HÖGSKOLAN
I SKÖVDE

KURSPLAN

Cybersäkerhet kring sakernas internet och kritiska infrastrukturer A1N

7,5 högskolepoäng

Kurskod: IT747A
Revisionsnummer: 5
Gäller från: 2021-01-01
Beslutad av: Utbildningskommittén för informationsteknologi
Beslutsdatum: 2020-08-27

1. Allmänt om kursen

Kursen ges av Högskolan i Skövde och benämns Cybersäkerhet kring sakernas internet och kritiska infrastrukturer A1N (Cyber Security for Internet of Things and Critical Infrastructures A1N). Omfattningen är 7,5 högskolepoäng (hp). Kursen är på avancerad nivå och har fördjupningsnivå A1N.

Kursen ingår i huvudområdet informationsteknologi. Kursens utbildningsområde är teknik.

2. Behörighetskrav

En kandidatexamen (motsvarande en svensk kandidatexamen) inom informationsteknologi, datavetenskap eller datalogi (eller motsvarande). Vidare krävs godkänt betyg i gymnasiekkursen Engelska 6 / Engelska B (eller motsvarande). Motsvarande kunskaper visas normalt genom ett internationellt erkänt språktest, till exempel IELTS eller TOEFL.

3. Innehåll

Sakernas internet (IoT) förväntas förändra tekniska infrastrukturer, inklusive kritiska infrastrukturer. Syftet med kursen är att introducera ett brett spektrum av säkerhets- och integritetsfrågor i samband med sakernas internet. Kursen diskuterar och problematiserar också samspelet mellan IoT och cyberfysiska system som i allt högre grad bidrar till att lägga grunden för utveckling av Smart-X-applikationer och till själva kärnan i Industri 4.0-revolutionen och modern kritisk infrastruktur. Sårbarheter inom dessa komplexa nätverksstrukturer presenteras tillsammans med metriker för att kvantifiera hur allvarliga dessa sårbarheter är. Vi arbetar med modeller av hot som involverar dessa sårbarheter och resulterande effekter av attacker för att förstå olika begrepp involverade i riskbedömning av cybersäkerhet.

4. Mål

Efter avslutad kurs ska studenten kunna:

- beskriva sakernas internet (Internet of Things; IoT) och kritiskt reflektera över relaterade säkerhetsproblem
- beskriva och kritiskt reflektera över IoT-plattformar och deras säkerhets- och integritetsaspekter
- på ett fördjupat sätt diskutera sårbarheter som påverkar kritisk infrastruktur
- analysera hot och attackmodeller samt utveckla motåtgärder för IoT-enheter
- kritiskt utvärdera potentiella hot mot cyberfysiska system vanliga i Industri 4.0 och kritiska

infrastrukturer

5. Examination

Kursen bedöms med betygen A (Utmärkt), B (Mycket bra), C (Bra), D (Tillfredställande), E (Tillräcklig) eller F (Underkänd).

Kursen har följande examinationsmoment:

- **Laborationsuppgifter**
  3 hp, betyg: A/B/C/D/E/F (bestämmer betyg på hel kurs)
- **Rapport**
  2 hp, betyg: G/U
- **Seminarieuppgifter**
  2,5 hp, betyg: G/U

Studenter med varaktig funktionsnedsättning som har fått beslut om riktat pedagogiskt stöd kan erbjudas anpassad eller alternativ examination.

6. Undervisningsformer och undervisningsspråk

Undervisningen består av föreläsningar och seminarier/gruppdiskussioner samt praktiska övningar där vi använder verktyg och applikationsprogrammeringsgränssnitt (API) i syfte att upptäcka sårbarheter relaterade till cybersäkerhet, modellera hot eller simulera attacker inklusive konsekvensen av att sårbarheter utnyttjas i en attack.

Undervisningen bedrivs på engelska.

7. Kurslitteratur och övriga läromedel

Artiklar och annat material tillhandahålls av kursanvarig.

8. Studentinflytande

Studentinflytande i kursen säkerställs genom kursvärdering. Studenterna informeras om resultatet av kursvärderingen och eventuella åtgärder som genomförts eller planeras, grundat på kursvärderingen.

9. Övrigt

På Högskolan i Skövdes webbplats finns ytterligare information om kursen samt nationella och lokala styrdokument för högskoleutbildning.