Cybersecurity in Aviation

Eesti Lennuakadeemia
Estonian Aviation Academy

Time of Training	12 February - 14 May 2021 (On Fridays)
Place of Training	Online, Hybrid classroom
Teaching Methods	Lectures & Seminars Individual/group study
Language of Instruction	English

Instructors	Nele Tootsi, Estonian Aviation Academy, Head of CNS Training, lecturer, MSc in Computer Engineering (University of Tartu);
	Olaf Maennel, Tallinn University of Technology, Centre for Digital Forensics and Cyber Security, Professor, PhD (Technical University of Munic);
	Erwin Orye, Tallinn University of Technology, PhD Student (field of research: cybersecurity in aviation), MSc, Royal Military Academy in Belgium

Base of Course Syllabus	Aeronautical Engineering, (*Registered in EHIS, code 194140)*
Curriculum Group	Transport Services
Volume of Training	78 academic hours
Price of Training	120 EUR
Target Group	Cybersecurity and/or aviation specialists
Size of Training Group	Up to 40 participants
Aim of Training	Give a introduction to cybersecurity and the importance of cybersecurity in aviation
Course Content	Basic Principles Used in Cybersecurity The Threat Landscape Overview of The Attack and Defence Methods in Cybersecurity Risk Management Demo Hacking Wireless Transmission Media Cybersecurity Regulations Aviation Regulations Wireless Systems - Working Principles and Cybersecurity Aspects Wireless Systems - Ads-B ANS Digital Systems - Working Principles and Cybersecurity Aspects ANSP Practical Cybersecurity Implementation Cyber Kill Chain in Cybersecurity Aircraft Digital Systems Aircraft Cyber Certification ICS Systems Cybersecurity in Airports - Cybersecurity Overview, Operational Aspects Military Aviation Drones and U-Space The Passenger Journey Cybersecurity from Pilot's View ATC Simulator Hack Strategic Impacts Cybersecurity for Airlines

Learning outcomes	The participant having passed the training can: 1. Describe terms related to the cybersecurity; 2. Explain the aviation threat landscape; 3. Explain the possible means to execute a cyberattack on aviation and the impact such an attack may have on the complex ecosystem; 4. Explain cybersecurity policies and practices to ensure the security of information and operational data; 5. Describe possible external interventions which may interrupt ATM, airport & airline services, and digital systems of aircrafts; 6. Describe relevant existing regulations, legislations and security standards related to cybersecurity in aviation.
Study materials	Handed over during the training
Passing the Training	Participation in the activities – 100%
Certificate	The participants having passed the course successfully shall be awarded the respective certificate by the EAVA Flying Training Organisation (*Certificate of Course Completion*)
Additional Information	Additional information from Nele Tootsi nele.tootsi@eava.ee