ECAR ENGINEERING CENTRE

Modular training program «Engineering Center Management School»

Catalogue of module «DIGITAL ENGINEERING CENTER 4.0»

Training list:

- Practical aspects of organizing the IT infrastructure of a modern engineering center (including the organization of remote work) (1 day training)

- Engineering Office Cyber Defense Methods and Practices (1 day training)

Moscow

Contacts:

Sakhin Igor +7 (495) 221-56-00 ext. 5954
igor.sakhin@airbus.com

Khimchenko Anna +7 (495) 221-56-00 ext. 5486
anna.khimchenko@airbus.com

JSC ENGINEERING CENTER ECAR

Seminar program:

"Practical aspects of organizing the IT infrastructure of a modern engineering center (including the organization of remote work)"

Moscow

	JSC ENGINEERING CENTER ECAR
	" Practical aspects of organizing the IT infrastructure of a modern engineering center (including the organization of remote work)"

1. SEMINAR PURPOSE:

To tell about the unique practical experience of IT infrastructure organization in the modern engineering center of the leading European aircraft corporation, paying attention to remote work organization for employees of the center.

2. TARGET AUDIENCE:

The seminar is meant for representatives of IT departments of industrial companies.

3. SEMINAR CHARACTERISTICS:

- ✓ The duration of the seminar – 8 acad. hours (1 day);
- ✓ Seminar timing – from 10.00 to 17.15;
- ✓ Breaks: two coffee breaks and lunch.

4. SEMINAR DESCRIPTION:

- ✓ During the seminar, practical aspects of IT infrastructure organization in the modern engineering center will be considered;
- ✓ The program, built on the principle "from theory to practice", will allow participants to master the material in a short time and then successfully use it in practice.

5. CRITERIA FOR SUCCESSFUL SEMINAR COMPLETION:

- ✓ Basic knowledge in IT infrastructure organization in a company;
- ✓ Compliance with the timing, rules of participation in the seminar;
- ✓ Initiative behavior of attendees;
- ✓ An open form of discussion of issues under consideration.

6. SEMINAR OUTPUT:

The attendee receives theoretical and practical knowledge in the field of IT infrastructure organization in the modern engineering center.

7. SEMINAR CONDITIONS:

- ✓ The possibility of conducting classes using teaching aids (computer or laptop, projector, screen, blackboard, etc.);
- ✓ The ability to work under normal lighting conditions and in ventilated classrooms;
- ✓ The ability to freely use sanitary facilities and break areas;
- ✓ The seminar can be held both face-to-face and online.

<u>Handout materials issued to attendees:</u>

- ✓ Seminar training program;
- ✓ Seminar handout material (for educational purposes).

8. SEMINAR SCHEDULE:

Topic No.	Topic name	Time, hour
1	Registration of attendees. Presentation of the lecturer. Seminar purposes. Information about JSC ECAR. The rules of the seminar.	09.30–10.00
2	IT mission and goals in the engineering center.	10.00–11.30
Break (coffee break)		11.30–11.45
3	Products and Services (PSL). Standardization. Key performance indicators and visualization boards (SQCDP) of IT and engineering departments, monitoring.	11.45–13.15
Break (lunch)		13.15–14.00
4	End-user administration (tools and processes). Operating mode, Service Desk, user feedback. Management and accounting of fixed assets in engineering project work. Interaction with the central office (local and global services, support).	14.00–15.20
Break (coffee break)		15.20–15.30
5	Distance work, VDI, DaaS. Organization and tools of CAD/CAE, the evolution of tools in the company. Work with CAD data, practical demonstrations.	15.30–16.45
6	Questions and answers. Summing-up and certificate issuing.	16.45–17.15

JSC ENGINEERING CENTER ECAR

Seminar program:

"Engineering Office Cyber Defense Methods and Practices"

Moscow

	JSC ENGINEERING CENTER ECAR
	" Engineering Office Cyber Defense Methods and Practices "

1. SEMINAR PURPOSE:

✓ To acquaint participants with methods and practical solutions in the field of cybersecurity;

✓ To tell about the unique experience to organize cybersecurity in the engineering center of the leading European aircraft corporation.

2. TARGET AUDIENCE:

The seminar is meant for information security specialists and specialists / heads of IT-departments of industrial companies.

3. SEMINAR CHARACTERISTICS:

✓ The duration of the seminar – 8 acad. hours (1 day);

✓ Seminar timing – from 10.00 to 17.15;

✓ Breaks: two coffee breaks and lunch.

4. SEMINAR DESCRIPTION:

✓ During the seminar built on the principle "from theory to practice", cybersecurity methods and their application in the engineering center will be considered;

✓ The program will allow attendees to master the material in a short time and then successfully use it in practice.

5. CRITERIA FOR SUCCESSFUL SEMINAR COMPLETION:

✓ Basic knowledge in the field of cybersecurity;

✓ Compliance with the timing, rules of participation in the seminar;

✓ Initiative behavior of attendees;

✓ An open form of discussion of issues under consideration.

6. SEMINAR OUTPUT:

The attendee receives theoretical knowledge about the principles of creating an effective cybersecurity system for an engineering office and practical skills on this topic.

7. SEMINAR CONDITIONS:

✓ The possibility of conducting classes using teaching aids (computer or laptop, projector, screen, blackboard, etc.);

✓ The ability to work under normal lighting conditions and in ventilated classrooms;

✓ The ability to freely use sanitary facilities and break areas;

✓ The seminar can be held both face-to-face and online.

<u>Handout materials issued to attendees:</u>

✓ Seminar training program;

✓ Seminar handout material (for educational purposes).

8. SEMINAR SCHEDULE:

Topic No.	Topic name	Time, hour
1	Registration of attendees. Presentation of the lecturer. Seminar purposes. Information about JSC ECAR. The rules of the seminar.	09.30–10.00
2	Information security (IS) threats and risk analysis. Development of IS policies.	10.00–11.30
Break (coffee break)		11.30–11.45
3	Company information security, selection of suppliers of information security hardware; Methodology for disaster recovery plan (DRP); Computer network security (SOC); Compliance with the requirements (Compliance methodology).	11.45–13.15
Break (lunch)		13.15–14.00
4	Human security. IAM (Identity Access Management). The "human factor" and social engineering. Use of DLP solutions to protect confidential information.	14.00–15.20
Break (coffee break)		15.20–15.30
5	Cryptographic methods of information protection. Information security monitoring and audit tools. Organization of access in the company. Information that should be provided to employees (training and maintaining the level of knowledge). Practice: Prepare for an incident: what should be done if an incident occurs?	15.30–16.45
6	Questions and answers. Summing-up and certificate issuing.	16.45-17.15