HOCHSCHULE FURTWANGEN UNIVERSITY HFU

Modulkatalog

IT-Sicherheit und Cyber Security

Inhaltsverzeichnis

Ausgewählte Fragen der Cyber Security **3**

Automaten und Formale Sprachen **5**

Computernetze **7**

Digitale Forensik **9**

Drahtlose Netzwerke **11**

Ethical Hacking und Pentesting **13**

Grundlagen der IT-Sicherheit **15**

Internetprotokolle **17**

IT-Sicherheitsmanagement und Datenschutz **19**

Kryptologie **21**

Künstliche Intelligenz für Cyber Security **23**

Mathematik für Informatiker 1 ..... **25**

Mathematik für Informatiker 2 ..... **27**

Netzwerkmanagement und -sicherheit **29**

Praktisches Studiensemester **31**

Programmierung **33**

Physische Sicherheit von Rechenzentren und Serverräumen **35**

Rechnerarchitektur und Betriebssysteme **38**

Security-Projekt 1 ..... **40**

Security-Projekt 2 ..... **42**

Sichere Programmierung **44**

Software Engineering **46**

Stochastik **48**

Studienkompetenzen **50**

Thesis **52**

Web Security und Intrusion Prevention **54**

Ausgewählte Fragen der Cyber Security

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	ITS7	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Ausgewählte Fragen der Cyber Security	a) Deutsch	a) 0 h	a) 180 h	a) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... übergreifende Fragen über die im Studium, insbesondere im Hauptstudium, erlernten Prinzipien, Konzepte, Methoden und Techniken erörtern

Verständnis (2):

... ihr Fachwissen und ihr wissenschaftliches Urteilsvermögen nutzen, um komplexe übergreifende Fragestellungen darzustellen,

Anwendung (3):

... die Fragestellungen in ihren Kernpunkten sowie wechselseitigen Zusammenhängen bearbeiten.

Analyse (4):

... ihr im Studium erworbenes Fachwissen und ihre Projekterfahrungen systematisch kombinieren, um Lösungsstrategien und -alternativen für die Fragestellungen zu entwickeln, zu begründen und vorzutragen.

Synthese (5):

... das erworbene Wissen auf ähnlich gelagerte Fragestellungen anwenden (Fähigkeit zum Wissenstransfer).

3 Inhalte

a) Es erfolgt eine intensive Auseinandersetzung mit neuesten Entwicklungen auf dem Gebiet der IT-Sicherheit und Cyber Security bzw. mit einem der Schwerpunktthemen des Studiengangs.

4 Lehrformen

a) Prüfung

5 Teilnahmevoraussetzungen

Gleichzeitige Anfertigung einer Bachelorarbeit

6 Prüfungsformen

a) Prüfungsleistung 1M (Mündliche Prüfung) (6 LP)

7	**Verwendung des Moduls** IT-Sicherheit und Cyber Security B. Sc. (ITS)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Studiendekan
9	**Literatur**

Automaten und Formale Sprachen

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	AIN3	Jedes Semester	1 Semester

	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
1	a) Automaten und Formale Sprachen b) Automaten und Formale Sprachen, Praktikum	a) Deutsch b) Deutsch	a) 22,5 h b) 22,5 h	a) 67,5 h b) 67,5 h	a) 45 b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... grundlegende formale Methoden der theoretischen Informatik benennen und ihre spezifischen Eigenschaften beschreiben.

... verschiedene Berechnungskonzepte darstellen.

Verständnis (2):

... die jeweiligen charakteristischen Eigenschaften der behandelten Automaten, Grammatiken und regulären Ausdrücke erklären und Zusammenhänge erläutern.

... Gemeinsamkeiten und Unterschiede verschiedener Ansätze zur Berechenbarkeit wiedergeben und die Grenzen der Berechenbarkeit aufzeigen.

Anwendung (3):

... ausgewählte formale Methoden aus dem Bereich der theoretischen Informatik anwenden – insbesondere im Bereich Compilerbau und der Modellierung von dynamischen Systemen – und bewerten.

3 Inhalte

a)

- Alphabete, Wörter, Wortmengen, Wortfunktionen
- Reguläre Ausdrücke
- Endliche Automaten
- Kellerautomaten
- Grammatiken
- Berechenbarkeit
- Turing-Maschinen
- Primitiv-rekursive und μ-rekursive Funktionen

b) Anhand von Übungsaufgaben werden die in der Vorlesung behandelten Methoden und Verfahren geübt.

4 Lehrformen

	a) Vorlesung b) Praktikum
5	**Teilnahmevoraussetzungen** Programmierung
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (3 LP) b) Studienleistung:1 sbA (Praktische Arbeit) (3 LP)
7	**Verwendung des Moduls** Allgemeine Informatik B. Sc. (AIN)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Prof. Dr. Bernhard Hollunder (Modulverantwortliche/r)
9	**Literatur** • Gottfried Vossen und Kurt-Ulrich Witt. Grundkurs Theoretische Informatik: Eine anwendungsbezogene Einführung - Für Studierende in allen Informatik-Studiengängen. Springer Fachmedien (2016) • Uwe Kastens und Hans Kleine Büning. Modellierung: Grundlagen und formale Methoden. Hanser (2021) • Peter Sander, Wolffried Stucky und Rudolf Herschel. Automaten, Sprachen, Berechenbarkeit; Grundkurs angewandte Informatik, Teubner (1995)

Computernetze

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	AIN2, KIR1, ITS1	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Computernetze b) Computernetze, Praktikum	a) Deutsch b) Deutsch	a) 45 h b) 22,5 h	a) 75 h b) 37,5 h	a) 75 b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... Konzepte, Technologien und die Integration von Computernetz-Infrastrukturen beschreiben.
... Dienste und Protokolle von Computernetzen im Lokalen und Weitverkehrs-Bereich erläutern.
... Kommunikationsarchitekturen und Netztopologien darstellen.

Verständnis (2):

... Entwurf, Umsetzung und Betrieb von Computernetz-Infrastrukturen mitgestalten.
... Computernetze für konkrete Anwendungsszenarien konzipieren.

Anwendung (3):

... Zusammenhänge der globalen Vernetzung und die heute de facto bestehende Abhängigkeit jedes größeren. Unternehmens von der Informations- und Kommunikationstechnik einordnen.

3 Inhalte

a)

- Computernetze und Referenzmodelle
- TCP/IP-Protokollsuite, IPv4 und IPv6 basiert
- LAN/WAN-Netz-Topologien
- Internetworking/Routing
- Infrastrukturen mobiler Netze (WLAN, Bluetooth, UMTS/LTE/5G)
- Software Defined Networking (SDN)
- Voice over IP Infrastrukturen
- Dienste in Kommunikationsnetzen (z.B. Verzeichnisdienste, Netzwerkmanagement, Security-Dienste)

b) Case Studies über Computer-Netzwerk-Infrastrukturen

4 Lehrformen

a) Vorlesung

	b) Praktikum
5	**Teilnahmevoraussetzungen** Grundlagen der Informatik
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (4 LP) b) Studienleistung: 1 sbA (Praktische Arbeit) (2 LP)
7	**Verwendung des Moduls** Allgemeine Informatik B. Sc. (AIN), IT-Sicherheit und Cyber Security B. Sc. (ITS), Künstliche Intelligenz und Robotik B. Sc. (KIR)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Prof. Dr. Achim Karduck (Modulverantwortliche/r) Prof. Dr. Richard Zahoransky (Modulverantwortliche/r)
9	**Literatur** • Schreiner R.: Computernetze, Hanser Verlag, 2019 • Bök, Noack et al: Computernetze und Internet of Things, Springer Verlag, 2021 • Badach, A. Hoffmann, E.: Technik der IP-Netze, Hanser Verlag, 2019 • Scherff, J.: Computernetzwerke, Vieweg Verlag, 2010 • Kurose, J.F., Ross, K.W.: Computer Networking, 8th Edition, Prentice Hall Int, 2021 • IEEE Digital Library

Digitale Forensik

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	ITS4	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Digitale Forensik b) Digitale Forensik, Praktikum	a) Deutsch b) Deutsch	a) 22,5 h b) 22,5 h	a) 67,5 h b) 67,5 h	a) 15 b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... Verstehen, was forensisch auswertbare Daten und Informationen sind und zu welchem Zweck forensische Daten genutzt werden können

... Verstehen, wie es in unterschiedlichen Anwendungen und Architekturen zu forensisch auswertbaren, digitalen Spuren kommt

... Welche Aktionen zu persistenten oder flüchtigen Spuren führen und wo diese gespeichert sind

... Welche extrahierbaren forensische Spuren existieren und wie diese manipulationssicher und integritätsgeschützt werden können

... Verstehen, welche mögliche auswertbare Spuren ein Angreifer auf einem IT-System hinterlässt und wie diese auswertbar sind

Verständnis (2):

... Wann ist eine Auswertung digitaler Spuren hilfreich

... Welchen Nutzen für die IT-Sicherheit bringt die Auswertung digitaler Spuren

... Die Aussagekraft digitaler Spuren beurteilen

... Wie können ausgewertete Ergebnisse revissionssicher aufbewahrt werden

Anwendung (3):

... Auswertung von Malware und Angriffen auf IT-Systeme und Infrastruktur

... Verbesserung des bestehenden IT-Sicherheitsystems und Management anhand gefundener digitaler Spuren

... Nutzen der Digitalen Forensik, um eine bestehende Bedrohung in einem IT-System zu finden

3 Inhalte

a)

- Was sind auswertbare Spuren in Linux, Windows- und Netzwerkumgebungen
- Log-Dateien von Anwendungen verstehen, aufarbeiten und auswerten
- Wiederherstellen von Daten auf nichtflüchtigen Speicher
- Speichern von forenisch auswertbaren Spuren
- Rekonstruktion von Daten und Aktionen aus forensisch auswertbaren Spuren
- Erkennen von Malware und Angriffe auf die IT-Sicherheit durch forensische Spuren

	b) Case Studies zu Digitaler Forensik
4	**Lehrformen** a) Vorlesung b) Praktikum
5	**Teilnahmevoraussetzungen** Grundlagen der IT-Sicherheit
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (3 LP) b) Studienleistung: 1 sbA (Praktische Arbeit) (3 LP)
7	**Verwendung des Moduls** IT-Sicherheit und Cyber Security B. Sc. (ITS)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Prof. Dr. Richard Zahoransky (Modulverantwortliche/r)
9	**Literatur** • Parasram, S.: Digital Forensics with Kali Linux - Third Edition, O'Reilly, 2023 • Johansen, G.: Digital Forensics and Incident Response - Third Edition • Casey, E.: Handbook of Digital Forensics and Investigation, Elsevier Academic Press, 2009 • IEEE Digital Library

Drahtlose Netzwerke

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	AIN-CN6, ITS4	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Drahtlose Netzwerke	a) Deutsch	a) 22,5 h	a) 67,5 h	a) 40
	b) Drahtlose Netzwerke, Praktikum	b) Deutsch	b) 22,5 h	b) 67,5 h	b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... Zugriffsverfahren, Modulationsarten und Leitungscodes verstehen

... Daten vor zufälliger und böswilliger Manipulation bei der Übertragung schützen

... Mobilfunk von 2G bis 5G sowie die Standards LoRa, NFC, Bluetooth, WLAN und ZigBee beschreiben

Verständnis (2):

... Anwendungen und Herausforderungen drahtloser Kommunikation und Standards verstehen

... Verschiedene Netzwerktopologien für drahtlose Netzwerke verstehen

... Anforderungen und Anwendung von Low-Power IoT bis zu Gigabit-Verbindungen verstehen

Anwendung (3):

... Das Gelernte anwenden, um je nach Anforderung und Problem verschiedene Drahtlosnetzwerke miteinander zu vergleichen

... Administration und Anwendungen von mobilen Drahtlosnetzwerken durchführen

3 Inhalte

a)

Datenübertragung über elektromagnetische Wellen
Modulationsverfahren
Leitungscodes
Zugriffsverfahren für drahtlose und mobile Netzwerke
Mobilfunknetzwerke (2G GSM - 5G NR)
Weitere drahtlose mobile Kommunikationsstandards: WLAN, Bluetooth
IoT-Standards wie LoRa, LoRaWAN und ZigBee

b) Praktische Umsetzung und Vertiefung der Vorlesungsinhalte durch Bearbeitung von Übungsaufgaben und praxisnaher Fallbeispiele.

4 Lehrformen

	a) Vorlesung b) Praktikum
5	**Teilnahmevoraussetzungen** **Internetprotokolle**
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (3 LP) b) Studienleistung: 1 sbA (Praktische Arbeit) (3 LP)
7	**Verwendung des Moduls** Allgemeine Informatik B. Sc. (AIN), IT-Sicherheit und Cyber Security B. Sc. (ITS)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** **Prof. Dr. Richard Zahoransky**
9	**Literatur** **Sauter, M.: Grundkurs Mobile Kommunikationssysteme, Springer Verlag, 2022** Brückner, V.: Globale Kommunikationsnetze, Springer Verlage, 2022 Karl, H., Willig, A.: Protocols and Architectures for Wireless, Wiley & Sons, 2007 Sauter M. Grundkurs Mobile Kommunikationssysteme : 5G New Radio und Kernnetz, LTE-Advanced Pro, GSM, Wireless LAN und Bluetooth, 8. Auflage, Springer 2022 A. Luntovskyy, D. Gütter: Moderne Rechnernetze: Protokolle, Standards und Apps in kombinierten drahtgebundenen, mobilen und drahtlosen Netzwerken, Springer Vieweg, 2020

Ethical Hacking und Pentesting

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	ITS6	Jedes Semester	1 Semester

	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
1	a) Ethical Hacking und Pentesting b) Ethical Hacking und Pentesting, Praktikum	a) Deutsch b) Deutsch	a) 22,5 h b) 22,5 h	a) 67,5 h b) 67,5 h	a) 15 b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... grundlegende Tools, Vorgehen und die Bedeutung von Pentesting erläutern.
... die rechtlichen Aspekte und Grundlagen eines Pentests.
... Bewertungsgrundlagen für Schwachstellen kennen

Verständnis (2):

... Pentesting als Möglichkeit eines Audits und von Zertifizierung verstehen und als solches beurteilen können.
... die Aussagekraft eines Pentests einordnen.
... die Techniken und Phasen eines Pentests sowie typische Schwachstellen verstehen.
... das Risiko von Schwachstellen bewerten
... ein Bericht erzeugen und Empfehlungen ableiten

Anwendung (3):

... bei Pentests mitwirken, gängige Tools benutzen und automatisierte Schwachstellenscanner nutzen
... einen Bericht mit gefundenen Schwachstellen, einer Risikobewertung und Empfehlungen erstellen.

3 Inhalte

a)

- Die Grundlagen, Tools und Konzepte von Pentests
- Einordnen und Beurteilen von Schwachstellen
- Die Phasen eines Pentests: Vorbereitung, Erkundung, Durchführung, Berichterstattung, Nachverfolgung
- Typische Tools und Vorgehen
- Risikobewertung und Erstellung eines Maßnahmenkatalogs

b) Praktische Umsetzung und Vertiefung der Vorlesungsinhalte durch Bearbeitung von Übungsaufgaben und praxisnaher Fallbeispiele.

4 Lehrformen

	a) Vorlesung b) Praktikum
5	**Teilnahmevoraussetzungen** Grundlagen der IT-Sicherheit
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (3 LP) b) Studienleistung: 1 sbA (Praktische Arbeit) (3 LP)
7	**Verwendung des Moduls** IT-Sicherheit und Cyber Security B. Sc. (ITS)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** N.N.
9	**Literatur** • Aigner, Gebeshuber, Hackner, Kania, Kloep, Kofler, Neugebauer, Widl, Zingsheim, Hacking & Security : das umfassende Handbuch. 2. Aufl. Rheinwerk Verlag, 2020. • Patrick Engebretson, The basics of hacking and penetration testing : ethical hacking and penetration testing made easy. Elsevier, 2010.

Grundlagen der IT-Sicherheit

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	AIN-CN3, ITS1	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Grundlagen der IT-Sicherheit b) Grundlagen der IT-Sicherheit, Praktikum	a) Deutsch b) Deutsch	a) 22,5 h b) 22,5 h	a) 67,5 h b) 67,5 h	a) 15 b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... die wichtigsten Schutzziele, Angreifertypen, Bedrohungen benennen und voneinander abgrenzen.

... Authentifizierungs- und Autorisierungsprotokolle verstehen.

Verständnis (2):

... grundlegende Angriffe und Sicherheitsmaßnahmen beschreiben.

... Bedrohungen und Gefahren für Computersysteme beurteilen.

... Zugriffskontrollverfahren und Rechteverteilung verstehen.

Anwendung (3):

... grundlegende Verfahren zum Schutz sensibler Daten und Systeme nutzen.

... Verschlüsselungssoftware zum Schutz von Daten und Emails einsetzen.

... Dateien sichern und wiederherstellen.

... Mit Passwörtern und anderen Authentifizierungsmöglichkeiten umgehen.

Analyse (4):

... Schutzbedarf für ein Computersystem abschätzen.

... Bedrohungen und Risiken für Computersysteme einschätzen.

3 Inhalte

a) Die Studierenden beherrschen die grundlegenden Sicherheitskonzepte und Angriffe. Sie kennen die allgemeinen Grundbegriffe und -konzepte der IT-Sicherheit, wie Schutzziele, Angreifer, Bedrohungen, Schaden, Risiken. Sie sind in der Lage Maßnahmen zum Schutz von Software und IT-Systemen festzulegen und umzusetzen. Dabei werden Authentifizierungsprotokolle, Verschlüsselung, Signaturen, Zertifikate, Zugrifsskontrollkonzepte , risikoorientiertes Vorgehen und grundlegende Datenschutzaspekte behandelt.

b) Die Inhalte der Vorlesung werden in Übungsaufgaben und in praktischen Aufgaben angewendet

4 Lehrformen

a) Vorlesung

	b) Praktikum
5	**Teilnahmevoraussetzungen** Keine
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (3 LP) b) Studienleistung: 1 sbA (Praktische Arbeit) (3 LP)
7	**Verwendung des Moduls** Allgemeine Informatik B. Sc. (AIN), IT-Sicherheit und Cyber Security B. Sc. (ITS)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Prof. Dr. Christoph Reich (Modulverantwortliche/r) Prof. Dr.-Ing. Richard Zahoransky (Modulverantwortliche/r)
9	**Literatur** Eckert, C. 2012. IT-Sicherheit. Konzepte - Verfahren - Protokolle. von Claudia Eckert. Oldenbourg, München. Anderson, R.J. 2010. Security Engineering. A Guide to Building Dependable Distributed Systems. John Wiley & Sons Inc, Hoboken McClure, S., Scambray, J., and Kurtz, G. 2012. Hacking exposed 7. Network security secrets and solutions. McGraw-Hill/Osborne, New York

Internetprotokolle

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	AIN-CN3, ITS2	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Internetprotokolle	a) Deutsch	a) 22,5 h	a) 67,5 h	a) 15
	b) Internetprotokolle, Praktikum	b) Deutsch	b) 22,5 h	b) 67,5 h	b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... Protokolle für Internetanwendungen erklären und deren Bedeutung darstellen

... Erläutern weswegen verschiedene Protokolle existieren und deren Vor- und Nachteile einordnen

… Die Funktionsweise von Protokollen auf der Anwendungsschicht (HTTP, SMTP, SIP, DNS), Transportschicht, Vermittlungsschicht und Netzzugriffsschicht erklären.

Verständnis (2):

... Verstehen, welche Anforderungen zu welchen Protokollentscheidungen führen

... Einordnen, welche Protokolle auf welcher Ebene des ISO/OSI Referenzmodell arbeiten

... Die Auswirkungen von Protokollentscheidungen auf Latenz, Zuverlässigkeit, Sicherheit und Nachrichtengröße verstehen

… Anforderungen, den Aufbau und die Funktionsweise verteilter Infrastrukturen für mobile Systeme verstehen

… Transport- & Routingprotokolle verstehen

Anwendung (3):

... Internetanwendungen mit verschiedenen Protokollen anbinden

... Mit Sockets arbeiten

…Entscheiden, welche Protokolle für welche Anwendungen sinnvoll sind

3 Inhalte

a)

Anwendung und Nutzen von Protokollen auf unterschiedlichen Ebenen
Aufbau und Ablauf von Anwendungsprotokollen: HTTP, SMTP, SIP, DNS
Verlustfreie Datenübertragung über TCP durch Retransmission, Flusskontrolle und Überlastkontrolle
Routing und Routing-Protokolle wie RIP, OSPF und BGP
Vorstellung von Protokollen auf unteren Netzwerkschichten: Ethernet, Bluetooth, Mobilfunk, WLAN, Mobilfunk

b) Die Inhalte der Vorlesung werden in Übungsaufgaben und in praktischen Aufgaben angewendet.

4	**Lehrformen** a) Vorlesung b) Praktikum
5	**Teilnahmevoraussetzungen** Computernetze
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (3 LP) b) Studienleistung: 1 sbA (Praktische Arbeit) (3 LP)
7	**Verwendung des Moduls** Allgemeine Informatik B. Sc. (AIN), IT-Sicherheit und Cyber Security B. Sc. (ITS)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Prof. Dr. Richard Zahoransky (Modulverantwortliche/r)
9	**Literatur** Kurose, J.F., Ross, K.W.: Computer Networking, 8th Edition, Prentice Hall Int, 2021 P. Bök, A. Noack, M. Müller, D. Behnke: Computernetze und Internet of Things : Technische Grundlagen und Spezialwissen, Springer Vieweg, 2020 A. Luntovskyy, D. Gütter: Moderne Rechnernetze: Protokolle, Standards und Apps in kombinierten drahtgebundenen, mobilen und drahtlosen Netzwerken, Springer Vieweg, 2020

IT-Sicherheitsmanagement und Datenschutz

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	ITS2	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) IT-Sicherheitsmanagement und Datenschutz	a) Deutsch	a) 22,5 h	a) 67,5 h	a) 15
	b) IT-Sicherheitsmanagement und Datenschutz, Workshop	b) Deutsch	b) 22,5 h	b) 67,5 h	b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... die Schritte, Prozesse und technischen Notwendigkeiten für ein IT-Sicherheitsmanagement verstehen

... die Aufgaben im Rahmen eines Informationssicherheitsmanagementsystems (ISMS) benennen

... beschreiben, wie eine Schutzbedarfs- und Risikoanalyse durchgeführt wird

Verständnis (2):

... ausgehend von IT-Sicherheitsstrategien Sicherheitskonzepte, konkrete Maßnahmen und Anforderungen erarbeiten

... BSI Grundschutz sowie die darin genannten Vorkehrungen verstehen

... technische Maßnahmen wie Zugriffsrechte- und Kontrolle, Monitoring, Backupstrategien, Firewalls, Netzwerksegmentierung, Intrusion Detection, Endpoint Security und Patchmanagement verstehen

... organisatorische Maßnahmen wie Zutrittsrecht, Berechtigungskonzept und Notfallmanagement verstehen

Anwendung (3):

... Sicherheitsstrategien und Prozesse erstellen und konkrete Maßnahmen ableiten

... Schutzbedarfs- und Risikoanalysen durchführen

3 Inhalte

a)

Inhalte und Bedeutung eines IT-Sicherheitsmanagements

Konzepte und Standards eines Informationssicherheitsmanagementsystem

Aufnahme des Datenschutzes in das ISMS

Grundschutzkonzepte zur Verringerung des Risikos eines IT-Sicherheitsvorfalls

Erkennen des Schutzbedarfs eines IT-Systems

Ableiten organisatorischer sowie technischer Sicherungsmaßnahmen

Risikoorientiertes Vorgehen

	b) Die Inhalte der Vorlesung werden in Übungsaufgaben und Beispielen angewendet.
4	**Lehrformen** a) Vorlesung b) Workshop
5	**Teilnahmevoraussetzungen** Grundlagen der IT-Sicherheit
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (3 LP) b) Studienleistung: 1 sbA (Praktische Arbeit) (3 LP)
7	**Verwendung des Moduls** IT-Sicherheit und Cyber Security B. Sc. (ITS)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** N.N.
9	**Literatur** Kersten, Heinrich, Klett, Gerhard, Reuter, Jürgen, Schröder, Klaus-Werner, IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Controls. Springer 2016 Dinger, Jochen, Hartenstein, Hannes, Netzwerk- und IT-Sicherheitsmanagement: eine Einführung, KIT Scientific Publishing, 2008

Kryptologie

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	ITS3	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Kryptologie b) Kryptologie, Übung	a) Deutsch b) Deutsch	a) 22,5 h b) 22,5 h	a) 67,5 h b) 67,5 h	a) 15 b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... die grundlegenden Konzepte und Verfahrensklassen der Kryptologie benennen.

... die wichtigsten aktuellen kryptographischen Verfahren, deren Funktionsweise und Anwendung beschreiben.

... zuordnen, welche Analysemethoden in welche Angriffsszenarien und und für welche Schwachstellen eingesetzt werden können.

... gezielt nach Normen und Empfehlungen zur Kryptographie suchen.

Verständnis (2):

... die Problemstellung in der Kryptographie identifizieren.

... die Quelle für die Sicherheit einiger kryptographischen Verfahren verstehen.

... übliche Verschlüsselungs- und Authentifizierungsvorgänge darstellen.

... Ablaufprotokolle und Spezifikationen von kryptographischen Produkten lesen

... die Vor- und Nachteilen sowie Angriffspunkte ausgewählter moderner Verfahren erkennen.

Anwendung (3):

... Beschreibungen von Produkten mit Bezug zur Kryptographie beurteilen und vergleichen.

... Pressemitteilungen zur IT-Sicherheit mit Bezug zur Kryptologie einordnen.

... gezielt nach Schwächen und Angriffen recherchieren.

... Authentifizierungsvorgänge analysieren

3 Inhalte

a)

- Grundlagen der Kryptologie (Ziele, Konzepte, Mechanismen, Normen, Mathematik)
- Verschlüsselungsmethoden (symmetrisch Chiffren, asymmetrisch Verfahren)
- Hashverfahren, MAC und digitale Unterschrift
- Zufallszahlen und Schlüsselgenerierung
- Beispiele aus dem Alltag

b) Anhand von Übungsaufgaben und kleinen Projekten werden die in der Vorlesung bereitgestellten Methoden und Verfahren auch mittels Lernsoftware (CrypTool oder Bibliotheken) geübt.

4	**Lehrformen** a) Vorlesung b) Übung
5	**Teilnahmevoraussetzungen** Schulwissen in Mathematik
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (3 LP) b) Studienleistung: 1 sbA (Praktische Arbeit) (3 LP)
7	**Verwendung des Moduls** IT-Sicherheit und Cyber Security B. Sc. (ITS)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Prof. Dr. Olaf Neiße (Modulverantwortliche/r)
9	**Literatur** • A. Beutelspacher: Moderne Verfahren der Kryptographie, Springer Spektrum, 2022 • J. Buchmann: Einführung in die Kryptographie, Springer 2013 • C. Paar, J. Pelzl: Kryptografie verständlich, Springer Vieweg, 2016 • B. Schneier: Applied cryptography, John Wiley & Sons, 2015 • J. Schwenk: Sicherheit und Kryptographie im Internet, Springer 2020 • D. Wong: Kryptografie in der Praxis, Dpunkt Verlag, 2023 • D. Wätjen: Kryptographie: Grundlagen, Algorithmen, Protokolle, Springer 2018

Künstliche Intelligenz für Cyber Security

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	ITS6	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Künstliche Intelligenz für Cyber Security	a) Deutsch	a) 22,5 h	a) 67,5 h	a) 15
	b) Künstliche Intelligenz für Cyber Security, Praktikum	b) Deutsch	b) 22,5 h	b) 67,5 h	b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... die Herausforderungen und Lösungen für den Einsatz von KI für die Sicherheit von Cyber Systems beschreiben.

... die verschiedenen ML-Ansätze mit ihren anwendungsspezifischen Anforderungen benennen.

... Metriken zur Bewertung von ML-Anwendungen für Cyber-Systems erklären

Verständnis (2):

... die Anforderungen an Hardware, Protokolle und die System-Architektur für sicherheitsspezifische Anwendungsfälle evaluieren.

... Vorgehensweisen für die Anwendung von KI-Ansätzen (z.B. Modellbau durch Lernen mit Daten) und CRITIS-Lösungen entwerfen.

... Interpretationen von ML-Ergebnissen und deren Weiterverarbeitung verstehen.

Anwendung (3):

... ein Konzept für ML-Anwendungen für Cyber-Sicherheit erstellen.

... ML-Modelle auswählen, erstellen und bewerten.

... Threat-Analysen für Anwendungsszenarien entwickeln.

Analyse (4):

... ML-Lösungen hinsichtlich Funktionsmehrung, Performanz und Sicherheitsanforderungen analysieren.

... Qualitätsanalysen von Daten für die ML-Verarbeitung ausführen und gegebenenfalls verbessern.

... Analysen von ML-Methoden zur Anwendung für Cyber-Sicherheit ausführen.

3 Inhalte

a)

- Sicherheitsbedrohungen in Cyber-Physical Systems
- Cybersicherheit und Widerstandsfähigkeit von industriellen Kontrollsystemen und kritischen Infrastrukturen
- Blockchain-Ansätze für Cyber-Sicherheit (z.B. Audit, Remote-Wartungsarbeiten)
- Datenqualitätsanalysemethoden im Bereich Cyber-Physical Systems

	• KI-Methoden zu Anomalie-Erkennung für verschiedene Cyber-Anwendungsfälle, Prozesse, Software, Netzwerk und Hardware • Angriffe auf ML-Anwendungen • Entwicklungs-Workflow für ML-Anwendungen und Re-Training-Methoden. • Kontextorientierte Anomalie-Erkennung b) In begleitenden Übungen werden die Kenntnisse zu KI und Cyber Security vertieft. Dabei werden aktuelle technische und wissenschaftliche Problemstellungen wie z.B. Threat-Analyse von Cyber-Infrastrukturen als praktische Übung im Team erarbeitet. Spezielle Themen werden als Seminararbeit vergeben wie beispielsweise: • Unterschiedliche Sicherheitsmechanismen bei der Zwei-Faktor-Authentifizierung für kollaborative Computer-Umgebungen • Entdeckung und Verfolgung von DDoS-Angriffsgruppen mit einem komplexen Netzwerk • IDS Anomalie-Erkennung mit maschinellem Lernen
4	**Lehrformen** a) Vorlesung b) Praktikum
5	**Teilnahmevoraussetzungen**
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (3 LP) b) Studienleistung: 1 sbA (Praktische Arbeit) (3 LP)
7	**Verwendung des Moduls** IT-Sicherheit und Cyber Security B. Sc. (ITS)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Prof. Dr. Christoph Reich
9	**Literatur** • Pohlmann; „Cyber-Sicherheit - Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“; Springer Vieweg Wiesbaden; 2022; https://doi.org/10.1007/978-3-658-36243-0 • Wendzel; „IT-Sicherheit für TCP/IP- und IoT-Netzwerke - Grundlagen, Konzepte, Protokolle, Härtung“; Springer Vieweg Wiesbaden; 2021; https://doi.org/10.1007/978-3-658-33423-9 • Tuomo Sipola, Tero Kokkonen, Mika Karjalainen; “Artificial Intelligence and Cybersecurity - Theory and Applications”; Springer Cham; 2023; https://doi.org/10.1007/978-3-031-15030-2 • Mockenhaupt; “Digitalisierung und Künstliche Intelligenz in der Produktion - Grundlagen und Anwendung“; Springer Vieweg Wiesbaden; 2021; https://doi.org/10.1007/978-3-658-32773-6

Mathematik für Informatiker 1

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	AIN1, KIR1, ITS1	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Mathematik für Informatiker 1 b) Mathematik für Informatiker 1, Übung	a) Deutsch b) Deutsch	a) 22,5 h b) 45 h	a) 37,5 h b) 75 h	a) 75 b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... mathematische und logische Strukturen identifizieren.
... spezifische Eigenschaften mathematischer Strukturen wiedergeben.
... einige Anwendungsszenarien mathematischer Strukturen benennen.

Verständnis (2):

... typische Fragestellungen aus der Informatik in Aufgabenstellungen aus der Mathematik umformulieren.
... Zusammenhänge zwischen mathematischen Objekten und Strukturen erklären.
... exakte mathematische Beweise nachvollziehen.
... grundlegende Merkmale mathematischer und logischer Systeme erkennen und beschreiben.

Anwendung (3):

... praxisbezogene Problemstellungen durch mathematische und logische Strukturen modellieren.
... etablierte Lösungsverfahren gebrauchen, um abstrakte und praxisnahe Aufgabenstellungen zu lösen.

Analyse (4):

... mathematische und logische Strukturen analysieren.

3 Inhalte

a)

- Grundlegende mathematische Strukturen (Zahlbereiche, Mengen, insbesondere Intervalle, Polynome, Funktionen)
- Boolesche Algebra (Boolesche Axiome, Schaltalgebra, insbesondere minimale Formen, Aussagenlogik, Einführung in die Prädikatenlogik, Relationen, insbesondere Ordnungen und Äquivalenzrelationen)
- Lineare Algebra (Lineare Gleichungssysteme, Lösungsverfahren, Vektorrechnung, Determinanten, Euklidsche Geometrie)
- Mathematische Grundlagen der Künstlichen Intelligenz
- Anwendungsbeispiele
  - Grundlagen der Bildverarbeitung
  - Codes (Gray, CRC, QR)
  - Einfaches Perzeptronenverfahren

	b) Übungsaufgaben, Selbsttests
4	**Lehrformen** a) Vorlesung b) Übung
5	**Teilnahmevoraussetzungen** Schulkenntnisse zur Mathematik
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (4 LP) b) Studienleistung: 1 sbA (Praktische Arbeit) (2 LP)
7	**Verwendung des Moduls** Allgemeine Informatik B. Sc. (AIN), IT-Sicherheit und Cyber Security B. Sc. (ITS), Künstliche Intelligenz und Robotik B. Sc. (KIR)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Prof. Dr. Olaf Neiße (Modulverantwortliche/r)
9	**Literatur** • R. Berghammer: Mathematik für Informatiker, Springer 2021 ebook • S. Goebbels, J. Rethmann: Mathematik für Informatiker - Eine aus der Informatik motivierte Einführung mit zahlreichen Anwendungs- und Programmbeispielen, Springer 2014 ebook • P. Hartmann: Mathematik für Informatiker - ein praxisbezogenes Lehrbuch, Springer 2019 ebook • U. Schöning: Logik für Informatiker, Spektrum, Akad. Verl. 2005 • W. Struckmann, D. Wätjen: Mathematik für Informatiker - Grundlagen und Anwendungen, Springer 2016 ebook • G. Teschl, S. Teschl: Mathematik für Informatiker 1 - Diskrete Mathematik und Lineare Algebra, Springer Spektrum 2013 e-Book • E. Weitz: Konkrete Mathematik (nicht nur) für Informatiker - mit vielen Grafiken und Algorithmen in Python, Springer Spektrum 2021 e-Book • C. Turtur: Prüfungstrainer Mathematik - Klausur- und Übungsaufgaben mit vollständigen Musterlösungen, Springer Spektrum 2014 • L. Papula: Mathematik Klausur- und Übungsbuch, Springer Vieweg 2020

Mathematik für Informatiker 2

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	AIN2, KIR2, ITS2	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Mathematik für Informatiker 2 b) Mathematik für Informatiker 2, Übung	a) Deutsch b) Deutsch	a) 22,5 h b) 45 h	a) 37,5 h b) 75 h	a) 75 b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... algebraische Strukturen mit algorithmischen Anwendungen in der Informatik benennen und diesen ihre Eigenschaften/Invarianten zuordnen.

... Methoden und Verfahren der Mathematik in der Anwendung bei informationsverarbeitenden Aufgabenstellungen benennen.

Verständnis (2):

... Eigenschaften / Invarianten von algebraischen Strukturen mit algorithmischen Anwendungen der Informatik verstehen und berechnen.

... mathematische Lösungsansätze für Problemstellungen aus der angewandten Informatik nachvollziehen.

Anwendung (3):

... algebraische Strukturen mit algorithmischen Anwendungen aus dem Bereich der Informatik anwenden und bewerten.

... mathematische Verfahren auf konkrete Beispiele der Datenverarbeitung und -analyse anwenden.

... mathematische Methoden zur optimalen Parameteranpassung einsetzen.

Analyse (4):

... mathematische Anforderungen und Lösungsansätze aus dem Bereich der Informatik darstellen und analysieren.

Evaluation / Bewertung (6)

... Ergebnisse mathematischer Lösungsansätze auf Fragestellungen aus der Informatik bewerten und interpretieren.

3 Inhalte

a)

- Angewandte Lineare Algebra (Orthogonalbasen, lineare Abbildungen und Matrizen, Kenngrößen von Matrizen, Matrizen im Umfeld der Statistik und Codierung und Datenanalyse)
- Mathematische Strukturen (Algebraische Strukturen, Permutationen, Komplexe Zahlen, Restklassengruppen)
- Methoden auf Basis diskreter Strukturen (Differentialrechnung mehrdimensionaler polynomialer Funktionen, mehrdimensionales Newton-Verfahren, Gradientenverfahren, Multivariate Analyse, Multidimensionale Skalierung)

	• Anwendungsbeispiele: Mathematische Grundlage für - Rendering - Bildverarbeitung (JPEG) - Trennkurvenbestimmung / Anomaliedetektion - fehlerkorrigierende Codierung - Regressionsanalyse - Markov-Kette b) Anhand von Übungsaufgaben werden die in der Vorlesung bereitgestellten Methoden und Verfahren geübt. Selbst- und Abschlusstests zur Lernstandermittlung.
4	**Lehrformen** a) Vorlesung b) Übung
5	**Teilnahmevoraussetzungen** Das Modul „Mathematik für Informatiker 1“ sollte absolviert sein.
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (4 LP) b) Studienleistung: 1 sbA (Praktische Arbeit) (2 LP)
7	**Verwendung des Moduls** Allgemeine Informatik B. Sc. (AIN), IT-Sicherheit und Cyber Security B. Sc. (ITS), Künstliche Intelligenz und Robotik B. Sc. (KIR)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Prof. Dr. Olaf Neiße (Modulverantwortliche/r)
9	**Literatur** • R. Berghammer: Mathematik für Informatiker, Springer 2021 ebook • L. Göllmann, Ch. Henig: Arbeitsbuch zur linearen Algebra : Aufgaben, Lösungen und Vertiefungen, Springer Spektrum 2019 • P. Hartmann: Mathematik für Informatiker - ein praxisbezogenes Lehrbuch, Springer 2019 ebook • C. Meinel, M. Mundhenk: Mathematische Grundlagen der Informatik -- Mathematisches Denken und Beweisen, Springer Vieweg 2015 • E. Weitz: Konkrete Mathematik (nicht nur) für Informatiker - mit vielen Grafiken und Algorithmen in Python, Springer Spektrum 2021 e-Book • R. Zobel: Diskrete Strukturen -- eine angewandte Algebra für Informatiker, Wissenschaftsverl. Bibliogr. Institut 1987

Netzwerkmanagement und -sicherheit

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	AIN-CN4, ITS3	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Netzwerkmanagement und -sicherheit b) Netzwerkmanagement und -sicherheit, Praktikum	a) Deutsch b) Deutsch	a) 22,5 h b) 22,5 h	a) 67,5 h b) 67,5 h	a) 40 b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... Technologien aus den Bereiench IT-Management, -Monitoring, sowie Netzwerkplanung und -Analyse benennen und damit umgehen.

... Notwendige organisatorische und technologische Vorkehrungen und Möglichkeiten zur Einführung und Aufrechterhaltung der IT-Sicherheit

Verständnis (2):

... wesentliche Konzepte bei der Planung und Strukturierung von IT-Netzen erklären.

... notwendige Grundlagen aus Elektro- und Messtechnik benennen.

... für die grundlegende Vorgehensweise für systematische Fehlersuche beschreiben.

... Netzwerk-Basisservices wie DHCP, DNS oder Mail unter IPv4 und IPv6 installieren.

Anwendung (3):

... Das Gelernte anwenden, um je nach Anforderung und Problem verschiedene drahtgebundene und drahtlose Netzwerke miteinander zu vergleichen

... Administration und Anwendungen von drahtgebundenen und drahtlosen Netzwerken durchführen

... Sicherheitspolicies und Sicherheitsanwendungen mitbestimmen

3 Inhalte

a)

Übersicht und Einordnung von Netzwerkkomponenten in das ISO/OSI Schichtenmodell
Einführung in SNMP zur Wartung und Diagnose von Netzwerkgeräten
Aufbau, Betrieb und Weiterentwicklung sowie Darstellung von Netzwerken
Elektrotechnische Grundlagen der Datenübertragung in Computernetzwerken
SAN- und NAS-Anwendungen
Umsetzung von Datensicherheit durch RAID
Umsetzung redundanter und sicherer Serveranwendungen
Prüfen von Netzwerkverkehr durch Firewall und Deep Packet Inspection
Planung, Management und Betrieb von Rechenzentren inklusive Notfallplan und Fehlersuche

	Übersicht über mobile Telekommunikationsnetzwerke b) Case Studies über Computer-Netzwerk-Infrastrukturen
4	**Lehrformen** a) Vorlesung b) Praktikum
5	**Teilnahmevoraussetzungen**
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (3 LP) b) Studienleistung: 1 sbA (Praktische Arbeit) (3 LP)
7	**Verwendung des Moduls** Allgemeine Informatik B. Sc. (AIN), IT-Sicherheit und Cyber Security B. Sc. (ITS)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Prof. Dr. Achim Karduck (Modulverantwortliche/r) Prof. Dr. Richard Zahoransky (Modulverantwortliche/r)
9	**Literatur** Sauter, M.: Grundkurs Mobile Kommunikationssysteme, Springer Verlag, 2022 Rech., J. Wireless LANs Brückner, V.: Globale Kommunikationsnetze, Springer Verlage, 2022 Sauter M. Grundkurs Mobile Kommunikationssysteme : 5G New Radio und Kernnetz, LTE-Advanced Pro, GSM, Wireless LAN und Bluetooth, 8. Auflage, Springer 2022 A. Luntovskyy, D. Gütter: Moderne Rechnernetze: Protokolle, Standards und Apps in kombinierten drahtgebundenen, mobilen und drahtlosen Netzwerken, Springer Vieweg, 2020 IEEE Digital Library

Praktisches Studiensemester

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	900 h	30	AIN5, KIR5, ITS5	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Einführung Praktisches Studiensemester	a) Deutsch	a) 11,25 h	a) 78,75 h	a) 75
	b) Praktisches Studiensemester	b) Deutsch	b) 0 h	b) 720 h	b) 75
	c) Praktisches Studiensemester, Seminar	c) Deutsch	c) 11,25 h	c) 78,75 h	c) 75

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... die im Studium erworbenen Kenntnisse und Fähigkeiten in einem IT-Unternehmen erproben und vertiefen sowie um die dort gewonnenen Erfahrungen ergänzen.

Verständnis (2):

... ein umfassendes Verständnis für die IT-Praxis (u. a. Struktur und Funktionsweise eines IT-Unternehmens) gewinnen.

Anwendung (3):

... ihre Fähigkeiten einsetzen, um in einem Team gemeinsam und verantwortlich an Lösungen zu arbeiten.

Analyse (4):

... konkrete Vorstellungen über die möglichen Arbeitsfelder von Informatikerinnen und Informatikern entwickeln.

... die Ergebnisse ihrer Arbeit sowie die dabei gewonnenen Erkenntnisse auf das Wesentliche reduzieren und präsentieren.

... ihr Fachwissen und ihre Erfahrungen systematisch nutzen, um Lösungsstrategien für komplexe Fragestellungen zu entwickeln.

... ihre individuellen Interessen und Fähigkeiten weiterentwickeln, um geeignete Schwerpunkte für das weitere Studium und die Bachelorarbeit auszuwählen sowie um konkrete Vorstellungen für ihre spätere Berufswahl zu entwickeln.

3 Inhalte

a) Die Studierenden werden in die organisatorischen und administrativen Belange des Praktischen Studiensemesters eingeführt.

b) Die Studierenden werden von erfahrenen Personen angeleitet und übernehmen anspruchsvolle Tätigkeiten, vorzugsweise der integrativen Art, in einem einschlägigen Unternehmen. Die Tätigkeiten entsprechen der fachlichen Ausrichtung des Studiengangs und sind so definiert, dass die Studierenden an den für Informatiker typischen Aufgaben mitwirken können.

	c) Die Studierenden präsentieren die wesentlichen Tätigkeiten und Erfahrungen aus dem Praktischen Studiensemester. Dabei sollen die Studierenden auch darauf eingehen, welche Fähigkeiten und Kompetenzen sie im Praxissemester in besonderem Maße vertiefen konnten.
4	**Lehrformen** a) Seminar b) c) Seminar
5	**Teilnahmevoraussetzungen** Abgeschlossenes Grundstudium (bei Antritt des Praktischen Studiensemesters). Das Seminar "Einführung in das Praktische Studiensemester“ muss ein Semester vor Antritt des Praktischen Studiensemesters absolviert werden. Um ein qualifizierendes Praxissemester zu ermöglichen, dürfen vor Antritt des Praktischen Studiensemesters nur bis zu zwei Module im Umfang von bis zu 12 Leistungspunkten offen sein. Bei Fragen wenden Sie sich bitte an den Studiendekan.
6	**Prüfungsformen** a) Studienleistung 1sbKO (Kolloquium) (3 LP) b) Studienleistung 1sbA (Praktische Arbeit) (24 LP) c) Studienleistung 1sbB (Bericht) (3 LP insgesamt für alle Teilprüfungsleistung dieser Lehrveranstaltung) c) Studienleistung 1sbPN (Präsentation)
7	**Verwendung des Moduls** Allgemeine Informatik B. Sc. (AIN), IT-Sicherheit und Cyber Security B. Sc. (ITS), Künstliche Intelligenz und Robotik B. Sc. (KIR)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Studiendekan
9	**Literatur**

Programmierung

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	AIN1, ITS1, KIR1	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Programmierung b) Programmierung, Praktikum	a) Deutsch b) Deutsch	a) 22,5 h b) 45 h	a) 37,5 h b) 75 h	a) 75 b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... einfache Programme in der Programmiersprache Python unter Verwendung gängiger Sprachelemente erstellen.

Verständnis (2):

... die Bedeutung grundsätzlicher Begriffe wie Variable, Kontrollstruktur, Datentyp, Funktion, Parameter sowie Klasse erklären

... in Python geschriebene Programme lesen und verstehen

... das Prinzip der Objektorientierung verstehen und einfache Klassen umsetzen

Anwendung (3):

... eigene Programme mit den behandelten Sprachelementen entwickeln.

3 Inhalte

a)

- einfache Datentypen
- zusammengesetzte Datentypen (Listen, Dictionaries)
- Variablen, Ausdrücke und Wertzuweisungen
- Funktionen, Parameter und Argumente
- Kontrollstrukturen (bedingte Anweisungen, Schleifen)
- Verwendung vordefinierter Klassen
- Definition eigener Klassen

b) Die Inhalte der Vorlesung werden in Übungsaufgaben angewendet.

4 Lehrformen

a) Vorlesung

b) Praktikum

5 Teilnahmevoraussetzungen

	Keine
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (2 LP) b) Studienleistung: 1 sbA (Praktische Arbeit) (4 LP)
7	**Verwendung des Moduls** Allgemeine Informatik B. Sc. (AIN), IT-Sicherheit und Cyber Security B. Sc. (ITS), Künstliche Intelligenz und Robotik B. Sc. (KIR)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** N.N. (Modulverantwortliche/r)
9	**Literatur** • N. Ceder: The Quick Python Book Taschenbuch; Manning (2018) • M. Inden: Python lernen – kurz & gut; O'Reilly (2023) • M. Kofler: Python: Der ideale Python-Einstieg für Informatikstudium, Ausbildung und Beruf; Rheinwerk (2021)

Physische Sicherheit von Rechenzentren und Serverräumen

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	6.	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Physische Sicherheit von Rechenzentren und Serverräumen	a) Deutsch	a) 22,5 h	a) 67,5 h	a) 30
	b) Physische Sicherheit von Rechenzentren und Serverräumen, Workshop	b) Deutsch	b) 22,5 h	b) 67,5 h	b) 12

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1) und Verständnis (2):

… die aus kriminellem Handeln resultierenden Risiken und Lastannahmen für die schutzbedürftigen Assets einer Einrichtung beschreiben.

… die Zusammenhänge zwischen der Gewährleistung hochverfügbarer IT-Systeme, der Informationssicherheit sowie des Datenschutzes einerseits und der physischen Sicherheit von Rechenzentren und Serverräumen andererseits herstellen (Verfügbarkeit, Vertraulichkeit, Integrität).

…die Bestandteile eines Sicherungskonzeptes zur Gewährleistung der infrastrukturellen Sicherheit und deren Wirkungszusammenhänge erkennen.

Anwendung (3) und Evaluation (6):

…die Risikobeurteilung und die daraus abzuleitenden Schutzzielbestimmung auf ein konkretes Schutzobjekt übertragen

…die risikomindernden Einzelmaßnahmen zum Schutz vor Intrusion und Gewährleistung der Informationssicherheit objektspezifisch zu einem Sicherungskonzept zusammenstellen,

…die Akzeptanz und Leistungsfähigkeit von festgelegten Sicherungsmaßnahmen durch Awareness-Maßnahmen, Qualitätsmanagement, Dokumentation und Berücksichtigung des kollektiven Arbeitsrechts verstetigen.

3 Inhalte

a)

- Sicherheit, Verfügbarkeit, Vertraulichkeit, Integrität
- Standortanalyse
- Erhebung und Identifizierung schutzbedürftiger Assets
- Kriminalitätsformen (Phänomenologie / Ätiologie), Risiken, Täterprofile, Schadensereignisse
- Risikobeurteilung (Risikoidentifikation, Risikoanalyse, Risikobewertung)
- Gebäude und Rechenzentrum / Serverräume / Datenträgerarchive / Büroarbeitsplätze / Heimarbeitsplätze
- Definition von Schutzzielen
- Schutzzonenmodell
- Erstellung von Sicherungskonzeptionen, Grundsätze der Sicherheitsplanung

	• Baul.-mechanische, technische, organisatorische u. personelle Sicherungsmaßnahmen als notwendige Bestandteile von Sicherungskonzepten und deren komplementäres Zusammenwirken • Redundanz und Diversität, Gleichwertigkeit • Gesetzliche Vorgaben, Normen und Standards physischer Sicherheit im Bereich von Informationssicherheit und Cyber-Security • Rechtliche Rahmenbedingungen: NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, IT-SicherheitsG, BSIG, KRITIS-Dachgesetz KRITIS-VO, BetriebsVG, DSGVO, BDSG, Strafrechtxxxx b) • Sicherheitstechnik (Einbruchmeldetechnik, Zutrittskontrolle, Videoüberwachung, Sensoren der Überwachungstechnik, physische Grenzen, Manipulationsmöglichkeiten, Alternativen), • baulich-mechanische Sicherheitslösungen (Stahl, Beton, Glas) • Umsetzung der in der Vorlesung behandelten Aspekte in ein konkretes Sicherungskonzept anhand eines konkreten Beispiels
4	**Lehrformen** a) Vorlesung b) Workshop
5	**Teilnahmevoraussetzungen**
6	**Prüfungsformen** a) Prüfungsleistung 1K (Klausur) (3 LP) b) Studienleistung: 1sbA (Praktische Arbeit) (3 LP)
7	**Verwendung des Moduls** IT-Sicherheit und Cyber Security B. Sc. (ITS)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Prof. Dr. Ludger Stienen
9	**Literatur** • Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK): Notstromversorgung in Unternehmen und Behörden, Bonn 2019 • Bundesamt für die Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kompendium • BSI-Standards 200-1, 200-2, 200-3 • Bundesministerium des Innern: Schutz Kritischer Infrastrukturen: Basisschutzkonzept - Empfehlungen für Unternehmen, Bonn 2005 Bundesministerium des Innern: Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement, Leitfaden für Unternehmen und Behörden, Bonn 2011 • DIN EN ISO/IEC 27001 • DIN EN ISO/IEC 27002 • DIN EN 50600-1 VDE 0801-600-1 • DIN EN 50600-2-1 VDE 0801-600-2-1

	• Friedl, Wolfgang J.: Rechenzentrums-Sicherheit - Sicherheitstechnische Beurteilung, Maßnahmen gegen Gefährdungen, Springer Verlag Berlin/Heidelberg 2012 • Gundel, Stephan/Mülli, Lars: Unternehmenssicherheit, München 2009 Müller, Klaus-Rainer: Handbuch Unternehmenssicherheit – Umfassendes Sicherheits-, Kontinuitäts- und Risikomanagement mit System, Wiesbaden 2015 • National Institute of Standards and Technology (NIST): Assessing Security and Privacy Controls for Federal Information Systems and Organizations, 2022 • Verband für Sicherheitstechnik (VfS): Elektroakustische Alarmierungseinrichtungen, Hamburg 2010 • Verband für Sicherheitstechnik (VfS): Videotechnik, Hamburg 2010 • Verband für Sicherheitstechnik (VfS): Gefahrenmanagement-Systeme, Hamburg 2010 • Verband für Sicherheitstechnik (VfS): Perimetersicherung, Hamburg 2014 • Von zur Mühlen, Rainer: Sicherheits-Management: Grundsätze der Sicherheitsplanung, Stuttgart 2014, Boorberg-Verlag

Rechnerarchitektur und Betriebssysteme

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	AIN2, KIR2, ITS2	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Rechnerarchitektur und Betriebssysteme	a) Deutsch	a) 22,5 h	a) 37,5 h	a) 60
	b) Rechnerarchitektur und Betriebssysteme, Praktikum	b) Deutsch	b) 45 h	b) 75 h	b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... die grundlegenden Eigenschaften und Komponenten eines Computers benennen.
... die Speicherstrukturierung nach Code, Data, BSS, Stack und Heap erläutern.
... gängige synchrone uns asynchrone Kommunikationsprotokolle erklären.
... Methoden und Aufgaben von Betriebssystemen verdeutlichen.

Verständnis (2):

... typische Probleme erkennen, die sich durch Nebenläufigkeit ergeben.
... die Zusammenarbeit von Programmen und Betriebssystemen verstehen.
... die Abarbeitung von normalen Befehlen, Interrupts und Ein-Ausgabe begreifen.
... das Zusammenspiel von CPU, RAM, ROM, E/A und Kommunikationsbus durchschauen.

Anwendung (3):

... Betriebssystemfunktionen anwenden.
... die grundlegenden Ein-Ausgabe Elemente und Interruptsteuerung eines Computers effizient in einer Anwendung konfigurieren und in Betrieb nehmen.
... Rechnerkomponenten etwa über I2C im Bereich der Kommunikation nutzen.

Analyse (4):

... wichtige Systemeigenschaften wie CPU- und interne Busarchitektur einschätzen und bewerten.
... Betriebssysteme anhand grundlegender Charakteristika analysieren und kritisch beurteilen.

3 Inhalte

a)

- Prozessorarchitekturen: von Neumann und Harvard, RISC und CISC
- Besonderheiten von C in der maschinennahen Programmierung
- Grundlagen von Assemblersprachen
- vektorisierter Interrupt, Unterprogramme und Stack
- GPIO, ADC, DAC, DMA, Timer, UART

	• Threads, Scheduling • Nebenläufigkeit, Deadlocks • Speicherverwaltung • Dateiverwaltung b) Die Vorlesungsinhalte werden in praktischen Übungen vertieft.
4	**Lehrformen** a) Vorlesung b) Praktikum
5	**Teilnahmevoraussetzungen** Programmierung
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (2 LP) b) Studienleistung: 1 sbA (Praktische Arbeit) (4 LP)
7	**Verwendung des Moduls** Allgemeine Informatik B. Sc. (AIN), Künstliche Intelligenz und Robotik B. Sc. (KIR), IT-Sicherheit und Cyber Security B. Sc. (ITS)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Prof. Dr. Ralf Gerlich
9	**Literatur** • H. Bähring: Mikrorechnertechnik Band I+II, Springer (2002) • R. Oechsle: Parallele und verteilte Anwendung in Java, Hanser (2022) • A. Silberschatz et al: Operating System Concepts, Wiley (2019) • W. Stallings: Operating Systems: Internals and Design Principles, Pearson (2017) • A. S. Tanenbaum: Moderne Betriebssysteme, Pearson (2016) • J. Yiu: The Definite Guide to ARM Cortex-M3 and Cortex-M4 Processors, Newnes (2013)

Security-Projekt 1

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	ITS4	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Security-Projekt 1 b) Security-Projekt 1, Seminar	a) Deutsch b) Deutsch	a) 0 h b) 11,25 h	a) 120 h b) 48,75 h	a) 15 b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... die im Studium erworbenen Kenntnisse und Fähigkeiten mit praktischen Erfahrungen bereichern und damit ein besseres Verständnis für die Projektarbeit (Organisation, Methodik und soziale Komponente der Projektarbeit) entwickeln.

Verständnis (2):

... den zur Durchführung eines Projekts notwendigen Informationsbedarf ermitteln und die erforderlichen Ergebnisse erarbeiten.

Anwendung (3):

... im Team und innerhalb einer vorgegebenen Frist eine Lösung für eine einschlägige Aufgabenstellung aus der Praxis bearbeiten (dabei werden sie die im bisherigen Verlauf des Studiums erworbenen Kenntnisse anwenden und vertiefen).

Analyse (4):

... ihre individuellen Interessen und Fähigkeiten weiterentwickeln, so dass sie geeignete Schwerpunkte für das restliche Studium setzen und sich auf geeignete Stellen im Praxissemester bewerben können.

... die Ergebnisse ihrer Arbeit auf das Wesentliche reduzieren, präsentieren und bewerten.

3 Inhalte

a) Es wird eine praktische Arbeit zu einer einschlägigen, in der Regel von einem Unternehmen der regionalen Wirtschaft vorgegebenen, praktischen Aufgabenstellung aus den Bereichen IT-Sicherheit und Cyber-Security angefertigt. Die Studierenden arbeiten im Team. Das Ziel liegt (auch) darin, dass die erarbeitete Problemlösung beim „Themensteller“ zum Einsatz kommt.

b)

4 Lehrformen

a) Workshop

b) Seminar

5	**Teilnahmevoraussetzungen** Programmieren, Software Engineering, Netzwerksicherheit, Grundlagen der IT-Sicherheit
6	**Prüfungsformen** a) Prüfungsleistung: 1 A (Praktische Arbeit) (4 LP) b) Studienleistung: 1 sbR (Referat) (2 LP)
7	**Verwendung des Moduls** IT-Sicherheit und Cyber Security B. Sc. (ITS),
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Studiendekan (Modulverantwortliche/r)
9	**Literatur**

Security-Projekt 2

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	ITS6	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Security-Projekt 2 b) Security-Projekt 2, Seminar	a) Deutsch b) Deutsch	a) 0 h b) 11,25 h	a) 120 h b) 48,75 h	a) 15 b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... die im Studium soweit erworbenen Kenntnisse und Fähigkeiten mit praktischen Erfahrungen bereichern.

... ein vertieftes Verständnis für die Anforderungen einer effizienten Teamarbeit an realen Projekten (Organisation, Methodik und soziale Komponente der Projektarbeit) entwickeln.

Verständnis (2):

... den zur Durchführung eines Projekts notwendigen Informationsbedarf ermitteln und die erforderlichen Ergebnisse erarbeiten.

Anwendung (3):

... im Team und innerhalb einer vorgegebenen Frist eine Lösung für eine einschlägige Aufgabenstellung aus der Praxis erarbeiten. Dabei werden die im bisherigen Verlauf des Studiums erworbenen Kenntnisse auf eine konkrete Aufgabenstellung übertragen und vertieft.

Analyse (4):

... die Ergebnisse ihrer Arbeit als Team auf das Wesentliche reduzieren, aufbereiten und präsentieren.

... ihre individuellen Interessen, Fähigkeiten und Studienschwerpunkte weiter vertiefen, so dass sie im weiteren Studienverlauf geeignete Themenstellungen für eine spätere Thesis suchen, erkennen und einordnen können.

3 Inhalte

a) Es wird eine praktische Arbeit zu einer einschlägigen, in der Regel von einem Unternehmen der regionalen Wirtschaft vorgegebenen, praktischen Aufgabenstellung aus den Bereichen IT-Sicherheit und Cyber-Security angefertigt. Die Studierenden arbeiten im Team. Das Ziel liegt (auch) darin, dass die erarbeitete Problemlösung beim „Themensteller“ zum Einsatz kommt.

b)

4 Lehrformen

a) Workshop

b) Seminar

5 Teilnahmevoraussetzungen

	Softwareprojekt 1, Projektmanagement
6	**Prüfungsformen** a) Prüfungsleistung: 1 A (Praktische Arbeit) (4 LP) b) Studienleistung: 1 sbR (Referat) (2 LP)
7	**Verwendung des Moduls** IT-Sicherheit und Cyber Security B. Sc. (ITS)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Studiendekan (Modulverantwortliche/r)
9	**Literatur** • S. Portney: Grundlagen des Projektmanagements, Wiley VCH (2019)

Sichere Programmierung

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	ITS3	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Sichere Programmierung	a) Deutsch	a) 22,5 h	a) 67,5 h	a) 15
	b) Sichere Programmierung, Praktikum	b) Deutsch	b) 22,5 h	b) 67,5 h	b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... den Unterschied zwischen kompilierten und interpretierten Sprachen nennen

... verstehen, wie es in kompilierten und interpretierten Programmen zu Schwachstellen kommen kann.

... verstehen, wie Software entwickelt wird und wie im Rahmen des Softwareentwicklungsprozesses typische Sicherheitslücken und Angriffsvektoren verhindert werden können

Verständnis (2):

... häufige Fehler verstehen, die in der Programmierung zu Sicherheitsschwachstellen führen können

… den Softwareentwicklungsprozess nachverfolgen und verstehen, wie Fehler zu Schwachstellen führen können

... Maßnahmen verstehen, die automatisiert oder manuell die Qualität von Software in Bezug der IT-Sicherheit erhöhen

Anwendung (3):

... einen sicheren Softwareentwicklungsprozess beschreiben und aufsetzen

… bestehenden Programmcode auf Sicherheitsrisiken untersuchen

3 Inhalte

a)

Interpretierte und kompilierte Programmiersprachen

Zusammenhang zwischen Stackspeicher, Rücksprungadressen, CPU, Instruction Pointer und Variablen in kompiliertem Programmcode

Sicherheitslücken in Programmen (z.B., Injection, Speicherüberlauf, fehlende Eingabevalidierung,...) und deren Funktionsweise

Tools und Prozesse zur Entwicklung sicherer Software wie Ticket-System, Build-Pipeline, dynamische und statische Software-Tests sowie Fuzzing.

b) Die Inhalte der Vorlesung werden in Übungsaufgaben und Beispielen angewandt.

4 Lehrformen

a) Vorlesung

	b) Praktikum
5	**Teilnahmevoraussetzungen** Grundlagen der IT-Sicherheit, Programmierung
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (3 LP) b) Studienleistung: 1 sbA (Praktische Arbeit) (3 LP)
7	**Verwendung des Moduls** IT-Sicherheit und Cyber Security B. Sc. (ITS)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** N.N.
9	**Literatur** Henning Wolf; Stefan Roock, Stefan Zumbrägel, Agile Softwareentwicklung : ein Überblick. dpunkt.verlag, 2023. Waidner, Michael, Bodden, Eric, Entwicklung sicherer Software durch Security by Design, Fraunhofer-Verlag, 2013.xxx

Software Engineering

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	AIN3, KI3	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Software Engineering b) Software Engineering, Praktikum	a) Deutsch b) Deutsch	a) 22,5 h b) 22,5 h	a) 67,5 h b) 67,5 h	a) 60 b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... die Methoden, Techniken und Werkzeuge zur systematischen Erstellung von Softwaresystemen, insbesondere in den Phasen Analyse und Entwurf, darlegen

... verschiedene Formalismen und Elemente der Unified Modeling Language (UML) zur statischen und dynamischen Modellierung von Software beschreiben

... die Rolle der Object Constraint Language (OCL) für die Spezifikation von Software erfassen und wichtige Sprachelemente der OCL erklären

... ausgewählte Entwurfsmuster wiedergeben

Verständnis (2):

... die Bedeutung eines systematischen Vorgehens zur effizienten Konzeption, Modellierung und Implementierung qualitativ hochwertiger Software verstehen

... die charakteristischen Eigenschaften sowie die Stärken und Schwächen ausgewählter UML-Diagrammtypen zur Analyse und Entwurf von Software beurteilen

... die Rolle von Software-Architekturen verstehen und zentrale Software-Architekturstile beschreiben

Anwendung (3):

... unterschiedliche Aspekte einer Anwendungsdomäne mit Hilfe eines UML-Werkzeugs modellieren und die Möglichkeiten der Generierung von Programmcode nutzen

... UML und OCL zur Modellierung ausgewählter Analyse- und Entwurfsmuster nutzen

... ausgewählte Entwurfsmuster zielgerichtet einsetzen.

3 Inhalte

a)

- Grundlegende Vorgehensmodelle sowie Phasen und Artefakte der Softwareentwicklung
- Grundlagen des Requirements Engineering
- Objektorientierte Analyse und Entwurf mit UML
- Statische und dynamische Modellierung mit UML
- OCL im Kontext der Modellierung von Software
- Transformation von Modellen in eine Zielsprache am Beispiel von Java

	• Ausgewählte Entwurfsmuster • Software-Architekturen b) Anhand von Übungsaufgaben wird das in der Vorlesung erworbene Wissen semesterbegleitend vertieft und verfestigt. Dies umfasst insbesondere die Modellierung vorgegebener Anwendungsdomänen mit UML und OCL sowie dem Einsatz von Entwurfsmustern.
4	**Lehrformen** a) Vorlesung b) Praktikum
5	**Teilnahmevoraussetzungen** Programmierung
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (3 LP) b) Studienleistung: 1 sbA (Praktische Arbeit) (3 LP)
7	**Verwendung des Moduls** Allgemeine Informatik B. Sc. (AIN), Künstliche Intelligenz und Robotik B. Sc. (KIR)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Prof. Dr. Bernhard Hollunder (Modulverantwortliche/r)
9	**Literatur** • Bernhard Rumpe. Modellierung mit UML. Springer Verlag (2012) • Stephan Kleuker. Grundkurs Software-Engineering mit UML. Springer Verlag (2018) • Chris Rupp, Stefan Queins. UML 2 glasklar. Hanser Verlag (2012) • Raul Sidnei Wazlawick. Object-oriented Analysis and Design for Information Systems. Elsevier / Morgan Kaufmann (2014) • http://www.omg.org/spec/UML/. • http://www.omg.org/spec/OCL/.

Stochastik

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	KIR3, ITS3	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Stochastik b) Stochastik, Übung	a) Deutsch b) Deutsch	a) 22,5 h b) 22,5 h	a) 67,5 h b) 67,5 h	a) 30 b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... die Grundbegriffe der Wahrscheinlichkeitslehre und Statistik sicher verwenden.
... verschiedene diskrete und kontinuierliche Modelle für Wahrscheinlichkeitsräume benennen und parametrisieren.
... Kenngrößen von zufallsbehafteten Datensätzen angeben und einordnen.
... iterative Verfahren zur Optimierung von Zielfunktionen (unter Nebenbedingungen) benennen.

Verständnis (2):

... grundlegenden Fragestellungen der Stochastik verstehen.
... Kenngrößen von zufallsbehafteten Datensätzen und Wahrscheinlichkeitsverteilungen in Beziehung stellen.
... die mathematischen Hintergründe von Optimierungsverfahren nachvollziehen.

Anwendung (3):

... zu gegebenen zufallsbehafteten Datensätze geeignete Modelle aufstellen und deren Parameter optimal belegen.
... zufallsbehafteten Datensätze softwareunterstützt bearbeiten und auswerten.
... Solver für Optimierungsprozesse anwenden.
... optimierte Stichprobenversuche planen.

3 Inhalte

a)

- Grundbegriffe der Wahrscheinlichkeitslehre (Ergebnis, Ereignis, Wahrscheinlichkeit mit Verteilungs- und Dichtefunktion, stochastische Unabhängigkeit)
- Zentrale Ergebnisse zur Wahrscheinlichkeit (Zentraler Grenzwertsatz, Satz von Bayes, Gesetze großer Zahlen)
- (ein- und mehrdimensionale) Zufallsgrößen und deren Invarianten (Erwartungswert, Varianz, Streuung)
- Beziehungen zwischen Zufallsgrößen (Kovarianz, Korrelation, Varianz, Streuung)
- Kenngrößen von Stichprobendatensätzen (Lage- und Streumaße)
- Schätzverfahren: Punkt- und Bereichsschätzer für Modellparameter (Maximum-Likelihood, erwartungstreu, stabil)
- Optimierungsverfahren von linearen Zielfunktionen unter linearen Nebenbedingungen (Simplex)
- Optimierungsverfahren von nichtlinearen (z.B. konvexen) Zielfunktionen unter Nebenbedingungen (Gradientenverfahren , Lagrangesche Multiplikatorenregel)

Anwendungsbeispiele:

	• Optimale Parameteranpassung • Funktionale Sicherheit, z.B. in Netzwerken oder in der Robotik • Empfehlungssysteme • Entscheidungmechanismen bei risikobehafteten Systemen b) Anhand von Übungsaufgaben werden die in der Vorlesung bereitgestellten Methoden und Verfahren geübt, auch unter Verwendung des Statistikprogramms R.
4	**Lehrformen** a) Vorlesung b) Übung
5	**Teilnahmevoraussetzungen** Das Modul „Mathematik für Informatiker 2“ sollte absolviert sein.
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (3 LP) b) Studienleistung: 1 sbA (Praktische Arbeit) (3 LP)
7	**Verwendung des Moduls** IT-Sicherheit und Cyber Security B. Sc. (ITS), Künstliche Intelligenz und Robotik B. Sc. (KIR)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Prof. Dr. Olaf Neiße (Modulverantwortliche/r)
9	**Literatur** • G. Fischer: Einführung in die Stochastik, Springer 2015 ebook • G. Kersting, A. Wakolbinger: Elementare Stochastik, Birkhauser 2010 • N. Kurt : Stochastik für Informatiker, Springer 2020 ebook • B. Walther: Statistik mit R Schnelleinstieg, mitp Verlag 2022 ebook • D. Wentura, B. Wirth, M. Pospeschill: Multivariate Datenanalyse mit R, Springer 2023 ebook

Studienkompetenzen

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	AIN, KIR, ITS 1 und 2	Jedes Semester	2 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Lern- und Präsentationkompetenzen, Seminar	a) Deutsch	a) 22,5 h	a) 67,5 h	a) 25
	b) Digital- und Schreibkompetenzen, Seminar	b) Deutsch	b) 22,5 h	b) 67,5 h	b) 25

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

... verschiedene Lernmethoden benennen,
... Präsentationsmedien und deren adäquaten Einsatz beschreiben,
... Grundlagen wissenschaftlichen Arbeitens definieren,
... Grundlagen der Kommunikation beschreiben,
... Merkmale einer Präsentation inkl. Regeln zur Foliengestaltung definieren.

Verständnis (2):

... die Wirkung von Präsentationen und persönlichem Auftreten verstehen,
... wissenschaftliche Texte erschließen und zentrale Aussagen herausarbeiten.

Anwendung (3):

… Fähigkeit zum kollaborativen Arbeiten anwenden,
… wirkungsvoll interagieren,
... Lernmethoden und -techniken in Lehrveranstaltungen und im Selbststudium effektiv und effizient anwenden,
... selbstständig und zielgerichtet wissenschaftliche Literatur recherchieren und wesentliche Inhalte herausarbeiten,
... wirkungsvolle und zielgruppenorientierte fachliche Präsentationen vorbereiten, erstellen und durchführen,
… aus digitalen Informationen valides Wissen zu ausgewählten Themengebieten aufbauen,
… wissenschaftliche Texte nach wissenschaftlichen Standards verfassen,
… digitale Informationen kritisch hinterfragen,
… die Auswirkungen des eigenen digitalen Handelns reflektieren und ethische Entscheidungen treffen.

3 Inhalte

a)

- Präsentation mit fachlichem Bezug
- wirkungsvolle und zielgerichtete Kommunikation (u.a. Feedback geben und nehmen)
- Interaktion über Online-Kanäle (u.a. digitale Umgangsformen)
- Teamarbeit (effizient und effektiv zusammenarbeiten)
- Zeit- und Selbstmanagement

	b) • Informationskompetenz (recherchieren, bewerten, zusammenfassen, dokumentieren) • Schreibkompetenz • Grundlagen des wissenschaftlichen Arbeitens • Digitale Ethik • Möglichkeiten und Grenzen des Einsatzes von KI -Tools beim Schreiben
4	**Lehrformen** a) Seminar b) Seminar
5	**Teilnahmevoraussetzungen**
6	**Prüfungsformen** a) Prüfungsleistung 1 sbR (Referat) (3 LP) b) Prüfungsleistung 1sbR (Referat) (3 LP)
7	**Verwendung des Moduls** Allgemeine Informatik B. Sc. (AIN), IT-Sicherheit und Cyber Security B. Sc. (ITS), Künstliche Intelligenz und Robotik B. Sc. (KIR)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** N.N.
9	**Literatur** a) • Leminsky, Carsten; Schulz-Wolfgramm, Eibo; Hackenberg, Wolfgang (2017): Key Message. Business-Präsentationen mit Struktur. 3. Auflage. Freiburg: Haufe-Lexware GmbH & Co. KG • Schoof, Axel; Binder, Karin (2017): Auf den Punkt: Präsentationen pyramidal strukturieren. Erfolgreicher kommunizieren mit klaren Botschaften und ergebnisorientierter Struktur. 2., überarb. Auflage. Wiesbaden: Springer Gabler • Seifert, J.W (2010). Visualisieren, Präsentieren, Moderieren. Offenbach: Gabal • Zelazny, Gene (2015): Wie aus Zahlen Bilder werden. Der Weg zur visuellen Kommunikation - Daten überzeugend präsentieren. 7., überarb. Aufl. 2015. Wiesbaden, s.l.: Springer Fachmedien Wiesbaden b) • Esselborn-Krumbiegel H. (2017): Von der Idee zum Text. Eine Anleitung zum wissenschaftlichen Schreiben, utb Paderborn • Klein, A. (2019). Wissenschaftliche Arbeiten schreiben - Praktischer Leitfaden mit über 100 Software-Tipps, 2. Auflage. mitp Verlag • Theisen, M. R., & Theisen, M. (2017). Wissenschaftliches Arbeiten: Erfolgreich bei Bachelor- und Masterarbeit, 17., aktualisierte und bearb. Aufl. München: Verlag Franz Vahlen • Voss, R. (2020). Wissenschaftliches Arbeiten: ... leicht verständlich! : mit zahlreichen Abbildungen und Übersichten. 7. überarb. Aufl. München: UVK Verlag

Thesis

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	540 h	18	AIN7, KIR7, ITS7	Jedes Semester	1 Semester

1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	a) Thesis Vorbereitungsseminar	a) Deutsch	a) 11,25 h	a) 78,75 h	a) 75
	b) Bachelorarbeit	b) Deutsch	b) 0 h	b) 360 h	b) 75
	c) Thesis Seminar	c) Deutsch	c) 11,25 h	c) 78,75 h	c) 75

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

… ein einschlägiges anwendungsorientiertes Thema der Informatik fachlich darstellen und beurteilen

Anwendung (3):

… den zur Bearbeitung notwendigen Informationsbedarf im Wesentlichen selbstständig ermitteln, einschlägige Quellen dafür identifizieren, die erforderlichen Informationen aus den Quellen extrahieren und Schlussfolgerungen daraus ziehen,

… innerhalb einer vorgegebenen Frist das ausgewählte Thema wissenschaftlich und selbstständig bearbeiten,

Analyse (4):

… zu den von anderen Studierenden erarbeiteten Ergebnissen Stellung nehmen (im Rahmen des Seminars).

… die wesentlichen Ergebnisse ihrer Arbeit begründen, auf das Wesentliche reduzieren und präsentieren.

… ihr Wissen systematisch kombinieren, um Lösungsstrategien für komplexe fachliche Fragestellungen zu entwickeln und zu dokumentieren.

3 Inhalte

a) Es wird eine wissenschaftliche Arbeit zu einem einschlägigen aktuellen Thema angefertigt. Die Arbeit soll Ergebnisse oder Erkenntnisse zu aktuellen Fragestellungen, im Wesentlichen Fragen aus der Praxis der Informatik, enthalten.

4 Lehrformen

a) Seminar

b)

c) Seminar

5 Teilnahmevoraussetzungen

Das Seminar „Einführung in das Thesissemester“ muss ein Semester vor Antritt der Bachelorarbeit absolviert werden. Sonstige Teilnahmevoraussetzungen: siehe den Allgemeinen Teil der Studien- und Prüfungsordnung der Hochschule

6 Prüfungsformen

a) Studienleistung 1sbKO (Kolloquium) (3 LP)

	b) Prüfungsleistung 1T (Thesis) (12 LP) c) Prüfungsleistung 1sbPN (Präsentation) (3 LP)
7	**Verwendung des Moduls** Allgemeine Informatik B. Sc. (AIN), IT-Sicherheit und Cyber Security B. Sc. (ITS), Künstliche Intelligenz und Robotik B. Sc. (KIR)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Studiendekan
9	**Literatur**

Web Security und Intrusion Prevention

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	ITS4	Jedes Semester	1 Semester

	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
1	a) Web Security und Intrusion Prevention b) Web Security und Intrusion Prevention, Workshop	a) Deutsch b) Deutsch	a) 22,5 h b) 22,5 h	a) 67,5 h b) 67,5 h	a) 15 b) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):
- ... Bekannte und häufige Schwachstellen in (Web-) Anwendungen kennen
- ... Darstellen, wie unsicherer Code in Webanwendungen angreifbar sein kann
- ... Maßnahmen, um Webanwendungen sicher zu gestalten, zu betreiben und Schwachstellen zu umgehen

Verständnis (2):
- ... Die Schwere, mögliche Angriffe und Gefahren von Schwachstellen verstehen
- ... Möglichkeiten zur Detektion von Angriffen

Anwendung (3):
- ... Anwendung des Gelernten, um die Sicherheit einer Webanwendung zu beurteilen
- ... Entwicklung sicherer Webanwendungen
- ... Administration und Monitoring einer Webanwendung

3 Inhalte

a)

Technologien von Webanwendungen
Code Injection
Cross-Site-Scripting
Weitere häufige Schwachstellen (OWASP Top 10)
Authentifizierung und Autorisierung
Auditierung und Monitoring

b) Die Inhalte der Vorlesung werden in Übungsaufgaben angewendet.

4 Lehrformen

a) Vorlesung

	b) Workshop
5	**Teilnahmevoraussetzungen** Computernetze
6	**Prüfungsformen** a) Prüfungsleistung: 1 K (Klausur) (3 LP) b) Studienleistung: 1 sbA (Praktische Arbeit) (3 LP)
7	**Verwendung des Moduls** IT-Sicherheit und Cyber Security B. Sc. (ITS)
8	**Modulbeauftragte/r und hauptamtlich Lehrende** Prof. Dr. Richard Zahoransky (Modulverantwortliche/r)
9	**Literatur** Paco Hope, Ben Walther, Web Security Testing Cookbook, O'Reilly, 2008 Gilberto Najera-Gutierrez, Juned Ahmed Ansari, Daniel Teixeira, Abhinav Singh: Improving your Penetration Testing Skills, O'Reilly, 2019 Dafydd Stuttard, Marcus Pinto:The Web Application Hacker's Handbook, Wiley, 2011 Ryan Soper, Nestor N. Torres, Ahmed Almoailu: ZED ATTACK PROXY COOKBOOK : hacking tactics, techniques, and procedures for testing web applications and APIs, O'Reilly, 2003 Scott Cosentino: The Complete Guide to Bug Bounty Hunting, O'Reilly, 2023 Owasp Top Ten, OWASP, 2021

Physical Protection / Gebäudesicherheit

Kennnummer	Workload	Credits	Studiensemester	Häufigkeit des Angebots	Dauer
	180 h	6	ITS6	Jedes Semester	1 Semester

	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
1	a) Ausgewählte Fragen der Cyber Security	a) Deutsch	a) ??? h	a) 180 h	a) 15

2 Lernergebnisse / Kompetenzen

Nach erfolgreicher Teilnahme am Modul können die Studierenden …

Wissen (1):

Verständnis (2):

...

Anwendung (3):

....

Analyse (4):

... i.

Synthese (5):

....

3 Inhalte

a)

4 Lehrformen

a) Prüfung

5 Teilnahmevoraussetzungen

6 Prüfungsformen

a)

7 Verwendung des Moduls

IT-Sicherheit und Cyber Security B. Sc. (ITS)

8 Modulbeauftragte/r und hauptamtlich Lehrende

Studiendekan

9	**Literatur**