Structure of protected system for collecting, storage and processing of telemetry data

V.V. Berkholts[1], A.I. Frid[1], M.B. Guzairov[1], A.D. Kirillova[1]

[1]Ufa State Aviation Technical University, K. Marks St. 12, Ufa, Russia, 450008

Abstract. The issues of improving the security of the modular system for collecting, storing and processing telemetric information on the state of the onboard subsystems of the aircraft in automatic mode are considered. It is based on an analysis of the use of modern technologies for the protection and processing of telemetric information to ensure certain aspects of the guaranteeability of the system as a whole.

1. Introduction

Emerging malfunctions and pre-failure states of the onboard equipment of the aircraft can be diagnosed based on telemetric information (TMI). This allows the specialists of ground technical services to plan repair and preventive measures based on an assessment of the current state of the equipment. Accumulated and processed TMI will allow specialists of the manufacturer to provide reasonable support to engineers of ground services in making decisions in case of technical failure of the blocks and modules of the aircraft. TMI analysis will improve the operational efficiency of the aircraft in case of any malfunctions and attacks by intruders.

The aim of the study is to increase the security of the system for collecting, storing and processing TMI on the state of the onboard aircraft subsystems in automatic mode. It is based on an analysis of the use of modern (including intellectual) technologies for the protection and processing of TMI.

To achieve this goal, a structural diagram of a protected system for collecting, storing and processing telemetric information on the state of the aircraft subsystems on the basis of a modular principle has been developed.

2. Analysis of the problem of secure collection, storage and processing of TMI in a geographically distributed information system

The proposed automated information system (AIS) of ground maintenance services is a set of software and hardware. They are necessary for the reception, storage and processing of information about the parameters of the state of complex technical products (CTP) on the aircraft. AIS is a geographically distributed system that combines the infrastructure of the information systems of ground-based maintenance stations and the information system of the manufacturer through secure communication channels. Preparation TMI realized by reading a status log for CTP aircraft during inspection and maintenance at ground stations via wireless and / or wired sensor networks.

The dependability of the TMI transmission systems with an aircraft allows for a comprehensive solution of the tasks of ensuring reliability, fault tolerance, availability, security, maintainability, and observability. An urgent task is to build a hierarchy of models that allow a comprehensive assessment of various aspects of the TMI transmission system and the development of a methodology for assessing the integral indicator of the system's guaranteed performance.

Ensuring the availability of TMI transmission systems is the primary task of ensuring the effective functioning of the aircraft (LA). The volume of TMI collected is significant. It is an incentive for the development of the concept of the industrial Internet of things (IIoT). It is a promising platform for use in solving such problems [1]. For example, a jet airliner demonstrated at the Bombardier Paris Air Show, whose engine is equipped with more than 5,000 sensors that generate up to 10 GB of data per second. One twin-engine aircraft can generate up to 844 TB of data average in 12-hour flight [2].

The ability to transfer TMI about the actual state of individual modules during operation and the entire LA equipment complex in real time to the manufacturer of aeronautical engineering components will improve the operational efficiency of the aircraft in its normal state and in the event of malfunctions and attacks by intruders when investigating incidents. Thus, a study of ground-to-air communication systems showed that ACARS, despite its versatility and widespread use, is vulnerable, and if hacked in conjunction with ADS-B, an attacker can gain access to the flight control system, download flight plans and detailed commands [3].

Ensuring the availability of telemetry information on the state of the aircraft

An automated information system (AIS) of ground maintenance services is a set of software and hardware. They are necessary for receiving, storing and processing information on the technological parameters of complex technical products (CTP) on board the aircraft.

A review of the main approaches to the relevance of the problem of ensuring the reliability of such systems is considered in the works of the authors [4, 5, 6]. AIS solves the main problems associated with the reception of TMI on the state of the onboard aircraft systems. The main methods of obtaining data are presented in the figure (Figure 1):

1. Directly from the CTP
2. By means of reading devices of the event log from the sensors of modules CTP. When carrying out technical inspection and maintenance, devices of this type read and store data on the state of the modules throughout the entire previous period of operation [5].
3. Entering events into the database manually. The operator processes the information and enters the information through the WEB application [4].

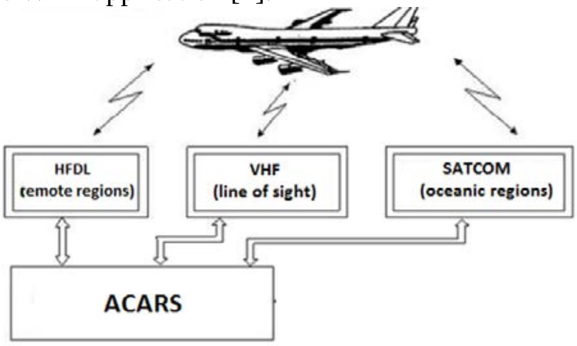

Figure 1. Methods for obtaining TMI.

In the first case, telemetry information is transmitted from the aircraft through a radio channel. To create a transmission channel, the following approaches can be used:

- Communication satellites (IRIDIUM, SATCOM).

Existing telemetry data transmission technologies use satellite communications. For example, the GE Aviation concern, producing aircraft engines, transmits telemetry from the aircraft in this way.

The obvious disadvantage of such way of transfer is its high cost. Streaming telemetry information involves the transfer of significant amounts (gigabytes) of data sent. The second disadvantage is the low noise immunity of the satellite communication channel. Incorrectly transmitted data can serve as a signal for a false alarm, or there is a chance to miss a system failure.

- Channel of wireless high-speed data transmission LTE and LTE-a.

Air to ground (A2G) LTE is capable of providing data rates of up to 75 Mbps for ground-to-air communications and up to 25 Mbps for air-to-ground communications at distances of 100 kilometers and speeds of 1,200 kilometers per hour using licenses. FDD 2x15 MHz. The standard 4G LTE can be used for continental flights, developed by Nokia.

Despite the currently available satellite and hybrid A2G systems, there is still no low-cost, high-throughput solution for broadband in-flight.

Thus, none of these technologies has no set of properties that allow for continuous broadcast telemetry data. ACARS does not allow to transfer a large amount of accumulated data, satellite communication is too expensive, and LTE-A is still at the development and implementation stage, and in the future it will cover only the continental part of flights.

Moreover, the current TMI transmission and processing systems demonstrate vulnerabilities that allow an attacker to gain access not only to passenger and airline data, but also to significantly affect flight parameters.

In the second and third cases, the information enters the database through a WEB application, which is an insulating layer between external networks and the internal structure of the AIS, since access from the external network is one of the most vulnerable points of the system. Improving the security of access to the database (DB) containing critical information about the product in use is based on the development of the architecture of a secure WEB application that acts as an insulating layer for external AIS clients, which allows for the possibility of transferring and analyzing ground-based service points from the aircraft and provide the ability to remotely access the necessary data. The architecture of this solution is presented in [5].

Preventing the appearance of vulnerabilities in the WEB application was carried out by implementing measures to develop secure software established by GOST R ISO / IEC 12207. Modeling security threats and identified vectors of possible attacks, as well as analyzing them, made it possible to formulate countermeasures for each of the vectors at different architectural levels WEB-applications. However, the analysis of the security of the entire TMI transmission system requires advanced modeling and the construction of a detailed model of interaction between the onboard information system of the aircraft and the ground-based AIS.

The growth of telemetry information forces the aviation industry to consider new approaches to the collection and analysis of a large amount of data on the state of individual components and elements of the aircraft. The concept of the industrial Internet of Things is being actively developed - an expanded network consisting of a large number of devices equipped with a set of sensors that communicate with each other through low-power and short-term wireless connections. The first step is to collect data from the sensors. One of the most promising solutions is a protocol with low power consumption and small radius of IEEE 802.15.4 IEEE 802.15.4e transmission. Short range is sufficient for data transmission within the ground service station. The IEEE 802.15.4 and IEEE 802.15.4e protocols and their architecture layers comply with IETF standards.

The question of analyzing the security of the system for collecting, transmitting and receiving telemetry information about the state of individual elements of the onboard aircraft systems during data transmission over the first two channels remains open.

The decomposition of the TMI transfer in the form of a hierarchical model of interacting levels of collecting, transmitting and analyzing information with the corresponding protocol stack is the basis for analyzing and building a system for analyzing the transmission system security (Figure 2).

In recent years, satellite communication systems in accordance with the Regulations of the International Telecommunication Union (ITU) are switching to a higher-frequency Ka-band (15.40-26.50 and 27.00-30.20 GHz).

The grouping of satellites in geostationary orbit and ground control centers make it possible to form a network infrastructure with high reliability indicators and the possibility of building distributed state networks. Channels of transmission of such networks provide a fairly high level of encryption and data protection.

Transmission of information in such networks is characterized by a low level of errors - no more than one per 10 million transmitted information bits and reliable operation - up to 100 thousand hours. The speed of work on the satellite channel is from 16 Kbps to 10 Mbps and more, which is comparable with the data transfer rate in the terrestrial channel.

The main methods for ensuring the security of telemetry information transmission in a wireless satellite channel is the use of software and hardware means of information protection. Widely used standards for secure protocols IPsec.

IPsec protocol (set of protocols) provides:

- integrity of the virtual connection, authentication of the source of information using the AH protocol (Authentication Header);
- encryption of information transmitted via the ESP (Encapsulating Security Payload) protocol;
- initial connection setup, mutual authentication and confidential key exchange.

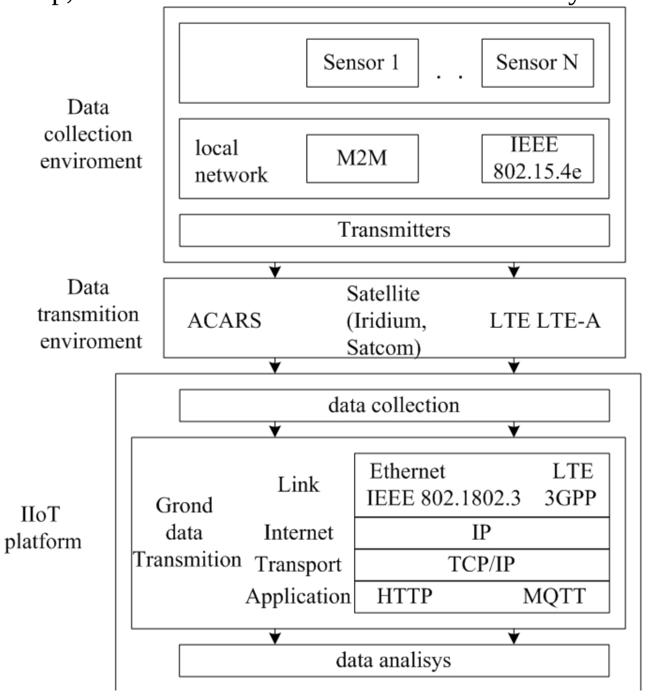

Figure 2. Extended scheme of data transmission from the aircraft.

At present, modern bilateral satellite communication networks use coding systems at the software and hardware level, which makes the interception and decoding of information over the radio channel almost impossible.

All data transmitted via satellite channel pass through a multi-stage system of transformation and encryption. The result of this:

- application of proprietary data encryption algorithms;
- terminal authentication when it is registered on the operator’s network (hardware key);
- encryption of both the entire session (software key) and each session separately (session keys);
- application of proprietary algorithms for converting source data into internal data formats (structures), which are then transmitted via satellite channel; thus, the tasks of additional protection of information, delivery of service information and error correction are solved;
- in the created virtual channels, source data in TCP sessions are grouped, compressed, and prioritized.

Satellite channels in the direction from LA to TMI processing centers are reverse satellite channels. Currently, the most common ways of functioning of transmitters in such channels are the principles of access with time-frequency division of TDMA / FDMA channels. Each reverse channel is located in a certain frequency range or has a carrier with frequency modulation and with a given coding algorithm for detecting and correcting errors of transmitted data - Turbo Coding.

To transmit TMI from the aircraft, it is necessary to provide a mechanism for changing the frequencies of the carrier reverse channels, which makes it much more difficult to intercept the transmitted data.

Data encryption in the satellite channel is carried out with the participation of both satellite terminals on board the aircraft and specialized high-performance servers at the TMI ground collection station. The server of the ground station for collection and processing of TMI hosts a secure database of encryption keys and session keys of all satellite terminals. In order for the aircraft board to operate in the transmission network, the information in the key database must match the hardware onboard key.

Telecommunications systems using the UMTS (Universal Mobile Telecommunications System) standards are third-generation mobile communication systems - 3G. For mobile communication of the third generation, the decimeter frequency band is used (about 2 GHz), and data transmission is provided at a speed of 2 Mbit / s.

All information security threats in the UMTS network can be distributed depending on the location of the impact of their respective attacks:

- on the radio access area (radio interface);
- on other parts of the network.

The radio section between the aircraft and the service network is one of the most vulnerable points of attack in UMTS. The threats related to this site and described below are divided into the following categories:

- unauthorized access to data;
- threats to data integrity;
- “denial of service”;
- unauthorized access to services.

Below are tables with descriptions of information security threats. The accepted designations of the threat TAn correspond to: T - the first letter of the English word "threat" (threat): A - the number corresponds to the number of the threat group (table number); n - the letter corresponds to the ordinal number of the threat in the threat group (in accordance with the list of threats in the ETSI document.

Table1. Describes some of the threats to unauthorized access to data on the radio site.

Threat designation	Threat name	Threat description
T1a	Interception of user traffic	Violators can intercept user traffic
T1b	Interception of alarm and control data	Violators can intercept alarm data and control data
T1c	Masking as a participant	Violators can be disguised as a network element
T1d	Passive traffic analysis	Violators can monitor the characteristics of messages
T1e	Active traffic analysis	Violators can actively initiate a connection and then access information

Table 2. Threats to the integrity of information.

Threat designation	Threat name	Threat description
T2a	User traffic manipulation	Violators can modify, insert, repeat or destroy user traffic. This manipulation may be accidental or intentional.
T2b	Alarm data manipulation	The intruder can modify, insert, repeat, or destroy alarm or control data.

Table 3. Denial of service threats.

Threat designation	Threat name	Threat description
T3a	Physical intervention	Violators can physically interfere with the transmission of user traffic, signaling data and control data.
T3b	Protocol Intervention	Violators may introduce special protocol failures.
T3c	Denial of service due to masking as a participant in communication	Violators may refuse to serve a legitimate user.

Table 4. Threat of unauthorized access to services.

Threat designation	Threat name	Threat description
T4a	Masking as another user	The intruder is disguised as another network user. First, the intruder is disguised as a base station with respect to the user.

3. Threats related to attacks on other parts of the system

Although attacks on a radio channel represent the most serious threats, attacks on other parts of the system also require analysis from the point of view of information security.

Table 5. Threats to unauthorized access to data.

Threat designation	Threat name	Threat description
T5e	Unauthorized access to data on the system object	Violators (by physical influence or logical control) can gain access to local or remote data.
T5f	Compromising information about the location	A legitimate user of a UMTS service may obtain information about the location of other users of the system
T6c	Manipulation of masking as a communication partner	Violators can be disguised as a network element in order to modify, insert, repeat or destroy traffic
T6f	Manipulation of data on the objects of the system	Violators can modify, insert, destroy data that is contained in the objects of the system.
T7a	Physical intervention	Violators may interfere with transmission on any system interface (wired or wireless). For example, the physical method of an obstacle on a wired interface could be a broken wire.
T7b	Protocol intervention	Violators can interfere with the transmission of user traffic or signaling data on any interface of the system (wired or wireless) or by signaling the protocol to fail.
T7c	Denial of service by masking communication partners	Violators can deny service to users by impeding the transmission of user traffic and signaling data, controlling them by blocking as a result of masking as a network element.
T7d	Incorrect use of emergency services	Violators can interfere with access to the services of other users and at the same time cause disruption of the equipment to perform functions in emergency situations.
T8a	Disagreement with the submitted invoice	Disagreement with the submitted invoice. This may be expressed in the refusal of the service or in the refusal that the service was actually provided.
T8b	Failure of user traffic source	The user can refuse to send traffic.
T9a	Custom masking	Violators can introduce themselves as a user in order to use the authorized services of this user. The intruder was able to get this opportunity from other objects such as the serving network, home environment and even the user himself.
T9b	Masking under the serving network	Violators can introduce themselves as a service network or part of a service network infrastructure.
T9c	Home environment masking	Violators can introduce themselves as a home environment in order to obtain information that enables them to disguise themselves as users.
T9d	Misuse of user priorities	Users may misuse their assigned priorities in order to gain unauthorized access to services or simply use their subscription intensively for free.
T9e	Incorrect use of serving network priorities	Service networks may misuse their priorities to gain unauthorized access to services.

Table 6. Threats related to attacks on the terminal and UICC / USIM.

Threat designation	Threat name	Threat description
T10h	Masking to receive data on the UICC interface - terminal.	Violators can be disguised as USIM or a terminal in order to intercept data on the interface of a UICC terminal.
T10j	Confidentiality of certain user data in the terminal and UICC / USIM	Violators may wish to gain access to personal user data stored in the terminal or UICC, for example, the telephone book of interacting subscribers.
T4a, T9a, T9c	It must be possible to prevent unauthorized access to 3G services by disguising themselves as legitimate users.	Requirements for security access to service.
T4a, T8a, T9d, T9e	An alarm should be provided to the provider informing him of the security event. Provide service providers with the ability to authenticate users upon request and during the provision of the service.	Security Requirements
T7b, T7c	Protection against unauthorized modification of user traffic should be provided.	System integrity requirements
T7a, T7b, T7c	Protection against unauthorized modification of certain signaling and control data must be provided.	System integrity requirements
T1a, T1b	The user should be provided with the ability to verify that his traffic and information about his calls are confidential.	Personal data protection requirement
T10h, T10k	It should not be possible to access USIM data that is intended for use only within USIM, such as authentication keys and algorithms	USIM security requirement

4. Development of a block diagram of a secure system for collecting, storing and processing telemetric information on the state of the aircraft subsystem

The generalized structure of a geographically distributed hierarchical system for the collection, storage and processing of TMIs arriving from airplanes based on ground maintenance stations is presented in Figure 4.

The creation of a secure channel through global communication networks and the transfer of TMI to a part of the AIS EM is realized at the transmission level of accumulated data. Organization levels of reception and distribution of information at the enterprise are realized according to the three-layer CISCO model. There is a level in the corporate information network of EM. It includes subsystems for storage and processing of TMI. Also, there is a segment designed to support and implement the business processes of the enterprise.

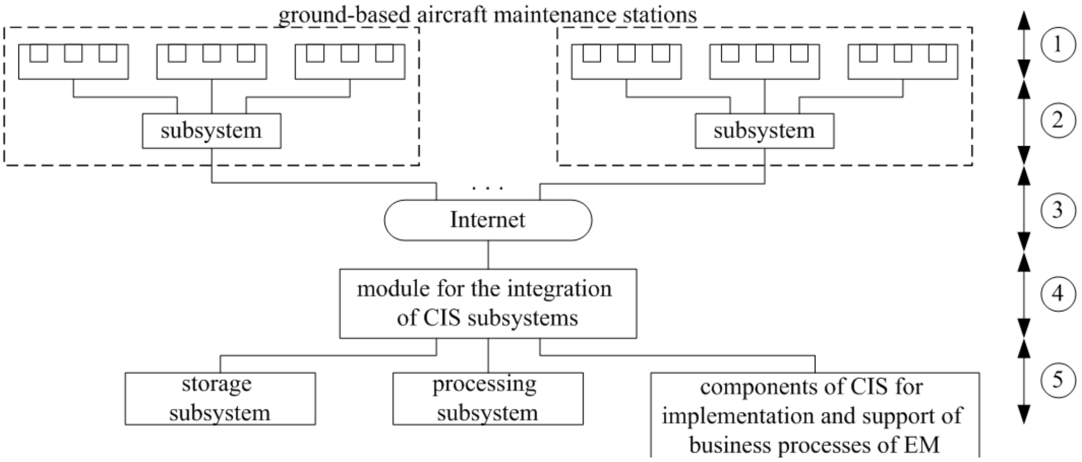
ground-based aircraft maintenance stations
subsystem
subsystem
. . .
Internet
module for the integration of CIS subsystems
storage subsystem
processing subsystem
components of CIS for implementation and support of business processes of EM
1
2
3
4
5

Figure 4. Generalized structural diagram of a protected system for collecting, storing and processing TMI (1 – level of TMI collection from wired and wireless sensors of ground-based aircraft servicing systems; 2 – level of primary surveillance and preparation of TMI for transmission to the AIS of the manufacturer's enterprise (AIS EM); 3 – level of data transmission over secure channels through global data networks in the AISEM; 4 – level of organization of reception and distribution of TMI on EM; 5 – level of storage and processing of TMI in the CIS).

5. Development of the structure of the collection and storage subsystem TMI at the ground stations of aircraft maintenance

The vast majority of Industrial Ethernet protocols do not have built-in security mechanisms. Consequently, the actual problem is the security of industrial networks.

To ensure the security of subsystems that implement the first two levels of the proposed structure, it is necessary to be guided by the normative documents of the international and federal standards. When designing the wireless sensor network collection subsystem of the TMI, take into account the requirements of GOST R ISO / IEC 27033-1-2011 and GOST R ISO / IEC 27033-3-2014.

The physical architecture of the TMI collection and storage subsystem at the ground is presented in Figure 5.

Mechanisms for collecting and storing a large amount of TMI on the state of individual components and elements of aircraft should take into account the actively developing concepts of the industrial Internet of things (IIoT). It is proposed to use heterogeneous wired (physical RS-485 interface) and wireless sensor networks (IEEE 802.15.4, IEEE 802.15.4e) to collect protocol-based TMI using embedded Modbus over TCP mechanisms to ensure the protection of transmitted data (streaming encryption). The IEEE 802.15.4 and IEEE 802.15.4e protocols and their architecture levels follow the IETF standards.

6. Development of the structure of the subsystem for receiving, storing and processing TMI in AIS

The organizations for receiving and distributing TMIs on PIs are implemented according to the three-tier CISCO model and Security Architecture for Enterprise (SAFE) design methodology, which allows to take into account modern experience in deploying secure networks based on the deep-echelon defense against external and internal attacks.

The main element of the TMI distributed processing system is the distributed file system HDFS. Additional measures to ensure the confidentiality of stored data is encryption at the level of individual database columns. To audit access to big data, you need to apply Database Activity Monitoring class solutions.

7. The concept of data integrity and verification of data sources

The actual problem is the security of industrial networks, which is not solved by existing approaches, since the attacker's intervention is possible not only at the network level from outside or inside, but also at the level of the data sources themselves. The main hardware and software part of the CTP is free from possible "bookmarks", which is guaranteed by the manufacturer, but it is necessary to comprehensively analyze the progress of the object, identifying abnormal situations not related to equipment breakdowns or failure of individual components and assemblies, but potentially caused by the intervention of an attacker.

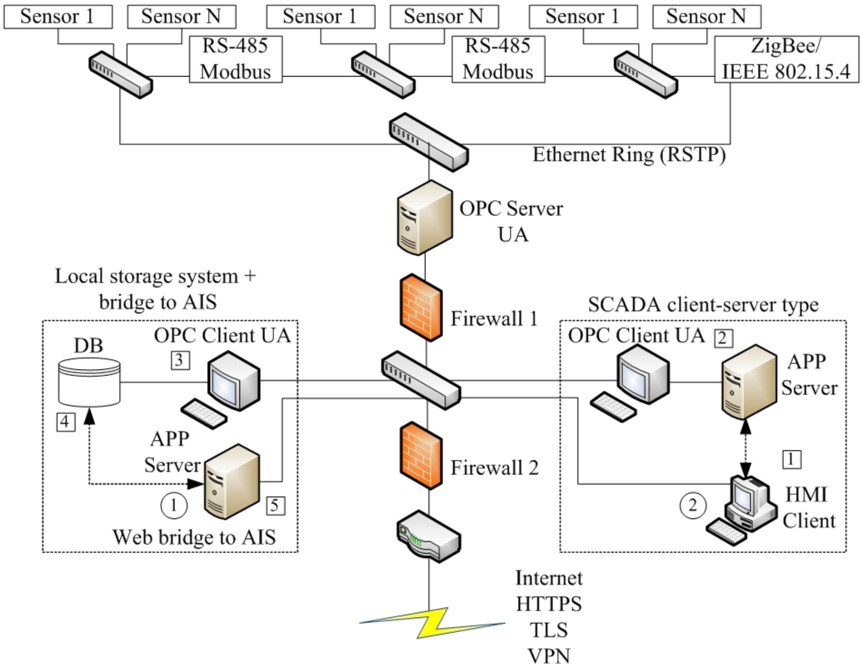

Figure 5. The subsystem of data collection and storage at aircraft service stations.

It is necessary to improve the monitoring system of CTP as an element of the intrusion detection system, considering the complexity of the control object, the nonlinearity of the processes and the possible conditions of the equipment that lead to emergency or catastrophic situations. The system of monitoring the condition of CTP, implemented as a component of the intrusion detection system, involves continuous monitoring of the parameters of CTP to identify significant deviations from the" normal behavior", which in turn will indicate possible malicious intentions. This approach is a development of the concept of Data Centric Security [7], which implies the security of the data itself. To determine deviations from the" normal behavior " it is proposed to use the system model of the object – the CTP, which is the development of the concept of Fault Detection and Identification [8]. The process of monitoring the state of the CTP is a sequential operation of collection, processing and analysis of technological information, the main of which is to detect the impact of an attacker on the course of the CTP and the components of the information system by comparing the mathematical model of the CTP and the current performance of the real object will improve the security of the object. Using the proposed concept of monitoring the CTP comparing the fixed state of the object with the real model is a tool that allows you to control the presence of hardware and software interventions in the infrastructure of the information system.

8. Conclusion

A block diagram of a protected system for collecting, storing and processing telemetric information on the state of aircraft subsystems based on the modular principle is proposed. The difference of the proposed solution is that it contains rather large subsystems with a high degree of connectivity of the components inside and a sufficient degree of autonomy at the level of interaction of the subsystems themselves. Each subsystem is built on the basis of organizational principles specific to the specifics of the problem being solved, and is governed by existing regulatory documents to ensure specific aspects of the system's reliability.

9. References

[1] Internet of Things Volume G4: Security Framework. Web [Electronic resource]. – Access mode: http://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf (10.11.2018).

[2] Internet of Aircraft Things: An Industry Set To Be Transformed 2Jan 18, 2016 Bhoopathi Rapolu [Electronic resource]. – Access mode: http://aviationweek.com/connected-aerospace/internet-aircraft-things-industry-set-be-transformed (10.11.2018).

[3] Aircraft Hacking Practical Aero Series, n.runs Professionals Stations [Electronic resource]. – Access mode: http://www.sita.aero/file/3744/Aircom (10.11.2018).

[4] Frid, A.I. Architecture of the security access system for information on the state of automatic control systems of aircraft / A.I. Frid, A.M. Vulfin, D.Ju. Zakharov, V.V. Berkholts, K.V. Mironov // Proceedings of the 19thInternational Workshop on Computer Science and Information Technologies. – Germany, 2017. – Vol. 2. – P. 21-27.

[5] Frid, A.I. Analysis of the methods of constructing information attack models for the system of telemetric information transmission / A.I. Frid, A.M. Vulfin, V.V. Berkholts // Proceedings of the Information Technology Intelligent Decision Support (ITIDS) [Electronic resource]. – Access mode: http://itids.ugatu.su/index.php/itids/itids2018/paper/view/50 (13.11.2018).

[6] Rapolu, B. Internet of aircraft things: an industry set to be transformed, aviation week network [Electronic resource]. – Access mode: http://aviationweek.com/connected-aerospace/internet-aircraft-things-industry-set-be-transformed (13.11.2018).

[7] Zhang, L. Named Data Networking / L. Zhang, A. Afanasyev, Je. Burke, V. Jacobson, P. Crowley, Ch. Papadopoulos, L. Wang, B. Zhang // ACM SIGCOMM Computer Communication Review. – 2014. – Vol. 44(3). – P. 66-73.

[8] Choi, S.W. Fault detection and identification of nonlinear processes based on kernel PCA / S.W. Choi, Ch. Lee, J.-M. Lee, J.H. Park, I.-B. Lee // Chemometrics and Intelligent Laboratory Systems. – 2005. – Vol. 75(1). – P. 55-67.

Acknowledgments

This work is partially supported by the Russian Science Foundation under grants № 17-07-00351.