Therefore appropriate to replace it with a non-contact transformer sensor PPU.

Potentiometric sensor replacement on transformer can increase the performance and life of the resource because the transformer sensor is not in contact and the related wear of moving parts sensor. This allows operation of the control system for the slats technical condition

For proper operation of the feedback sensor input shaft it should do 140 rpm during full output (input) slats, which lasts 7 seconds.

The output of the mechanism for moving slats №8 shaft makes 0.68 revolutions. It is necessary to design and calculate gear that is placed in front of the sensor to obtain the required parameters, namely gear ratio U = 1 / 205.88.

During the project the prototype aircraft was examined on the basis of medium-range passenger aircraft An-148 and its characteristics.

The analysis of the control system and directly examined its components. This allowed us to select an object of study – slats management system.

An analysis of the study shows that the system meets all requirements of the operation. Disadvantages include sensor feedback, who asked to be replaced.

As a result of the work was composed kinematic scheme of the new gear to accommodate the sensor PPU, and made his calculations. In particular were calculated to determine the gear ratio calculation spur transmission, calculation and design of the output shaft. Was conducted selection of rolling bearings and their calculation on durability. As a result of the calculations we made sure that the chosen gear scheme meets all the requirements, and the strength of individual parts is accomplished with considerable margin.

Scientific supervisor: Yashchuk O.P.,
Lecturer

UDC 004.056 (043.2)

Golestanekh A.K.
National Aviation University, Kyiv

THE PROBLEMS OF CYBER-SECURITY IN UKRAINE

Information Age creates a knowledge-based society surrounded by a high-tech global economy that brings significant benefits for individual, small and large social groups. Advantages of the new information society are obvious. A worldwide Internet network is a vivid example that demonstrates the impact of innovative processes changing relationship between people, expanding their contacts and opportunities and facilitating daily life. However, rapidly developing information technologies create serious threats to national and international security all over the world.

The need to adopt provisions on cyber security is long overdue in Ukraine because cyberspace sphere in our country has always been vulnerable. Current cyber security protection is rather low; cases of illegal collection, storage, use and distribution of personal data; illegal financial transactions; theft and fraud are becoming more and more common. These problems are complicated by the lack of clear legal regulation of the national state policy on cyber security and the absence of common state regulation structure for cyber crimes counteractions, which inevitably result in growth of threats to state infrastructure, computer piracy and copyright violations. Businesses and individuals do not know how to behave in case of cyber-problems, to which they are completely unprepared.

The Ukrainian government has finally approved a new cyber security strategy aimed at creating conditions that ensure safe cyberspace and its use in the interests of individual, society and government. The new strategy involves the design and approval of new standards for Ukrainian cyber security that follow with European Union and NATO standards.

The main focus of the strategy is on developing national cyber security system; enhancing capabilities across security and defense sector; ensuring cyber security of critical information infrastructure and government information resources. It should be implemented on the guiding principles of respect for human and civil rights and freedoms; ensuring national interests of Ukraine; open, accessible, sustainable and secure cyberspace; cooperation with private sector, civil society and international community; adequate risk-based cyber security measures; priority given to preventive measures; inevitable punishment for cybercriminals; priority focus on the development of domestic scientific and technical industrial capacity; ensuring democratic civil control in the area of cyber security.

Ukraine's National Cyber Security System should ensure collaboration between all governmental agencies, local authorities, military units, law enforcement agencies, research and educational institutions, civil groups and businesses that deal with electronic communication and information security.

To implement this strategy Ukraine needs tangible assistance from advanced countries to confront current internal and external threats: cyber threats of military nature, cyber espionage, cyber terrorism and different cybercrimes. In cyberspace the implementation of this strategy entails projects in three main issues: cyber defense skills and capabilities development; cyber security policy; legislation and strategy.

Key areas of ensuring cyber security in Ukraine are development of safe, sustainable and reliable cyberspace; cyber security of the government electronic information resources; critical infrastructure cyber security; development of cyber security capacity in defense sector; and fighting criminals. The last includes establishment of a contact center for reporting cybercrimes and fraud in the cyberspace; improved procedural tools for digital forensics; training of judges, detectives and prosecutors with regard to handing digital evidence; training law enforcement personnel.