UDC 004.056:629. 7 (043.2)

Marchuk E.V.
National Aviation University, Kiyv

CYBER TERRORISM IN AVIATION

Cyber Terrorism defines our times. It has brought changes to the way we approach terrorism. This is because global and national reliance placed on cyber space for the development and sustenance of human interaction will continue to grow in the years to come and with that continued development will come ominous threats and daunting challenges from cyber terrorism.

The aviation industry is especially important when analyzing computer security because the involved risks include human life, expensive equipment, cargo, and transportation infrastructure. Security can be compromised by hardware and software malpractice, human error, and faulty operating environments. Threats that exploit computer vulnerabilities can stem from sabotage, espionage, industrial competition, terrorist attack, mechanical malfunction, and human error.

Cyber terrorism, whether conducted by individuals, corporations or States could target the electronic systems of companies which design and develop hardware and software used in airports, air traffic control systems. It could target industries involved in the construction of aircraft and components whet her they be used for civil or military purposes.

Most computer systems have weak authentication and are relatively easy to penetrate. Most such systems have weak access controls and tend to be poorly configured, and are as a result relatively easy to misuse once initial access is attained. These systems often have monitoring facilities that are ill adapted to determining when threats are mounting and what damage may have occurred. Consequently, misuse by outsiders and insiders is potentially easy to achieve and sometimes very difficult to detect. A proper attack does not need to be very high tech or well funded; for a power outage at an airport alone can cause repercussions worldwide. One of the easiest and, arguably, the most difficult to trace security vulnerabilities is achievable by transmitting unauthorized communications over specific radio frequencies. These transmissions may spoof air traffic controllers or simply disrupt communications altogether. These incidents are very common, having altered flight courses of commercial aircraft and caused panic and confusion in the past. Controlling aircraft over oceans is especially dangerous because radar surveillance only extends 175 to 225 miles offshore. Beyond the radar's sight controllers must rely on periodic radio communications with a third party.

A conclusion from that observation is that a sensible approach to security must encompass a sensible approach to system safety and overall system reliability to terminate attempts of cyber crimes.

Supervisor –A.Chunareva, Candidate of Technical Sciences