan Li, Scott A. Lintelman, K.Sampigethaya, Radha Poovendran, David von Oheimb, Jens-Uwe Buber, 2007, Impact of Public Key Enabled Applications on the Operation and Maintenance of Commercial Airplanes. DOI: 10.2514/6.2007-7769. [Accessed: 22 march 2020] (in English).

[10] Appendix 17 to the Convention on International Civil Aviation «Security. Protection of international civil aviation from acts of unlawful interference». [Online]. Available: http://www.6pl.ru/asmap/Annexes//an17_cons_ru.pdf [Accessed: 22 march 2020] (in Russian).

[11] Doc 8973 ICAO «Aviation Security Manual» (Restricted) [Онлайн]. – [Online]. Available: http://dspk.cs.gkovd.ru/library/data/8973_cons_ru_ruk__vo_po_ab_izd_9_e_2014g_.pdf Accessed: 22 march 2020] (in Russian).

[12] Ian Moir, Allan Seabridge, Malcolm Jukes. Civil Avionics Systems. [Online]. Available: http://dl.booktolearn.com/ebooks2/engineering/aeronautical/9781118341803_civil_avionics_systems_fffd.pdf [Accessed: 22 march 2020] (in English).

[13] Ian Moir, Allan Seabridge. Aircraft Systems Mechanical, electrical, and avionics subsystems integration. [Online]. Available: https://soaneemrana.org/onewebmedia/AIRCRAFT%20SYSTEMS%20BY%20IAN%20MOIR%20&%20ALLAN%20SEABRIDGE%20TRIBIKRAM.pdf [Accessed: 22 march 2020] (in English).

[14] Kazmirchuk, S., Anna, I., Sergii, I.: Digital signature authentication scheme with message recovery based on the use of elliptic curves. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds.) ICCSEEA 2019. AISC, vol. 938, pp. 279–288. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-16621-2_26. [Accessed: 22 march 2020] (in English).