© Gnatyuk S., Vasyliev D. Modern critical aviation information systems // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 1, p. 51-57.

СУЧАСНІ КРИТИЧНІ АВІАЦІЙНІ ІНФОРМАЦІЙНІ СИСТЕМИ

Сергій Гнатюк[1], Денис Васильєв[1,2]

[1]Національний авіаційний університет, Україна
[2]Державне підприємство обслуговування повітряного руху України «Украероруx», Україна

ГНАТЮК Сергій Олександрович, к.т.н.

Рік та місце народження: 1985 рік, м. Нетішин, Хмельницька область, Україна.
Освіта: Національний авіаційний університет, 2007 рік.
Посада: доцент кафедри безпеки інформаційних технологій з 2012 року, голова Наукового товариства студентів, аспірантів, докторантів та молодих вчених з 2015 року.
Наукові інтереси: інформаційна безпека, квантова криптографія, управління інцидентами інформаційної безпеки, захист критичної інформаційної інфраструктури держави.
Публікації: більше 200 наукових публікацій, серед яких монографії, статті у рецензованих вітчизняних та закордонних наукових журналах, патенти та авторські свідоцтва.
E-mail: s.gnatyuk@nau.edu.ua

ВАСИЛЬЄВ Денис Володимирович, к.т.н.

Рік та місце народження: 1987 рік, м. Київ, Україна
Освіта: Національний авіаційний університет, 2010 рік
Посада: інструктор відділу підготовки інженерно-технічного персоналу Навчально-сертифікаційного центру, доцент кафедри аеронавігаційних систем НАУ.
Наукові інтереси: ситуаційний аналіз та прийняття рішень при організації повітряного руху.
Публікації: більше 30 друкованих наукових праць, в тому числі статті у міжнародних та вітчизняних рецензованих наукових журналах
E-mail: dvasyliev@nau.edu.ua

Анотація. *Проблема кібертероризму носить глобальний характер і досить гостро постає у сучасному інформаційному суспільстві. Провідні держави світу все більше уваги приділяють кіберзахисту власних критичних інформаційних ресурсів у різних галузях. У галузі цивільної авіації рівень критичності значно підсилюється підвищеним ступенем зв'язності та взаємодії між наземними системами і повітряними суднами, а впровадження сучасних інформаційних та комунікаційних технологій з одного боку підвищує ефективність діяльності цивільної авіації, проте з іншого боку породжує цілу низку нових уразливостей та потенційних загроз. Крім того, жоден із керівних документів щодо забезпечення захисту міжнародної цивільної авіації не містить повний перелік критичних авіаційних інформаційних систем, їх функціональні особливості та рівень критичності – це значно ускладнює аналіз уразливостей таких систем, розробку моделей загроз та порушників, аналіз та оцінку ризиків, а також не дозволяє чітко формалізувати методи захисту таких систем від різного роду кіберзагроз. У цій статті здійснено пошук та систематизацію сучасних авіаційних інформаційних систем (інформаційні системи аеронавігаційного обслуговування, бортові інформаційні системи повітряних суден, інформаційні системи авіакомпаній та аеропортів), проведено їх аналіз та виділено базові ознаки для класифікації. Отримані результати будуть використані для подальшої розробки розширеної класифікації і методу визначення рівня критичності авіаційних інформаційних систем.*

Ключові слова: *кібербезпека, критична інформаційна інфраструктура держави, цивільна авіація, критична інформаційна авіаційна система, класифікація.*

Вступ

На початку XXI сторіччя спостерігається підсилення й збільшення різноманітності терористичної діяльності, діапазон методів якої є доволі широким – від використання вибухових пристроїв для руйнування об'єктів критичної інфраструктури до здійснення кібератак на критичні (критично важливі) інформаційні системи (інформаційний тероризм, кібертероризм) [1]. Відповідно до [2] серед об'єктів, які є уразливими до терактів, поряд із критичними об'єктами газотранспортного та енергетичного комплексів виділяють транспортну інфраструктуру. Хоча сьогодні в Україні, на відміну від більшості європейських держав, не затверджений остаточний перелік об'єктів критичної інфраструктури, проте очевидно, що несанкціоноване втручання у роботу транспортної системи може призвести до значних економічних збитків, людських жертв і руйнування загальнодержавної інфраструктури. У галузі цивільної авіації рівень критичності значно підсилюється підвищеним ступенем зв'язності та

взаємодії між наземними системами і повітряними суднами (ПС), а впровадження сучасних інформаційних та комунікаційних технологій (ІКТ) з одного боку підвищує ефективність діяльності цивільної авіації, проте з іншого боку породжує цілу низку нових уразливостей та потенційних загроз різного характеру [3].

Аналіз джерел

Нова редакція Додатку 17 до Конвенції про міжнародну цивільну авіацію [4] декларує необхідність для кожної держави, що є членом ІКАО, розробляти методи захисту ІКТ, що використовуються для цілей цивільної авіації, від втручання, що може поставити під загрозу безпеку цивільної авіації (під *ІКТ* у галузі цивільної авіації розуміють будь-яку інформацію або пристрій зв'язку (аналоговий чи цифровий), чи застосунок, включаючи радіо, телебачення, телефони, смартфони, смартпеди, комп'ютерні і мережеві апаратні та програмні засоби, системи та пристрої збереження даних, супутникові системи, системи спостереження, навігаційні системи, а також пов'язані з ними різного роду служби та застосунки [7]). Керівний документ ЄКЦА [5] вказує на те, що відповідний повноважний орган (у нашій державі це Державіаслужба України) повинен забезпечити, щоб заходи щодо захисту від кіберзагроз у цивільній авіації були включені до Національної програми безпеки цивільної авіації, Національної програми контролю якості та Національної програми навчання і підготовки з питань безпеки цивільної авіації. Керівництво ІКАО [6] визначає орієнтовний (проте невичерпний) перелік критичних авіаційних інформаційних систем (тобто систем, які містять інформацію, що має критичне значення для безпечного виконання польотів і безпечної діяльності цивільної авіації), а також вказує на необхідність застосування багаторівневого підходу для забезпечення стійкості таких систем до кібератак. Інший керівний документ ІКАО [7], що вийшов у світ минулого року (затверджений в кінці 2013 року), доповнює попереднє керівництво, містить інструктивні відомості щодо забезпечення безпеки системи організації повітряного руху (ОрПР) і визначає деякі важливі поняття, що не були раніше визначені в керівних авіаційних документах глобального чи регіонального рівнів. Для прикладу, в керівництві [7] наводяться визначення понять «ІКТ», «забезпечення безпеки ІКТ», «конфіденційність», «цілісність», «доступність», «кіберпростір», «інформаційні ресурси», «кіберресурси ІКТ», «кіберсистеми інформаційних технологій», «кіберсистеми комунікаційних технологій», «критичність кіберсистем ІКТ» тощо. Цей документ фактично є компіляцією і консолідацією базових вимог міжнародних стандартів ISO/IEC 27001:2005, ISO/IEC 13335-4 та COBIT, у ньому виділено такі основні заходи захисту ІКТ: 1) організаційне керівництво та політика; 2) організація, культура та менеджмент; 3) людські ресурси; 4) фізична безпека та захист інформації від витоку в мережі; 5) функціонування системи ІКТ; 6) технічні засоби та інфраструктура; 7) придбання і розробка обладнання; 8) моніторинг і аудит; 9) дотримання вимог.

Постановка завдання

Таким чином, забезпечення захисту критичних авіаційних інформаційних систем (КАІС) від кіберзагроз є актуальним завданням, від розв'язання якого залежить безпека пасажирів, членів екіпажів та наземного персоналу, а міжнародний характер цивільної авіації робить це завдання загальнообов'язковим для кожної держави, яка є і хоче залишатись частиною міжнародної авіаційної спільноти. Проте, жоден із керівних документів щодо забезпечення захисту міжнародної цивільної авіації не містить повний перелік КАІС, їх функціональні особливості та рівень критичності – це значно ускладнює аналіз уразливостей таких систем, розробку моделей загроз та порушників, аналіз та оцінку ризиків, а також не дозволяє чітко формалізувати методи захисту КАІС від різного роду кіберзагроз. З огляду на це, **метою** цієї статті є пошук та систематизація сучасних авіаційних інформаційних систем (АІС), їх аналіз та виділення базових ознак для класифікації.

Основна частина дослідження

1. Інформаційні системи аеронавігаційного обслуговування

Критичними інформаційними системами аеронавігаційного обслуговування є всі наземні технічні засоби та обладнання зв'язку, навігації та спостереження для ОрПР (обслуговування повітряного руху, організації потоків повітряного руху та організації повітряного простору), а також засоби для обслуговування аеронавігаційною інформацією і метеорологічного забезпечення аеронавігації.

У результаті проведеного аналізу засобів та систем [14-18] до критичних інформаційних систем аеронавігаційного обслуговування можна віднести наступні:

1) Системи авіаційного електрозв'язку (Communication Systems): системи авіаційного повітряного електрозв'язку, а саме наземні засоби радіозв'язку «повітря – земля», в тому числі обладнання для передачі даних Controller-Pilot Data Link Communications (CPDLC) та Aircraft Communications Addressing and Reporting System (ACARS); системи та мережі авіаційного наземного електрозв'язку, а саме засоби проводового (оперативного і телефонного) та радіозв'язку «земля – земля», системи комутації голосового зв'язку, засоби радіорелейного зв'язку, мережа авіаційного фіксованого електрозв'язку (Aeronautical Fixed Telecommunication Network, AFTN), системи обміну повідомленнями обслуговування повітряного руху (Air Traffic Service Message Handling System, AMHS), мережі обміну даними; засоби авіаційного радіомовлення, а саме обладнання ДВЧ-радіомовних передач типів VOLMET, ATIS; системи авіаційного супутникового зв'язку; магістральні телекомунікаційні мережі.

2) Радіонавігаційні засоби забезпечення

польотів (Navigation Systems): ненаправлені радіомаяки (Non-Directional Beacons, NDB); всенаправлені радіомаяки (Very High Frequency Omni-Directional Range, VOR); далекомірні радіомаяки (Distance Measuring Equipment, DME); радіомаячні системи посадки (Instrument Landing Systems, ILS).

3) Системи спостереження (Surveillance Systems): первинні оглядові радіолокатори (Primary Surveillance Radars, PSR); вторинні оглядові радіолокатори (Secondary Surveillance Radars, SSR); моноімпульсні вторинні оглядові радіолокатори (Monopulse Secondary Surveillance Radars, MSSR); радіолокаційні комплекси у складі первинних та вторинних радіолокаторів (Radar Sites, PSR+ SSR); радіолокатори огляду льотного поля (Surface Movement Radars, SMR); метеорологічні радіолокатори (Weather Radars); мультилатераційні системи (Multilateration Systems, MLAT); наземні станції систем автоматичного залежного спостереження (Automatic Dependent Surveillance, ADS); автоматичні радіопеленгатори (Direction Finders, DF).

4) Системи обробки даних (Data Processing Systems): автоматизовані системи управління повітряним рухом (АС УПР) – системи, які складаються з апаратно-програмних засобів автоматизації процесів управління повітряним рухом і забезпечують оцінку та прогноз повітряного руху, підтримку прийняття рішень диспетчерами органів обслуговування повітряного руху та контроль їх реалізації; автоматизовані системи планування використання повітряного простору – системи, які складаються з апаратно-програмних засобів автоматизації процесів планування та координації використання повітряного простору; централізовані системи обробки та розповсюдження даних спостереження Європейської організації з безпеки аеронавігації EUROCONTROL (European Organisation for the Safety of Air Navigation), а саме ATM suRveillance Tracker And Server (ARTAS), Surveillance Data Distribution System (SDDS); системи обробки та передачі польотних даних, наприклад, EUROCONTROL Integrated Initial Flight Plan Processing System (IFPS); системи обробки та передачі аеронавігаційної інформації.

5) Системи метеорологічного забезпечення: система централізованого метеозабезпечення аеронавігації Украероруху; комплексні радіотехнічні аеродромні метеорологічні станції (КРАМС); супутникова система розповсюдження інформації для аеронавігації (Satellite Distribution System for Information Relating to Air Navigation, SADIS).

Найбільшої уваги необхідно приділити АС УПР (структурна схема відображена на рис. 1), яка є інтегруючою системою, що використовує системи спостереження (джерела інформації про повітряну обстановку), системи зв'язку (забезпечують передачу даних та голосовий зв'язок) та супутникові навігаційні системи (використовуються для синхронізації часу) і забезпечує обробку та відображення даних спостереження, польотних даних, аеронавігаційної та метеорологічної інформації, реалізує функції підтримки прийняття рішень.

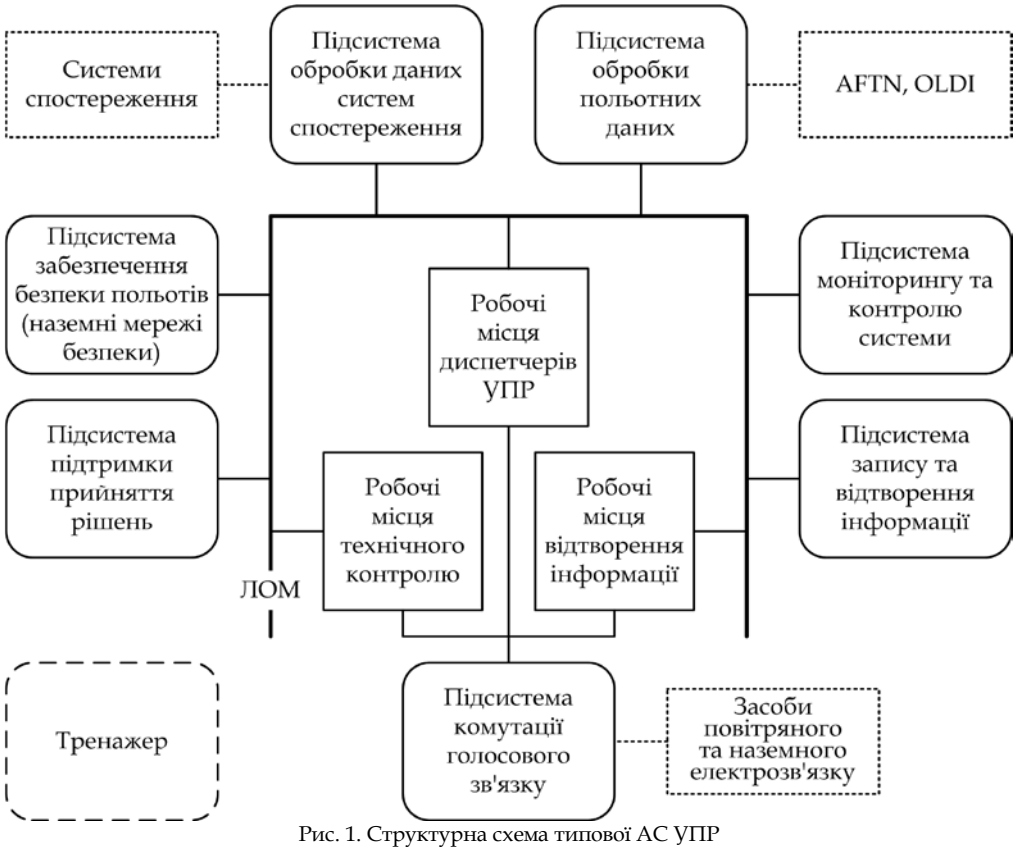

Рис. 1. Структурна схема типової АС УПР

Основними групами функцій АС УПР є: 1) обробка даних систем спостереження; 2) обробка польотних даних; 3) моніторинг повітряного руху, забезпечення безпеки польотів та підтримка прийняття рішень; 4) відображення та управління інформацією; 5) документування та відтворення інформації; 6) моніторинг та контроль системи; 7) забезпечення диспетчерів УПР авіаційним повітряним та наземним голосовим зв'язком; 8) відтворення та забезпечення функцій диспетчерського тренажера. Сучасні АС УПР будуються за модульною структурою з використанням локальних обчислювальних мереж (ЛОМ), до яких підключені підсистеми та робочі місця.

Відмова (несправність) інформаційної системи ОрПР є подією, пов'язаною із безпекою польотів у системі ОрПР (Air Traffic Management Safety Occurrence). За класифікацією відмова (несправність) обладнання є порушенням, тобто подією, можливими наслідками якої є авіаційна подія та інцидент (або надзвичайна подія), а також припинення (або затримка) приймання чи випуску ПС, порушення безпеки польотів, що сталися через відмову (несправність) наземних засобів радіотехнічного забезпечення польотів і авіаційного електрозв'язку. Виділяються порушення функції зв'язку (Failure of Communication function), порушення функції навігації (Failure of Navigation function), порушення функції спостереження (Failure of Surveillance function) та порушення функції з обробки даних та їхнього розповсюдження (Failure of Data Processing and Distribution function). Відповідно до регулятивних вимог з безпеки EUROCONTROL Safety Regulatory Requirements (ESARR) такі порушення є специфічними подіями при ОрПР (Air Traffic Management Specific Occurrences), які передбачають доповіді про них, аналіз та, за потреби, розслідування [19, 20].

2. Бортові інформаційні системи повітряних суден

В результаті проведеного аналізу систем та обладнання ПС [21] до критичних бортових інформаційних систем можна віднести наступні:

1) Система повітряних сигналів, яка вимірює та розраховує висотно-швидкісні параметри, а також температуру повітря, кути атаки і ковзання тощо.

2) Системи зв'язку, а саме бортові радіостанції, в тому числі обладнання для передачі даних CPDLC та ACARS.

3) Навігаційні системи:

– супутникові навігаційні системи (СНС);

– інерціальні навігаційні системи (ІНС);

– автоматичні радіокомпаси (АРК);

– радіовисотоміри (РВ);

– бортове обладнання системи VOR;

– бортові далекоміри;

– бортове обладнання системи ILS;

– допплерівський вимірювач швидкості та кута зносу;

4) Системи спостереження та попередження зіткнень:

– транспондери;

– бортові системи попередження зіткнень (ACAS/TCAS);

– системи раннього попередження небезпечних зближень із землею;

– бортові метеонавігаційні радіолокатори.

5) Обчислювальні системи літаководіння (Flight Management System, FMS).

6) Системи відображення інформації.

7) Автоматичні бортові системи керування.

3. Інформаційні системи авіакомпаній та аеропортів

До цієї категорії АІС, у першу чергу, відноситься ***система комп'ютерного бронювання (Computer Reservation System, CRS)*** – автоматизована система, що використовується для зберігання і отримання інформації та проведення операцій, пов'язаних з повітряним транспортом, бронюванням готелів, прокатом автомобілів, або іншою туристичною діяльністю [8]. З часом системи CRS почали використовуватись не лише авіаперевізниками, а й туристичними агентствами, а різке збільшення масштабів застосування цих систем призвело до трансформування абревіатури CRS в ***GDS (Global Distribution Systems) – глобальна система резервування (бронювання)*** (рис. 2), яка фактично представляє собою інформаційну систему, що дозволяє автоматизувати операції між третіми особами та агентами бронювання щодо забезпечення кінцевих користувачів сервісами, необхідними для подорожі (бронювання авіаквитків, готелів, оренда автомобілів тощо).

Рис. 2. Архітектура типової системи GDS

На сьогодні найбільш поширеними системами GDS є *Amadeus, Travelport GDS* (включає такі системи як *Apollo, Galileo* та *Worldspan), Sabre, TameliaRES, Avantik PSS, Abacus, AccelAero, Axess, Internet Booking Engine, KIU, Mercator, Navitaire, Patheo, Radixx, akeflite, Travel Technology Interactive, WorldTicket Sell-More-Seats, Сирена* та ін. Як альтернативу системам GDS розробники позиціонують Інтернет

системи бронювання (Internet Distribution Systems, IDS) чи альтернативні системи бронювання (Alternative Distribution Systems, ADS) [9], які з'явилися вкінці минулого сторіччя і мають цілу низку переваг над GDS системами. Основною перевагою IDS (ADS) систем є можливість їх використання кінцевим споживачем самостійно – тобто клієнт може, використавши один з порталів IDS (ADS), вибрати необхідний йому сервіс, забронювати його і отримати миттєве підтвердження на електронну пошту (для отримання ж сервісів GDS систем клієнт повинен звернутися до агентів авіакомпаній чи туристичних компаній). Найпопулярнішими системами IDS (ADS) є *Booking.com, Oktogo, Expedia.com, Orbitz.com, HRS.com, Travelocity.com, Hotels.com, Priceline.com* тощо.

Управління усіма системами он-лайн бронювання здійснюється через спеціальний інструмент Channel Management, що дає можливість: зберігати інформацію про всі бронювання у єдиному сховищі (екстранеті); доступу через Інтернет за допомогою мобільних пристроїв без попереднього встановлення будь-якого програмного забезпечення; інтегрування з модулями он-лайн бронювання та відомими системами менеджменту об'єктами на базі хмарних технологій (наприклад, Property Management Systems).

Іншим типом АІС у цій категорії є ***система взаєморозрахунків (Billing and Settlement Plan, BSP)*** – універсальна система, що покликана замінити індивідуальні схеми відносин агентів та перевізників [10]. Система BSP призначена для ефективної взаємодії учасників міжнародної організації IATA за рахунок консолідації інформаційних та фінансових потоків. Організація IATA надає агентам бланки квитків установленого зразка, після чого агенти мають можливість продавати квитки у власному офісі (без безпосередньої участі авіаперевізника). За продані усіма агентами квитки авіакомпанія отримує платіж через систему BSP. Агенти сповіщають про продажі і повернення вкінці звітного періоду в електронному вигляді через цілодобову он-лайнову систему BSPlink, розроблену IATA. Дані щодо угод передаються в центр обробки даних (Data Processing Centre, DPC) [10].

Крім того, важливу роль для суб'єктів цивільної авіації відіграють ***системи управління відправками (Departure Control System, DCS)*** – автоматизовані системи, що використовуються для управління інформацією на стійках реєстрації, друкування посадкових талонів, прийняття багажу, посадки, контролю завантаження ПС та його перевірок. До найбільш поширених на сьогодні систем DCS можна віднести *SITA* (рис. 3) [11], *TAIS* (рис. 4) [12], системи від *Amadeus, John Keells Computer Services, Hitit Computer Services* тощо.

Крім того, відповідно до [7], для більш ефективної оцінки захищеності та подальшої розробки методів і систем захисту суб'єктів цивільної авіації від кіберзагроз необхідно врахувати *портативні та непортативні електронні пристрої, що використовуються для обробки, збереження і передачі критично важливої інформації* (наприклад, настільні комп'ютери, портативні персональні комп'ютери, нетбуки, планшети, стільникові телефони, що базуються на мобільних комп'ютерних платформах, кишенькові комп'ютери, цифрові фотокамери та пристрої зберігання даних, включаючи пристрої зберігання даних з підключенням до універсальних послідовних шин і плати пам'яті).

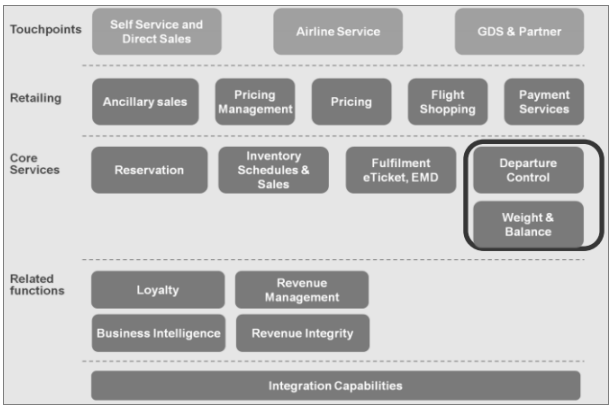

Рис. 3. Система DCS SITA у складі горизонтально орієнтованої системи обслуговування пасажирів

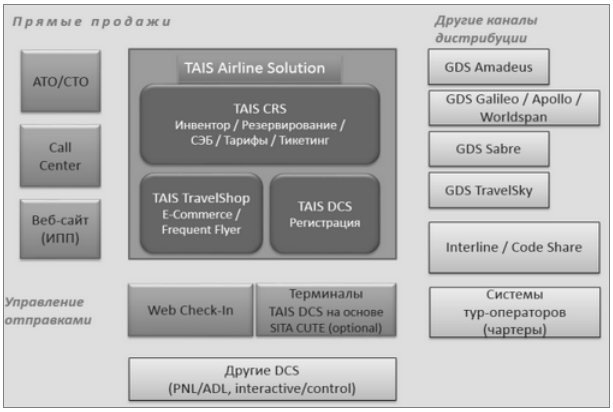

Рис. 4. Приклад застосування системи обслуговування пасажирів TAIS Airline Solution

4. Підходи до класифікації авіаційних інформаційних систем

Класифікація АІС може бути здійснена за такими ознаками: за призначенням; за розташуванням; за взаємодією наземних та бортових засобів; за розташуванням користувачів інформації; за рівнем інтеграції засобів та систем; за способом реалізації, за рівнем критичності.

1) За *призначенням* АІС поділяються на такі:

– для аеронавігаційного обслуговування та льотної експлуатації (інформаційні системи аеронавігаційного обслуговування, бортові інформаційні системи ПС);

– для виробничо-комерційної діяльності авіапідприємств (інформаційні системи авіакомпаній та аеропортів).

2) За *розташуванням* АІС поділяються на такі:

– наземні (наприклад, АС УПР, CRS, GDS);

– бортові (наприклад, FMS, ІНС);

3) За *взаємодією наземних та бортових засобів*

при здійсненні основних функцій АІС поділяються на такі:

– некооперативні (наземне та бортове обладнання не взаємодіє, наприклад, засоби проводового та радіозв'язку «земля – земля»);

– кооперативні (наземне та бортове обладнання взаємодіє, наприклад, вторинні оглядові радіолокатори та борові транспондери, системи авіаційного повітряного електрозв'язку у складі наземних засобів радіозв'язку та бортових радіостанцій).

4) За *розташуванням користувачів інформації* кооперативні АІС поділяються на такі:

– наземні: наприклад, вторинні оглядові радіолокатори;

– бортові: наприклад, засоби авіаційного радіомовлення;

– розподілені: наприклад, системи авіаційного повітряного електрозв'язку.

5) За *рівнем інтеграції засобів та систем* АІС поділяються на такі:

– неінтегровані;

– інтегровані у спеціальні системи або мережі;

– інтегровані у глобальні системи або мережі.

6) За *способом реалізації* АІС поділяються на такі:

– програмні;

– апаратні;

– програмно-апаратні.

7) За *рівнем критичності* АІС поділяються на такі:

– з високим рівнем критичності;

– з середнім рівнем критичності;

– з низьким рівнем критичності.

Для розрахунку критичності [22] АІС можна використати один з підходів, описаних у роботах [23-24] (наприклад, методи CHAZOP, PHA, HACCP, FMECA тощо).

Висновки

Таким чином, у цій роботі здійснено пошук та систематизацію сучасних АІС (поділено на три основні категорії: інформаційні системи аеронавігаційного обслуговування, бортові інформаційні системи повітряних суден, інформаційні системи авіакомпаній та аеропортів), проведено їх аналіз та виділено базові ознаки для класифікації. Отримані результати будуть використані у подальших роботах для розробки розширеної класифікації КАІС, а також методу визначення (розрахунку) рівня критичності АІС.

Література

[1] Гнатюк С.О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С.О. Гнатюк // Безпека інформації. — Том 19, №2. — 2013. — С. 118-129.

[2] Формирование организационно-правовой системы защиты национальной инфраструктуры от киберугроз / [Бик В.В., Климчук А.А., Панченко В.Н., Петров В.В.]. —К. : Академпресс, 2013. — 220 с.

[3] Харченко В.П. Кибертерроризм на авиационном транспорте / В.П. Харченко, Ю.Б. Чеботаренко, О.Г. Корченко, Є.В. Паціра, С.О. Гнатюк // Проблеми інформатизації та управління: Зб. наук. пр. : Вип. 4 (28). — К. : НАУ, 2009. — С. 131-140.

[4] Приложение 17 к Конвенции о международной гражданской авиации «Безопасность. Защита международной гражданской авиации от актов незаконного вмешательства». — Изд. 9. — 2011. — 60 с.

[5] Doc 30 «Политика ЕКГА в сфере авиационной безопасности» (Restricted). — Изд. 13. — 2010. — 138 с.

[6] Doc 8973 ICAO «Руководство по авиационной безопасности» (Restricted). — Изд. 8. — 2011. — 748 с.

[7] Doc 9985 ICAO «Руководство по безопасности системы организации воздушного движения» (Restricted). — Изд. 1. — 2013. — 174 с.

[8] Computer reservations system [Електронний ресурс]. — Режим доступу: https://en.wikipedia.org/wiki/Computer_reservations_system

[9] Системы GDS и ADS. Для кого и зачем [Електронний ресурс]. — Режим доступу: http://www.nbcrs.ru/gds_ads.html

[10] Billing and Settlement Plan (BSP) [Електронний ресурс]. — Режим доступу: https://www.iata.org/services/finance/bsp/Pages/index.aspx

[11] Departure Control Services. End-to-end solution for airline and ground handlers [Електронний ресурс]. — Режим доступу: http://www.sita.aero/globalassets/docs/use-cases/departure-control-services-use-case.pdf

[12] Система управления отправками TAIS DCS [Електронний ресурс]. — Режим доступу: http://tais.ru/solution/icarus/regina

[13] Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс]. — Режим доступу: http://zakon3.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

[14] Технические средства и системы для обслуживания воздушного движения: учеб. пособ. / [Быковцев И.С., Демьянчук В.С., Клименко В.А. и др.] — К: Украэрорух, 2012. — 508 с.

[15] Автоматизированные системы управления воздушным движением: Новые информационные технологии в авиации: учеб. пособ. / [Ахмедов Р.М., Бибутов А.А., Васильев А.В. и др.]; под ред. С.Г. Пятко и А.С. Красова. — СПб.: Политехника, 2004. — 446 с.

[16] Ground Based Surveillance Techniques [Електронний ресурс]. — Режим доступу: http://www.eurocontrol.int/articles/ground-based-surveillance-techniques.

[17] Правила технічної експлуатації наземних засобів радіотехнічного забезпечення в цивільній авіації України: затв. наказом Міністерства транспорту та зв'язку України від 08.05.2007, №381; зареєстр. в Міністерстві юстиції України 21.06.2007

за № 705/13972. [Електронний ресурс]. — Режим доступу: http://zakon3.rada.gov.ua/laws/show/z0705-07.

[18] Правила авіаційного електрозв'язку в цивільній авіації України: затв. наказом Міністерства транспорту України від 23.09.2003, № 736; зареєстр. в Міністерстві юстиції України 31.10.2003 за № 1001/8322. [Електронний ресурс]. — Режим доступу http://zakon3.rada.gov.ua/laws/show/z1001-03.

[19] EUROCONTROL Safety Regulatory Requirement (ESARR). ESARR 2 Reporting and Assessment of Safety Occurrences in ATM. - Brussels: EUROCONTROL, 2009. — 30 p.

[20] Положення про нагляд за безпекою польотів у системі організації повітряного руху: затв. Наказом Міністерства транспорту та зв'язку України від 31.05.2010, № 302.; зареєстр. в Міністерстві юстиції України 30.06.2010 за № 446/17741 [Електронний ресурс]. — Режим доступу: http://zakon4.rada.gov.ua/laws/show/z0446-10.

[21] Кучерявый А.А. Бортовые информационные системы: курс лекций / А.А. Кучерявый; под. ред. В.А. Мишина и Г.И. Клюева. — 2-е изд., перераб. и доп. — Ульяновск: УлГТУ, 2004. — 504 с.

[22] Сидоренко В.М. Сучасні підходи до виявлення та ідентифікації найбільш важливих об'єктів критичної інфраструктури / В.М. Сидоренко, С.О.Гнатюк, О.П. Дуксенко // Безпека інформації. — 2015. — №3(21). — С. 269-275.

[23] Харченко В.С. Комплексный анализ гарантоспособности информационно-управляющих систем и инфраструктур: FME(C)A-модели и информационная технология / В.С. Харченко, Ирадж Эльяси Комари // Проблеми інформатизації та управління: зб. наук. пр. — Вип. 1 (23). — К., 2008. — С. 92-97.

[24] Гнатюк С.О. Аналіз методів розрахунку критичності інформаційних систем / С.О. Гнатюк, Р.С. Одарченко, В.М. Сидоренко // Інтегровані інтелектуальні робототехнічні комплекси (ІНТК-2016) : IX міжнар. наук.-практ. конф., 17-18 травня 2016 р. : тези доп. — К., 2016. — С. 239-241.

УДК 004.056.5:343.326 (045)

Гнатюк С.А., Васильев Д.В. Современные критические авиационные информационные системы

Аннотация. *Проблема кибертерроризма носит глобальный характер и довольно остро стоит в современном информационном обществе. Ведущие государства мира все большее внимание уделяют киберзащите собственных критических информационных ресурсов в различных отраслях. В области гражданской авиации уровень критичности значительно усиливается повышенной степенью связности и взаимодействия между наземными системами и воздушными судами, а внедрение современных информационных и коммуникационных технологий с одной стороны повышает эффективность деятельности гражданской авиации, однако с другой стороны порождает целый ряд новых уязвимостей и потенциальных угроз. Кроме того, ни один из руководящих документов по обеспечению защиты международной гражданской авиации не содержит полный перечень критических авиационных информационных систем, их функциональные особенности и уровень критичности – это значительно усложняет анализ уязвимостей таких систем, разработку моделей угроз и нарушителей, анализ и оценку рисков, а также не позволяет четко формализовать методы защиты таких систем от различного рода киберугроз. В этой статье осуществлен поиск и систематизация современных авиационных информационных систем (информационные системы аэронавигационного обслуживания, бортовые информационные системы воздушных судов, информационные системы авиакомпаний и аэропортов), проведен их анализ и выделены базовые признаки для классификации. Полученные результаты будут использованы для дальнейшей разработки расширенной классификации и метода определения уровня критичности авиационных информационных систем.*

Ключевые слова: *кибербезопасность, критическая информационная инфраструктура государства, гражданская авиация, критическая информационная авиационная система, классификация.*

Gnatyuk S., Vasyliev D. Modern critical aviation information systems

Abstract. *The problem of cyberterrorism is global and quite acute in today's information society. Leading world states are increasingly focused on critical information resources protection in different spheres. In civil aviation criticality level is amplified by communication and interaction between ground systems and aircrafts. Modern information and communication technology implementation in one hand increases civil aviation operation efficiency and in the other hand generates a set of new vulnerabilities and potential threats. Besides no one aviation security control document doesn't include full list of critical aviation information systems, its functional features and criticality level. These make difficult the analysis of such systems, creation threat and intruder models, risk analysis and assessment and also not allow to formalize security methods against different cyberthreats. In the paper search and systematization of modern aviation information systems (information systems of aero navigation service, aircraft board information systems, information systems of air companies and airports) was carried out. Also critical aviation information systems analysis was fulfilled and basic features for its classification were defined. Given results should be used for further creation the extended classification and criticality level determining for critical aviation information systems.*

Key words: *cybersecurity, critical information infrastructure of the state, civil aviation, critical aviation information system, classification.*

Отримано *24 листопада 2015 року*, затверджено редколегією *14 березня 2016 року*