TECHNISCHE HOCHSCHULE DEGGENDORF

Modulhandbuch
Bachelor Cyber Security

Fakultät Angewandte Informatik
Prüfungsordnung 13.04.2019
Stand: Montag 08.03.2021 13:28

CY-B-01 Mathematik 1

Modul Nr.	CY-B-01
Modulverantwortliche/r	Prof. Dr. Johannes Grabmeier
Kursnummer und Kursname	Mathematik 1
Lehrende	Prof. Dr. Marcus Barkowsky Prof. Dr. Johannes Grabmeier Prof. Dr. Dr. Heribert Popp Prof. Dr. Thomas Störtkuhl
Semester	1
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden erwerben die für das Bechelorstudium der Cyber Security erforderlichen mathematischen Grundkenntnisse aus Analysis, Linearer Algebra, Fuzzy Mathematik und Zahlentheorie. Die Studierenden erwerben formale und mathematische Kompetenz, so dass sie Probleme formal beschreiben können. Sie wenden ihre mathematischen Kenntnisse bei der Lösung formaler Aufgaben erfolgreich an. Die Studierenden sind in der Lage geeignete mathematische Werkzeuge wie ein Computeralgebra-System oder ein

Tabellenkalkulationsprogramm zur Lösung der Aufgabenstellungen einzusetzen. Durch Gruppenarbeit lernen die Studierenden Kooperationsfähigkeit.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Studierenden verfügen über Grundkenntnisse der mathematischen Modellierung im Bereich Cyber Security.

Methodenkompetenz

- Die Studierenden verfügen über vertiefte Kenntnisse mathematischer Methoden zur Bearbeitung praktischer Aufgaben (Behandlung komplexer Zusammenhänge mit Matrizen, Lineare Gleichungssysteme, Funktionen (mehrerer) Variablen als Basis zum Verständnis von Modellen).

Persönliche Kompetenz

- Die Studierenden sind zu vertieften eigenem Zeitmanagement und zum Selbststudium befähigt, da sie ca. 50 % mit virt. Lehre den Stoff erarbeiten.

Sozialkompetenz

- Die Studierenden verfügen über einen Einblick in die Lösung von Problemen durch Gruppenarbeit und Teamarbeit.

Verwendbarkeit in diesem und in anderen Studiengängen

Dieses Modul ist Grundlage für das Modul CY-B-07 Mathematik 2. Die Inhalte des Moduls werden in weiteren Modulen des Studiengangs aufgegriffen.

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- mathematisches und abstraktes Denkvermögen

Inhalt

1 Mathematische Grundkenntnisse
   - Logik und Boolsche Algebra sowie Induktionsbeweis
   - Mengenlehre und Relationen
   - Zahlbereiche und Arithmetik
   - Folgen und Reihen
   - Abbildungs-/Funktionsbegriff

2 Lineare und nichtlineare Funktionen und ihre Eigenschaften

3 Differentiation (Differentiationsregeln, Höhere Ableitungen, Kurvendiskussion)
4 Grundlagen der Integralrechnung
- Der Riemannsche Integralbegriff
- Regeln zur Integration (Partielle Integration, Substitutionsregel, Partialbruchzerlegung)

5 Differentialrechnung bei Funktionen mit mehreren unabhängigen Variablen
- Lineare und Nichtlineare Funktionen mit mehreren unabhängigen Variablen
- Partielle Ableitungen
- Hessematrix und Extremwertbestimmung
- Extremwertbestimmung unter Nebenbedingungen (Lagrange)

6 Lineare Algebra und Matrizenrechnung
- Vektorräume, Basis und lineare Gleichungssysteme
- Lineare Abbildungen und invertierbare Matrizen
- Der Gauss'sche Algorithmus zur Lösung linearer Gleichungssysteme
- Determinanten

7 Fuzzy Mathematik
- Fuzzy Mengen und ihre Operationen
- Unscharfe Zahlen und unscharfe Relationen
- Linquistische Variablen und Fuzzy-Regeln
- Fuzzy Multi-Kriteria-Analyse

8 Einführung in Graphentheorie

Lehr- und Lernmethoden

- Vorlesung und Übungen
- vorlesungsbegleitende Tutorien
- kollaboratives Lernen mit E-Learning
- Studierende erhalten eine Liste, welche Teilkapitel sie virtuell bis zu welchem Präsenztermin vorbereiten müssen

Besonderes

Bis zum Ende des zweiten Semesters müssen die Studierenden die Prüfung dieses Moduls erstmals angetreten haben.

Empfohlene Literaturliste

- Auer, Benjamin, Seitz, Franz, Grundkurs Wirtschaftsmathematik. 2. Aufl. Gabler, Wiesbaden, 2009

- Bauer, Ch., Clausen, M., Kerber, A., Meier-Reinhold, H., Mathematik für Wirtschaftswissenschaftler, Schäffer-Poeschel, 5. überarbeitete Aufl., 2008
- Bradley, Teresa, Patton, Paul, Essential Mathematics for Economics and Business, John Wiley & Sons, 1998
- Holland, Heinrich, Holland, Doris, Mathematik im Betrieb, 7. Aufl., Gabler Verlag, Wiesbaden, 2004
- Jenks, R. D., Sutor, R. S., AXIOM -- The Scientific Computation System, Springer Verlag, Heidelberg, 1992
- Ohse, Dietrich, Mathematik für Wirtschaftswissenschaftler II, Lineare Wirtschaftsalgebra, 4. Aufl. Verlag Vahlen, 2000
- Pfuff, Franz, Mathematik für Wirtschaftswissenschaftler kompakt , 3. Aufl., Vieweg+Teubner Verlag, Braunschweig, 2009
- Popp, Heribert: Anwendungen der Fuzzy-set-Theorie in Industrie- und Handelsbetrieben, Wirtschaftsinformatik, 1994
- Tilli, T. A: Fuzzy-Logik, 2. Auflage, Francis 1992

CY-B-02 Programmierung 1

Modul Nr.	CY-B-02
Modulverantwortliche/r	Prof. Dr. Marcus Barkowsky
Kursnummer und Kursname	Programmierung 1
Lehrende	Prof. Dr. Marcus Barkowsky Prof. Dr. Benedikt Elser
Semester	1
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	LN, schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden verfügen über grundlegendes allgemeines Wissen und grundlegendes Fachwissen im Bereich der Programmierung. Der Fokus liegt noch stark auf imperativer Programmierung aber es werden auch erste objektorientierte Konzepte vermittelt. Die Studierenden sind in der Lage das Wissen praktisch anzuwenden und einfache bis mittelschwere Probleme zu lösen.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Studierenden verstehen die Konzepte der modularen Gestaltung von Software.
- Die Studierenden können eigene einfache softwaretechnische Ideen umsetzen.

Methodenkompetenz

- Die Studierenden haben die Fähigkeit, Programme unter Einsatz einer modernen objektorientierten Programmier-Plattform zu erstellen.

Persönliche Kompetenz

- Die Studierenden können eigene einfache softwaretechnische Ideen gegenüber konkurrierenden Ansätzen verteidigen.

Sozialkompetenz

- Im Rahmen der Lehrveranstaltung finden Programmierübungen statt. Die Studierenden sind damit in der Lage, die Inhalte von Programmen Ihrer Kommilitonen zu verstehen, zu kritisieren und duch eigene Programme zu komplementieren. Sie sind in der Lage, Programme in einer Form zu erstellen, die eine Kooperation im Team zulässt.

Verwendbarkeit in diesem und in anderen Studiengängen

Grundlegende Einführung in die Programmierung

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- abstraktes Denkvermögen

Inhalt

Programmierung 1: Einführung mit Java

Teil 1: Schnelleinstieg in die Imperative Programmierung

1 Überblick
   - Hallo Welt
   - Variablen, Abbildung im Arbeitsspeicher
   - Datentypen
   - Operatoren

2 Kontrollstrukturen
   - Verzweigungen
   - Schleifen

3 Programmierung
- Programmiersprachen, Maschinensprache vs. Hochsprache
- Compiler
- Programmerstellung
- Compilierfehler vs. Laufzeitfehler

4 Funktionen und Methoden
- Rückgabewert, Name und Parameterliste
- Rekursion

Teil 2: Objektorientierte Programmierung

1 Abstraktion
- Klassen und Objekte
- Instanzvariablen, Klassenvariablen, lokale Variablen
- Methoden und Überladung
- Konstruktoren

2 Datentypen und Operatoren
- Primitive Datentypen
- Boolsche Operatoren
- Bitweise Operatoren
- Referenzdatentypen
- Zuweisung
- Object
- Operatoren
- Unterschiede zwischen Datentypen
- Zuweisung, Kopie, Vergleiche
- Parameterübergabe
- Cast
- Spezielle Referenzdatentypen
- String, Array
- Wrapper, Enum

3 Kapselung
- Abstrakte Datentypen
- Geheimnisprinzip und Modularisierung
- Modifikatoren
- JavaDoc
- Packages

4 Beziehugen
- Arten von Beziehungen
- Vererbung
- Polymorphismus
- Abstrakte Klassen
- Interfaces
- Generics

Lehr- und Lernmethoden

- Lehrveranstaltung mit PowerPoint
- Praktikum mit vielen Übungsaufgaben
- Gruppenarbeit

Besonderes

Bis zum Ende des zweiten Semesters müssen die Studierenden die Prüfung dieses Moduls erstmals angetreten haben.

Empfohlene Literaturliste

- Krüger, G.: Java-Programmierung ? Das Handbuch zu Java 8, O'Reilly Verlag GmbH & Co. KG, Auflage: 8 (31. Mai 2014), ISBN-13: 978-3955615147
- Krüger, G.: Handbuch der Java-Programmierung, Addison-Wesley Verlag; Auflage: 7. Auflage (1. Oktober 2011), ISBN-13: 978-3827327512
- Krüger, G.: freie HTML-Ausgabe der 7. Auflage (Stand 2011): http://javabuch.de/download.html
- Ullenboom C.: Java ist auch eine Insel: Das Standardwerk für Programmierer, Rheinwerk Computing; Auflage: 15 (25. Juni 2020), ISBN-13: 978-3836277372
- Ullenboom C.: Java ist auch eine Insel, Auflage: 12: http://openbook.rheinwerk-verlag.de/javainsel/

CY-B-03 Grundlagen der Informatik

Modul Nr.	CY-B-03
Modulverantwortliche/r	Prof. Dr. Thomas Störtkuhl
Kursnummer und Kursname	Grundlagen Informatik
Lehrende	Prof. Dr. Cezar Ionescu Prof. Dr. Thomas Störtkuhl
Semester	1
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden verfügen über grundlegendes allgemeines Wissen und grundlegendes Fachwissen im Bereichen Informatik.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Kenntnis und Verständnis von wesentlichen Grundlagen der Informatik, deren Konzepten und Methoden

- Fachliche Kompetenz diese Grundlagen selbständig nachzuvollziehen und an Beispielen anzuwenden

Methodenkompetenz

- Formale Beweise durchführen, schriftlich und mit geeigneter Software
- Syntax von symbolischen Ausdrücken formal beschreiben
- Reguläre Ausdrücke mit endlichen Automaten implementieren
- Digitale Schaltkreise entwicklen

Persönliche Kompetenz

- Studierende formulieren eigenständig logisch stichhaltige Argumente
- Studierende finden die Lücken in fehlerhaften Argumenten
- Studierende erkennen die Vor- und Nachteile der Digitalisierung

Verwendbarkeit in diesem und in anderen Studiengängen

Modul kann in anderen Studiengängen verwendet werden wie Ba. WI, Ba. AI oder Ba. Cyber Security

Zugangs- bzw. empfohlene Voraussetzungen

keine

Inhalt

- Grundlagen der theoretischen Informatik
  - Logik
  - Berechenbarkeit
  - Endliche Automaten
  - Formale Sprachen
  - Komplexitätstheorie
- Grundlagen der technischen Informatik:
  - Schaltnetze und Schaltwerke
  - Rechnerarchitektur
  - Speicherorganisation
  - Internettechnologie

Lehr- und Lernmethoden

- Seminaristiches Unterricht
- Bei jedem Thema, werden entsprechende Software-Werkzeuge eingeführt und für die Übungen benutzt.

Empfohlene Literaturliste

- Jon Barwise und John Etchemendy: Sprache, Beweis und Logik, Band I, Mentis 2005
- Susan H. Rodger und Thomas W. Finley: JFLAP: An Interactive Formal Languages and Automata Package, online bei http://jflap.org/
- Erich Hehner: Digital Circuit Design, Vorlesungsskript online bei http://www.cs.toronto.edu/~hehner/DCD/DCD.pdf
- J. Glenn Brookshear und Dennis Brylow: Computer Science--An Overview, 12th Ed, Pearson, 2015

CY-B-04 Betriebssysteme und Netzwerke

Modul Nr.	CY-B-04
Modulverantwortliche/r	Prof. Dr. Andreas Fischer
Kursnummer und Kursname	Betriebssysteme und Netzwerke
Lehrende	Prof. Dr. Peter Faber Prof. Dr. Andreas Fischer
Semester	1
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Teil Betriebssysteme

Die Studierenden erhalten Einblick in die Bedeutung von Betriebssystemen als zentrale Grundlage für die Informationsverarbeitung in Unternehmen. Für die heutigen Ausprägungen von Betriebssystemen bauen sie Verständnis auf. Nach Absolvieren des Teilmoduls Betriebssysteme haben die Studierenden folgende Lernziele erreicht:

- Die Studierenden erlangen Kenntnis von Konzepten und Technologien, die für den Aufbau von Betriebssystemen notwendig sind und Wissen über den modularen Aufbau und die Funktionsweise von Betriebssystemen.

- Die Studierenden erwerben Wissen und Fertigkeiten über die Konfiguration, die Administration und die sichere Anwendung von Betriebssystemen anhand von kommerziellen Betriebssystemen.
- Die Studierenden ordnen und bewerten moderne Betriebsformen von Rechenzentren, wie z. B. Virtualisierung oder Cloud Computing im Kontext der Betriebssysteme.
- Die Studierende erhalten einen Einblick in die theoretischen Grundlagen eines Linuxsystems sowie einen Überblick über die wichtigsten Shellbefehle.
- Die Studierenden installieren und administrieren einen Linuxserver.

Teil Netzwerke

- Bedeutung von Schichtenmodellen und die Aufgaben und Funktionen der Schichten des ISO/OSI-Modells sowie die wichtigsten Dienstvertreter jeder Schicht erläutern.
- Die Konzepte von Anwendungsprotokollen wie HTTP und SMTP wiedergeben und ihre Funktionsweise z.B. mit Sequenzdiagrammen nachvollziehen.
- Einfache Internetanwendungen unter Zuhilfenahme von Sockets programmieren.
- Netzwerkprobleme mit geeigneten Tools analysieren und diagnostizieren

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach

Anrechenbar für das gleichnamiges Pflichtfach im Ba. Cyber Security.

Zugangs- bzw. empfohlene Voraussetzungen

Keine

Inhalt

- Rechtemanagement (Authentifizierung, Authorisierung)
- Prozesse & Threads, Inter-Prozess Kommunikation
- Deadlocks, Mutex-Verfahren
- Peripherie / Ein-/Ausgabe
- Betriebssystem API, Userspace / Kernelspace
- Umgang mit Linux / Unix / POSIX
- Umgang mit Shells - graphisch und textbasiert (insbesondere praktischer Umgang mit der Kommandozeile)

- Nutzung von Systemvirtualisierung (z.B.: Hypervisors, VirtualBox, XEN, Docker, ...)
- Verwendung von Systemcalls
- Schichtenmodell: OSI
- Netzwerktopologien (Bus, Baum, Stern, teil-/vollvermascht)
- Anwendungsschicht: HTTP, SMTP & IMAP, DNS
- Transportschicht: Sockets, UDP, TCP
- Ausblick auf die Netzwerkschicht: IPv4/v6
- Verwendung von Werkzeugen und Techniken zur Netzwerkanalyse und -konfiguration (z.B. Ping, Traceroute, PuTTY/telnet, nslookup, ...)
- Verwendung von Browser Debugging Tools (Netzwerkkonsole, ...)
- Textbasierte Anwendungsprotokolle verstehen und umsetzen (z.B. HTTP Interaktionen)

Lehr- und Lernmethoden

Seminaristischer Unterricht mit praktischen Übungen

Empfohlene Literaturliste

- Andrew S. Tanenbaum, Herbert Bos; Modern Operating Systems; Prentice Hall, 4th ed., 2014
- Evi Nemeth, Garth Snyder, Trent R. Hein et ak.; Unix and Linux System Administration Handbook, Addison-Wesley, 5th ed., 2018
- Micha Gorelick & Ian Ozsvald; High Performance Python; O'Reilly, 2014
- James F. Kurose, Keith F. Ross; Computer Networking: A Top-Down Approach; Pearson, 7th ed., 2017
- Andrew S. Tanenbaum, David J. Wetherall; Computer Networks; Pearson, 5th ed., 2014

CY-B-05 Grundlagen der Informationssicherheit

Modul Nr.	CY-B-05
Modulverantwortliche/r	Prof. Dr. Martin Schramm
Kursnummer und Kursname	Grundlagen der Informationssicherheit
Lehrende	Amar Almaini
Semester	1
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden verfügen über grundlegendes allgemeines Wissen und grundlegendes Fachwissen im Bereich Informationssicherheit.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Studierenden können die gängigen Begriffe der Informationssicherheit abgrenzen und erklären.
- Sie können die grundlegenden Schutzziele der informationssicherheit beschreiben.

- Die Studierenden können die unterschiedliche Risiken unterscheiden, diese in Schadensklassen klassifizieren und geeignete Behandlungen vorschlagen.
- Sie können unterschiedliche klassische Verschlüsselungs- und Entschlüsselungsverfahen vergleichen und diese anwenden.
- Sie kennen die Funktionsweise der asymmetrischen Kryptographie und können gängige asymmetrische kryptographische Verfahren vergleichen.
- Sie können die Grundprinzipien der Kryptografischen Protokolle (Schlüsselvereinbarung; Entitätsauthentifizierung; Symmetrische Verschlüsselung; Nachrichtenauthentifizierungs) zusammenfassen.
- Sie können den Begriff Programmsicherheit erläutern, und bsp. einen Pufferüberlauf-Angriff im Code identifizieren.
- Sie können die Grundprinzipien eines sicheren Betriebssystems diskutieren und die Funktionsweise der Speicherverwaltung erklären.
- Sie können der verschiedenen Firewall-Typen abgrenzen und exemplarisch einen Paketfilter implementieren.

Methodenkompetenz

- Die Studierenden können die Methoden der Kryptoanalyse beschreiben und diese auf Geheimtexte anwenden, um Rückschlüsse zum Originaltext zu gewinnen.

Persönliche Kompetenz

- Durch die Teilnahme an Gruppendiskussionen, dem respektvollen Zuhören und der Demonstration von Interesse am Fachgebiet entwickeln die Studierenden ein Bewusstsein und eine verstärkte Aufnahmebereitschaft.

Sozialkompetenz

- Durch Gruppenarbeit, trainieren die Studierende die Teamfähigkeit und steigern Ihre Ziel- und Ergebnisorientierung.

Verwendbarkeit in diesem und in anderen Studiengängen

Wahlpflichtmodul anderer Bachelorstudiengänge (wie z.B.: Angewandte Informatik/Infotronik, Interaktive Systeme/Internet of Things, Künstliche Intelligenz, Wirtschaftsinformatik, Elektro- und Informationstechnik)

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

keine spezifischen

Inhalt

1 Einführung, Motivation und Begriffe
2 Schutzziele der Informationssicherheit
3 Risiken
  - Risikoanalyse
  - Schadensklassen
  - Risikomatrix
  - Risikobehandlung
4 Einführung in die Kryptologie
  - Grundlegende klassische Verfahren
  - Grundzüge der Kryptoanalyse
  - Einführung in die moderne Kryptographie
5 Einführung in kryptographische Kommunikationsbeziehungen
6 Grundbegriffe der Programmsicherheit
7 Grundlagen der Betriebssystemsicherheit
8 Grundlagen der Netzwerksicherheit
9 Schwachstellen, -analyse und -datenbanken
10 Arten und Typen von Hacker und Cracker
11 Information Security Management Systeme

Lehr- und Lernmethoden

- Seminaristischer Unterricht mit praktischen Übungen

Besonderes

Bis zum Ende des zweiten Semesters müssen die Studierenden die Prüfung dieses Moduls erstmals angetreten haben.

Empfohlene Literaturliste

- Secorvo: Informationssicherheit und Datenschutz, Handbuch für Praktiker und Begleitbuch zum T.I.S.P., dpunkt Verlag, 3., aktualisierte und erweiterte Auflage, September 2019, 824 Seiten, ISBN-13 : 978-3864905964
- Hanschke, I.: Informationssicherheit & Datenschutz ? einfach & effektiv: Integriertes Managementinstrumentarium systematisch aufbauen und verankern, Carl Hanser Verlag GmbH & Co. KG, ISBN-13 : 978-3446458185
- BSI - Bundesamt für Sicherheit in der Informationstechnik: Informationssicherheit und IT-Grundschutz, BSI-Standards 200-1,

200-2, 200-3 (Deutsch) Taschenbuch ? 9. Oktober 2017, ISBN-13 : 978-3846208151
- Sowa, A.: Management der Informationssicherheit: Kontrolle und Optimierung, Springer Vieweg; 1. Aufl. 2017 Auflage (16. Januar 2017), ISBN-13 : 978-3658156268
- Weber, K.: Grundlagen und Anwendung von Information Security Awareness: Mitarbeiter zielgerichtet für Informationssicherheit sensibilisieren, Springer Vieweg; 1. Aufl. 2019 Auflage (10. Mai 2019), ISBN-13 : 978-3658262570
- Eckert, C.: IT-Sicherheit: Konzepte - Verfahren - Protokolle, De Gruyter Oldenbourg; 10th expanded and updated edition Auflage (21. August 2018), ISBN-13 : 978-3110551587

CY-B-06 Schlüsselqualifikation 1

Modul Nr.	CY-B-06
Modulverantwortliche/r	Prof. Dr. Roland Zink
Kursnummer und Kursname	Betriebswirtschaft Medienkompetenz und Selbstorganisation
Lehrende	Prof. Dr. Thomas Bartscher Christian Bauer Prof. Dr. Christina Bauer Melanie Hazod Prof. Dr. Thomas Meier NN NN PK AI/IAS/CS Melanie Piser Prof. Dr. Konrad Schindlbeck Prof. Dr. Roland Zink
Semester	1
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210

Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Der Umstieg von der Schule zu Hochschule stellt viele Studierende gleich zu Beginn ihres Studiums vor Herausforderungen. Weg von vorgegebenen Stundenplänen und Lehrplanbezug, hin zu Eigen- und Selbstständigkeit sowie Verantwortung. Das Modul Schlüsselqualifikation 1 soll auf diese Herausforderungen insbesondere auch mit Blick auf die Digitalisierung und den wirtschaftlichen Bezug (Betriebspraktikum im 5. Semester) vorbereiten. Die Lernergebnisse des Moduls setzen sich folglich aus den beiden Fächer "Betriebswirtschaft" (**Fach A**) und "Medienkompetenz und Selbstorganisation" (**Fach B**) zusammen.

Fach A

Im Fach Betriebswirtschaft setzen sich die Studierenden insbesondere mit der Allgemeinen BWL, der Kosten- und Leistungsrechnung sowie dem Personalmanagement auseinander. Obwohl die Studierenden einen technischen bzw. informatikorientierten Studiengang belegen, soll durch das angeeignete betriebswirtschaftliche Wissen der Berufseinstieg erleichtert werden. Durch die Verbreiterung der Wissensbasis bei den Studierenden sollen suboptimale Entscheidungen in Unternehmen vermieden werden.

Fachkompetenz

- Die Studierenden lernen die betrieblichen Funktionalbereiche im Überblick und ausgewählte Konzepte der Unternehmensführung/Strategieentwicklung kennen.
- Die Studierenden kennen und verstehen die Grundsätze und Methoden einer systematischen Entscheidungsfindung.
- Die Studierenden kennen die Zwecke der Kosten- und Leistungsrechnung (KLR) und den Aufbau eines KLR-Systems
- Sie sind mit wichtigen Instrumenten der KLR, der Kostenstellen- und Kostenträgerrechnung sowie der kurzfristigen Erfolgsrechnung vertraut
- Sie werden befähigt, kostenstellen- und auftragsbezogene Soll-Ist-Vergleiche (SIV) durchzuführen und bewerten
- Sie können die Teilkostenrechnung in Form der Deckungsbeitragsrechnung anwenden
- Sie werden befähigt, Entscheidungsrechnungen auf Basis der KLR durchzuführen

Fach B

Die digitale Transformation der Gesellschaft dringt immer weiter in unser Berufs- und Alltagsleben vor und ist gekennzeichnet durch eine rasch ansteigende Informationsfülle. Um mit dieser Informationsfülle umgehen und kommunizieren zu können, bedarf es bei Studierenden eine hohe Medienkompetenz. Die Inhalte orientieren sich am Medienkompetenzraster der Kultusministerkonferenz (2016) mit seinen sechs Säulen:

1 Suchen, Verarbeiten und Aufbewahren
2 Kommunizieren und Kooperieren
3 Produzieren und Präsentieren
4 Schützen und sicher Agieren
5 Problemlösen und Handeln
6 Analysieren und Reflektieren

Die in der Schule erworbenen Kompetenzen sollen gezielt für die Herausforderung des Studiums erweitert werden. Dabei stehen nicht mehr das Suchen und Präsentieren von Informationen, sondern deren Auswahl, Bewertung und Interpretation im Vordergrund, also Analyse und Synthese. Das Fach führt sowohl in die Nutzung digitaler Medien im Kontext Studium, Datenschutz und Urheberrechte sowie in die eigenständige Studienorganisation ein.

Fachkompetenz

- Die Studierenden kennen verschiedene digitale Medien zur Lernorganisation und können diese anwenden.
- Die Studierenden werden befähig, sowohl analoge als auch digitale Lehr- und Lerninhalte gezielt für ihr Studium auszuwählen.
- Die Studierenden sind befähig, mit digitalen Medien kompetent und zielgerichtet umzugehen.
- Die Studierenden können ihr Studium zeitlich wie inhaltlich organisieren und die Informationsfülle zielgerichtet bearbeiten.

Fach A und B

Methodenkompetenz

- Die Studierenden werden in der KLR zu einem transparenz-, struktur- und entscheidungsorientierten Arbeiten befähigt
- Den Studierenden wird bewusst, dass die KLR zweckorientiert zu konzipieren ist
- Die Studierenden werden zu selbstständigen Arbeiten befähigt.
- Die Studierenden erwerben Kompetenzen beim Umgang mit digitalen Medien.
- Die Studierenden erlernen Strategien der Wissensaneignung mit Blended Learning Verfahren.

Persönliche Kompetenz

- Die Studierenden erlernen durch Übungen selbstständige und problem-, lösungs- bzw. handlungsorientiertes Arbeiten.

Sozialkompetenz

- Die Studierenden trainieren in den Übungen Partner- und Teamarbeit.
- Die Studierenden erlernen eigenverantwortliches Arbeiten.

Verwendbarkeit in diesem und in anderen Studiengängen

Das Modul legt Grundlagen für das Studium im Allgemeinen und ist insbesondere mit folgendem weiterführenden Modul verknüpft:

KI-B und CY-B: Schlüsselqualifikation 3

KI-B und CY-B: Schlüsselqualifikation 4

KI-B und CY-B: Praxismodul

KI-B und CY-B: Bachelormodul

Studiengang: BA Cyber Security und BA Künstliche Intelligenz

Zugangs- bzw. empfohlene Voraussetzungen

Keine Voraussetzungen.

Inhalt

Fach A

- Das Unternehmen im Überblick
    - Unternehmensführung und Unternehmenspolitik
    - Vision, Ziele, Strategien
    - Konstitutive Unternehmensentscheidungen
    - Produktionsfaktoren
    - Betriebliche Funktionen
- Überblick über die Ansätze der Entscheidungstheorie
- Zwecke der KLR u. Kostenzuordnungsprinzipien
- Systeme der KLR
- Spezifische kostenrechnerische Inhalte in den Bereichen KI und CS
- Die KLR auf der Vollkostenbasis
    - Kostenartenrechnung
    - Kostenstellenrechnung
    - Kostenträgerrechnung
- Die KLR auf Teilkostenbasis (Deckungsbeitragsrechnung)
- Die kurzfristige Erfolgsrechnung
- Entscheidungsorientierte KLR inkl. des Grundsatzes der relevanten Kosten

Fach B

- Informationen, Daten und Wissen
- Selbstorganisation und Studium gestalten
- Digitale Medien im studentischen Lernkontext
- Digitale Medien in der Wissenschaft und Kommunikation
- Datenschutz und Netiquette

- Urheber- und Nutzungsrechte
- Mediennutzung und Säulen der Medienkompetenz

Lehr- und Lernmethoden

- Seminaristischer Unterricht mit Gruppen- und Partnerarbeit
- Projektarbeit
- Blended Learning

Empfohlene Literaturliste

Fach A

- Däumler K., Grabe J. (2013): Kostenrechnung 1 ? Grundlagen, 11. Aufl., NWB-Verlag, Herne.
- Dörsam, P. (2013): Grundlagen der Entscheidungstheorie anschaulich dargestellt, 6. Auflage, PD-Verlag, Heidenau.
- Friedl G., Hofmann Ch., Pedell B. (2017): Kostenrechnung: Eine entscheidungsorientierte Einführung, 3. Aufl., Vahlen Verlag, München.
- Jorasz W., Baltzer B. (2019): Grundlagen der Kosten- und Leistungsrechnung: Lehrbuch mit Aufgaben und Lösungen, Schäffer-Poeschel Verlag, Stuttgart.
- Wöhe, G. (2016), Einführung in die allgemeine Betriebswirtschaftslehre, 26. Auflage, Vahlen, München.

Fach B

- Bänisch, A. & Alewell, D. (2013): Wissenschaftliches Arbeiten. De Gruyter Oldenbourg.
- Gapski, H., Oberle, M. & Staufer, W. (2017): Medienkompetenz. Herausforderung für Politik, politische Bildung und Medienbildung. Bonn.
- Bühler, P. & Schlaich, P. (2016): Medienkompetenz. Digitale Medien verstehen ? erstellen ? einsetzen.
- (Zusätzlich werden Internetdokumente und Leitfäden verwendet!)

CY-B-07 Mathematik 2

Modul Nr.	CY-B-07
Modulverantwortliche/r	Prof. Dr. Johannes Grabmeier
Kursnummer und Kursname	Mathematik 2
Lehrende	Prof. Dr. Johannes Grabmeier
Semester	2
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden erwerben vertiefte Kenntnisse mathematischer Themen, die in Anwendung in der Informatik und in mathematischen Gebieten, die für die Anwendungen der Künstlichen Intelligenz bzw. Cyber Security von Bedeutung sind oder die zur vertieften Abrundung mathematischer Grundkonzepte notwendig sind. Der Fokus liegt dabei auch auf mathematischen Denk-, Arbeits- und Modellierungsmethoden.

Die Studierenden sind in der Lage mathematische Fragestellungen aus der Informatik, insbesondere der Künstlichen Intelligenz bzw. Cyber Security zu erkennen, zu modellieren und zu lösen. Dazu sind sie in der Lage ein Computeralgebra-System für mathematische Modellierungen und Berechnungen einzusetzen. Die zugehörigen algorithmischen

Methoden der Mathematik werden exemplarisch erarbeitet. Die Studierenden sind in der Lage weiterführenden Veranstaltungen mit mathematischer Modellbildung erfolgreich zu absolvieren.

Im Vordergrund steht die **Fach- und die Methodenkompetenz** in den behandelten Themenfeldern.

Der Erwerb von **sozialen Kompetenzen** steht bei diesem Modul naturgemäß nicht im Vordergrund, wird aber durch Kooperation der Studierenden und gemeinsames Erarbeiten von Lösungen gefördert.

Die **persönliche Kompetenz** wird durch vertieftes selbständiges Erarbeiten und Lösen komplexer Probleme gefördert. Durch die Anwendung mathematischer Lösungstechniken und deren kritische Durchdringung erarbeiten sich die Studierende die Fähigkeit zum abstrakten und analytischen Denken.

Verwendbarkeit in diesem und in anderen Studiengängen

Die Studierenden sind in der Lage weiterführenden Veranstaltungen mit mathematischer Modellbildung erfolgreich zu absolvieren.

Weiter kann das Modul für weiterbildende, konsekutive und aufbauende Masterstudiengänge verwendet werden.

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- Inhalt des Moduls Mathematik 1

Inhalt

1 Analytische Geometrie und Eigenwerte
   - Skalarprodukte, Winkel, Abstand, Norm
   - Affine Vektorräume
   - Eigenwerte und Eigenvektoren

2 Quadriken und Bezierkurven
   - Quadriken als Lösungsmengen quadratischer Gleichungen
   - Bezierkurven

3 Ausgewählte Kapitel der diskreten Mathematik
   - Kombinatorik
   - Einführung in die Graphentheorie

4 Mathematische Grundlagen der Kryptographie
- Zahlentheoretische Grundlagen
- Anwendungen im RSA-Verfahren
- Endliche Körper

5 Komplexe Zahlen und trigonometrische Funktionen
- Komplexe Zahlen
- Trigonometrische Funktionen
- Kreisteilung und Hauptsatz der Algebra

6 Lineare Differentialgleichungen
- Lösungverfahren für linearer Differentialgleichungen
- Die Bernoulli-Differentialgleichung
- Separable Differentialgleichungen

7 Ausgewählte Kapitel der numerischen Mathematik
- Gleitkommaarithmetik und Rundungsfehler
- Hornerschema
- Iterationsverfahren zur Bestimmung von Nullstellen

Lehr- und Lernmethoden

In klassischer Vortragstechnik verbunden mit dem direkten Einsatz eines Computeralgebrasystems wird Theorie und Anwendungen vermittelt und dargestellt. Viele Konzepte werden anhand konkreter Aufgabenstellungen erarbeitet und mit einem Computeralgebrasystem gelöst. Übungsaufgaben zur eigenen Bearbeitung durch die Studierenden werden gestellt. Lösungen zu einer Auswahl davon werden zu Beginn der nächsten Vorlesung durch Studierende vorgetragen. Alternativ werden Lösungsvorschläge der Studierenden im iLearn-System diskutiert.

Kollaboratives Lernen mit E-Learning.

Besonderes

Eine der 4 SWS wird als Übung im Computerraum in 2 Gruppen vom Dozenten angeboten.

Empfohlene Literaturliste

- Bauer, Ch., Clausen, M., Kerber, A., Meier-Reinhold, H., Mathematik für Wirtschaftswissenschaftler, Schäffer-Poeschel, 5. überarbeitete Aufl., 2008
- Buchmann, J., Einführung in die Kryptographie, 4. erweiterte Aufl., Springer-Verlag, Heidelberg, 2008
- Fischer, G., Analytische Geometrie, Vieweg+Teubner, 7., durchges. Aufl., 2001

- Gathen von zur, J., Gerhard, J., Modern Computer Algebra, Cambridge-University Press, 1999
- Hämmerlin, G., Hoffmann, K.-H., Numerische Mathematik, 4. Auflage, Springer-Verlag, Berlin, 1994
- Jenks, R. D., Sutor, R. S., AXIOM -- The Scientific Computation System, Springer Verlag, Heidelberg, 1992
- Walter, W., Gewöhnliche Differentialgleichungen, 7. neubearb. u. erw. Aufl., Springer-Verlag, Berlin, 2000

CY-B-08 Programmierung 2

Modul Nr.	CY-B-08
Modulverantwortliche/r	Prof. Dr. Patrick Glauner
Kursnummer und Kursname	Programmierung 2
Lehrende	Prof. Dr. Patrick Glauner
Semester	2
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	LN, schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Das Ziel dieses Moduls ist es, den Studierenden fortgeschrittene Programmierkonzepte, Modellierungsmethoden, verschiedene Programmierparadigmen und verschiedene Werkzeuge zu vermitteln. Die Studierenden erwerben eine solidere Grundlage für den Entwurf und die Implementierung von Software. Sie lernen auch, wie man professionelle Software-Werkzeuge benutzt. Dadurch werden sie in der Lage sein, in Teams hochwertige Software zu schreiben.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Studierenden verstehen die Konzepte der professionellen Erstellung von Software.
- Die Studierenden können eigene softwaretechnische Ideen umsetzen.

Methodenkompetenz

- Die Studierenden haben die Fähigkeit, hochqualitative Programme unter Einsatz moderner Werkzeuge zu erstellen.

Persönliche Kompetenz

- Die Studierenden können eigene softwaretechnische Ideen gegenüber konkurrierenden Ansätzen verteidigen.

Sozialkompetenz

- Im Rahmen der Lehrveranstaltung finden Programmierübungen statt. Die Studierenden sind damit auch in der Lage, Programme anderer Studierenden zu verstehen, zu kritisieren und zu komplementieren.

Verwendbarkeit in diesem und in anderen Studiengängen

Unter anderem:

- Software Engineering
- Sichere Programmierung
- Penetration Testing

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- Inhalt des ersten Semesters, insbesondere Programmierung 1
- Grundlagen der Mathematik

Inhalt

- Einführung: Wiederholung der grundlegenden Programmierkonzepte, Einführung in Python
- Werkzeuge: IDEs, interaktive Umgebungen, Jupyter-Notebooks, Revisionskontrolle, Debugger, Timing von Code, Profiler, Cython, Logger, Arbeitspaket-Tracker, Bugtracker, Build Chains
- Code-Konventionen: Styleguides, Clean Code
- Modellierung: Anwendungsfalldiagramme, Aktivitätsdiagramme, Klassendiagramme, Objektdiagramme
- OOP: Decorators, Refactoring, Entwurfsmuster
- Testen: Unit-Tests, testgetriebene Entwicklung, Testabdeckung

- Speicherverwaltung: Stack und Heap, manuelles Freigeben von Speicher, Garbage Collection, Interning
- Ausnahmebehandlung: Raising und Catching, Asserts
- Dateien: Lesen und Schreiben, Löschen, Serialisierung, JSON, pickle, tabellarische Daten
- Multithreading: Parallelism und Concurrency, Erstellen von Threads, Global Interpreter Lock (GIL)
- Logik-Programmierung: Logik, deklarative Programmierung, Prolog

Lehr- und Lernmethoden

- Vorlesungen
- Diskussion von wissenschaftlichen Artikeln und aktuellen Nachrichten
- Übungen, einschließlich Rechnerübungen

Empfohlene Literaturliste

- S. Chacon and B. Straub, "Pro Git", Apress, 2nd edition, 2014.
- M. Goodrich et al., "Data Structures and Algorithms in Python", John Wiley & Sons, 2013.
- C. Larman, "Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development", 3rd edition, Prentice Hall, 2004.
- E. Matthes, "Python Crash Course: A Hands-On, Project-Based Introduction to Programming", 2nd edition, 2019.

CY-B-09 Algorithmen und Datenstrukturen

Modul Nr.	CY-B-09
Modulverantwortliche/r	Prof. Dr. Patrick Glauner
Kursnummer und Kursname	Algorithmen und Datenstrukturen
Lehrende	Prof. Dr. Patrick Glauner
Semester	2
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Ziel dieses Moduls ist es, eine Einführung in eine der wichtigsten Grundlagen eines Informatikstudiums zu geben: Algorithmen und Datenstrukturen. Eine Datenstruktur ermöglicht es einem Programmierer, Daten in konzeptionell handhabbare Zusammenhänge zu strukturieren. Ein Algorithmus ist eine endliche Folge von wohldefinierten, computer-implementierbaren Anweisungen, um eine Klasse von Problemen zu lösen oder eine Berechnung durchzuführen. Algorithmen arbeiten oft mit Datenstrukturen. Dieser Kurs bietet eine Reise durch die Informatik. Die Studierenden erwerben eine solide Grundlage davon, wie die wichtigsten Algorithmen und Datenstrukturen funktionieren. Sie lernen auch, wie man effiziente Algorithmen und Datenstrukturen entwirft.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Studierenden verstehen die Konzepte der gängigsten Algorithmen und Datenstrukturen.
- Die Studierenden können eigene Algorithmen und Datenstrukturen umsetzen.

Methodenkompetenz

- Die Studierenden haben die Fähigkeit, hochqualitative Programme unter Einsatz von Algorithmen und Datenstrukturen zu erstellen.

Persönliche Kompetenz

- Die Studierenden können eigene Algorithmen und Datenstrukturen gegenüber konkurrierenden Ansätzen verteidigen.

Sozialkompetenz

- Im Rahmen der Lehrveranstaltung finden Programmierübungen statt. Die Studierenden sind damit auch in der Lage, Algorithmen und Datenstrukturen anderer Studierenden zu verstehen, zu kritisieren und zu komplementieren.

Verwendbarkeit in diesem und in anderen Studiengängen

Unter anderem:

- Software Engineering
- Sichere Programmierung

Zugangs- bzw. empfohlene Voraussetzungen

- Inhalt des ersten Semesters, insbesondere Programmierung 1
- Grundlagen Mathematik

Inhalt

- Einführung: Algorithmen-Definition, Klassifizierung von Algorithmen
- Graphen: Graphen-Definitionen, Anwendungen in der Informatik, Shortest Path, Lowest Cost, A*
- Komplexitätsanalyse: Zeitkomplexität, O-, Omega-, Theta, o- und O-Tilde-Kalküle, Speicherkomplexität
- Listen: Arrays, dynamische Arrays/Listen, Basisoperationen, Stacks, Warteschlangen, verkettete Listen
- Rekursion: Suche, Divide and Conquer, Rekurrenzgleichungen, Master Theorem, Backtracking dynamische Programmierung

- Sortierung: Bubble Sort, Selection Sort, Insertion Sort, Merge Sort, Quicksort, untere Schranken
- Bäume: Binärbäume, Traversieren, fortgeschrittene Arten von Bäumen, Entscheidungsbäume
- Maps und Hash-Tabellen: Key-Value-Speicher, Hashing, Kollisions-Behandlung
- Ausgewählte Algorithmen: schnelle Matrix-Multiplikation, String-Matching, Primzahlen
- Quantencomputing: Qubits, Quantengatter, Quantencomputer, Quantenalgorithmen

Lehr- und Lernmethoden

- Vorlesungen
- Diskussion von wissenschaftlichen Artikeln und aktuellen Nachrichten
- Übungen, einschließlich Rechnerübungen

Empfohlene Literaturliste

- M. Goodrich et al., "Data Structures and Algorithms in Python", John Wiley & Sons, 2013.
- R. Sedgewick, "Algorithms", Addison Wesley, fourth edition, 2011.
- M. Sipser, "Introduction to the Theory of Computation", Cengage Learning, third edition, 2012.

CY-B-10 Internettechnologien

Modul Nr.	CY-B-10
Modulverantwortliche/r	Prof. Dr. Goetz Winterfeldt
Kursnummer und Kursname	Internettechnologien
Lehrende	Prof. Dr. Goetz Winterfeldt
Semester	2
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Studenten nutzen Commandozeilen Werkzeuge, um sich im mit Servern zu verbinden und Daten auszutauschen. Sie nutzen Server und Client Technologien, um einfache Kommunikationen zwischen Systemen aufzubauen.

Sie setzten eine nodjs Infrastruktur auf und integrieren Webkomponenten, um Inhalte an den Browser auszuliefern. Studenten gestalten Webseiten. Sie wissen, wie man Seiten strukturiert und kennen grundlegende Sprachen um Webseiten zu gestalten (CSS, HTML, Java Script). Sie habe kleine JavaScript Programme geschrieben.

Basierend auf diesen Kenntnissen führen Projekte ein eigenes Projekt durch. Sie wenden dabei ihre Wissen über Webtechnologien an. Sie bewerten die Ergebnisse anderer Gruppen und werden selber mit ihrem Projekt bewertet worden. Dabei

haben die Studenten Standard-Werkzeuge (GIT, Visual Code, Command Line) der Webprogrammierung genutzt.

Nach Beendigung des Kurses können Studenten eigene Projekte durchführen und Internet (Web) Applikationen entwickeln. Im Kurs wird nicht auf Datenbanken und Netzwerktechnologien eingegangen, da diese Themen in anderen Vorlesungen verankert sind.

Verwendbarkeit in diesem und in anderen Studiengängen

Das Modul ist für die Studiengänge "angewandte Informatik", "Interaktive Systeme" und verwandte Studiengänge geeignet

Zugangs- bzw. empfohlene Voraussetzungen

Grundlagen der Programmierung mit Java oder einer anderen Objekt orientierten Sprache. Kenntnisse aus dem Bereich Netzwerktechnologien und Datenbanken erleichtern die Projektdurchführung.

Inhalt

Das Modul setzt sich aus zwei Teilen zusammen:

Teil I Internettechnologien Grundlagen und einem Teil II Projektarbeit Internettechnologien

Inhalt Teil 1

(1) Werkzeuge und Installation

(2) Gundlagen Client - Server, Protokolle

(3) Client Webtechnologien

- Html

-CSS

- Java Script

(4) Server Technologien

(5) Propritäre Applikationen

- Sockets

- Datenformate

- Session Management

Inhalte Teil 2

Workshop: Setup Infrastruktur - Cloud based Services

Projekt: Realisierung einer Webapplikation

Lehr- und Lernmethoden

Vorlesungen, Tutorials und kleine Praktika.

Besonderes

Das Modul finde in zwei Teilen statt. Es ist notwendig, dass der erste Teil beendet wurde, bevor der zweite Teil gestartet wird. Da sonst wichtige Voraussetzungen fehlen (Projektarbeit Teil 2).

CY-B-11 Kryptologie 1

Modul Nr.	CY-B-11
Modulverantwortliche/r	Prof. Dr. Martin Schramm
Kursnummer und Kursname	Kryptologie 1
Lehrende	Prof. Dr. Martin Schramm
Semester	2
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	LN Praxis, schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden verfügen über grundlegendes allgemeines Wissen und grundlegendes Fachwissen in den Bereichen Kryptographie, Krytoanalyse und Steganographie.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Studierenden können die grundlegenden existierenden Schutzziele und schützenswerte Güter (assets) darstellen und erklären.
- Sie können unterschiedliche klassische Verschlüsselungs- und Entschlüsselungsverfahen anwenden und diese kryptoanalytisch untersuchen.

- Sie können existierende Primzahlentests (deterministisch wie probabilistisch) erklären und diese implementieren, um Primzahlen beliebiger Länge zu testen/generieren.
- Sie können die gängigen symmetrischen kryptographischen Algorithmen erklären und können Betriebsmodi von Blockchiffren hinsichtliche Vor- und Nachteile gegenüberstellen.
- Sie können die Grundprinzipien der asymmetrischen Kryptographie (Ver-, Entschlüsselung / Erzeugung und Verifikation digitaler Signaturen) sowie gängige asymmetrische kryptographische Verfahren und Integritätsalgorithmen beschreiben.
- Sie können unterschiedliche Angriffe auf mathematische Problemklassen der modernen Kryptographie durchführen und begründen, wesshalb gewisse Parameter kryptographischer Verfahren gut/schlecht gewählt wurden.

Methodenkompetenz

- Die Studierenden können für ein gegebenes Szenario beurteilen, welche Assets wichtig sind, welche Schutzziele in diesem Kontext erfüllt werden müssen sowie passende kryptographische Mechanismen hierzu auswählen.
- Sie können weiterführende (nicht-behandelte) kryptographische Verfahren vergleichen, differenzieren und gegenüberstellen.

Persönliche Kompetenz

- Durch die Teilnahme an Gruppendiskussionen, dem respektvollen Zuhören und der Demonstration von Interesse am Fachgebiet entwickeln die Studierenden ein Bewusstsein und eine verstärkte Aufnahmebereitschaft und empfinden Befriedigung durch die aktive Teilnahme am eigenen Lernen.

Sozialkompetenz

- Durch Gruppenarbeit in praktischen Versuchen, trainieren die Studierende die Teamfähigkeit und steigern Ihre Ziel- und Ergebnisorientierung.

Verwendbarkeit in diesem und in anderen Studiengängen

Wahlpflichtmodul anderer Bachelorstudiengänge (wie z.B.: Angewandte Informatik/Infotronik, Interaktive Systeme/Internet of Things, Künstliche Intelligenz, Wirtschaftsinformatik, Elektro- und Informationstechnik)

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- mathematisches und abstraktes Denkvermögen
- Kenntnisse der Grundlagen der elementaren Zahlentheorie

Inhalt

1 Einführung
   - Thematische Einordnung
   - Schutzziele und Assets
   - Bedrohungen, Gefährdungen und Gegenmaßnahmen
   - Elemente der Kryptologie

2 Klassische Verfahren
   - Konstruktionsprinzipien
   - Transpositionsverfahren
   - Substitutionsverfahren
   - Analyse monoalphabetischer Chiffren
   - homophone, polygraphische und polyalphabetische Verfahren
   - Kombination aus Substitution und Transposition
   - Übergang zur modernen Kryptographie

3 Moderne Verfahren
   - Mathematische Grundlagen der modernen Kryptographie
   - Primzahlen und Primzahlentests
   - Primkörper und binärer Erweiterungskörper
   - Symmetrische Chiffren
   - Blockchiffren und Betriebsmodi
   - Stromchiffren
   - Asymmetrische Kryptographie
   - Hashfunktionen und Message Authentication Codes
   - Digitale Signaturen
   - Digitale Zertifikate und Public-Key-Infrastrukturen

4 Sicherheit von kryptographischen Verfahren
   - perfekte und pragmatische Sicherheit
   - ausgewählte Angriffe auf das DLP
   - ausgewählte Angriffe auf das Faktorisierungsproblem

5 Grundlagen der System- und Transaktionssicherheit
   - Maßnahmen zur Datenintegrität und Verbindlichkeit
   - Maßnahmen zur Authentifizierung I: Zugangskontrolle
   - Maßnahmen zur Authentifizierung II: Identifizierung von Partnern
   - Maßnahmen zur Authentifizierung III: Dokumentenechtheit

Lehr- und Lernmethoden

- Seminaristischer Unterricht mit praktischen Übungen

- Praktika

Besonderes

Praktikumsleistung (PrL) als Zulassungsvoraussetzung zur Prüfung.

Empfohlene Literaturliste

Literatur:

- Eckert, C.: IT-Sicherheit, Konzepte - Verfahren - Protokolle, De Gruyter Oldenbourg; 10th expanded and updated edition Auflage (21. August 2018), ISBN-13 : 978-3110551587
- Schäfer, G.: Netzsicherheit, Algorithmische Grundlagen und Protokolle, dpunkt; 1., Aufl. Auflage (1. Februar 2003), ISBN-13 : 978-3898642125
- Buchmann, J.: Einführung in die Kryptologie, Springer Spektrum; 6., überarb. Aufl. 2016 Auflage (26. April 2016), ISBN-13 978-3-642-39775-2
- Schneier, B.: Angewandte Kryptographie, Pearson Studium; 1. Auflage (3. Dezember 2005), ISBN-13 : 978-3827372284
- Schneier, B.: Secrets and Lies, Wiley; 1. Auflage (24. April 2015), ISBN-13 : 978-1119092438
- Wätjen, D.: Kryptographie, Grundlagen, Algorithmen, Protokolle, Springer Vieweg; 3. Auflage (14. Juni 2018), ISBN-13 978-3-658-22474-5
- Ertel, W.: Angewandte Kryptographie, Carl Hanser Verlag GmbH & Co. KG; 6., aktualisierte Auflage (11. November 2019), ISBN-13 : 978-3446463134

Webseiten:

- Bundesamt für Sicherheit in der Informationstechnik
- www.CrypTool.de (kryptographische Software)

CY-B-12 Schlüsselqualifikation 2

Modul Nr.	CY-B-12
Modulverantwortliche/r	Tanja Mertadana
Kursnummer und Kursname	Fachsprache englisch
Lehrende	Tanja Mertadana
Semester	2
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Das Modul Fachsprache zielt darauf ab, den Studierenden spezialisierte Sprachkenntnisse zu vermitteln, die für eine selbständige Tätigkeit in einem globalisierten Bereich der Cyber Security notwendig sind. Deutsche Studierende oder internationale Studierende mit Deutschkenntnissen der Niveaustufe C1 gemäß dem Gemeinsamen Europäischen Referenzrahmen besuchen den im Stundenplan verankerten Englischkurs und internationale Studierende (kein abgeschlossenes und zertifiziertes B2-Niveau) nehmen an den Deutschkursen aus dem Angebot des AWP- und Sprachenzentrums teil.

Fachsprache Englisch

Im Modul werden die vier Grundfertigkeiten - Hören, Lesen, Sprechen und Schreiben - trainiert. Studierende erweitern ihren fachspezifischen Wortschatz und vertiefen ihre Kenntnisse in Bezug auf die sprachlichen Strukturen. Dabei gestalten Studierende ihren eigenen Wissenserwerb durch gezielte Bedürfnisanalysen und eigengesteuerte Projekte.

Das Hauptaugenmerk des Moduls ist die Optimierung der Sprachgewandtheit und die Verbesserung der Fähigkeit auf Englisch zu kommunizieren, um Texte und Gespräche besser zu verstehen. Durch aufgabenbezogene Sprech-, Hör-, Lese- und Schreibaktivitäten verbessern Studierende ihre kommunikativen Fähigkeiten und erweitern ihr Ausdrucksvermögen. Dies ermöglicht ihnen sowohl das Teilnehmen an Diskussionen und das selbständige Erstellen geschäftlicher Korrespondenz, als auch das Erstellen effektiver Software Dokumentation und das erfolgreiche Präsentieren auf Englisch.

Nach Absolvieren des Moduls haben die Studierenden folgende Kompetenzen erlangt:

Fachkompetenz

- Die Studierenden beherrschen die englische Sprache auf einem sicheren Sprachniveau (B2, GER) und können im Bereich Cyber Security auch Fachdiskussionen verstehen.
- Sie verfügen über Fähigkeiten, um Fachliteratur zu verstehen und auf einem B2 Niveau selbständig Texte zu produzieren.
- Die Studierenden besitzen Wissen über sprachliche Ausdrucksmittel auf B2 Niveau im formalen und professionellen Kontext.
- Sie verstehen Diskussionen und komplexere Inhalte ihres Spezialgebietes.
- Sie erwerben die Fähigkeit grammatikalische Strukturen funktionell in ihren zukünftigen Berufsfeldern anzuwenden.
- Sie sind in der Lage verständliche und detaillierte Präsentationen zu relevanten Themen der Cyber Security zu halten. Eigene Meinungen, wie auch unterschiedliche Gesichtspunkte, können verständlich vorgebracht werden.
- Die Studierenden verfügen über interkulturelle Ansätze.

Methodenkompetenz

- Die Studierenden erweitern ihre Fähigkeiten im Spracherwerb in dem sie ihre individuellen Lernstile reflektieren.
- Sie können Informationen aus unterschiedlichen englischen Quellen filtern und für Präsentationen verarbeiten.

Sozialkompetenz

- Die Studierenden trainieren ihre sozialen Kompetenzen der Teamfähigkeit, Zuverlässigkeit und der Integrität.
- Sie verfügen über kommunikative Fertigkeiten, dadurch, dass sie gemeinsam mit anderen Lösungen erarbeiten.
- Sie reflektieren ihre Lernerfahrungen aus eigenständigen Projekten und Teamarbeit.

Fachsprache Deutsch

Die Qualifikationsziele des Moduls können der entsprechenden Kursbeschreibung auf der Homepage des AWP- und Sprachenzentrums entnommen werden.

Verwendbarkeit in diesem und in anderen Studiengängen

Schlüsselqualifikation 2, KI-2 (Fachsprache)

Zugangs- bzw. empfohlene Voraussetzungen

Fachsprache Englisch: Die Voraussetzung, um am Modul erfolgreich teilnehmen zu können ist das Beherrschen der englischen Sprache auf einem B2 Niveau, in Anlehnung an den Gemeinsamen Europäischen Referenzrahmen für Sprachen (GER).

Fachsprache Deutsch: Zum Studienstart werden die Deutschkenntnisse der Studierenden durch einen Einstufungstest ermittelt. Je nach Ergebnis werden die Studierenden in einen ihrem Sprachniveau entsprechenden Kurs eingeteilt. Nach erfolgreichem Abschluss eines Kurses können die Studierenden im folgenden Semester einen aufbauenden Deutschkurs besuchen.

Inhalt

Fachsprache Englisch

1 Computer im Kontext
2 Computer und Zahlen 2.1 Die Sprache der Mathematik 2.2 Informationen binär repräsentieren
3 Grundlagen der Informatik 3.1 Computerarchitektur 3.2 Betriebssysteme 3.3 Netzwerke 3.4 Datenstrukturen
4 Software engineering
5 Fallstudien (z.B.: Alan Turing, Cybersecurity, KI)
6 Kommunikative Fähigkeiten (z.B.: Präsentationen, Besprechungen)
7 Schreibfertigkeiten (z.B.: Geschäftskorrespondenz, Software Dokumentation)
8 Grammatik (z.B.: Zeiten, Passivstrukturen)

Fachsprache Deutsch

Die Inhalte können der entsprechenden Kursbeschreibung auf der Homepage des AWP- und Sprachenzentrums entnommen werden.

Lehr- und Lernmethoden

Der Fokus der Lehrmethoden liegt auf der Verbesserung der vier Hauptsprachfertigkeiten (Hörverständnis, Sprechen, Lesen und Schreiben) und der Optimierung von beruflichen und sozialen Kompetenzen. Beispiele der angewendeten Lehrmethoden sind diverse Formen der Gruppen- und Einzelarbeit, Minipräsentationen, Übungen zum intensiven Lesen und Hören, Rollen- und Grammatikspiele, Laufdiktate, Übersetzungen, Peer-Feedback, Arbeit mit Lernstationen, und verschiedenen Schreibaktivitäten zur Vertiefung des erlernten Stoffes.

Es werden wöchentlich Aufgaben zum Selbststudium gestellt.

Besonderes

Anwesenheitspflicht 75%

Empfohlene Literaturliste

Fachsprache Englisch

- Bonamy, David. Technical English 4. Harlow, England: Pearson Education, 2011. Print.
- Brieger, Nick & Alison Pohl. Technical English: Vocabulary and Grammar. Oxford: Summertown, 2002. Print.
- Büchel, Wolfram, et al. Technical Milestones: Englisch für technische Berufe. Stuttgart: Ernst Klett, 2013. Print.
- Butterfield, Andrew & Gerard Ekembe Ngondi, editors. Oxford Dictionary of Computer Science. Oxford: OUP, 2016. Print.
- Dasgupta, Subrata. Computer Science: A Very Short Introduction. Oxford: OUP, 2016. Print.
- DK. The Science Book: Big Ideas Simply Explained. London: DK, 2014. Print.
- Emmerson, Paul. Business Vocabulary Builder. London: Macmillan, 2009. Print.
- Emmerson, Paul. Business English Handbook. London: Macmillan, 2007. Print.
- engine: Englisch für Ingenieure. <www.engine-magazin.de> (Darmstadt). Various issues. Print.
- Glendinning, Eric H. & John McEwan. Oxford English for Information Technology. 2nd ed. Oxford: OUP, 2006. Print.
- Ibbotson, Mark. Cambridge English for Engineering. Cambridge: Cambridge UP, 2008. Print.

- Ince, David. The Computer: A Very Short Introduction. Oxford: OUP, 2011. Print.
- Inch: Technical English. (Karlsruhe). Various Issues. Print.
- Munroe, Randall. What If? London: John Murray, 2015. Print.
- Schäfer, Wolfgang, et al. IT Milestones: Englisch für IT-Berufe. Stuttgart: Ernst Klett, 2013. Print.
- Schulze, Hans Herbert. Computer-Englisch: Ein englisch-deutsches und deutsch-englisches Fachwörterbuch. Hamburg: Rowohlt Taschenbuch Verlag, 2015. Print.
- Vince, Michael. Advanced Language Practice. London: Macmillan, 2009. Print.
- Wagner, Georg & Maureen Lloyd Zo?rner. Technical Grammar and Vocabulary: A Practice Book for Foreign Students. Berlin: Cornelsen, 1998. Print.

Fachsprache Deutsch

Literaturempfehlungen können der entsprechenden Kursbeschreibung auf der Homepage des AWP- und Sprachenzentrums entnommen werden.

CY-B-13 Datenbanken

Modul Nr.	CY-B-13
Modulverantwortliche/r	Prof. Dr. Benedikt Elser
Kursnummer und Kursname	Datenbanken
Lehrende	Prof. Dr. Wolfgang Dorner Prof. Dr. Udo Garmann
Semester	3
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Nach Abschluss des Moduls verstehen die Studierenden die Bedeutung von Datenbanken und können Ihren Einsatz differnziert betrachten. Sie lernen die Vorgehensweise bei der Erstellung eines Datenmodells kennen und können diese in einer konkreten Datenbank umsetzen. Im Rahmen dieses Kurses erlernen sie, wie sie auf relationale Datenbanken mit SQL zugreifen und entwickeln Anwendungen auf Basis einer Datenbank. Die Teilnehmer erwerben Kenntnisse von Performanceoptimierung bei Ablage und Zugriff auf Daten und verstehen das Zusammenspiel von Applikations-, Präsentations- und Datenbankserver bei der Programmierung, insbesondere auch in einer Web-Umgebung.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernziele erreicht:

Fachkompetenz

Die Studierenden verstehen die Konzepte von Datenbanken und deren Einsatz

Sozialkompetenz

Im Rahmen der Vorlesungen finden Übungen statt. Die Studierenden sind damit in der Lage, die Datenbankentwürfe ihrer Kollegen zu verstehen, zu kritisieren und durch eigene Beiträge zu komplementieren.

Methodenkompetenz

Die Studenten haben die Fähigkeit Software unter Einsatz einer Datenbank zu erstellen.

Persönliche Kompetenz

Die Studierenden können eigene softwaretechnische Ideen mit Hilfe von Datenbanken umsetzten und gegenüber konkurrierenden Ansätzen verteidigen.

Verwendbarkeit in diesem und in anderen Studiengängen

Die Module Programmieren, Informatik und Software Engineering bauen thematisch auf das Modul auf. Das Modul kann in anderen Studiengängen wi Ba. WI und Ba. Cyber Security verwendet werden

Zugangs- bzw. empfohlene Voraussetzungen

formal:

keine

inhaltlich:

Informatik Grundkurse z.B. Modul Grundlagen der Informatik

Die Kenntnis einer Programmiersprache ist wünschenswert.

Office-Anwendungen werden vorausgesetzt.

Inhalt

Lehr- und Lernmethoden

Vorlesungen mit Übungen

Der Anteil der begleitenden Übung entspricht ca. 25% der Präsenzveranstaltungen. In einem ähnlichen Umfang zum Lehrmaterial werden begleitende Übungsaufgaben zur Vertiefung und Prüfungsvorbereitung zur Vorlesungsnachbereitung zur Verfügung gestellt.

Empfohlene Literaturliste

Thomas M. Conolly, Carolyn E. Begg: Database systems, A practical approach to design, implementation, and managment. Addison-Wesley, an imprint of Pearson Education, 4th edition 2005.

Kemper A., Eickler A.: Datenbanksysteme: Eine Einführung, Oldenbourg Wissenschaftsverlag

Preiß, N. (2007), Entwurf und Verarbeitung relationaler Datenbanken, Oldenbourg, München u.a.

CY-B-14 Stochastik

Modul Nr.	CY-B-14
Modulverantwortliche/r	Prof. Dr. Johannes Grabmeier
Kursnummer und Kursname	Stochastik
Lehrende	Prof. Dr. Johannes Grabmeier Prof. Dr. Stefan Hagl
Semester	3
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden haben nach Abschluss des Moduls folgende Lernziele erreicht:

Im Vordergrund steht die Fach- und die Methodenkompetenz in Stochastik. Die Studierenden verfügen über Kenntnisse der Konzepte der deskriptiven und induktiven Statistk. Der Erwerb von sozialen Kompetenzen steht bei diesem Modul naturgemäß nicht im Vordergrund, wird aber durch Kooperation der Studierenden und gemeinsames Erarbeiten von Lösung gefördert. Die persönliche Kompetenz wird durch vertiefte selbständiges Erarbeiten und Lösen komplexer Probleme geschärft.

Deskriptive Statistik:

Die Studierenden kennen die Konzepte der deskriptiven Statistik insbesondere für univariate und bivariate Beschreibungen. Sie sind in der Lage statistische Fragestellungen dieser Gebiets aus der betrieblichen Praxis zu erkennen, zu modellieren und zu lösen. Dazu setzen sie Softwarewerkzeuge wie die Statistikfunktionen in Tabellenkalkulationsprogrammen wie MS Excel, OpenOffice Calc oder LibreOffice ein.

Induktive Statistik:

Die Studierenden kennen die Konzepte der induktiven Statistik basierend auf Wahrscheinlichkeitstheorie. Die in der Praxis vorkommenden statistischen Fragenstellung des Schließens von einer Stichprobe auf Gesamtpopulationen können je nach Themenstellung mit einer statistischen Technik des Schätzens von Parametern, dem Durchführen von parametrischen Hypothesentests und von Anpassungstests gelöst werden. Sie sind in der Lage dazu die notwendige Modellbildung mit Zufallsvariablen, Testfunktionen und ihren Wahrscheinlichkeitsverteilungen zu erstellen. Dazu setzen sie Softwarewerkzeuge wie die Statistikfunktionen in Tabellenkalkulationsprogrammen wie MS Excel, OpenOffice Calc oder LibreOffice ein.

Verwendbarkeit in diesem und in anderen Studiengängen

Verwendbarkeit des Moduls für Bachelor Cyber Security:

- CY-B-20: Wahlpflichtmodul Projekt
- CY-B-21: Kryptologie 2
- CY-B-22: Management von IT-Sicherheitsvorfällen
- CY-B-27: Digitale Forensik
- CY-B-29: Security Engineering
- CY-B-32: Auditierung von IT-Systemen

Zugangs- bzw. empfohlene Voraussetzungen

Mathematikvorlesung des 1. Semesters

Inhalt

Teil Deskriptive Statistik:

1 Grundlagen und Grundbegriffe
   - Merkmale, Merkmalsträger
   - Ausprägungen, Skalenniveau
   - Grundgesamtheit, Voll-/Teilerhebung
   - Primär- und sekundärstatistische Erhebung
   - Erhebungstechniken

2 Häufigkeitsverteilungen
- Urliste
- Häufigkeitsverteilung
- Gruppierung und Klassifikation
- Graphischen Darstellungen

3 Lageparameter
- Das arithmetische Mittel
- Das gewogene arithmetische Mittel
- Der Median oder Zentralwert
- Der Modus oder Modalwert
- Das geometrische Mittel
- Das harmonische Mittel und das gestutzte Mittel

4 Streuungsmaße
- Spannweite
- Mittlere absolute Abweichung
- Mittlere quadratische Abweichung (Varianz)
- Standardabweichung
- Quantile, Quartile und Semiquartilsabstand
- Der Quartilskoeffizient

5 Konzentrationsmaße
- absolute und relative Konzentration
- Herfindahl-Index
- Konzentrationsraten und Konzentrationskurven
- Das Maß von Lorenz/Münzner
- Der Lorenzkoeffizient
- Die Lorenzkurve

6 Indexzahlen
- Zeitreihen
- Gliederungszahlen, Messziffern, Wachstumsraten
- Umbasierung und Verkettung
- Preisindex
- Mengenindizes
- Wertindex

7 Regression
- Regressionsrechnung
- Lineare Einfachregression
- Die Methode der kleinsten Quadrate
- Determinationskoeffizient
- Prognose
- Nichtlineare Regression und Mehrfachregression

8 Korrelaton
- Der Korrelationskoeffizient von Bravais-Pearson
- Eigenschaften von Varianz und Covarianz
- Rangkorrelation nach Spearman-Pearson
- Korrelationsmaßzahlen für nominale Variablen

Teil Induktive Statistik:

1 Elementare Wahrscheinlichkeitstheorie
- Wahrscheinlichkeitsbegriffe
- Zufallsexperimente und Ereignisse
- Axiome nach Kolmogorov
- Zweistufige Experimente und bedingte Wahrscheinlichkeit
- Satz von Bayes

2 Zufallsvariablen
- Zufallsvariablen
- Diskrete Wahrscheinlichkeitsverteilungen und Verteilungsfunktion
- Stetige Wahrscheinlichkeitsverteilungen und Dichtefunktion
- Erwartungswert und Varianz einer Zufallsvariablen

3 Verteilungen I
- Binomialverteilung
- Normalverteilung
- Multinomialverteilung
- Hypergeometrische Verteilung
- Poissonverteilung

4 Stichprobenverteilungen
- Stichproben
- Auswahlverfahren
- Stichprobenverteilung

5 Zentraler Grenzwertsatz und Anwendungen
- Zentraler Grenzwertsatz
- Stichprobenverteilung des Mittelwerts
- Stichprobenverteilung des Anteilswerts
- Stichprobenverteilung der Standardabweichungen
- Stichprobenverteilung von Differenzen

6 Parametrische Hypothesentests
- Nullhypothesen und Testtheorie
- Entscheidungsfehler
- Tests für Mittelwert, Anteilswert, Standardabweichung und Differenzen
- Güte eines Tests

7 Schaetzstatistik
- Punktschätzverfahren: Momentenmethode
- Punktschätzverfahren: Maximum-Likelihood
- Gütekriterien
- Intervallschätzung und Konfidenzintervall

8 Verteilungen II
- Student-t-Verteilung
- Chi-Quadrat-Verteilung
- F-Verteilung

9 Parametrische Hypothesentests mit kleine Stichproben
- Anteilswerttest - Binomialtest
- Anteilswertdifferenztest - Fishertest
- Mittelwert- und Mittelwertdifferenztest
- Varianzquotiententest

10 Anpassungstests
- Verteilungshypothesen
- Chi-Quadrat-Anpassungstest
- Unabhängigkeitstests

Lehr- und Lernmethoden

In klassischer Vortragstechnik wird Theorie und Anwendungen vermittelt und dargestellt. Viele Konzepte werden anhand konkreter Aufgabenstellungen erarbeitet und mit einem SW-Werkzeug gelöst. Übungsaufgaben zur eigenen Bearbeitung durch die Studierenden werden gestellt. Lösungen zu einer Auswahl davon werden zu Beginn der nächsten Vorlesung durch Studierende vorgetragen. Alternativ werden Lösungsvorschläge der Studierenden im iLearn-System diskutiert.

Empfohlene Literaturliste

Literatur:

- Bourier G. , Wahrscheinlichkeitsrechnung und schließende Statistik, Praxisorientierte Einführung. Mit Aufgaben und Lösungen, 6. Aufl. Gabler-Verlag, ISBN 978-3-8349-1500-9, 2009.
- Falk, Becker, Marohn (1995), Angewandte Statistik mit SAS, Springer Verlag, Berlin
- Georgii, H.O. (2002), Stochastik, Einführung in die Wahrscheinlichkeitstheorie und Statistik, Walter de Gruyter, Berlin
- Grabmeier J., Hagl St. (2012), Statistik - Grundwissen und Formeln, 2. Auflage, Haufe Taschen Guide 215, ISBN: 978-3-648-00319-0
- Hagl, S. (2008), Schnelleinstieg Statistik - Daten erheben, analysieren, präsentieren, Haufe Verlag

- Monka, Michael, Voss, Werner, Schöneck, Nadine (2008), Statistik am PC, Lösungen mit Excel, 5., aktualisierte und erweiterte Auflage, Hanser-Verlag, München
- Pflaumer, Heine, Hartung (2001), Statistik für Wirtschafts- und Sozialwissenschaftler, Deskriptive Statistik, Oldenbourg, München
- Puhani (2005), Statistik, Einführung mit praktischen Beispielen, Lexika-Verlag, Würzburg
- Schwarze, J. (2014), Grundlagen der Statistik: Band 1, 12. Aufl., nwb Studium.
- Schwarze, J. (2013), Grundlagen der Statistik: Band 2, 10. Aufl., nwb Studium
- Stockburger, David W., Introductory Statistics, Concepts, Models, and Applications, http://www.psychstat.missouristate.edu/sbk00.htm
- Wernecke, Klaus-Dieter (1995), Angewandte Statistik in der Praxis, Addison-Wesley, München
- Zwerenz, Karlheinz (2008), Statistik verstehen mit Excel, R. Oldenbourg Verlag, München Wien

Internetquellen:

- Zwerenz, K., VHB-Grundkurs Statistik I und II, http://lerne-statistik.de

CY-B-15 Projektmanagement

Modul Nr.	CY-B-15
Modulverantwortliche/r	Prof. Dr. Michael Ponader
Kursnummer und Kursname	Projektmanagement
Lehrende	Prof. Dr. Michael Ponader
Semester	3
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	LN, schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden verfügen über grundlegendes allgemeines Wissen und grundlegendes Fach- und Methodenwissen in dem Bereich Projektmanagement.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Studierenden erwerben Kenntnisse im Planen, Überwachen und Steuern von Projekten und in der Gestaltung der hierfür erforderlichen Aufbau- und Ablauforganisation.

Methodenkompetenz

- Die Studierenden wenden ausgewählte Techniken des Projektmangements an.

Persönliche Kompetenz

- Die Studierenden erwerben Kenntnisse in der Eigenorganisation.

Sozialkompetenz

- Diese Kenntnisse wenden sie in verschiedenen Teams anhand eines praxisorientierten Software- oder Organisationsprojektes an. Dadurch werden Kooperations- und Kommunikationsfähigkeit sowie Konfliktfähigkeit gefördert.

Verwendbarkeit in diesem und in anderen Studiengängen

alle Module mit umfangreicheren Gruppen-/Projektarbeiten

Zugangs- bzw. empfohlene Voraussetzungen

keine spezifischen

Inhalt

1 Klassisches Projektmanagement
   - Erkennen der Charakteristika von Projekten im Vergleich zu Linienaufgaben in einem Unternehmen, Anforderungen an einen Projektleiter und seine Aufgaben
   - Projektorganisation - Darstellung und Diskussion unterschiedlicher Formen der Organisation eines Projektteams, Mögliche Aufgaben- und Kompetenzverteilungen zwischen Projektleiter und Linienführungskräften, Zusammensetzung, Aufgaben und Kompetenzen anderer Gremien in einer Projektorganisation
   - Projektplanung und -controlling - Darstellung unterschiedlicher Arten von Projektplänen und ihrer Abhängigkeiten, Vorgehensweise bei der Projektplanung, Darstellung des Risikomanagements in Projekten, Dimensionen der Projektsteuerung und -kontrolle mit den zugehörigen Werkzeugen, Verfahren und Vorgehensweisen
   - Projektphasen - Vorstellung ausgewählter Projektphasen, Erlernen der Aufgaben in diesen Phasen
   - Techniken - Vorstellung von Softskills eines Projektleiters (Kreativitätstechniken, Moderation, Präsentation)
   - Erwerb von Kenntnissen im Umgang mit SW zur Projektplanung und -steuerung anhand von praktischen Übungen

2 Agiles Projektmanagement
- Agile Werte/Prinzipien
- Scrum - Rollen, Ereignisse, Artefakte
- Kanban - Praktiken, Prozess, Regeln, Best Practices

3 Einsatzfelder und Kombination von Klassischen und Agilen Ansätzen
4 Projektmanagement mit MS Project
5 Teilweise Durchführung eines praxisorientierten Software- oder Organisationsprojektes im Team

Lehr- und Lernmethoden

- Vorlesungen
- Übungen/Fallstudien in Einzel- und Gruppenarbeit
- Präsentationen

Empfohlene Literaturliste

- Chatfield, C. u.a., (2011), Microsoft Project 2010 - Das offizielle Trainingsbuch, O`Reilly, Köln
- GPM Deutsche Gesellschaft für Projektmanagement, Gessler, M. (Hrsg.) (2019), Kompetenzbasiertes Projektmanagement (PM4)- Handbuch für die Projektarbeit, Qualifizierung und Zertifizierung auf Basis der IPMA Competence Baseline Version 4, 1. Auflage, GPM Deutsche Gesellschaft für Projektmanagement, Nürnberg
- Kerzner, H. (2003), Projektmanagement Fallstudien, mitp-Verlag, Bonn
- Kuster, J. et al. (2019), Handbuch Projektmanagement, 4. Auflage, Springer Verlag, Berlin
- Martinelli, R.J., Milosevic, D.Z. (2016), Project Management ToolBox - Tools and Techniques for the Practicing Project Manager, 2. Auflage, Wiley, Hoboken, NJ
- Project Management Institute (Hrsg.) (2017), A guide to the project management body of knowledge. PMBOK(R) Guide, 6. Auflage, Project Management Institute, Newtown Square, Pa
- Schwaber, K., Sutherland, J. (2016), Der Scrum Guide, Scrum.Org and ScrumInc, o.O.
- Timinger, H. (2017), Modernes Projektmanagement: Mit traditionellem, agilem und hybridem Vorgehen zum Erfolg, Wiley, Hoboken, NJ
- Verzuh, E. (2016), The Fast Forward MBA in Project Management, 5. Auflage, Wiley, Hoboken, NJ
- Wies, P. (2014), Project 2013 Grundlagen, Herdt-Verlag, Bodenheim

CY-B-16 Sichere Programmierung

Modul Nr.	CY-B-16
Modulverantwortliche/r	Prof. Dr. Martin Schramm
Kursnummer und Kursname	Sichere Programmierung
Lehrende	Michael Heigl
Semester	3
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	PrA
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden verfügen über vertieftes Wissen und spezialisiertes Fachwissen in den Bereichen der sicheren Programmierung, sichere Codierungs-Richtlinien und der Entwicklung sicherer Software.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Studierenden können die grundlegenden zu beachtenden Kriterien für sichere Softwareentwicklung darstellen und erklären.
- Sie können eigene softwaretechnische Ideen sicher umsetzen und Software hinsichtlich Einhaltung der Grundsätze sicherer Programmierung evaluieren.

- Sie können die Bedeutung von Maßnamen zur Validierung von Eingabewerten erklären und diese in eigenen Softwareentwicklungen berücksichtigen.
- Sie können den Unterschied der Sicherheitsmaßnahen für Eingabe-Validierung und der Einbindung externer Komponenten (Bibliotheksfunktionen, etc.) veranschaulichen und zwischen nötigen und unnötigen Maßnahmen differenzieren.
- Sie kennen die Top-Schwachstellenlisten, sowie Codierungs-Richtlinien und können diese für die sichere Softwareentwicklung nutzen.

Methodenkompetenz

- Sie kennen die aktuellen Tools zur statischen und dynamischen Code-Analyse und können diese anwenden.
- Die Studierenden können für eine gegebene Anforderungsliste für ein Programm beurteilen, welche Angriffsvektoren existieren, welche Schutzziele in diesem Kontext erfüllt werden müssen und dieses Programm sicher erstellen.

Persönliche Kompetenz

- Durch die Diskussion von aktuellen Schwachstellen und Software entwickeln die Studierenden ein Bewusstsein und eine verstärkte Aufnahmebereitschaft und empfinden Befriedigung durch die aktive Teilnahme am eigenen Lernen.

Sozialkompetenz

- Durch Gruppenarbeit in praktischen Programmierübungen, trainieren die Studierende die Teamfähigkeit und steigern Ihre Ziel- und Ergebnisorientierung.

Verwendbarkeit in diesem und in anderen Studiengängen

Wahlpflichtmodul anderer Bachelorstudiengänge (wie z.B.: Angewandte Informatik/Infotronik, Interaktive Systeme/Internet of Things, Künstliche Intelligenz, Wirtschaftsinformatik, Elektro- und Informationstechnik)

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- fundierte Kenntnisse der Inhalte von Programmierung 1 und Programmierung 2
- Kenntnisse der Inhalte von Algorithmen und Datenstrukturen

Inhalt

10 Code-Analyse
   - statische Analyse
   - dynamische Analyse
   - Fuzzing
11 Formale Methoden

Lehr- und Lernmethoden

- Seminaristischer Unterricht mit vielen praktischen Übungen
- Semesterübergreifende Projektarbeit

Empfohlene Literaturliste

- Seacord, R.: Secure Coding in C and C++, Addison-Wesley Professional; Auflage: 2nd edition (2. April 2013), ISBN-13: 978-0321822130
- Seacord, R.: CERT® C Coding Standard, Second Edition, The: 98 Rules for Developing Safe, Reliable, and Secure Systems, Addison-Wesley Professional, Auflage: 2 (14. April 2014), ISBN-13: 978-0321984043
- Gebeshuber, K.: Exploit!: Code härten, Bugs analysieren, Hacking verstehen. Das Handbuch für sichere Softwareentwicklung, Rheinwerk Computing, Auflage: 1 (26. Juli 2019), ISBN-13: 978-3836265980
- Basu, T.: Secure Programming with Python, Packt Publishing Limited (31. Januar 2017), ISBN-13: 978-1786466464

CY-B-17 Netzwerksicherheit

Modul Nr.	CY-B-17
Modulverantwortliche/r	Prof. Dr. Thomas Störtkuhl
Kursnummer und Kursname	Netzwerksicherheit
Lehrende	Karl Leidl NN NN PK AI/IAS/CS Prof. Dr. Thomas Störtkuhl
Semester	3
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	LN Praxis, schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden verfügen über grundlegendes allgemeines Wissen und grundlegendes Fachwissen im Bereich Netzwerksicherheit.

Nach Absolvieren des Moduls haben die Studierenden folgende Kompetenzen erlangt:

Fachkompetenz

- Die Studierenden können die Sicherheitsprotokolle der einzelnen Netzwerkschichten vergleichen und die Unterschiede erläutern.

- Sie können veranschaulichen, wie sich unterschiedliche Konfigurationen (z.B.: Cipher Suits) sich auf die Sicherheit der Kommunikationsbeziehung auswirken.
- Sie kennen Techniken zur logischen Separierung von Netzwerken und können diese in einem Netzwerk implementieren.
- Sie können generelle Methoden für die Authentifizierung und Autorisierung in Netzwerken diskutieren.
- Sie können die Sicherheitsmaßnahmen für Verbindungen in kabellosen Netzwerken formulieren.

Methodenkompetenz

- Die Studierenden können für ein gegebenes Szenario entscheiden, auf welcher Netzwerkschicht Sicherheitsmaßnahmen getroffen werden müssen.
- Sie können für ein gegebenes Netzwerk und Kommunikationsbeziehungen entscheiden, welche Schutzsturkturen und Filer in welcher Art eingesetzt und konfiguriert werden müssen.

Persönliche Kompetenz

- Durch die stattfindenden Praktika werden die Studierenden angesprochen, was die aktve Teilnahme am eigenen Lernen steigert.

Sozialkompetenz

- Durch die Teilnahme an Gruppendiskussionen hinsichtlich der Absicherung von Kommunikationsinfrastrukturen lernen die Studierenden sich für die Ideen anderer einzusetzen.

Verwendbarkeit in diesem und in anderen Studiengängen

Wahlpflichtmodul anderer Bachelorstudiengänge (wie z.B.: Angewandte Informatik/Infotronik, Interaktive Systeme/Internet of Things, Künstliche Intelligenz, Wirtschaftsinformatik, Elektro- und Informationstechnik)

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- Kenntnisse der Inhalte von Modul CY-B-04 Betriebssysteme und Netzwerke

Inhalt

1 Netzsicherheit
- Motivation und Hinführung: Integration von Sicherheitsdiensten
- Protokolle der einzelnen Schichten
- Physical Layer Security
- Data Link Layer Security
- IEEE 802.1Q VLAN
- IEEE 802.1X - Extensible Authentication Protocol (EAP)
- IEEE 802.1AE MACsec
- PPP und PPTP
- Network Layer Security - IPSec
- Authentication Header
- Encapsulating Security Payload
- Security Association - ISAKMP
- Transport Layer Security
- SSL
- (D)TLS
- SSH
- Virtual Private Networks

2 sichere drahtlose und mobile Kommunikation
- IEEE 802.11 (WLAN)
- Sicherheit in GSM, UMTS, LTE, 4G
- Sicherheit in 5G

3 Schutz von Kommunikationsinfrastrukturen
- Routing-Sicherheit
- Sicherung von DNS
- Schutzstukturen und Filter
- Firewall
- Deep Packet Inspection
- Intrusion Detection/Prevention/Reaction Systeme
- Sicherheit bei Software Defined Networking

Lehr- und Lernmethoden

- Seminaristischer Unterricht mit praktischen Übungen
- Praktika

Besonderes

Praktikumsleistung (PrL) als Zulassungsvoraussetzung zur Prüfung.

Die Durchführung von Praktika und Übungen in dem Modul Netzwerksicherheit erfordert grundlegende Vorkenntnisse. Die Zulassung zu diesen Modulen erhält deshalb nur, wer mindestens 40 ECTS-Leistungspunkte erreicht hat und mindestens zwei Grundlagen- und Orientierungsprüfungen bestanden hat.

Empfohlene Literaturliste

- Schäfer, G.: Netzsicherheit, Algorithmische Grundlagen und Protokolle, dpunkt-Verlag;
- Wendzel, S.: IT-Sicherheit für TCP/IP- und IoT-Netzwerke: Grundlagen, Konzepte, Protokolle, Härtung, Springer Vieweg
- Alexander, M.: Netzwerke und Netzwerksicherheit - Das Lehrbuch, mitp/ bhv;

CY-B-18 Schlüsselqualifikation 3

Modul Nr.	CY-B-18
Modulverantwortliche/r	Prof. Dr. Roland Zink
Kursnummer und Kursname	Technikethik und Nachhaltigkeit Wissenschaftliches Arbeiten
Lehrende	Christian Bauer Prof. Dr. Christina Bauer Prof. Dr. Bernhard Bleyer Prof. Dr. Wolfgang Dorner NN NN PK AI/IAS/CS Prof. Dr. Roland Zink
Semester	3
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	PrA
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Inhalte des Moduls setzen sich aus den Inhaltsangaben der zwei Fächer "Technikethik und Nachhaltigkeit" (**Fach A**) und "Wissenschaftliches Arbeiten" (**Fach B**) zusammen.

Fach A

Mit der Formulierung von Sustainable Development Goals (SDGs) durch die Vereinten Nationen besteht ein umfassender Orientierungsrahmen, wie sich die Menschheit in Zukunft entwickeln soll und wie Handlungen bzw. Verhalten von Menschen hinsichtlich dieses Entwicklungsziels zu bewerten ist. Dies gilt im Besonderen auch für technische Entwicklungen, indem ständig geprüft werden muss, ob die neuen Techniken sowohl ethischen als auch den nachhaltigen Vorgaben entsprechen.

Fachkompetenz

- Die Studierenden verstehen die Grundidee einer nachhaltigen Entwicklung und deren zukünftige Notwendigkeit.
- Die Studierenden kennen die globalen Entwicklungsziele (SDGs) und können ihr eigenes Verhalten und sowohl bestehende Technologien als auch potenzielle Erfindungen in diesem Rahmen bewerten.
- Die Studierenden kennen diesbezüglich speziell auch das Verfahren "Life Cycle Assessment" und die Idee von "Cradle to Cradle"

Fach B

"Wissenschaftlich oder technisch schreiben zu können ist eine Schlüsselkompetenz, die für das Vorankommen in Studium und Beruf entscheidend ist. Diese akademische Schreibkompetenz bringen Studierende in der Regel nicht aus der Schule mit, sondern erwerben sie parallel zur Akkulturation im Fach." Dieses Zitat aus der Broschüre des Zentrums für Hochschuldidaktik (DIZ, 2016) zeigt die inhaltliche Ausrichtung des Moduls auf. Die Studierenden sollen mit den Inhalten früh auf das Studium uns wissenschaftliches Arbeiten vorbereitet werden.

Fachkompetenz

- Die Studierenden kennen die Anforderungen des wissenschaftlichen Arbeitens.
- Die Studierenden werden befähigt, selbstständig wissenschaftlich zu arbeiten, insbesondere Recherche-, Bibliotheks- und Literaturarbeit.
- Die Studierenden kennen die Regeln zum Verfassen von studentischen Arbeiten und Qualitätskriterien für wissenschaftliches Arbeiten und können diese anwenden.

Fach A und B

Methodenkompetenz

- Die Studierenden werden zu selbstständigen Arbeiten befähigt.

Sozialkompetenz

- Die Studierenden trainieren in den Übungen Partner- und Teamarbeit.
- Die Studierenden können die in den Übungen selbstständig erzielten Lösungen vor der Gruppe erklären und präsentieren.
- Die Studierenden erlernen eigenverantwortliches Arbeiten.

Persönliche Kompetenz

- Die Studierenden erlernen durch Übungen selbstständiges und problem- bzw. handlungsorientiertes Arbeiten.

Verwendbarkeit in diesem und in anderen Studiengängen

Das Modul legt Grundlagen für das Studium im Allgemeinen und ist insbesondere mit folgendem weiterführenden Modul verknüpft:

CY-B und KI-B: Schlüsselqualifikation 5

CY-B und KI-B: Bachelormodul

Studiengang: BA Künstliche Intelligenz und BA Cyber Security

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

Inhalt

Fach A

- Konzepte und Definitionen von Nachhaltigkeit bzw. Nachhaltiger Entwicklung
- Digitale Transformation und ethische und nachhaltige Aspekte
- Cradle to Cradle
- Life Cycle Assessment

Fach B

- Wissenschaftliches Arbeiten - ein Prozess
- Literatursuche, -bewertung und -auswertung
- Forschungsstand und Theorie
- Wissenschaftliche Methoden
- Anfertigen einer wissenschaftlichen Arbeit

Lehr- und Lernmethoden

- Seminaristischer Unterricht mit Gruppen- und Partnerarbeit
- Projektarbeit
- Blended Learning

Empfohlene Literaturliste

Fach A

- Braungart, M. & McDonough, W. (2014): Cradle to Cradle: Remaking the Way We Make Things. Piper Verlag.
- Pufe, I. (2018): Nachhaltigkeit. Bundeszentrale für politische Bildung. Bonn.
- Wissenschaftlicher Beirat der Bundesregierung Globale Umweltveränderungen (WBGU) (2019): Unsere gemeinsame digitale Zukunft. Berlin.

Fach B

- Bänisch, A. & Alewell, D. (2013): Wissenschaftliches Arbeiten. De Gruyter Oldenbourg.
- Karmasin, M. & Ribing, R. (2017): Die Gestaltung wissenschaftlicher Arbeiten. Utb.
- Metschl, Ulrich (2016): Vom Wert der Wissenschaft und vom Nutzen der Forschung. Zur gesellschaftlichen Rolle akademischer Wissenschaft. Wiesbaden.
- Sandberg, Berit (2017): Wissenschaftliches Arbeiten von Abbildung bis Zitat. Lehr- und Übungsbuch für Bachelor, Master und Promotion. De Gruyter Oldenbourg.

(Zusätzlich werden Internetdokumente und Leitfäden verwendet!)

CY-B-19 Software Engineering

Modul Nr.	CY-B-19
Modulverantwortliche/r	Prof. Dr. Thomas Störtkuhl
Kursnummer und Kursname	Software Engineering
Lehrende	Prof. Dr. Thomas Störtkuhl
Semester	4
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	PrA
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden verfügen über detailliertes Fachwissen und Methodenwissen im Bereich der Softwareentwicklung.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Studierenden können die Grundlagen des Projektmanagements anwenden.
- Sie können Anforderungen formulieren und bewerten.
- Sie kennen die Codierregeln und können diese anwenden.
- Sie sind in der Lage Reviews von Arbeitsergebnissen durchzuführen.

Methodenkompetenz

- Sie sind in der Lage aus Anforderungen auf systematsche Weise einen objektorientierten Entwurf (Analyse und Design) mittels UML durchzuführen.
- Sie können ausgehend von Anforderungen und auf Basis des Codes Testfälle gemäß Black-Box- und White-Box-Teststrategien definieren, Testendekriterien festlegen und Tests durchführen.

Persönliche Kompetenz

- Durch zielorientiertes Arbeiten entwickeln die Studierenden ein hohes Maß an Zielstrebigkeit.
- Durch agile Methoden wird die Selbstmotivation der Studierenden gefördert.
- Durch die Task-orientierte Arbeitsweise wird das problemlösende Denker der Studierenden geschärft.

Sozialkompetenz

- Die Studierenden sind in der Lage sich selbständig für ein Projekt in Arbeitsgruppen zu organisieren und das Projekt gemeinsam durchzuführen.
- Durch die aktive Teilnahme an Teammeetings wird die Teamfähigkeit gestärkt.

Verwendbarkeit in diesem und in anderen Studiengängen

Wahlpflichtmodul anderer Bachelorstudiengänge (wie z.B.: Angewandte Informatik/Infotronik, Interaktive Systeme/Internet of Things, Künstliche Intelligenz, Wirtschaftsinformatik, Elektro- und Informationstechnik)

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- Kentnisse der Inhalte der Module
  - Grundlagen der Informatik
  - Programmierung 1
  - Programmierung 2
  - Sichere Programmierung (Bachelor Cyber Security)

Inhalt

1 Motivation und Definition
2 Elemente des Software Engineering

3 Methodik
- Requirements Engineering
- Software Entwurf (allgemein)
- Software Entwurf
- Architektur und Detaildesign allgemein
- Objektorientierte Analyse und Design (OOA, OOD)
- UML Einführung
- UML Workshop (Diagramme und ihre Anwendung)
- Anwendungsbeispiel
- Übergang von Analyse zum Design

4 Implementierung
- Codierungsregeln (z.B. MISRA)
- Statische Codeanalyse
- Codemetriken

5 Software Test
- Statischer Test
- Dynamischer Test
- Testprozeß
- Testmethoden und Teststrategien

6 Software Qualitätssicherung
- Definition
- Reviews

Lehr- und Lernmethoden

- Seminaristischer Unterricht mit praktischen Übungen, teilweise Gruppenarbeit
- Semesterbegleitende Projektarbeit in Gruppenarbeit

Empfohlene Literaturliste

- H. Balzer, Lehrbuch der Software-Technik, Spektrum Akademischer Verlag
- I. Sommerville, Software Engineering, Addison Wesley Verlag
- B. Kahlbrandt, Software-Engineering mit der UML, Springer Verlag
- C Rupp et. al., UML 2 - Glasklar, Hanser Verlag
- A. Spillner, T. Linz, Basiswissen Softwaretest, dpunkt Verlag
- B. Beizer, Black - Box Testing: Techniques for Functional Testing of Software and Systems, Wiley Verlag
- P. Liggesmeyer, Software - Qualität: Testen, Analysieren und Verifizieren von Software, Spektrum Verlag
- H. Sneed, M. Winter, Testen objektorientierter Software, Hanser Verlag

CY-B-20 Wahlpflichtmodul Projekt

Modul Nr.	CY-B-20
Modulverantwortliche/r	Prof. Dr. Martin Schramm
Kursnummer und Kursname	Wahlpflichtmodul Projekt
Lehrende	Prof. Dr. Andreas Grzemba Prof. Dr. Martin Schramm
Semester	4
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 0 Stunden Selbststudium: 90 Stunden Virtueller Anteil: 60 Stunden Gesamt: 150 Stunden
Prüfungsarten	PrA
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden verfügen praxisnahes Wissen und praxisnahes Fachwissen im Bereich der Informatik, speziell der Informationssicherheit und IT-Sicherheit.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Studierenden entwickelt eigenständig Lösungen für fachliche Aufgabenstellungen.
- Sie können Ihre Arbeitsergebnisse werten und beurteilen.

Methodenkompetenz

- Die Studierenden haben die Fähigkeit, Detail-Informationen zu einer konkreten Aufgabenstellung zu beschaffen.
- Die Studierenden können Konzepte zur Bewältigung einer Aufgabenstellung in einem begrenzten Zeitrahmen erstellen.

Persönliche Kompetenz

- Die Studierenden entwicklen durch die an Sie gestellte praktische Aufgabenstellung ein hohes Maß an Eigenverantwortung.
- Sie stärken Ihre Sebstständigkeit, indem Sie Arbeiten selbstständig durchführen und passende Arbeitstechniken anwenden.
- Sie lernen Ihre eigene Belastbarkeit kennen und entwicklen Resilienz.

Sozialkompetenz

- Durch die selbstorganisierte Arbeit in kleinen Teams wird Respekt und Toleranz, sowie Hilfsbereitschaft bei den Studierenden gefördert.
- Die Studierenden erlernen Konfliktfähigkeit und Kooperationsbereitschaft.

Verwendbarkeit in diesem und in anderen Studiengängen

Es handelt sich um ein spezielles Modul zur Vertiefung und Erlangung praktischer Kompetenzen im Bereich Cyber Security.

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- die Inhalte der Module des 1. - 3. Studiensemesters

Inhalt

individuell, abhängig von konkreter Themenstellung

Lehr- und Lernmethoden

- praktische Arbeit
- fachliche Unterstützung durch Themensteller

Besonderes

- die Studierenden lernen, ein Projekt selbständig oder im kleinen Team zu bearbeiten

- das Thema wird von einem Professor der THD gegebenenfalls in Kooperation mit einem regionalen Unternehmen gestellt
- der themenstellende Professor bewertet die Arbeit

Empfohlene Literaturliste

individuell, abhängig von konkreter Themenstellung

CY-B-21 Kryptologie 2

Modul Nr.	CY-B-21
Modulverantwortliche/r	Prof. Dr. Martin Schramm
Kursnummer und Kursname	Kryptologie 2
Lehrende	Prof. Dr. Martin Schramm
Semester	4
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	PrA, LN Praxis
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden verfügen über tiefgreifendes allgemeines Wissen und tiefgreifendes Fachwissen in dem Bereich Kryptologie.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Studierenden können die Facetten der Elliptischen Kurven Kryptographie präsentieren.
- Sie können kryptographische Berechungen, sowie Faktosierungen durch Verwendung Elliptischer Kruven durchführen.
- Sie kennen die Typen von Zufallszahlengeneratoren und können diese kritisch vergleichen.

- Die Studierenden können die Grundprinzipien der Paarungsbasierten Kryptographie erläutern.
- Sie können die aktuellen Bestrebungen der Post-Quanten-Technologie demonstrieren und diskutieren.
- Sie können Maßnahmen der leichtgewichtigen Kryptographie und Maßnahmen der konventionellen Kryptographie beschreiben.

Methodenkompetenz

- Die Studierenden können für ein gegebenes Szenario entscheiden, ob konventionelle kryptographische Maßnahmen, oder leichtgewichtige Maßnahmen besser geeignet sind.
- Sie können bewerten, wie lange aktuelle (nicht-PQC) Verfahren noch Gültigkeit haben und entscheiden welche PCQ-Verfahren für einen Anwendungsfall am besten geeignet sind.

Persönliche Kompetenz

- Druch die Bearbeitung einer individuellen Projektarbeit, sowie durch die Praktika wird die Motivation, Neugier und die Belastbarkeit trainiert.

Sozialkompetenz

- Durch die Umsetzung der Projektarbeit und der gemeinsamen Diskussion der Projektgruppen wird die Empathie, die Teamfähigkeit sowie die Kritikfähigkeit geschärft.

Verwendbarkeit in diesem und in anderen Studiengängen

Weiterführendes Wahlpflichtmodul anderer Bachelorstudiengänge (wie z.B.: Angewandte Informatik/Infotronik, Interaktive Systeme/Internet of Things, Künstliche Intelligenz, Wirtschaftsinformatik, Elektro- und Informationstechnik)

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- mathematisches und abstraktes Denkvermögen
- Kenntnisse der Inhalte von Modul CY-B-11 Kryptologie 1

Inhalt

Lehr- und Lernmethoden

- Seminaristischer Unterricht mit praktischen Übungen
- Praktika

Besonderes

Praktikumsleistung (PrL) als Zulassungsvoraussetzung zur Prüfung.

Die Durchführung von Praktika und Übungen in dem Modul Netzwerksicherheit erfordert grundlegende Vorkenntnisse. Die Zulassung zu diesen Modulen erhält deshalb nur, wer mindestens 40 ECTS-Leistungspunkte erreicht hat und mindestens zwei Grundlagen- und Orientierungsprüfungen bestanden hat.

Empfohlene Literaturliste

Literatur:

- Werner, A.: Elliptische Kurven in der Kryptographie, Springer; 2002. Auflage (4. Oktober 2013), ISBN-13 : 978-3540425182
- Jonas, T.: Elliptische-Kurven-Kryptographie, GRIN Publishing; 1. Auflage (24. August 2016), ISBN-13 : 978-3668270381
- Mirbach, A.: Elliptische Kurven: Die Bestimmung ihrer Punktezahl und Anwendung in der Kryptographie, Verlagshaus Monsenstein und Vannerdat; 1., Aufl. Auflage (1. November 2003), ISBN-13 : 978-3937312224
- Johnston, D.: Random Number Generators?Principles and Practice: A Guide for Engineers and Programmers, Walter de Gruyter (7. Mai 2018), ISBN-13 : 978-1501506079

Webseiten:

- BSI - Anwendungshinweise und Interpretationen (AIS) - AIS 20/31
- https://csrc.nist.gov/projects/post-quantum-cryptography
- https://csrc.nist.gov/projects/lightweight-cryptography
- www.CrypTool.de (kryptographische Software)

CY-B-22 Management von IT-Sicherheitsvorfällen

Modul Nr.	CY-B-22
Modulverantwortliche/r	Prof. Dr. Thomas Störtkuhl
Kursnummer und Kursname	Management von IT-Sicherheitvorfällen
Lehrende	Prof. Dr. Thomas Störtkuhl
Semester	4
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	PrA
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden verfügen über tiefgreifendes allgemeines Wissen und tiefgreifendes Fachwissen in dem Bereich Management der Informationssicherheit.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Studierenden können alle Elemente des Managements der Informationssicherheit in ihrer Funktion für die Informationssicherheit beschreiben.
- Die Studierenden können alle Elemente des Managements der Informationssicherheit in Bezug auf den kontinuierlichen Verbesserungsprozess in Beziehung setzen.

- Die Studierenden kennen wesentliche Methoden der Informationssicherheit wie z.B. Analysemethoden und können Analysen auf IT-Systeme und IACS anwenden.
- Die Studierenden kennen wesentliche Inhalte einschlägiger Standards.
- Die Studierenden können wesentliche Inhalte einschlägiger Standards auf IT-Systeme und IACS anwenden.

Methodenkompetenz

- Die Studierenden können für ein gegebenes IT System und IACS sinnvolle IT Security Maßnahmen auf Basis einer Analyse ableiten.
- Die Studierenden können beurteilen, ob bestimmte IT Security Maßnahmen geeignet sind, bestimmte Bedrohungen und Risiken abzuwehren bzw. zu mindern.

Persönliche Kompetenz

- Durch die stattfindenden Übungen werden die Studierenden angehalten, Sachverhalte eigenständig zu erarbeiten und verständlich zu präsentieren.

Sozialkompetenz

- Durch die Erarbeitung von Analysen durch ein Team an reellen Beispielen aus der Praxis, lernen die Studierenden die konstruktive Zusammenarbeit, in der das Wissen und die Ideen anderer Studierender als hilfreich und förderlich erfahren wird.

Verwendbarkeit in diesem und in anderen Studiengängen

Weiterführendes Wahlpflichtmodul anderer Bachelorstudiengänge (wie z.B.: Angewandte Informatik/Infotronik, Interaktive Systeme/Internet of Things, Künstliche Intelligenz, Wirtschaftsinformatik, Elektro- und Informationstechnik)

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- Kenntnisse der Inhalte von Modul CY-B-04 Betriebssysteme und Netzwerke
- Kenntnisse der Inhalte von Modul CY-B-17 Netzwerksicherheit

Inhalt

- Motivation für das Management der Informationssicherheit: aktuelle Lage der Informationssicherheit; regulatorische Anforderungen auf nationaler und europäischer Ebene; Schutz kritischer Infrastrukturen

- Sichten der Informationssicherheit mit ganzheitlichem Ansatz: ISO/IEC 27001, Defense-in-Depth, kontinuierlicher Verbesserungsprozess, Lifecycle eines IT-Systems oder eines IACS (Industrial Automation and Control System), Zyklus Prävention, Dedektion, Reaktion.
- Elemente des Managements von Informationssicherheit: entlang des knotinuierlichen Verbesserungsprozesses werden alle Elemente angesprochen: Definition des Geltungsbereichs, Analyse Stakeholder, Beschreibung des Kontextes, Dokumentenlenkung, Schutzbedarfs-, Bedrohungs- und Risikoanalyse, Definition einer IT Security Architektur, Prozesse: User & Rights Management, Change Management, Backup & Recovery, Security Incident Management, Vulnerability Management, Audititerung und Management Review, Business Continuity, Prozess zur Entwicklung von Produkten mit IT Security Qualität, Management von Zulieferern und Diensleistern
- Schwerpunkt bzgl. der Elemente des Managements von Informationssicherheit sind Risikoanalyse und Business Continuity: Methoden, Vorgehen, Dokumentation
- Wesentliche Inhalte der Standards wie ISO/IEC 27001, IEC 62443, BSI Grundschutzkompendium oder ICS Security Kompendium oder National Institute of Standards and Technology (NIST) werden dargestellt.

Lehr- und Lernmethoden

- Seminaristischer Unterricht mit praktischen Übungen

Empfohlene Literaturliste

- ISO/IEC 27000: Information technology - Security techniques - Information security management systems - Overview and vocabulary, Third edition, 2014-01-15
- ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013 + Cor. 1:2014), English translation of DIN ISO/IEC 27001:2015-03
- ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls, Second edition, 2013-10-01
- ISO/IEC 27005:2018-07 Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Risikomanagement, Englischer Titel: Information technology - Security techniques - Information security risk management
- IT-Grundschutz-Kompendium, Bundesamt für Sicherheit in der Informationstechnik, Bonn 2020; https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html (zuletzt aufgerufen am 3.10.2020)

- 65/756/CDV:2019-08 - IEC 62443-2-1 Ed.2.0 - Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners
- IEC 62443-2-3, Edition 1, 2015-06, Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment
- DIN EN 62443-3-2:2018-10; VDE 0802-3-2 - Entwurf Sicherheit für industrielle Automatisierungssysteme - Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung (IEC 65/690/CDV:2018); Deutsche und Englische Fassung prEN 62443-3-2:2018; Englischer Titel: Security for industrial automation and control systems - Part 3-2: Security risk assessment and system design (IEC 65/690/CDV:2018)
- IEC 62443-3-3, Edition 1, 2013-08, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels
- Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, February 12, 2014
- DIN ISO 31000:2018-10: Risikomanagement - Leitlinien (ISO 31000:2018), Englischer Titel: Risk management - Guidelines (ISO 31000:2018), 2018-10
- Zusammenhang von Security und Funktionaler Sicherheit, Felix Wieczorek, Frank Schiller, Roland Fiat, Thomas Störtkuhl, atp edition, 6/2013
- Ganzheitliches Management der Informationssicherheit, Thomas Störtkuhl, et al., SecuMedia, 19. September 2008
- Alles im Blick, Ganzheitliches Sicherheitsmanagement mit Kennzahlen für IT-Betrieb und -Sicherheit, Udo Adlmanninger, Thomas Störtkuhl

CY-B-23 Distributed-Ledger-Technologien

Modul Nr.	CY-B-23
Modulverantwortliche/r	Prof. Dr. Thomas Störtkuhl
Kursnummer und Kursname	Distributed-Ledger-Technologien
Lehrende	Prof. Dr. Thomas Störtkuhl
Semester	4
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden verfügen über grundlegendes allgemeines Wissen und grundlegendes Fachwissen sowie prozedurales Wissen in dem Bereich der Distributed Ledger Technologien (Techniken verteilter Kassenbücher)

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Studierenden können die unterschiedlichen Lösungsvorschläge für Distributed Ledgers klassifizieren und erläutern.

- Sie können die unterschiedlichen Methoden zur Konsensbildung zusammenfassen und erklären.
- Sie können die möglichen Anwendungen unterschiedlicher Distributed Ledger Technologien angeben und weitere mögliche Anwendungen ableiten.
- Sie können ausgewählte Beispiele von verteilten Kontobüchern und Konsensprotokolle implementieren.

Methodenkompetenz

- Die Studierenden sind in der Lage, existierende und zukünftige Vorschläge für Distributed Ledgers zu Differenzieren und Ihre jeweiligen Vor- und Nachteile gegenüberzustellen.
- Sie sind in der Lage, für einen gegebenen Anwendungsfall zu überprüfen, ob für diesen der Einsatz einer DLT-Technologie sinnvoll erscheint, bzw. ob konventionelle Datenbank-Lösungen ausreichend sind.

Persönliche Kompetenz

- Durch die Erarbeitung und Aufarbeitung eines aktuellen Themas im Bereich DLT wird die Sorgfalt und Gewissenhaftigkeit der Studierenden geschult.

Sozialkompetenz

- Durch die Gruppendiskussionen und Verzahnung der Praxisprojekte wird die Networking-Kompetenz, Konflikt- und Kritikkompetenz gefördert.

Verwendbarkeit in diesem und in anderen Studiengängen

Wahlpflichtmodul anderer Bachelorstudiengänge (wie z.B.: Angewandte Informatik/Infotronik, Interaktive Systeme/Internet of Things, Künstliche Intelligenz, Wirtschaftsinformatik, Elektro- und Informationstechnik)

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- Kentnisse der Inhalte der Module CY-B-11 Kryptologie 1, CY-B-13 Datenbanken und CY-B-17 Netzwerksicherheit

Inhalt

1 Einführung
   - Motivation
   - Überblick
   - Distributed Ledger Taxonomie

2 Konsensbildung
- Proof-Based / Computational-Based Konsensprotokolle
- Proof of Work (PoW)
- Proof of Stake (PoS)
- weitere Konzepte
- Voting-Based / Communication-Based Konsensprotokolle
- (Byzantine) Fault Tolerance
- Practical-Byzantine-Fault-Tolerance (PBFT)
- weitere Konzepte

3 Anwendungen
- Kryptowährung - z.B.: Bitcoin - BTC (Blockchain)
- Smart Contracts und DApps - z.B.: Ethereum
- Mobilitätskonzepte - z.B.: IOTA (Tangle - Transaction Directed Acyclic Graph (TDAG))
- Plattform für BlockchainAnwendungen auf Open-Source Basis

4 Potentiale
- 5 Thesen für das Potential von DLT
- Wie man einen Anwendungsfall auf Eignung hinsichtlich DLT-Einsatz evaluiert
- Hilfestellung zur Entscheidungsfindung

5 Praxisprojekt

Lehr- und Lernmethoden

Seminaristischer Unterricht mit praktischen Übungen

Empfohlene Literaturliste

Literatur:

- Schütz, A., Fertig, T.: Blockchain für Entwickler: Das Handbuch für Software Engineers. Grundlagen, Programmierung, Anwendung. Mit vielen Praxisbeispielen, Rheinwerk Computing; 1. Auflage (22. Februar 2019), ISBN-13 : 978-3836263900
- Hellwig, D., Karlic, G.: Build Your Own Blockchain: A Practical Guide to Distributed Ledger Technology, Springer; 1st ed. 2020 Auflage (30. Juni 2020), ISBN-13 : 978-3030401412
- Treiblmaier, H., Clohessy, T.: Blockchain and Distributed Ledger Technology Use Cases: Applications and Lessons Learned, Springer; 1st ed. 2020 Auflage (13. Juli 2020), ISBN-13 : 978-3030443368
- Lemieux, V., Feng, C.: Building Decentralized Trust: Multidisciplinary Perspectives on the Design of Blockchains and Distributed Ledgers,

Springer; 1st ed. 2021 Auflage (13. Dezember 2020), ISBN-13 : 978-3030544133
- Köhler-Schute, C.: Blockchains und Distributed-Ledger-Technologien in Unternehmen: Grundlagen, Konzepte und Praxisbeispiele, juristische Aspekte, KS-Energy-Verlag (26. September 2019), ISBN-13 : 978-3945622094

Webseiten:

- Blockchain - https://www.blockchain.com/de/
- Ethereum - https://ethereum.org/
- IOTA Tangle - https://www.iota.org/
- HaderaHashgraph - https://www.hedera.com
- Hyperledger - https://www.hyperledger.org

CY-B-24 Schlüsselqualifikation 4

Modul Nr.	CY-B-24
Modulverantwortliche/r	Prof. Dr. Josef Scherer
Kursnummer und Kursname	Compliance, Datenschutz und IT-Recht
Lehrende	Prof. Dr. A Admin Michael Donnert Anke Hofmeyer Prof. Dr. Josef Scherer
Semester	4
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Teilnehmer sollen im dargestellten Bereich *Compliance, Datenschutz und IT-Recht* grundlegende Kenntnisse erwerben und in die Lage versetzt werden, praxisrelevante Problemstellungen aus diesem Bereich einer betrieblich organisatorischen Lösung, bei Standardproblemen unter Umständen sogar in Form von Verfahrensanweisungen und Prozessbeschreibungen zuzuführen.

Darüber hinaus wird erwartet, dass der Teilnehmer nach Absolvierung dieses Moduls die relevanten Inhalte mit eigenen Worten verständlich erklären kann.

1 Die Veranstaltung soll Transparenz und Verständnis für das oft "nebulös" wirkende Thema erzeugen und klare Strukturen und praktische Arbeitshilfen aufzeigen.
2 Die Teilnehmer sollen nach der Veranstaltung wissen, verstehen und mit einfachen Worten erklären können,
   - was die relevanten Bestandteile der dargestellten Prozesse / Systeme / Organisation sind,
   - inwieweit es sie selbst betrifft (Rolle, Aufgaben, Verantwortung, Nutzen) und
   - wie die für sie relevanten Prozessabläufe diesbezüglich angereichert werden.
3 Außerdem sollen die Teilnehmer befähigt werden, die einschlägigen Anforderungen an ihren eigenen Arbeitsbereich als Ziele transparent zu machen und zu erfüllen.
4 Durch Darstellung der Wertbeiträge des Systems / der Prozesse für Unternehmen / Organisation und Mitarbeiter soll Bewusstsein, Interesse und Motivation zum "proaktiven Leben" des Systems erzeugt werden.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Teilnehmer sind in der Lage, ein digitalisiertes Integriertes Managementsystem im Bereich Compliance, Datenschutz und IT-Recht bzw. einschlägige Prozessabläufe zu konzeptionieren und zu implementieren und die Aufbau- und Ablauforganisation mit entsprechenden Compliance-, Risiko- und IKS-Komponenten anzureichern.
- Die Teilnehmer können Problemfälle über die Methode der richterlichen Falllösungsmethode lösen.
- Die Teilnehmenden können das erworbene Wissen über Soll-Ist-Vergleiche und Handlungsempfehlungen in Unternehmen / Organisationen umsetzen.
- Die Teilnehmer haben die Fähigkeit, Sachverhalte und Aufgabenstellungen dem passenden Bereich im Unternehmen oder Umfeld zuzuordnen und die Schnittstellen zu anderen Funktionen zu erkennen.
- Die Teilnehmer sind in der Lage, unter Beachtung der rechtlichen Rahmenbedingungen, die Vernetzung innerhalb der diversen Unternehmensfunktionen (Führungs-, Kern, - und Unterstützungsprozessthemen) zu verstehen und eine entsprechende Architektur zu konzipieren und zu verbessern.

Methodenkompetenz

- Mittels SWOT-Analysen, Soll-Ist-Vergleichen, etc. sind die Teilnehmer in der Lage, Handlungsempfehlungen zur Steuerung von Governance- (Unternehmensführung und -Überwachung-) Risiken abzugeben.
- Die Teilnehmenden kennen die Methoden von Audits und orientieren sich bzgl. der einschlägigen Themen primär am "Aktuellen Stand von Gesetzgebung und Rechtsprechung (Compliance)" und sekundär am "Anerkannten Stand von Wissenschaft und Praxis". Dabei ziehen sie die ihnen dem Grunde nach bekannten Standards (Regelwerken (internationaler) institutionalisierter Sachverständigen/Gremien) (z.B. DIN/ ISO/COSO/IDW/DIIR/etc.) heran.

Persönliche Kompetenz

- SWOT-Analysen und Soll-Ist-Vergleiche im Rahmen von praktischer Tätigkeit im Unternehmen (oder anhand von Case-studies) ermöglichen dem Teilnehmer, im Berufsleben die Organisation von Unternehmen oder Teilbereichen zu verbessern.

Sozialkompetenz

- Die Teilnehmer reflektieren die Thematik im internationalen Kontext (z. B. internationales Recht, internationale Standards), die Teilnehmer reflektieren alle Inhalte unter dem Aspekt der Digitalen Transformation und der Modellierung als Prozessabläufe.

Verwendbarkeit in diesem und in anderen Studiengängen

Verwendbarkeit des Moduls für diesen Studiengang

- Dieses Modul zählt zu den interdisziplinären Schlüsselqualifikationen.

Verwendbarkeit des Moduls für andere Studiengänge

- Diese Modul kann in allen sonstigen technischen, rechtlichen, wirtschaftspsychologischen und betriebswirtschaftlichen Studiengängen verwendet werden, da das Wissen über Governance, Compliance und Corporate Social Responsibility / Nachhaltigkeit sowie die Rechte und Pflichten von Managern, sonstigen Führungskräften und Mitarbeitern nahezu unverzichtbar für "ordentliches und gewissenhaftes" Management ist.

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

Dieses Modul baut auf die Inhalte der einschlägigen Aufsätze von *Scherer/Fruth/N.N.* auf:

Vgl. hierzu scherer-grc.net/publikationen und die Bücher *Scherer/Fruth* (Hrsg.):

- Unternehmensführung 4.0 ("Digital Governance") - Die Verknüpfung von Digitalisierung und GRC mit Strategie, Zielerreichung und (Nachhaltigkeits-) Berichterstattung, 2020
- Integriertes Managementsystem "on demand", 2018
- Integriertes Compliance-Managementsystem, 2018
- Digitalisiertes Integriertes Risiko-Managementsystem, 2019
- Integriertes Qualitäts-Managementsystem, 2018
- Handbuch Integriertes Personal-Managementsystem, 2018
- Handbuch Integriertes Corporate Social Responsibility (CSR)- / Nachhaltigkeits-Managementsystem, 2019

Inhalt

Teil Scherer:

vhb: Governance, Risk und Compliance im Bereich Personal / HR

1 Gemeinsamkeiten und Unterschiede zwischen persönlicher Zufriedenheit und Management-Zielen Einführung (I)
   - Gemeinsamkeit und Unterschied zwischen persönlicher Zufriedenheit und Erreichung der Management-Ziele: Die unverzichtbaren Basics -Erkenntnisse zu Governance, Management, Risk und Compliance (- Perspektivenwechsel) - Teil I: Persönliche Zufriedenheit und Glück
   - Gemeinsamkeit und Unterschied zwischen persönlicher Zufriedenheit und Erreichung der Management-Ziele: Die unverzichtbaren Basics -Erkenntnisse zu Governance, Management, Risk und Compliance (- Perspektivenwechsel) - Teil II: Probleme bei Nichteinhaltung von Standards / Normen / technischen Entwicklungsständen
   - Gemeinsamkeit und Unterschied zwischen persönlicher Zufriedenheit und Erreichung der Management-Ziele: Die unverzichtbaren Basics -Erkenntnisse zu Governance, Management, Risk und Compliance (- Perspektivenwechsel) - Teil III: Management-Ziele und Zufriedenheit
   - Prozesse im Integrierten Personal-Managementsystem mit Governance, Risk und Compliance
   - Die "Verschmelzung" von Standards im Integrierten Personal-Managementsystem mit Governance, Risk und Compliance

2 Human Workflow-Management-Prozesse und Digitale Transformation im Bereich Personal Einführung (II)
- Digitale Transformation und Integriertes Personal-Managementsystem
- Standardorientiertes, Integriertes Personal-Managementsystem: "Das Richtige richtig tun"
- Human Workflow-Management-Prozesse und Integriertes Personal-Managementsystem im Lichte aktueller Rechtsprechung des BGH
- Hohe Anforderungen an Unternehmer
- Die "Evolution" des Prozessmanagements
- "Stand der Technik" im Prozessmanagement
- Exkurs: Unternehmensführung 4.0 und Integriertes Personal-Managementsystem mit GRC-PS-Perso

3 Enthaftung und Wertbeiträge durch ein Integriertes Personal-Management-system (PMS) Einführung (III)
- "Homo rationalis" durch Human Workflowmanagement
- Monitoring, Reporting und Prozesskostenrechnung für die "lines of defense"
- Integriertes Managementsystem on demand
- Ein Digitaler Workflow-Prozess zur Implementierung eines "Integrierten Managementsystems"
- Enthaftung durch ein Integriertes Personal Managementsystem mit GRC und Workflowmanagement
- Wertbeiträge und Enthaftung

4 Definitionen, rechtlicher Rahmen, Tools und Konzep-tionierung des PMS (Block 1)
- Die Komponenten des Integrierten Personal Managementsystems
- Komponente K1 - Integration von "Insel"-Managementsystemen in ein Personal-Managementsystem auf Basis von (Universal-)Standards
- Komponente K2 - Verständliche Definitionen der relevanten Begriffe für ein Personal-Managementsystem
- Komponente K3 - Rechtliche Rahmenbedingungen für ein Personal-Managementsystem und Rechtskataster
- Komponente K4 - Tools und Methoden im Personal-Managementsystem
- Komponente K5 - Konzeptionierung des Personal-Managementsystems (mit Zielen, Wertbeitrag, Soll-Ist-Abgleich, Bewertung, Handlungsbedarf mit erforderlichen Ressourcen, Entscheidung, Projektierung und Managementsystem-Beschreibung)

5 Analyse von Unternehmen, Umfeld, etc. und Ableitung des Unternehmensrahmens Block 2 (I)
   - Komponente K6 - Unternehmensanalyse
   - Komponente K7 - Umfeldanalyse
   - Komponente K8 - Interested Parties Analyse
   - Komponente K9 - Bewertung der Analysen und Ableitung von Maßnahmen
   - Komponente K10 - Unternehmensvision, Mission, Leitbild, Ziele, Strategie, Planung und Unternehmenspolitik
   - Komponente K11 - Organisatorischer Rahmen (unternehmensweit) - Rechtssichere, prozessorientierte Unternehmensorganisation

6 Aufbau-organisation im PMS Block 2 (II)
   - Komponente K11 - Unternehmensweiter organisatorischer Rahmen - Einführung Teil I: Definitionen, Tools & Methoden, Komponenten, Konzeptionierung
   - Komponente K11 - Unternehmensweiter organisatorischer Rahmen - Einführung Teil II: Rechtliche Rahmenbedingungen und Standards
   - Komponente K11 - Unternehmensweiter organisatorischer Rahmen - Einführung Teil III: "Die prozessorientierte Organisation"
   - Komponente K11/1 - Unternehmensweiter organisatorischer Rahmen / Gesellschaftsrechtlich angemessene Unternehmens(gruppen)struktur
   - Komponente K11/2 - Unternehmensweiter organisatorischer Rahmen / Rechtssichere Organigramme
   - Komponente K11/3 - Unternehmensweiter organisatorischer Rahmen / Schnittstellenmanagement
   - Komponente K11/4 - Unternehmensweiter organisatorischer Rahmen / Rechtssichere Stellenbeschreibungen

7 Ablauforganisation, Kommunikation und Dokumentation Block 2 (II)
- Komponente K11/5 - Unternehmensweiter organisatorischer Rahmen / Rechtssicheres Interaktionsmanagement
- Komponente K11/6 - Unternehmensweiter organisatorischer Rahmen / Rechtssichere Delegation
- Komponente K11/7 - Unternehmensweiter organisatorischer Rahmen / Rechtssichere Prozessbeschreibungen
- Komponente K11/8 - Unternehmensweiter organisatorischer Rahmen / Wirksame Aufsichts- bzw. Kontrollmechanismen
- Komponente K11/9 - Unternehmensweiter organisatorischer Rahmen / Implementiertes und wirksames Informations- und Kommunikationsmanagement
- Komponente K11/10 - Unternehmensweiter organisatorischer Rahmen / Implementiertes und wirksames Dokumentationsmanagement
- Komponente K11/11 - Unternehmensweiter organisatorischer Rahmen / Unterstützendes (Integriertes) Managementsystem
- Komponente K11/12 - Unternehmensweiter organisatorischer Rahmen / Angemessene (Personal-) Ressourcen
- Komponente K12 - Kommunikationsrahmen (unternehmensweit)
- Komponente K13 - Dokumentationsrahmen (unternehmensweit)

OPEN vhb: Unternehmensführung 4.0: Der Ordentliche Kaufmann und sein digitalisiertes Integriertes Managementsystem mit GRC

"Digital, fit, proper, sustainable, successful & safe: Der Ordentliche Kaufmann 4.0!"

1 Einführung: "Auf einen Blick und Überblick": Die Fakten und die Story
2 "Das Richtige richtig tun": Der "Ordentliche Kaufmann 4.0": OK!
3 Enthaftende Wirkung und sonstige Wertbeiträge eines digitalisierten Integrierten Managementsystems 4.0
4 Welche(s) Managementsystem(e) und wieviel(e) Standard(s) für Digitalisierung und GRC braucht der Manager?
5 Begriffe, die der Ordentliche Kaufmann und seine Mitarbeiter kennen müssen
6 Was heißt Digitalisierung von Geschäftsprozessen und Anreicherung mit GRC -Methoden und Tools?
7 Unternehmens-, Umfeld-, interested-parties-, Risiko- und SWOT-Analyse: Alle wollen das Gleiche: Keine Schwächen bei Digitalisierung und GRC
8 "Ready for take off: Der neue Tone from the Top im Unternehmensflugschiff"
9 Governance: Interaktion der Organe, gewissenhafte Unternehmensführung und -überwachung
10 "Hard Facts": Worum hat sich der Ordentliche Kaufmann zu kümmern und welche Sachkenntnisse sind gefragt?

11 Wie Top-Manager ihre wichtigste Ressource - Zeit - auf ihre wichtigsten Aufgaben verteilen sollten
12 "Wir nicht so einfach verbesserlich!" - Der "Habitus" des "Ordentlichen Kaufmanns 4.0": Wissens-, Soziales, Kulturelles, Sprachliches, Physisches, Psychisches, Digitales Kapital und Softskills
13 Managerhaftung: Zivil- und strafrechtliche Haftung der Organe und (Sonder-)Beauftragten
14 Der Manager-Risikokoffer und die Haftungs-Firewall
15 Neue Ziele in einer neuen Welt
16 (Digitalisierung-) Vision / -Ziele / -Strategie / -Planung
17 "Warum klappts oft nicht?": Homo irrationalis versus fit & proper: Verhaltensökonomie und Wirtschaftspsychologie
18 Umsetzung von (Digitalisierungs-) Maßnahmen mit begleitender Steuerung und Überwachung

"One fits all": Das digitalisierte Integrierte Managementsystem (IMS) mit GRC

1 "Step by step" - Die ersten Schritte bei Einführung eines digitalisierten Integrierten GRC-Managementsystems
2 "Das Rückgrat der Organisation" - Prozessmodellierung
3 Anwendungsbereich (Scope) von Standards für ein digitalisiertes "Integriertes Managementsystem mit GRC" (IMS) - Welche(s) Managementsystem(e) und Standards braucht der Manager?
4 Relevante Standards, Werkzeuge und Methoden
5 Erklärung relevanter Begriffe
6 Kontext der Organisation, Ziele, Wertbeitrag, Anwendungsbereich, Aufbau und Komponenten des digitalisierten Integrierten GRC-Managementsystems
7 Integriertes Finanz-Managementsystem
8 Integriertes Qualitäts-Managementsystem, Product Compliance und Vertragsmanagement mit GRC
9 Integriertes Compliance-Managementsystem
10 Integriertes Risiko-Managementsystem mit GRC
11 Integriertes Personal-Managementsystem mit GRC
12 Integriertes Nachhaltigkeits-Managementsystem
13 Integriertes Digitalisierungs-, IT-, Informationssicherheits-, Datenschutz-Managementsystem
14 Der "Tone from the Top" macht die Musik
15 Planung eines angemessenen digitalisierten GRC-Managementsystems
16 Unterstützung: Implementierung des digitalisierten Integrierten GRC-Managementsystems und angemessene Rahmenbedingungen
17 Betrieb: Umsetzung und Wirksamkeit (Betrieb) des digitalisierten Integrierten GRC-Managementsystems und der Prozess

18 Begleitende Steuerung, Überwachung und Bewertung des digitalisierten Integrierten GRC-Managementsystems (durch die "lines-of-defense")
19 Anpassungen bei Schwächen und Änderung in Organisation und Umfeld

Lehr- und Lernmethoden

Seminaristischer Unterricht, Übungen, Falllösungen anhand von Beispielen aus der (höchst-) richterlichen Rechtsprechung, Selbststudium, studentische Referate und Studienarbeiten.

Durch einen in der Lehrveranstaltung vermittelten und von Teilnehmern verstandenen multifunktionalen, interdisziplinären Ansatzes (Recht, BWL, Technik, Wirtschaftspsychologie, Verhaltensökonomie) werden den Teilnehmern unterschiedliche Sichtweisen und Erkenntnisse bzgl. der Subjekte und Objekte des (Wirtschafts-) Lebens sowie auch bzgl. der eigenen Person vertraut.

Besonderes

Das Modul enthält virtuelle Anteile:

- 2 SWS: Prof. Dr. Josef Scherer:
- vhb-Kurs: "Integriertes Managementsystem im Bereich Personal/HR mit Governance, Risk und Compliance", Kapitel 1-7
- OPEN vhb-Kurs: "Unternehmensführung 4.0 mit Governance, Risk und Compliance" - Der Ordentliche Kaufmann und sein digitalisiertes Integriertes Managementsystem mit GRC, ganzer Kurs

Empfohlene Literaturliste

Teil Scherer:

Einführende Literatur:

- Scherer, Good Governance und ganzheitliches, strategisches und operatives Management: Die Anreicherung des ?unternehmerischen Bauchgefühls? mit Risiko-, Chancen- und Compliancemanagement, in: Corporate Compliance Zeitschrift (CCZ), 6/2012, S. 201-211.
- Scherer/Fruth (Hrsg.), Stark in die Zukunft, 2011.
- Scherer/Fruth (Hrsg.), Governance-Management Band 1 (2014).
- Scherer/Fruth (Hrsg.), Governance-Management Band 2 (2015).
- Scherer/Fruth (Hrsg.), Anlagenband zu Governance-Management Band 2 (2015).

Skript:

- die Skripte zu den vhb-Lerneinheiten sind in den jeweiligen Kursen verfügbar.

Vertiefende Literatur:

- Scherer/Fruth (Hrsg), Handbuch: Integriertes Managementsystem (IMS), 2018
- Scherer/Fruth (Hrsg), Handbuch: Integriertes Qualitäts-Managementsystem, 2018
- Scherer/Fruth (Hrsg), Handbuch: Integriertes Compliance-Managementsystem, 2018
- Scherer/Fruth (Hrsg), Handbuch: Integriertes Product-Compliance-, Vertragsmanagement und Qualitätsmanagement, 2018
- Scherer/Fruth (Hrsg), Handbuch: Integriertes Personal-Managementsystem, 2018
- Scherer/ Fruth (Hrsg.), Geschäftsführer-Compliance, Praxiswissen zu Pflichten, Haftungsrisiken und Vermeidungsstrategien, 2009
- Scherer/ Fruth (Hrsg.), Gesellschafter-Compliance, Praxiswissen zu Pflichten, Haftungsrisiken und Vermeidungsstrategien, 2011
- Scherer, Grziwotz, Kittl, Praxis des gewerblichen Rechtsschutzes und des Wettbewerbsrechts, 2006.

CY-B-25 Praxismodul

Modul Nr.	CY-B-25
Modulverantwortliche/r	Prof. Dr. Udo Garmann
Kursnummer und Kursname	Betriebspraktikum Praxisseminar Praxisergänzende Vertiefung
Semester	5
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	30
Workload	Präsenzzeit: 60 Stunden Selbststudium: 45 Stunden Virtueller Anteil: 45 Stunden Gesamt: 150 Stunden
Gewichtung der Note	30/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die bislang im Studium erworbenen Kenntnisse, Fähigkeiten und Fertigkeiten sollen in einem Projekt aus dem Bereich der Cyber Security methodisch und im Zusammenhang eingesetzt werden mit dem Ziel der Verankerung und Erweiterung des bereits Erlernten durch praktische Erfahrung. Zudem lernen die Studierenden Bedeutung der Teamarbeit in der industriellen Praxis kennen.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Durch die Bearbeitung des Themas des Betriebspraktikum verfügen die Studierenden über praktische Erfahrung in dem jeweiligen Schwerpunkt.

- Die die Studierenden haben die Kompetenz, die bislang im Studium erworbenen Kenntnisse und Fähigkeiten auf teilweise komplexe Aufgabenstellungen selbständig anwenden zu können und präsentieren diese in einer angemessenen mündlicher und schriftlicher Form.

Methodenkompetenz

- Durch die Planung der Arbeitsschritte, ihre Ausführung und den Abschluss in Form eines Praktikumsberichts verfügen die Studierenden über die Fähigkeit ein praktisches Projekt selbständig erfolgreich abzuschließen.

Persönliche Kompetenz

- Sie Studierenden erlangen durch den Abschluss des Praxismoduls Eigenverantwortung, Selbstdisziplin, Selbstreflexion und Selbstvertrauen.

Sozialkompetenz

- Die Studierenden erlangen die Fähigkeit der zielgruppengerechten Präsentation der Aufgabenbestandteile während des Betriebspraktikums und der im Betriebspraktikum erzielten Resultate.

Verwendbarkeit in diesem und in anderen Studiengängen

es handelt sich um ein spezielles Modul für diesen Studiengang

Zugangs- bzw. empfohlene Voraussetzungen

Formal:

- Gemäß § 6 der Studien- und Prüfungsordnung setzt der Eintritt in das praktische Studiensemester voraus, dass mindestens 70 ECTS-Leistungspunkte erzielt wurden.

Inhaltlich:

- Kentnisse und Anwendbarkeit der Studienganginhalte der vorangegangenen Semester

Inhalt

Das Praxismodul des praktischen Studiensemester besteht aus den Teilen **Betriebspraktikum**, **Praxisseminar** und **Praxisergänzende Vertiefung**. Das Modul umfasst mindestens 20 Wochen und beinhaltet ein Praktikum in einem Betrieb (Teil **Betriebspraktikum**), Seminare des Career Service (Teil **Praxisergänzende Vertiefung**), sowie praxisbegleitende Lehrveranstaltungen laut Studienplan (Teil **Praxisseminar**), die in Blockveranstaltungen zu Semesterbeginn und/oder Semesterende stattfinden.

Nähere Informationen zum Teil **Praxisergänzende Vertiefung**:

Dieser wird durch sieben Seminare des Career Service ersetzt. Jeder Studierende des Studiengangs Cyber Security muss bis zum Ende des 7. Semesters fünf Seminare der Rubrik ?Studien- und Persönlichkeitskompetenz? und zwei Seminare der Rubrik ? Berufskompetenz? belegt haben.

Bis zu Beginn des Praktikums im 5. Semester müssen **mindestens** fünf Seminare aus den beiden Rubriken belegt werden.

Verpflichtende Seminare:

- Präsentationstechniken
- LaTex
- Bibliotheksseminar "Datenbanken / Lieteraturrecherche"

Frei wählbare Seminare:

- Seminarthema frei wählbar aus Studien-und Persönlichkeitskompetenz
- Seminarthema frei wählbar aus Studien-und Persönlichkeitskompetenz
- Seminarthema frei wählbar aus Berufskompetenz
- Seminarthema frei wählbar aus Berufskompetenz

Nähere Informationen hinsichtlich der jeweils angebotenen Seminare erhalten die Studierenden seites des Career Service.

Lehr- und Lernmethoden

- Teil Betriebspraktikum: Praktikum
- Teil Praxisseminar: Seminarisitischer Unterricht
- Teil Praxisergänzende Vertiefung: Seminar

Besonderes

- Der Nachweis der praktischen Tätigkeit (Teil Betriebspraktikum) kann in besonders begründeten Ausnahmefällen durch eine einschlägige fachpraktische Ausbildung ersetzt werden.
- Das praktische Studiensemester (Teil Betriebspraktikum) kann auch im Ausland geleistet werden.

Empfohlene Literaturliste

keine

CY-B-26 Penetration Testing

Modul Nr.	CY-B-26
Modulverantwortliche/r	Prof. Dr. Martin Schramm
Kursnummer und Kursname	Penetration Testing
Lehrende	Karl Leidl
Semester	6
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	PrA, LN Praxis
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden verfügen über grundlegendes tiefgreifendes Fachwissen und Methodenwissen in den Bereichen Penetration Testing und Schwachstellenanalyse.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Studierenden können die einzelnen Phasen eines Penetrationtests erläutern.
- Sie kennen die existierenden Exploiting-Frameworks und können diese anwenden.
- Sie können Hilfsmodulen der einzelnen Phasen eines Penetrationstests bestimmen und diese ausführen.

- Sie können existierende Automatisierungsmechanismen für einen gegebenen Anwendungsfall auf ihre Tauglichkeit hin analysieren und diese anwenden.
- Sie können eigenständig eine Schwachstellenanalyse ausführen und die Ergebnisse dieser bewerten.

Methodenkompetenz

- Die Studierenden können für einen exemplarischen Penetrationtest beurteilen, welche Art der Dokumentation während des Tests am besten geeignet ist.
- Die Studierenden sind in der Lage, eigene Tools für das Penetrationtesting zu entwickeln.

Persönliche Kompetenz

- Durch die eigenständige Durchführung eines Penetrationstests mit all seinen Phasen wird die Eigenverantwortung und Selbstdisziplin gefordert, was die Selbstwirksamkeit der Studierenden fördert.

Sozialkompetenz

- Durch die Projektarbeit im Team wird durch das gemeinsame Bearbeiten einer Aufgabenstellung die Kommunikationsfähigkeit, die Kompromissbereitschaft, sowie die Kritikfähigkeit gestärkt.

Verwendbarkeit in diesem und in anderen Studiengängen

Wahlpflichtmodul anderer Bachelorstudiengänge (wie z.B.: Angewandte Informatik/Infotronik, Interaktive Systeme/Internet of Things, Künstliche Intelligenz, Wirtschaftsinformatik, Elektro- und Informationstechnik)

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- Kenntnisse der Inhalte der Grundlagenmodule
- Kenntnisse der Inhalte des Moduls Netzwerksicherheit
- Kenntnisse der Inhalte der Module Kryptologie 1 und Kryptologie 2

Inhalt

1 Einführung
   - Motivation
   - Thematische Einordnung
   - Was ist Pentesting?

2 Methodik - die Phasen eines Penetrationtests
- Vorbereitung
- Informationsbeschaffung und -auswertung
- Bewertung der Informationen / Risikoanalyse
- Aktive Eindringversuche
- Abschlussanalyse

3 Exploiting Frameworks
- Umfang von Exploiting-Frameworks
- Vorhandenen Frameworks

4 Dokumentation während eines Penetrationstests

5 Einführung in das Metasploit-Framework
- Geschichte und Architektur
- Installation und Updates
- Benutzeroberflächen
- Datenstore und Datenbanken
- Workspaces
- Logging und Debugging

6 Die Pre-Exploitation-Phase
- Hilfsmodule und deren Anwendung
- Shodan-Suchmaschine
- Internet-Archive
- Analyse der DNS-Umgebung
- Discovery-Scanner
- Portscanner
- SNMP-Community Scanner
- VNC-Angriffe
- weitere ausgewählte Hilfsmodule
- Netcat

7 Die Exploiting-Phase
- Einführung in die Exploiting-Thematik
- Metasploit-Konsole

8 Die Post-Exploitation-Phase
- Grundlagen Meterpreter
- Eigenschaften und Grundfunktionalitäten
- Post-Exploitation-Module
- Post-Information Gathering
- VNC-Verbindung
- Netzwerk-Enumeration
- weitere ausgewählte Module
- Timestomp
- Privilegien erweitern
- Programme aus Speicher ausführen
- Pivoting

9 Automatisierungsmechanismen
10 Spezielle Anwendungsgebiete
11 Schwachstellenscanner

Lehr- und Lernmethoden

- Seminaristischer Unterricht mit praktischen Übungen
- Praktika

Besonderes

Praktikumsleistung (PrL) als Zulassungsvoraussetzung zur Prüfung.

Empfohlene Literaturliste

- Messner, M.: Hacking mit Metasploit: Das umfassende Handbuch zu Penetration Testing und Metasploit, dpunkt.verlag GmbH; 3., akt. u. erw. Auflage (30. Oktober 2017), ISBN-13 : 978-3864905230
- Brabetz, S.: Penetration Testing mit Metasploit: Praxiswissen für mehr IT-Sicherheit, mitp; 2018. Auflage (31. März 2018), ISBN-13 : 978-3958455955
- Kofler, M., Zingsheim, A., et al.: Hacking & Security: Das umfassende Handbuch, Rheinwerk Computing; 1. Auflage (27. April 2018), ISBN-13 : 978-3836245487
- Seitz, J.: Mehr Hacking mit Python: Eigene Tools entwickeln für Hacker und Pentester, dpunkt.verlag GmbH; 1. Auflage (1. September 2015), ISBN-13 : 978-3864902864
- Noors, A.: Hacken mit Python und Kali-Linux: Entwicklung eigener Hackingtools mit Python unter Kali-Linux, Books on Demand; 1. Auflage (6. November 2018), ISBN-13 : 978-3748165811

CY-B-27 Digitale Forensik

Modul Nr.	CY-B-27
Modulverantwortliche/r	Prof. Dr. Martin Schramm
Kursnummer und Kursname	Digitale Forensik
Lehrende	Michael Heigl
Semester	6
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 45 Stunden Selbststudium: 90 Stunden Gesamt: 135 Stunden
Prüfungsarten	PrA, LN Praxis
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden verfügen über grundlegendes tiefgreifendes Fachwissen und Methodenwissen in dem Bereich Digitale Forensik.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Studierenden kennen die Begrifflichkeiten der Digitalen Forensik und können Arten digitaler Spuren beschreiben.
- Sie können die Methodik und Vorgehensweise der Digitalen Forensik erläutern.
- Sie können die aktuelle Rechtlage, sowie aktuelle Standards und Normen im Bereich der digitalen Forensik präsentieren.

- Sie verstehen die Bestandteile der Computer Forensik, Mobilen und Embedded Forensik, sowie Internet Forensik und können forensische Untersuchungen in diesen Bereichen durchfüren.

Methodenkompetenz

- Die Studierenden können zwischen relevanten und irrelevanten Informationen bei einer forensischen Untersuchung unterscheiden.
- Für ein gegebenes Szenario können die Studierenden beurteilen, welche Schritte der Phasen der Digitalen Forensik in welcher Reihenfolge vollzogen werden müssen.
- Die Studierenden sind in der Lage, eigenständig Digitale Forensik zu planen und durchzuführen.

Persönliche Kompetenz

- Durch die eigenständige Durchführung forensicher Untersuchungen wird die Neugier der Studierenden am Fachgebiet geweckt sowie die Bereitschaft des vertiefenden Selbststudiums gefördert.

Sozialkompetenz

- Druch das Anwenden forensischer Methoden im Rahmen einer Gruppen-basierten Projektarbeit üben sich die Studierenden in Kooperationsbereitschaft und Motivationsfähigkeit.

Verwendbarkeit in diesem und in anderen Studiengängen

Wahlpflichtmodul anderer Bachelorstudiengänge (wie z.B.: Angewandte Informatik/Infotronik, Interaktive Systeme/Internet of Things, Künstliche Intelligenz, Wirtschaftsinformatik, Elektro- und Informationstechnik)

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- Kenntnisse der Inhalte der Grundlagenmodule
- Kenntnisse der Inhalte des Moduls Netzwerksicherheit
- Kenntnisse der Inhalte des Moduls Management von IT-Sicherheitsvorfällen

Inhalt

1 Einleitung
   - Geschichte der Forensik
   - Begrifflichkeiten
   - Vorgehensweise
   - Dokumentation
   - Digitale Spuren
   - Anti-Forensik
2 Der Prozess der Digitalen Forensik
   - Identifikations-Phase
   - Erfassungs-Phase
   - Untersuchungs-Phase
   - Analyse-Phase
   - Präsentations-Phase
3 Rechtslage, Standards und Normen
4 Digitale Forensik - Anwendungsfälle im Detail
   - Datenträgerforensik
   - Betriebssystemforensik
   - Arbeitsspeicherforensik
   - (Datei-/) Anwendungsforensik
   - Malwareanalyse & Reverse Engineering
   - Netzwerkforensik
   - Mobile Device Forensik
   - Cloud Forensik
   - VM Forensik
5 Herausforderungen Digitaler Forensik

Lehr- und Lernmethoden

- Seminaristischer Unterricht mit praktischen Übungen
- Praktika

Besonderes

Praktikumsleistung (PrL) als Zulassungsvoraussetzung zur Prüfung.

Empfohlene Literaturliste

- Geschonneck, A.: Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklären, dpunkt.verlag GmbH; 6., akt. u. erw. Auflage (1. März 2014), ISBN-13 : 978-3864901331

- Meseke, B.: Digitale Forensik: Praxiswissen Cybercrime für Manager, Erich Schmidt Verlag GmbH & Co; 1. Auflage (27. Juni 2019), ISBN-13 : 978-3503182671
- Kuhlee, L.: Computer-Forensik Hacks, O'Reilly Verlag GmbH & Co. KG; 1. Auflage (1. April 2012), ISBN-13 : 978-3868991215
- Siegert, M.: Forensisches Reverse Engineering: Entwurf eines Teilgebietes der digitalen Forensik unter besonderer Berücksichtigung der Systemmodellierung, Books on Demand; 2. Auflage (10. November 2017), ISBN-13 : 978-3744815727
- Årnes, A.: Digital Forensics, Wiley; 1. Auflage (21. Juli 2017), ISBN-13 : 978-1119262381

CY-B-28 Sicherheit interaktiver Systeme

Modul Nr.	CY-B-28
Modulverantwortliche/r	Prof. Dr. Thomas Störtkuhl
Kursnummer und Kursname	Sicherheit interaktiver Systeme
Semester	6
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 45 Stunden Selbststudium: 90 Stunden Gesamt: 135 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden verfügen über tiefgreifendes allgemeines Wissen und tiefgreifendes Fachwissen in dem Bereich der Sicherheit interaktiver Systeme.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Studierenden können verschiedenste IoT bzw. IIoT Infrastrukturen mit ihren Komponenten beschreiben.
- Die Studierenden kennen die wesentlichen (Security) Elemente einer IT Security Architektur für die verschiedenen, diskutierten Infrastrukturen.
- Die Studierenden kennen wesentliche Protokolle und ihre Sicherheitseigenschaften, die in diesen Umgebungen implementiert werden.

- Die Studierenden sind in der Lage Security Analysen für die eingeführten IoT und IIoT infrastrukturen durchzuführen
- Die Studierenden kennen wesentliche Security Anfoderungen aus den einschlägigen Standards, die für die eingeführten IoT und IIoT infrastrukturen gelten sollen.
- Die Studierenden können Audits für einen Untersuchungsgegenstand (IT-System, Teil eines IT-Systems, Prozess) durchführen.

Methodenkompetenz

- Die Studierenden können beurteilen, ob eine IT Security Architektur für die diskutierten Infrastrukturen ausreichend Schutz beitet oder Mängel aufweist.

Persönliche Kompetenz

- Durch die stattfindenden Übungen, die die Erarbeitung/Präsentation bestimmter Themen beinhalten, werden die Studierenden angehalten, Sachverhalte eigenständig zu erarbeiten und verständlich zu präsentieren.

Sozialkompetenz

- Die Studierenden führen im Team an Fallbeispielen Security Analysen durch oder entwerfen eine IT Security Architektur. Durch diese Zusammenarbeit werden das Wissen und die Fähigkeiten anderer Studierender als hilfreich und förderlich erfahren.

Verwendbarkeit in diesem und in anderen Studiengängen

Weiterführendes Wahlpflichtmodul anderer Bachelorstudiengänge (wie z.B.: Angewandte Informatik/Infotronik, Interaktive Systeme/Internet of Things, Künstliche Intelligenz, Wirtschaftsinformatik, Elektro- und Informationstechnik)

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- Kenntnisse der Inhalte von Modul CY-B-04 Betriebssysteme und Netzwerke
- Kenntnisse der Inhalte von Modul CY-B-17 Netzwerksicherheit
- Kenntnisse der Inhalte von Modul CY-B-11 Kryptologie 1
- Kenntnisse der Inhalte von Modul CY-B-21 Kryptologie 2
- Kenntnisse der Inhalte von Modul CY-B-22 Management von IT-Sicherheitsvorfällen

Inhalt

- Motivation für die Sicherheit interaktiver Systeme: die immer tiefere Vernetzung von Systemen z.B. im Umfeld von Industrie 4.0; die voranschreitende Integration von Geräten in Netzwerke und über Kommunikationsplattformen für neue Geschäftsmodelle
- IT Security im IoT Umfeld:
    - typische Infrastrukturen für für IoT Umgebungen zum Beispiel im Umfeld von Protokollen MQTT oder LoRaWan; Anwendung von Analysen für die Ableitung geeigneter IT Security Maßnahmen wie z.B. Implementierung von abgesicherten Kommunikationstunneln via TLS oder IPsec. Darstellung von IT Security Archtekturen von Kommunikationsplattformen im IoT Umfeld.
- IT Security im industriellen Umfeld (IIoT, Industrial IoT):
    - Lösungen bzgl. Predictive Maintenance und Data Analytics werden aufgezeigt. Hierbei werden Cloud-Technologien einbezogen. Insbesondere werden abgesicherte Machine2Machine Kommunikationen und Anbindungen über Plattformen erläutert. Dabei werden verschiedene Infrastrukturen aus den Bereichen wie Fertigung (z.B. der Einsatz von OPC UA, Defense-in-Depth Ansätze wie sie z.B. auch von Herstellern/System Integratoren angeboten werden), Eisenbahn (Zugführung, Zugsteuerung, ERTMS (European Rail Traffic Management System)), Chemie (hier das speziell das Protokoll wirelessHART) und Energie (z.B. MMS, Standard IEC 62351) mit ihren Besonderheiten dargestellt.
- Anbindung an eine Public Key Infrastructure:
    - da viele Sicherheitsprotokolle auf Zertifikaten basieren, ist gerade auch das Management von Identitäten, von Zertifikaten und Rechten in den verteilten Infrastrukturen eine Herausforderung. Zum Beispiel wird ein automatischen Ausrollen von Zertifikaten via Protokollen wie Simple Certificate Enrollment Protocol (SCEP) / Network Device Enrollment Service (NDES) erläutert.
- Netzwerkstrukturierung:
    - Bzgl. Einbindung von Kommunikationsplattformen und Cloud-Services wird eine geeignete Netzwerkstrukturierung mit Netzsegmenten (Zones) und Kommunikationskanälen (Conduits) zur Absicherung der Kommunikationen erläutert.
- Security Incident and Event Monitoring:
    - Möglichkeiten des technischen Security Incident and Event Monitoring (SIEM) werden aufgezeigt, z.B. mittels Honeypot-Lösungen oder durch neue Ansätze der Überwachung mittels Edge Computing.

Lehr- und Lernmethoden

- Seminaristischer Unterricht mit praktischen Übungen

Empfohlene Literaturliste

- ZVEI - German Electrical and Electronic Manufacturers - Association, Industrie 4.0: The Reference Architectural Model Industrie 4.0 (RAMI 4.0), Frankfurt am Main, 2015
- Industrial Internet Consortium, Industrial Internet Reference Architecture. Link: http://www.iiconsortium.org/IIRA.htm (zuletzt zugegriffen am 4.12.2020).
- ENISA, Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, NOVEMBER 2017
- ENISA, Towards secure convergence of Cloud and IoT, TLP GREEN | SEPTEMBER 2018
- Fraunhofer AISEC: White Paper, IoT 2020: Smart and secure IoT platform, October 2003, Link: r10secu.lo (cmu.edu) (zuletzt zugegriffen am 4.12.2020).
- SANS Institute Information Security Reading Room, Tools and Standards for Cyber Threat Intelligence Projects, 2020, Link: Tools and Standards for Cyber Threat Intelligence Projects (sans.org) (zuletzt zugegriffen am 4.12.2020).
- Jin-Yong Yu, Young-Gab Kim: Analysis of IoT Platform Security: A Survey; 2019 International Conference on Platform Technology and Service (PlatCon)
- Security and Privacy in Sensor Networks, Haowen Chan and Adrian Perrig, Carnegie Mellon University,
- Klasen Frithjof, Oestreich Volker, Volz Michael (Hrsg.): Industrielle Kommunikation mit Feldbus und Ethernet, VDE Verlag, Berlin, Offenbach, 2010
- BDEW Bundesverband der Energie- und Wasserwirtschaft e.V. & Oesterreichs E-Wirtschaft, Whitepaper Anforderungen an Österreich sichere Steuerungs- und Telekommunikationssysteme, Vollständig überarbeitete Version 2.0 05/2018: Wien/Berlin, 8. Mai 2018
- Sicherheitsanalyse Open Platform Communications Unified Architecture (OPC UA), im Auftrag des BSI veröffentlich unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/OPCUA/OPCUA.pdf
- Risikoanalyse industrieller Steuerungsumgebungen, itsecurity, Juli-August, 2014

CY-B-29 Security Engineering

Modul Nr.	CY-B-29
Modulverantwortliche/r	Prof. Dr. Martin Schramm
Kursnummer und Kursname	Security Engineering
Semester	6
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 45 Stunden Selbststudium: 90 Stunden Gesamt: 135 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden verfügen über grundlegendes allgemeines Wissen und grundlegendes Fachwissen in dem Bereich des interdisziplinären Security Engineering.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Studierenden verstehen die Prinzipien des interdisziplinären Security Engineerings und können diese auch erläutern.
- Die Studierenden werden befähigt, den Security / Privacy by Design Ansatz bei der Umsetzung von eigenen Lösungen anzuwenden.
- Die Studierenden können Reifegradbeurteilungen hins. der Qualität von Prozessen bei der Entwicklung sicherer IT-Systeme durchführen.

Methodenkompetenz

- Die Studierenden können existierende Produkte und Lösungen auf die Einhaltung der Prinzipien des Security Engineering hin analysieren.
- Weiterhin können Sie diese auf Ihre Sicherheit hin evaluieren und entscheiden, welche zusätzliche Schitte für eine erhöhte Sicherheit getroffen werden müssen.
- Die Studierenden können beurteilen, welches interdisziplinäre Fachkräfteteam zur Bewältigung einer konkreten Herausforderung des Crytpographic Engineering bzw. Security Engineering von Nöten ist.

Persönliche Kompetenz

- Die Studierenden erlernen durch Übungen selbstständige und problem- bzw. handlungsorientiertes Arbeiten.

Sozialkompetenz

- Durch Gruppenarbeit an praxisorientierten Fallbeispielen, trainieren die Studierende die Teamfähigkeit und steigern Ihre Ziel- und Ergebnisorientierung.

Verwendbarkeit in diesem und in anderen Studiengängen

Wahlpflichtmodul anderer Bachelorstudiengänge (wie z.B.: Angewandte Informatik/Infotronik, Interaktive Systeme/Internet of Things, Künstliche Intelligenz, Wirtschaftsinformatik, Elektro- und Informationstechnik)

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- Kenntnisse der Inhalte der Grundlagenmodule (CY-B-01 bis CY-B-05, CY-B-08 bis CY-B-11, CY-B-13 und CY-B-14)
- Kenntnisse der Inhalte von Modul CY-B-16 Sichere Programmierung
- Kenntnisse der Inhalte von Modul CY-B-17 Netzwerksicherheit
- Kenntnisse der Inhalte von Modul CY-B-21 Kryptologie 2
- Kenntnisse der Inhalte von Modul CY-B-22 Management von IT-Sicherheitsvorfällen
- Kenntnisse der Inhalte von Modul CY-B-23 Distributed-Ledger-Technologien

Inhalt

1 Einführung
   - Thematische Einordnung und Begriffsdefinition
   - Security Engineering als ganzheitlicher Ansatz
   - Vergleich Software Engineering - Security Engineering
2 Überblick Bestandteile von Security Engineering (Auszug)
   - Protokolle
   - Zugriffsschutz
   - Kryptographie
   - Mehrschichtige Sicherheit
   - Mehrseitige Sicherheit
   - Überwachung
   - Biometrie
   - Physischer Verfälschungsschutz
   - Kopierschutz und Datenschutz
   - Prozesse, Management und Evaluierung
3 Security Engineering
   - Prinzipien
   - Sicherheit im Entwicklungsprozess
   - Reifegradmodell zur Qualitätsbeurteilung
   - Mechanismen, Maßnahmen, Werkzeuge
   - Evaluierung und Zertifizierung
4 Cryptograhic Engineering
   - Nachrichtensicherheit
   - Schlüsselvereinbarung
   - Schlüsselmanagement
   - Güte von Zufallszahlengeneratoren
   - Seitenkanalangriffe - Grundlagen
   - Seitenkanalangriffe - Fortgeschrittene Techniken
5 Aktuelle Themen und (Forschungs-) Aktivitäten

Lehr- und Lernmethoden

- Seminaristischer Unterricht mit praktischen Übungen

Empfohlene Literaturliste

Literatur:

- Anderson, S.: Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley; 3. Edition (22. Dezember 2020), ISBN-13 : 978-1119642787

- Koc, C. K.: Cryptographic Engineering, Springer; Softcover reprint of hardcover 1st ed. 2009 Edition (4. November 2010), ISBN-13 : 978-1441944177
- Ferguson, N., Schneier, B., Kohno, T., Cryptography Engineering: Design Principles and Practical Applications, Wiley; 1. Edition (15. März 2010), ISBN-13 : 978-0470474242

CY-B-30 Wahlpflichtmodul 1

Modul Nr.	CY-B-30
Modulverantwortliche/r	Prof. Dr. Martin Schramm
Kursnummer und Kursname	Wahlpflichtmodul 1
Semester	6
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	FWP
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 45 Stunden Selbststudium: 90 Stunden Gesamt: 135 Stunden
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

In den Wahlpflichtmodulen können die Studierenden ein Modul frei aus einem vorgegebenen Modulkatalog wählen. Inhalte sind fachbezogen zum Studium z.B. aus den Themengebieten Informatik, Cyber Security, Künstliche Intelligenz oder sonstige einschlägige Module. Der Modulkatalog wird stets mit dem Studienplan bekannt gegeben.

Dies ermöglicht eine individuelle Schwerpunktsetzung, Vertiefung und/oder Verbreiterung der Kompetenzen.

Fach- und **Methodenkompetenzen** sowie **persönliche Kompetenzen** und **Sozialkompetenzen** werden je nach gewähltem Modul unterschiedlich betont.

Verwendbarkeit in diesem und in anderen Studiengängen

gemäß Modulbescheibung des gewählten Pflichtmoduls

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- Kenntnisse der Inhalte der Grundlagenmodule

Inhalt

Inhalte werden durch das gewählte Modul bestimmt.

Lehr- und Lernmethoden

gemäß Modulbescheibung des gewählten Pflichtmoduls

Besonderes

Ein Anspruch darauf, dass sämtliche vorgesehene Wahlpflichtmodule und Wahlmodule tatsächlich angeboten werden, besteht nicht. Desgleichen besteht kein Anspruch darauf, dass die dazugehörigen Lehrveranstaltungen bei nicht ausreichender Teilnehmerzahl durchgeführt werden.

Empfohlene Literaturliste

gemäß Modulbescheibung des gewählten Pflichtmoduls

CY-B-31 Schlüsselqualifikation 5

Modul Nr.	CY-B-31
Modulverantwortliche/r	Prof. Dr. Thomas Geiß
Kursnummer und Kursname	Unternehmensgründung Team-Entwicklung und interkulturelle Kommunikation
Lehrende	Prof. Dr. Thomas Geiß
Semester	6
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	PrA
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Lernergebnisse des Moduls setzen sich folglich aus den beiden Fächer "Team-Entwicklung und interkulturelle Kommunikation" (**Fach A**) und "Unternehmensgründung " (**Fach B**) zusammen.

Fach A

Learning Outcomes of the Module:

Cultural and interdisciplinary differences among international business partners, customers and suppliers often result in tension and misunderstandings in the IT world, specifically for individuals working in modern fields like Artificial Intelligence. Managers and team

members who competently navigate in different cultural and disciplinary environments and teams can contribute substantially to the success of globally active enterprises.

A condition for the acquisition of ?intercultural and interdisciplinary competence? is the recognition that one?s own actions are influenced by one?s own values and norms. Reflecting on one?s own cultural and disciplinary background forms the basis for the understanding of other cultures and functions.

In the first part of the course the participants acquire the knowledge they need to explain and understand various cultures and disciplines. Through the study of comparative cultures, they discover the relevance of the cultural framework to management theory and for explaining management and team behavior.

Participants learn how to independently apply the ?culture assimilator? technique to broaden their knowledge through a qualitative research project. This involves soliciting international and functional managers and employees and collecting ?critical incidents? of cross-cultural and cross-functional business and team interactions, which are then analyzed with the help of theory. Carrying out qualitative interviews with members of foreign cultures und functions further develops the participants? social, cross-functional and intercultural skills.

The second part of the course is conducted as an off-campus intensive ?teambuilding and social, interdisciplinary and intercultural competence? training workshop. Here the results of the culture-assimilator research projects are presented through role-playing in situational reenactments. The implications are further clarified through a variety of interaction exercises. For example, simulation of expatriate and cross-functional team situations is used to transfer concrete practical knowledge.

The social, interdisciplinary, and intercultural competence training assists the participants in their ability to reflect on cultural and disciplinary identities, to avoid value judgements in their perception of foreign and functional cultures, to empathize and accept differences as well as to develop additional options for actions international and cross-functional managers and employees can take.

In the context of the learning environment, the students enjoy the opportunity to increase their observation, communication, co-operation, self-reflection, teamwork, and management skills as well as their self-confidence. By working together to solve complex problems and through structured feedback sessions, the participants become sensitized to the roles they assume in group interactions, to the limitations imposed by the German and their own cultures, and to the conditions required for effective team work. The participants learn to influence the co-operation in team positively and learn how to avoid negative team atmospheres.

Fach B

Qualifikationsziele

Die Wichtigkeit einer detaillierten Unternehmensplanung wird durch Beispiele verdeutlicht. Dabei wird für das Thema Existenzgründung sensibilisiert und motiviert.

Den Studierenden wird ferner die Möglichkeit geboten, durch das Erstellen eines individuellen Businessplans im Rahmen eines Gruppenprojektes das vermittelte Wissen anzuwenden, zu trainieren und dadurch die Vorgehensweise, mögliche Probleme und Grenzen der Unternehmensplanung an einem praxisnahen Beispiel nachzuvollziehen. Dieser Kurs vermittelt die 'Startvorrichtung' anhand unternehmerischer Grundlagen, Managementkenntnisse und persönlicher Schlüsselqualifikationen für den Start in das unternehmerische Rennen und sensibilisiert zu Themen der Selbstständigkeit und Existenzgründung. Neben theoretischem Wissen zur Entrepreneurship werden Kenntnisse zur Identifikation von Marktchancen und Geschäftsmodellen vermittelt. Erweiterung praktischer Kenntnisse aus dem Startprozess > von der Idee über das Produkt/ Dienstleistung zum Geschäftsmodell. Das Gruppenprojekt umfasst die Gesamtplanung einer Geschäftsidee von der Ideenfindung, der Informationsbeschaffung bis hin zur Erstellung eines detaillierten Geschäftsplanes. Das Engagement der Teilnehmer und die Gruppendynamik während des Projektes tragen dabei entscheidend zum Lernerfolg bei.

Fachkompetenz

Die Studierenden sind in der Lage, im Rahmen des Ideengenerierung (Design Thinking Prozesses, Where2Play-Methode) iterativ Lösungen für eine Problemstellung zu generieren und zu evaluieren. Sie können aus einem Methodenset auswählen und an geeigneter Stelle Problemstellungen hinterfragen und analysieren. Sie können ihre Ideen in Prototypen umsetzen und diese mit ihren Nutzern testen und evaluieren.

Methodenkompetenz

Die Studierenden sind befähigt, Methoden zu den geeigneten Phasen zuzuordnen und anzuwenden. Die Lernmethoden dazu: Interaktives Seminar, Problem Based Learning, Referate/ Präsentationen zu speziellen Aspekten, Selbstorganisation, Coaching-Sitzungen mit dem Dozenten. Das Ziel, bereits vorhandene Wissen mit zu integrieren und mit hohen Kommunikationsbereitschaft Lösungen zu finden.

Persönliche Kompetenz

Die vorgestellten Konzepte und die Unternehmensbeispiele ermöglichen einen großen Interpretationsraum für mögliche Lösungsalternativen. Jeder Studierende muss eigenständig Strategiemöglichkeiten der Unternehmensführung entwickeln und die Auswirkungen reflektieren. In Form von Gruppenarbeit werden ausgewählte Managementtools vorbereitet und im Rahmen der Lehrveranstaltungen präsentiert. Die Studierenden haben zudem ein StartUp-Mindset, das sie befähigt disruptive Problemstellungen zu erfassen und nutzerzentrierte Lösungen zu entwickeln.

Sozialkompetenz

Die Studierenden verfügen über Diskussionsvermögen, Teamfähigkeit und Kritikfähigkeit. Sie sind in der Lage ihre Stärken in den Entwicklungsprozess und Geschäftsmodelldesign einzubringen und verfügen über ein kreatives Selbstbewusstsein. Durch die Analyse aktueller Unternehmenssituationen in Teamarbeit erfolgt ein vertiefter Austausch über unterschiedliche strategische Konzepte zur Unternehmensführung im Spannungsfeld von finanzieller Wertorientierung und werteorientierter Unternehmensführung. Durch

Heterogenität der Gruppenmeinungen und Standpunkte in diesen Diskussionen wird die Konflikt- und Kritikfähigkeit geschult.

Verwendbarkeit in diesem und in anderen Studiengängen

Verwendbarkeit des Moduls für diesen Studiengang

- Dieses Modul zählt zu den interdisziplinären Schlüsselqualifikationen.

Verwendbarkeit des Moduls für andere Studiengänge

- Diese Modul kann in allen sonstigen technischen, rechtlichen, wirtschaftspsychologischen und betriebswirtschaftlichen Studiengängen verwendet werden, z.B. im Ba. Cyber Security

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

Inhalt

Fach A

- The following concepts are emphasized in theoretical discussions, research projects and in the practical training workshop:
  - Defining Culture
  - The Characteristics of Culture
  - The Functions of Culture
  - Organizational Culture
  - The Layers and Elements of Culture
  - Comparing Cultures
  - The Impact on the Individual: the ?Culture Shock?
  - Cultural Contexts: Hall
  - Culture and the Workplace: Hofstede Practical Aspects of Intercultural Behavior
  - International Human Resource Development
  - Expatriate Management
  - Language and Social Reality
  - Reasons for Cross Cultural Misunderstandings
  - Improving Cross Cultural Cooperation
  - Group dynamics, processes, and structures in groups
  - Roles in groups (roles in tasks and supporting roles)
  - Group leadership
  - Effect of one?s actions in groups
  - The ?give and take? of feedback
  - Self-image and how others see you
  - Communication levels (content versus relationship)
  - Conditions for successful co-operation
  - Cultural influences on teamwork.
  - Teambuilding

  More topics are to be added based on the actual demand for graduates in this programme, evaluated constantly by qualitative and quantitative research of future employers

Fach B

Der Kurs baut auf den Grundlagen der Unternehmensführung auf und motiviert die Studierenden, ihre Kenntnisse auf konkrete Fallbeispiele der Unternehmensgründung zu übertragen. Dabei kommen analytische Instrumente und Lösungsansätze aus der Entrepreneurshipforschung und verschiedenen unternehmerischen Funktionen zum Einsatz. Ferner werden die unternehmerischen Entscheidungswege und die Konsequenzen unternehmerischen Handelns mit Fokus auf Unternehmen diverser Branchen aufgezeigt.

- Gründungsrelevante Kompetenzen
- Ideenfindung und Evaluation von Geschäftsideen
- Aufbau und Inhalte von Businessplänen
- Geschäftsmodelle

- Venture Capital und Unternehmensfinanzierung
- Finanzplanung, Szenariobildung und Sensitivitätsanalyse
- Investitionsplanung und Anlagespiegel
- Personalplanung
- öffentliche Fördermittel
- Möglichkeiten der Haftungsbegrenzung
- Gründerhaftung
- Praktische Anwendung des theoretischen Wissen bei der Erstellung eines Businessplanes als Gruppenprojekt

Lehr- und Lernmethoden

Fach A:

The course begins by conveying the fundamentals of cross-cultural and interdisciplinary management as well as teambuilding via theoretical lectures and moderated discussions. Since most of the participants have teamwork, intercultural and interdisciplinary experiences assembled from a wide variety of cultures and functions, the theory can be directly tied to many of the individual experiences.

The theoretical fundamentals are then extended through the development, application and presentation of the culture and functional assimilators. The qualitative research projects are performed in groups organized along the principles of self-organized learning. The projects help develop individual competence in applying the scientific method and further the development of presentation, social and intercultural skills.

Short case studies, ?critical incidents?, are selected from the international and interdisciplinary business world. Explanations and analysis of these cases support the integration of the participants? existing management knowledge with intercultural and interdisciplinary perspectives.

Social, interdisciplinary and intercultural skills as well as teambuilding capabilities are further developed in the training workshop through roll playing, interaction exercises, problem solving tasks, simulations and feedback rounds.

Fach B:

Vorlesung mit Übungen, Seminar, Schreibwerkstatt, Präsentationen, Diskussionen, Vermittlung der Grundlagen durch fallbezogene Darstellung. Systematische Darstellung der Theorie mit Methodentransfer, Schaubildern und Fallbeispielen.

Besonderes

Fach A:

Led by Prof. Dr. Johann Nagengast, the course implements a multi-cultural and multi-functional team teaching approach.

Mr. Florian Oberhofer offers expertise in expatriate management, global entrepreneurship and international human resources and add a foreign cultural and management perspective.

Various external tutors (carefully selected and already being experienced in the content of this module) assure that the participants get small group, qualified feedback.

Kurs wird stets won zwei Dozenten durchgeführt, um die individuelle Betreuung der TN sicher zustellen. Bei höherer Teilnehmerzahl wird evtl. ein dritten Dozent hinzugezogen in Abstimmung mit dem jeweiligen Studiengangsleiter

Empfohlene Literaturliste

Fach A

- Hall, E. T., Hall, M. R.: Understanding Cultural Differences, reprint, Yarmouth, Intercultural Press (2015)
- Hofstede, G.: Cultures and Organizations, 2nd ed., New York et al., Mc Graw-Hill (2015)
- Hofstede, G.: Culture?s Consequences, 2nd ed., Thousand Oaks, Sage, (2014)
- Trompenaars, F., Hampden-Turner, C.: Riding the Waves of Culture, London, Brealey Publishing, (1997)
- Trompenaars, F., Hampden-Turner, C.: Managing People across Cultures, Chichester, Capstone Publishing (2004)
- Lewis, R. D.: When Cultures Collide, 3rd ed. (or more current), London, Brealey Publishing (2006)
- Baron, R. S.: Group Process, Group Decision, Group Action, 2nd. Ed., Buckingham, 2003
- Buchanan, D., Huczynski, A.: Organizational Behavior, 5th Ed., Harlow, 2004

Fach B

- Koch, Wolfgang / Wegmann, Jürgen (2002): Praktiker-Handbuch Due Diligence, Analyse mittelständischer Unternehmen, 2. überarbeitete und aktualisierte Auflage, Schäffer-Poeschel Verlag, Stuttgart 2002.
- Kreditanstalt für Wiederaufbau (KfW)-Akademie, (2004): Finanzierungsmöglichkeiten der KfW bei Unternehmensübernahmen und Beteiligungen, Frankfurt a. M. 2004, S. 32-34.
- Timmons, Jeffrey A.: New venture creation, McGraw-Hill Verlag, Boston, 2004
- Sahlman, William A.: The entrepreneurial venture, Havard Business School Press, Boston, 1999
- Dowling, Michael J.: Gründungsmanagement, Springer Verlag, Berlin, 2003

- Bernd Fischl / Stefan Wagner: Der perfekte Businessplan, 2010 - Verlag Franz Vahlen GmbH
- C. Bayerl; 30 Minuten für Kreativitätstechniken; GABAL Verlag GmbH; 3. Auflage 2007; Offenbach
- G. Bayer; G.R. Berrit; Diagnose der Innovationbedingungen im Unternehmen; Digitale Fachbibliothek Innovationsmanagement; Symposium Publishing GmbH; 2007
- A. Blumenschein; I.U. Ehlers; ?Ideen managen?; Rosenberger Fachverlag; Leonberg; 2007
- BPW Nordbayern GmbH Schritt für Schritt wachsen - finanzieren - gründen - planen; Teilnehmerhandbuch 2020; 4. überarbeitete Auflage;
- Pott , Oliver, Pott , André: Entrepreneurship, Unternehmensgründung, Businessplan und Finanzierung, Rechtsformen und gewerblicher Rechtsschutz, Poeschl-Verlag, 2017
- A. Förster; P. Kreuz; Different Thinking; Redline Wirtschaft; Frankfurt 2005
- Engelen Andreas: Corporate Entrepreneurship, Taschenbuch, , 2014, Gabler.
- Fritsch Michael: Entrepreneurship, Theorie, Empirie, Politik, Engelen, Bachmann, Springer, 2017

CY-B-32 Auditierung von IT-Systemen

Modul Nr.	CY-B-32
Modulverantwortliche/r	Prof. Dr. Thomas Störtkuhl
Kursnummer und Kursname	Auditierung von IT-Systemen
Semester	7
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	PrA
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die Studierenden verfügen über tiefgreifendes allgemeines Wissen und tiefgreifendes Fachwissen in dem Bereich der Auditierung von IT-Systemen.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Die Studierenden können alle Schritte eines Auditierprozesses für Informationssicherheit für IT-Systeme / IACS / Prozesse beschreiben.
- Die Studierenden kennen alle wesentliche Schritte/Phasen des Auditiertprozesses und können Auditierprozesse auf IT-Systeme, IACS und Prozesse anwenden.
- Die Studierenden kennen wesentliche Anfoderungen an einen Auditierprozess der einschlägigen Standards.

- Die Studierenden können Audits für einen Untersuchungsgegenstand (IT-System, Teil eines IT-Systems, Prozess) durchführen.

Methodenkompetenz

- Die Studierenden können die korrekte Art und das passende Vorgehen eines Audits für einen Untersuchungsgegenstand (IT-System, Teil eines IT-Systems, Prozess) auswählen und die Kritikalität identifizierter Mängel bewerten.
- Die Studierenden können beurteilen, ob bestimmte Maßnahmen geeignet sind, identifizierte Mängel / Schwachstellen / Feststellungen zu beheben bzw. zu lindern.

Persönliche Kompetenz

- Durch die stattfindenden Übungen werden die Studierenden angehalten, Sachverhalte eigenständig zu erarbeiten und verständlich zu präsentieren.

Sozialkompetenz

- Die Studierenden führen an Fallbeispielen Audits im Team in wechselnden Rollen durch. Durch diese Zusammenarbeit werden das Wissen und die Fähigkeiten anderer Studierender als hilfreich und förderlich erfahren.

Verwendbarkeit in diesem und in anderen Studiengängen

Weiterführendes Wahlpflichtmodul anderer Bachelorstudiengänge (wie z.B.: Angewandte Informatik/Infotronik, Interaktive Systeme/Internet of Things, Künstliche Intelligenz, Wirtschaftsinformatik, Elektro- und Informationstechnik)

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- Kenntnisse der Inhalte von Modul CY-B-04 Betriebssysteme und Netzwerke
- Kenntnisse der Inhalte von Modul CY-B-17 Netzwerksicherheit

Inhalt

- Motivation für die Auditierung von IT-Systemen: Management der Informationssicherheit; aktuelle Lage der Informationssicherheit; regulatorische Anforderungen auf nationaler und europäischer Ebene; Schutz kritischer Infrastrukturen
- Arten der Auditierung: technische Audits, Management-Audits, Audits von Prozessen, Penetrationstests, Audit von Dokumenten, Management-Review, Zertifizieraudits.

- Methoden: Simulation am Round Table, Interview, Workshop, technischer Schwachstellenaudit
- Elemente der Audit-Prozesses der verschiedenen Arten der Audits wie Vorbereitung, Durchführung, Protokollierung und Berichterstellung, Einbeziehung der verschiedenen Rollen/Stakeholder. Insbesondere wird betrachtet, wie Audit als Kontrollinstrument im Falle von Outsourcing eingesetzt werden kann.
- Definition und Bewertung des Reifegrades von Prozessen: der Auditierprozesse identifiziert nicht nur Schwachstellen, sondern beurteilt auch den Reifegrad (Maturity Level) der auditierten Prozesse anhand klar definierter Kriterien. Hierzu werden Anforderungen an Prozesse aus einschlägigen Standards (siehe unten) herangezogen.
- Einbettung der Audits in den kontinuierlichen Verbesserungsprozess für die Informationssicherheit und in das Meldesystem nach dem IT-Sicherheitsgesetz. Schwerpunkt ist hier:
    - der Auditprozess für das Management von Informationssicherheit; als Basis wird hier z.B. die ISO 19011 eingeführt
    - die Entwicklung von Produkten mit der Qualität IT Security; als Basis wird hier z.B. der Standard IEC 62443-4-1 verwendet
    - Zertifizieraudits (ISO/IEC 27001 und IEC 62443) für Betreiber, System Integratoren und Hersteller

Lehr- und Lernmethoden

- Seminaristischer Unterricht mit praktischen Übungen

Empfohlene Literaturliste

- DIN EN ISO 19011, Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2011); Deutsche und Englische Fassung EN ISO 19011:2011, Dezember 2011
- ISO/IEC 27000: Information technology - Security techniques - Information security management systems - Overview and vocabulary, Third edition, 2014-01-15
- ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013 + Cor. 1:2014), English translation of DIN ISO/IEC 27001:2015-03
- ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls, Second edition, 2013-10-01
- ISO/IEC 27005:2018-07 Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Risikomanagement, Englischer Titel: Information technology - Security techniques - Information security risk management

- IT-Grundschutz-Kompendium, Bundesamt für Sicherheit in der Informationstechnik, Bonn 2020; https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html (zuletzt aufgerufen am 3.10.2020)
- ISO/IEC 21827: Information technology ? Security techniques ? Systems Security Engineering ? Capability Maturity Model® (SSE-CMM®), 2008
- DIN ISO 31000:2018-10: Risikomanagement - Leitlinien (ISO 31000:2018), Englischer Titel: Risk management - Guidelines (ISO 31000:2018), 2018-10
- ENISA, GOOD PRACTICES FOR SECURITY OF IOT, Secure Software Development Lifecycle, November 2019
- ENISA, IoT Security Standards Gap Analysis, Mapping of existing standards against requirements on security and privacy in the area of IoT, V1.0, December 2018
- Zertifizierung nach IEC 62443 für Hersteller und Systemintegratoren, Kai Wollenweber, Thomas Störtkuhl, Special it-sa, Oktober 2015

CY-B-33 Wahlpflichtmodul 2

Modul Nr.	CY-B-33
Modulverantwortliche/r	Prof. Dr. Martin Schramm
Kursnummer und Kursname	Wahlpflichtmodul 2
Semester	7
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	FWP
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

In den Wahlpflichtmodulen können die Studierenden ein Modul frei aus einem vorgegebenen Modulkatalog wählen. Inhalte sind fachbezogen zum Studium z.B. aus den Themengebieten Informatik, Cyber Security, Künstliche Intelligenz oder sonstige einschlägige Module. Der Modulkatalog wird stets mit dem Studienplan bekannt gegeben.

Dies ermöglicht eine individuelle Schwerpunktsetzung, Vertiefung und/oder Verbreiterung der Kompetenzen.

Fach- und **Methodenkompetenzen** sowie **persönliche Kompetenzen** und **Sozialkompetenzen** werden je nach gewähltem Modul unterschiedlich betont.

Verwendbarkeit in diesem und in anderen Studiengängen

gemäß Modulbescheibung des gewählten Pflichtmoduls

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- Kenntnisse der Inhalte der Grundlagenmodule

Inhalt

Inhalte werden durch das gewählte Modul bestimmt.

Lehr- und Lernmethoden

gemäß Modulbescheibung des gewählten Pflichtmoduls

Besonderes

Ein Anspruch darauf, dass sämtliche vorgesehene Wahlpflichtmodule und Wahlmodule tatsächlich angeboten werden, besteht nicht. Desgleichen besteht kein Anspruch darauf, dass die dazugehörigen Lehrveranstaltungen bei nicht ausreichender Teilnehmerzahl durchgeführt werden.

Empfohlene Literaturliste

gemäß Modulbescheibung des gewählten Pflichtmoduls

CY-B-34 Wahlpflichtmodul 3

Modul Nr.	CY-B-34
Modulverantwortliche/r	Prof. Dr. Martin Schramm
Kursnummer und Kursname	Wahlpflichtmodul 3
Semester	7
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Gewichtung der Note	5/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

In den Wahlpflichtmodulen können die Studierenden ein Modul frei aus einem vorgegebenen Modulkatalog wählen. Inhalte sind fachbezogen zum Studium z.B. aus den Themengebieten Informatik, Cyber Security, Künstliche Intelligenz oder sonstige einschlägige Module. Der Modulkatalog wird stets mit dem Studienplan bekannt gegeben.

Dies ermöglicht eine individuelle Schwerpunktsetzung, Vertiefung und/oder Verbreiterung der Kompetenzen.

Fach- und **Methodenkompetenzen** sowie **persönliche Kompetenzen** und **Sozialkompetenzen** werden je nach gewähltem Modul unterschiedlich betont.

Verwendbarkeit in diesem und in anderen Studiengängen

gemäß Modulbescheibung des gewählten Pflichtmoduls

Zugangs- bzw. empfohlene Voraussetzungen

Zugangsvoraussetzungen:

- keine spezifischen

empfohlene Voraussetzungen:

- Kenntnisse der Inhalte der Grundlagenmodule

Inhalt

Inhalte werden durch das gewählte Modul bestimmt.

Lehr- und Lernmethoden

gemäß Modulbescheibung des gewählten Pflichtmoduls

Besonderes

Ein Anspruch darauf, dass sämtliche vorgesehene Wahlpflichtmodule und Wahlmodule tatsächlich angeboten werden, besteht nicht. Desgleichen besteht kein Anspruch darauf, dass die dazugehörigen Lehrveranstaltungen bei nicht ausreichender Teilnehmerzahl durchgeführt werden.

Empfohlene Literaturliste

gemäß Modulbescheibung des gewählten Pflichtmoduls

CY-B-35 Bachelormodul

Modul Nr.	CY-B-35
Modulverantwortliche/r	Prof. Dr. Martin Schramm
Kursnummer und Kursname	Bachelorarbeit Bachelorseminar
Semester	7
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Undergraduate
SWS	2
ECTS	15
Workload	Präsenzzeit: 30 Stunden Selbststudium: 360 Stunden Virtueller Anteil: 45 Stunden Gesamt: 435 Stunden
Prüfungsarten	Bachelorarbeit
Gewichtung der Note	15/210
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Die im Studium erworbenen Kenntnisse, Fähigkeiten und Fertigkeiten sollen in einem umfangreichen Projekt aus dem Bereich der Cyber Security methodisch und im Zusammenhang eingesetzt werden. Eine Problemstellung soll innerhalb einer vorgegebenen Frist selbstständig strukturiert werden, nach wissenschaftlichen Methoden systematisch bearbeitet und schließlich transparent dokumentiert werden. Im abschießenden Vortrag soll eine zielgruppengerechte Präsentation des Projektes und der in der Arbeit erzielten Resultate erfolgen. In der Bachelorarbeit stellen die Studierenden unter Beweis, dass sie das Bachelor-Studium erfolgreich absolviert haben und die Fertigkeit zum eigenständigen wissenschaftlichen Arbeiten erworben haben.

Im Einzelnen haben die Studierenden nach Abschluss des Moduls folgende Lernergebnisse erreicht:

Fachkompetenz

- Durch die Bearbeitung des Themas der Bachelorarbeit verfügen die Studierenden über vertiefte fachliche Kentnisse in dem jeweiligen Schwerpunkt.
- Die die Studierenden haben die Kompetenz, die im Studium erworbenen Kenntnisse und Fähigkeiten auf komplexe Aufgabenstellungen selbständig anwenden zu können und präsentieren diese in einer angemessenen schriftlichen Form.

Methodenkompetenz

- Durch die Planung der Arbeitsschritte, ihre Ausführung und den Abschluss in Form eines Dokuments verfügen die Studierenden über die Fähigkeit ein umfangreiches Projekt selbständig erfolgreich abzuschließen.

Persönliche Kompetenz

- Sie Studierenden erlangen durch den Abschluss des Bachelormoduls ein hohes Maß an Eigenverantwortung, Selbstdisziplin, Selbstreflexion und Selbstvertrauen.

Sozialkompetenz

- Bachelorarbeiten finden häufig in Kooperation mit Unternehmen der Region statt. Die Studierenden verfügen durch die Einbindung in ein Projektteam des Unternehmens über die Fähigkeit eine persönliche Herausforderung in einem sozialen Kontext zu meistern.
- Die Studierenden können eine umfangreiche Aufgabe lösen und eine Argumentation/Strategie entwerfen, um Ihre These zu vertreten und verteidigen.

Verwendbarkeit in diesem und in anderen Studiengängen

es handelt sich um ein spezielles Modul für diesen Studiengang

Zugangs- bzw. empfohlene Voraussetzungen

Formal:

- Gemäß § 11 der Studien- und Prüfungsordnung kann sich zur Bachelorarbeit anmelden, wer die Module der Grundlagen- und Orientierungsprüfung erfolgreich absolviert hat und mindestens 120 ECTS-Leistungspunkte erreicht hat.

Inhaltlich:

- Kentnisse der Studienganginhalte

Inhalt

Die Bachelorarbeit ist eine schriftliche Ausarbeitung einer individuellen Themenstellung. Sie wird von einer im Studiengang prüfungsberechtigten Person (Hochschullehrer/in, Dozent/in) ausgegeben und von dieser betreut und bewertet. Der Studierende kann Vorschläge für das Thema machen. Die Bearbeitungszeit für die Bachelorarbeit beträgt 6 Monate. Während der Abschlussarbeit findet ein Kolloquium als Seminar (eine mündliche Präsentation) statt. Im Rahmen des Kolloquiums verteidigen die Studierenden ihre Abschlussarbeit.

Lehr- und Lernmethoden

Anleitung zu eigenständiger Arbeit nach wissenschaftlichen Methoden

Besonderes

- Die Bachelorarbeit kann in Abstimmung mit dem Prüfer oder der Prüferin in deutscher oder englischer Sprache verfasst werden.
- Die Bearbeitungszeit für die Bachelorarbeit beträgt 6 Monate.
- Die Bachelorarbeit ist nach den Richtlinien der Rahmenprüfungsordnung (RaPO) und der Allgemeinen Prüfungsordnung (APO) der Hochschule Deggendorf anzufertigen.

Empfohlene Literaturliste

- Individuell, abhängig von konkreter Themenstellung.

Die Arbeit muss ein vollständiges Verzeichnis der benutzten Literatur, der erhaltenen Auskünfte und sonstigen Quellen enthalten. Bezüglich der formellen Anforderungen wird im Übrigen verwiesen auf:

- Lück, W. (1990), Technik des wissenschaftlichen Arbeitens, 4. Auflage, Oldenbourg, München, Seite 10ff.
- Lück, W., Henke, M. (2009), Technik des wissenschaftlichen Arbeitens, Seminararbeit, Diplomarbeit, Dissertation, 10. überarbeitete und erweiterte Auflage, Oldenbourg, München