Composition of the course

The course includes two one-week classroom training sessions and online learning activities in between. It includes also two technical visits, e.g. to a nuclear research reactor and speeches by leading IT/cyber experts.

The course provides theoretical and practical IT/cyber security knowledge. Various practical exercises and case studies support the lectures. The interactive teaching sessions are led by international IT/cyber security experts.

Between classroom training sessions each participant prepares a teaching concept on one of the topics covered in the first week of the course. Presentations of homework take place during the second week.

The course is wrapped up with feedback session on homework and delivery of certificate.

ISS has developed the course concept, which took into account the aspect that this content is new and rather of technical knowledge for most people from the nuclear sector.

Since 2012, ISS has gathered experience in teaching the material, and during the process it has also modified the course and adjusted it to the actual need and suggestions of universities and participants. ISS has gained good bases of know-how for transferring its knowledge and experience.

If you feel addressed and if you are willing to establish a Professional Development Course on IT/Cyber Security in your country or company, please contact us:

Institute for Security and Safety (ISS)
at Brandenburg University of Applied Sciences

David-Gilly-Str. 1
14469 Potsdam
Germany

Phone +49 331 58 14 83 30
Web www.uniss.org
E-Mail info@uniss.org

Fachhochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

Professional Development Course on IT/Cyber Security

Cyber Security

The threat from cyber attacks is increasingly perceived as a problem of national and international security as cyber attacks grow in number and sophistication and as actors behind them are no longer only private hackers and organized criminals but also states.

Nation states need to seriously address the way to protect their information networks – especially those related to national security and critical infrastructure – from any attacker. But recent developments have shown that there is more to this debate than the solution of technical questions, in particular as many technical problems do not seem solvable at all. A larger approach that includes international norms of behavior and regulation to ensure the peaceful use of cyberspace is needed. To enable such an approach, an education framework has to be addressed.

For the nuclear sector a framework was developed following the "NS22 IT/cyber security" set out in IAEA Nuclear Security Series No. 12, Educational Programme in Nuclear Security. Based on this framework the ISS has developed an education format called **Professional Development Course.**

Professional Development Course on IT/Cyber Security

Because of their knowledge and experience in the field of IT/cyber security, the Brandenburg University was the first one chosen to implement a Professional Development Course (PDC) on IT/cyber security as described in the IAEA's Educational Programme in Nuclear Security, referred to as NSS12. For the implementation of NS22 'IT/Cyber Security' a detailed concept was developed.

The course is based on the "train-the-trainer" approach: Experienced lecturers from academia in the nuclear academic community give lectures in a two week course to those academics and key constituents at nuclear technical organizations including scientists, technicians, as well as engineers and technical organization decision makers, who are interested in expanding their knowledge in nuclear security.

The Professional Development Course on IT/Cyber Security meet the ever growing need to educate IT/cyber security specialists in the nuclear field. PDCs, based on the **IAEA Textbook "NS22 *Computer Security for Nuclear Security Professionals",*** have proven of being on raising demand in academic education.

Course Modules

With regard to the content, the course is based on the INSEN Textbook "NS 22 Cyber Security for Nuclear Security Professionals" and covers following topics:

Ch. 1. Guns, Guards, Gates, and Geeks
Ch. 2. Threats and Their Sources
Ch. 3. Computer Security Basics
Ch. 4. Authentication
Ch. 5. Computer Access Control
Ch. 6. Cryptography
Ch. 7. Network Security
Ch. 8. Network Firewall Concepts
Ch. 9. The Hypothetical Hacker
Ch. 10. Intrusion Detection
Ch. 11. Computer Security Management
Ch. 12. System Assessment and Evaluation
Ch. 13. Computer Incident Management and Information Recovery
Ch. 14. Computer Incident Investigation and Computer Forensics