ENSURING EUROPEAN CIVIL AVIATION CYBERSECURITY

Sergiy Gnatyuk[1], Maksim Iavich[2], Giorgi Iashvili[2], Andriy Fesenko[3]
[1]National Aviation University, [2]Caucasus University, [3]Taras Shevchenko Kyiv National University

ABSTRACT. The criticality level of civil aviation (CA) information infrastructure is considerably amplified by high degree of connectivity and interaction between ground and aircraft systems. Malicious interference into mentioned systems puts at threats passengers, crew and ground staff security. Unauthorized access to so-called critical aviation information system (CAIS) is very crucial and it may have serious and tragic consequences. The control aviation security documents declare following requirements to ensure CAIS security against cyberthreats (potential cause of an unwanted incident, which may result in harm to a system, individual or organization – ISO / IEC 27032). Doc 30 declares that measures addressing cyberthreats to CA have been included in the National Civil Aviation Security Programme, the National Quality Control Programme and the National Civil Aviation Security Training Programme. Similar requirements are declared in Annex 17 to Chicago Convention on International Civil Aviation, Doc 8973 as well as in Doc 9985. However, there are still a lot of unsolved problems related to CAIS identifying, its criticality assessment and development of methods to provide its cybersecurity. From this viewpoint in the paper integrated complex approach to provide CA cybersecurity was proposed.

KEWORDS: cybersecurity, critical information infrastructure, European civil aviation, complex information security system, critical aviation information system

Introduction

Cyberterrorism evolution (since the birth of computer technology in the 1960s) shows that attacks in cyberspace [1] today have a strong political overtones and more evident in cybernetic influence on international level. Only the first half of 2014 may be noted such cyberincidents: hackers broke into the Schengen Information System; powerful DDoS attack focused on 3 biggest NATO sites (http://ccdcoe.org/, http://nato.int/ & http://nato-pa.int/) from pseudo-Ukrainian groups named «CyberBerkut» & «Anonymous Ukraine»; cyberattacks on Ukrainian Cabinet of Ministers, Prosecutor General's Office of Ukraine & National Security and Defense Council of Ukraine; 1.3 millions of big communication operator Orange France were victims of cyberattack focused on their personnel data; Russia launched large-scale cyberwar against Ukraine, it is bound to the revolutionary events and carries political overtones to destabilize the situation in the state and the violation of its sovereignty & integrity; powerful DDoS attacks from Russian Federation territory on Ukrainian Central Election Commission in preparation and voting in Presidential election.

Cyberattacks and acts of cyberterrorism are very crucial for critical infrastructure of any state (Fig. 1), because these may have serious and tragic consequences. For instance in Civil Aviation (CA) any unauthorized access to control system calls into shot hundreds and thousands of passengers' lives. CA is moving away from traditional radar systems in favor of more modern digital tools connection – the problem is that new technologies potentially allow attackers get stuck between the pilot and dispatcher. The guidance aviation security documents declare following requirements to ensure cybersecurity [1].

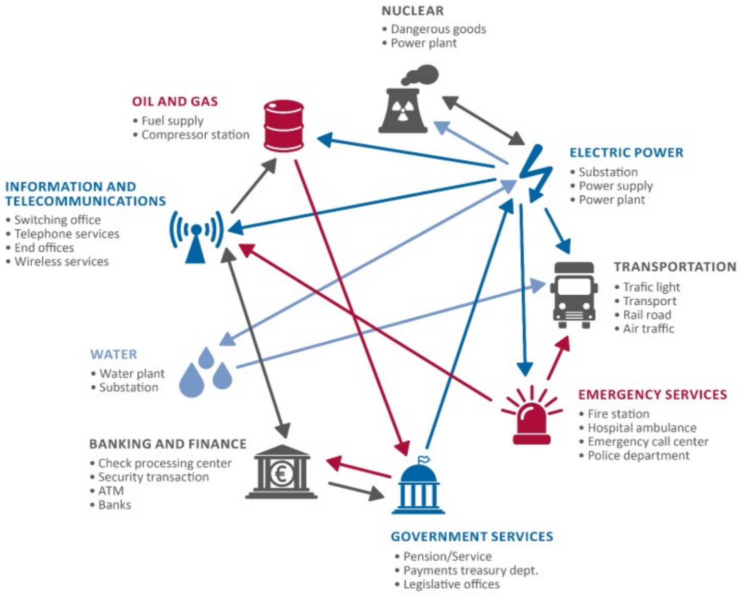

Fig.1. Critical infrastructure in accordance to ENISA

European and world requirements for CA cybersecurity

ECAC Doc 30 [2] declares that measures addressing cyber threats to CA have been included in the National Civil Aviation Security Programme, the National Quality Control Programme and the National Civil Aviation Security Training Programme. A set of security control consists of below measures [2]:

1) Implementation of effective measures to protect Critical Aviation Information Systems (CAIS);

2) Including the CAIS in their threats assessment processes;

3) Separating the CAIS networks from public;

4) Responsibility for securing CAIS is allocated by operators to a properly selected, recruited and trained individual;

5) Security measures are considered in the design, implementation, operation and disposal of new CAIS;

6) Supply chain security measures for hardware and software should be applied to CAIS;

7) Remote access to CAIS is only permitted under pre-arranged and secure conditions;

8) Cyber attack incidents must be recorded for future evaluation and counter & preventive measures efficiency increasing.

It is also worth noting that the most comprehensive list of measures to mitigate cyberthreats' negative influence on CAIS there is in ICAO Doc 8973 [3]. Among them is noted as follows: 1) Administrative Measures; 2) Virtual (Logic) Control Measures; 3) Physical Controls. Besides this document, also focuses on CAIS: security by design, networks separation & secured remote access for legitimate users, supply chain security & cyber attack incidents records [3]. Despite the examples of the last cyberattacks and requirements of guidance aviation security documents, the main purpose of this paper is offer an integrated complex approach to provide CA cybersecurity.

Basic issues of cyberspace security

Modern threats to information security (cybersecurity) [4] characterizes of asymmetric and flexibility. Cyberattacks has long ceased to be an end in itself and become an effective means to achieve a wide range of purposes; their variety is limited only by the imagination and fantasy of violator. All existed cyberattacks can be differentiated into 3 categories: attacks adversely affecting on confidentiality, integrity and availability on the information. All other types are derived from these. By the way, confidentiality, integrity and availability (so-called CIA-triad) are the main features of information security (and consequently cybersecurity).

In [2] cyberspace was defined as the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form. Multi-criteria analysis was carried out and the following conceptual definitions were proposed [4]: *Cyberspace* is virtual space resulting from the interaction of users, software, hardware and network technologies (including Internet) for information (electronic information resources) transformation processes on purpose of ensuring the information needs of society. *Cyberterrorism* is kind of terrorism that is a conscious and purposeful application of information system resources to implement terrorist acts in cyberspace and also to achieve other related purposes in terrorist groups' interests. *Cyberattack* is attempt or realization of security threats in cyberspace aimed at its components (in particular confidentiality, integrity and availability) considering its vulnerabilities.

Complex approach to provide European CA cybersecurity

Considered examples of cyberattacks and acts of cyberterrorism are very crucial for critical infrastructure of any state, because these may have serious and tragic consequences. For instance in CA any unauthorized access to control system calls into shot hundreds and thousands of passengers' lives. CA is moving away from traditional radar systems in favor of more modern digital tools connection – the problem is that new technologies potentially allow attackers get stuck between the pilot and dispatcher.

As well many tools to take control of aircraft in the air were created and tested successfully. During The Fourth HITB Annual Conference (was held in Amsterdam, 2013) the practical demonstration on how to remotely attack and take full control of an aircraft was carried out. The attack performed will follow the classical methodology, divided in discovery, information gathering, exploitation and post-exploitation phases. The complete attack will be accomplished remotely, without needing physical access to the target aircraft at any time, and a testing laboratory will be used to attack virtual airplanes systems. ADS-B (Automatic Dependent Surveillance – Broadcast) and ACARS (Aircraft Communications Addressing and Reporting System) protocols will be used during the discovery and information gather phases, but none of those protocols are the objective of this research, I will just use them to plot and analyze the potential targets. Very basic information on such protocols will be displayed as well as additional references for further reading. The real target of the attacks will be some on-board systems, complex enough to be vulnerable to (almost) common vulnerability research and exploitation techniques. Different post-exploitation vectors will finally be considered in order to gain better aircraft control.

Today we know many examples of attacks to CA throughout the world (e.g. Malaysia, Turkey et al), but most of these cases are not advertised. This is the purpose of hidden blocking vulnerabilities, but appearance of unwanted consequences can make the world community in a loud voice to talk about cyberterrorism in aviation and respond in the short term.

The cybersecurity will be successful only if a comprehensive approach to building a system of CAIS security (Fig.2). That's why Ukrainian complex approach includes a set of organizational and engineering measures that are intended to secure from disclosure, leakage and unauthorized access.

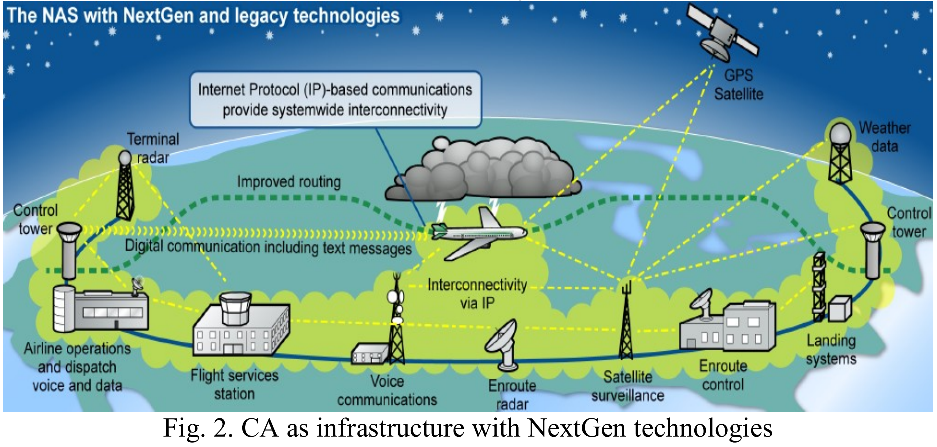
The NAS with NextGen and legacy technologies
GPS Satellite
Internet Protocol (IP)-based communications provide systemwide interconnectivity
Terminal radar
Weather data
Improved routing
Control tower
Control tower
Digital communication including text messages
Interconnectivity via IP
Airline operations and dispatch voice and data
Flight services station
Voice communications
Enroute radar
Satellite surveillance
Enroute control
Landing systems

Fig. 2. CA as infrastructure with NextGen technologies

Let's look at stages of *CAIS' complex information security system (CISS)* development in detail (steps from 1st to 13th):

1. Documents Preparing. At this stage, the project of documents is prepared that defines the organizational component of the system (the order project of CISS creation, the condition project of Information Security (IS) service, projects on job descriptions, procedures etc.) that are approved by the administration. It can be also created an IS service or appointed persons who are entrusted to ensure IS and control over them. Responsibility relies on the owner of the system.

2. Audit. The following documents are developed: the Certificate of CAIS inspection (contains the description, principles of CAIS construction and architecture); the list of CAIS objects which require protection. During the CAIS inspection should be analyzed and described: the general block diagram and structure (the list and structure of the equipment, technique and software, their communication, features of configuration, architecture and topology, program and hardware-software IS means, mutual arrangement of means etc.); types and characteristics of liaison channels; interactive features of separate components, their mutual influence in private; possible restrictions etc. Such characteristics of the physical environment are a subject matter of the analysis: territorial arrangement of CAIS components (the general plan, the situational plan); availability of territory protection and facility access procedure; the influence of environment factors, protection from the means of technical investigation; availability of communication elements, life-support systems and communications, which have an output for borders of a controllable zone; availability and characteristics of grounding systems; storage conditions of magnetic, paper and other data carriers; availability of the design and operational documentation on components of physical environment.

3. Threats & Violator Model Development. Using the information which is presented in the Environment Certificate of Inspection of CAIS operation, the potential threats to the data are defined. There is a research of some possible ways for CAIS data threats realization that is: outflow channels; special purpose channels & unauthorized data access methods. The results of Environmental Inspection of CAIS operation affirm the list of protection objects, as well as potential data threats are defined and the model of threats and violator model are developed. Model of threats (threats model) is the abstract formalized or unformalized methods and means description of threats realization. Violator model is the comprehensive structured characteristic of the perpetrator which is used together with the threats model for development of IS policy. On what information properties violation or CAIS threat is directed: confidentiality violation, integrity violation, data availability violation, surveillance and management of CAIS violation.

4. Security Policy Development. Security policy is a set of requirements, rules, restrictions, and recommendations etc. which regulate the data processing order and directed on IS from the certain cyber threats. Security policy offers the following guarantees: a) It is provided an adequacy of IS level to a level of its criticality in CAIS; b) Realization of IS measures profitability; c) In any environment of CAIS operation the assessment and testing are provided; d) Personification of security policy positions is provided, the reporting (registration, audit) for all critical from the security point of view resources to which an access is provided during CAIS operation; e) The personnel and users are provided with the Full Documentation Set according to the IS support; f) Critical from the point of view of IS CAIS technologies (function) have all corresponding support plans of continuous work and its renewal in case of unforeseen situations.

5. Technical Specification. The main stages of technical specification formation: a) Classification and description of CAIS resources; b) Development (design) of an information model for existing CAIS, information CAIS flows, interfaces between the user and CAIS etc; c) A list of threats and possible channels of information leakage determination; d) Expert Assessments of expected loss in case of threats; e) Identification of security services; f) Requirements identification for organizational, physical and other protective measures implemented in addition to the complex software and hardware protection; g) Requirements identification for metrological work; h) Models identification that is designed, and technological stand; i) Cost-efficiency assessment of selected assets; j) Making the final decision on the CISS content.

6. Technical Project. CISS technical project is developed on founding and in accordance with technical specification on CISS creation. In the process of CISS project (design) development there are proved and designed decisions which give an opportunity to realize technical specification requirements, to provide compatibility and co-operation of different CISS components, and also different measures and technical specification methods. A technical project on CISS creation includes: a) Development of general design decisions necessary for realization of technical specification on CISS requirements; b) The decision on CISS structure, operation algorithms and conditions of use of defense (security) facilities; c) The decision on CISS architecture and implementation mechanism, defined by a functional structure of IS services; d) Procedure description of technical events on support of CISS development sequence, architecture, tests, the operational environment and CISS documentation according to the set of realization guarantees of security services; e) Development, registration, coordination and the documentation affirmation corresponding to the technical specification size, on CISS; f) Documentation development on IS resources supply and-or technical requirements on their development; g) Preparation and documentation registration on security means deliveries or production containing them in the structure, for CISS complete set (configuration); h) Development, registration and the affirmation of working and operational CISS documentation and, if necessary, its separate component parts.

7. IS Plan. At this stage it is required to realize organizational, primary, technical and basic technical measures of restricted access IS, to establish required IS zones, to lead certification of technical equipment of an information activity support, IS means, workplaces (facilities) according to the IS requirements.

8. Operational Documentation. At this stage there is a development, registration and the affirmation of working and operational documentation and, if necessary, its separate parts. The working documentation contains detailed decisions on CISS design realization, maintenance of CISS management and interaction of its components, and also the necessary documentation for testing, carrying out of starting-up and adjustment works, carrying out CISS tests.

9. CISS Implementation. Implementation of organizational IS measures in CAIS provides: work on administrative documents preparations which regulate an activity of CISS support; compiling of instruction to person who participates in processing or IS in CAIS according to the list specified in the project on CISS; completion of work and the affirmation of documents which are included into IS plan in CAIS except those documents for which the results of the following stages are necessary. Commissioning works, according to the requirements of the preliminary CISS design in CAIS, provide installation, initialization and testing the work ability of CISS. Installation and initialization of CISS, which has the expert conclusion about its compliance with the requirements of normative documents, is carried out in accordance with the procedure specified in the maintenance documentation for this complex.

10. Preliminary Tests. The purpose of the preliminary tests is checking the work ability of the CISS and possibility of taking it to the research operation. The CISS work ability and its compliance with technical specification requirements is checked during the tests. Preliminary tests are carried out according to the program and test methods. Developer of the CISS prepares program and test methods and the customer agrees CAIS. Results of the preliminary tests are reiterated in «Protocol Testing», which contains findings regarding the possibility of taking CISS in research operation (exploitation), as well as a list of identified weaknesses, the necessary measures for its removal, and recommended time for doing these tasks.

11. Research Operation. During research operation of the CISS: a) Technologies of information processing, a turnover of machine data carriers, management of security means, access differentiations of users to CAIS resources and the automated control over users' actions are examined; b) Employees and IS users get practical skills with the help of technical and hardware-software IS means, study conditions of organizational and administrative documents concerning access differentiation to technical means and information resources; c) Performing (if necessary) the revision of the software, additional tuning and configuration. According to the results of the arbitrary shape work the report on completion of the research is operation drawn up, which includes the conclusion on the possibility (impossibility) of CISS representation on the public examination.

12. Public Examination. Public examination of the CISS is a separate step of acceptance tests of the CAIS. Public examination is conducted to determine CISS conformity with the requirements of normative documents on IS and its possibility of introducing CISS consisting of CAIS in the operation (exploitation).

13. CISS Support. CISS support contains (accordantly IS plan and operational documentation): warranty & after sales technical service.

Conclusions

Accordingly in this paper, based on guidance aviation security documents and analysis of last attacks in cyberspace, the complex approach to ensure CA cybersecurity was offered. It consists of 13 steps (from documents preparing to exploitation and support) and its implementation can allow to provide an effective cybersecurity of CAIS as well as European CA.

References

1. ISO/IEC 27032, Information technology – Security techniques – Guidelines for cybersecurity, 2012, 50 p.
2. ECAC Policy Statement in the Field of Civil Aviation Security, 13th edition, 2010, 138 p.
3. Doc 8973, Aviation Security Manual, 10th edition, ICAO, 2017, 808 p.
4. S. Gnatyuk, Critical Aviation Information Systems Cybersecurity, Meeting Security Challenges Through Data Analytics and Decision Support, NATO Science for Peace and Security Series, D: Information and Communication Security. – IOS Press Ebooks, Vol.47, №3, pp. 308-316, 2016.