Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Modulhandbuch

Fakultät Informatik
Studiengang IT Security

StuPO, 17.2
ab Wintersemester 2020/21
Ersteller: Prof. Dr. Bernd Stauß, Studiendekan
Verantwortlich: *Prof. Dr. Bernd Stauß, Studiendekan*

Inhaltsverzeichnis

1 Vorwort

2 Übersicht der Modulbeschreibungen

2.1 1. Semester

11000	Mathematik 1
11500	Einführung Informatik
12000	Programmierung 1
12500	Einführung IT Security
13000	Einführung offensive Security-Methoden
13500	Digitale Logik

2.2 2. Semester

14000	Mathematik 2
14500	Programmierung 2
15000	Betriebssysteme
15500	Kryptologie 1
16000	Web Anwendungen 1
16500	Formale Grundlagen

2.3 3. Semester

21000	Sichere Datenbanken
21100	Betriebswirtschaftslehre und Management
21200	Netzwerke
21300	Rechnertechnik
21400	Kryptologie 2
21500	Algorithmik

2.4 4. Semester

22000	Web-Anwendungen 2
22100	Wirtschafts- und IT-Recht
22200	Betriebssicherheit
22300	Software Engineering
22400	Cybersecurity
22500	Reverse Engineering
22600	Netzwerk- und Systemsicherheit

2.5 5. Semester Vertiefungsrichtung Cyber-Physical Systems (CPS)

23000	Projektmanagement
23100	Unternehmenskonzepte / Digitale Fabrik
23200	Verteilte Systeme (Technik)
23300	Intelligente Lernende Systeme
23400	Wahlpflichtmodul 1 (WPM 1)
23500	Projektstudium

2.6 6. Semester Vertiefungsrichtung Cyber-Physical Systems (CPS)

31000	Integriertes praktisches Studiensemester
31500	Berufsfertigkeit

2.7 7. Semester Vertiefungsrichtung Cyber-Physical Systems (CPS)

32000	Simulationstechnik
32100	Mobile Systeme und Cloud
32200	Wahlpflichtmodule 2 (WPM 2)
5100	Bachelor-Thesis

2.8 5. Semester Vertiefungsrichtung Application Development (AD)

23000	Projektmanagement
23400	Wahlpflichtmodul 1 (WPM 1)
23500	Projektstudium
23600	Datenbanken 2
23700	GUI Development
23800	Softwarearchitektur

2.9 6. Semester Vertiefungsrichtung Application Development (AD)

31000	Integriertes praktisches Studiensemester
31500	Berufsfertigkeit

2.10 7. Semester Vertiefungsrichtung Application Development (AD)

32300	IT-GRC
32100	Mobile Systeme und Cloud
32200	Wahlpflichtmodule 2 (WPM 2)
51000	Bachelor-Thesis

2.11 5. Semester Vertiefungsrichtung IT Management (ITM)

23000	Projektmanagement
23400	Wahlpflichtmodul 1 (WPM 1)
23500	Projektstudium
23900	Big Data
24000	IT-Management
24100	IT Consulting
24200	E-Business

2.12 6. Semester Vertiefungsrichtung IT Management (ITM)

31000	Integriertes praktisches Studiensemester
31500	Berufsfertigkeit

2.13 7. Semester Vertiefungsrichtung IT Management (ITM)

32300	IT-GRC
32100	Mobile Systeme und Cloud
32200	Wahlpflichtmodule 2 (WPM 2)
51000	Bachelor-Thesis

2.14 5. Semester Vertiefungsrichtung Applied ITS (AITS)

23000	Projektmanagement
23400	Wahlpflichtmodul 1 (WPM 1)
23500	Projektstudium
23900	Big Data
24300	Digitale Forensik
24400	Offensive Sicherheitsmethoden

2.15 6. Semester Vertiefungsrichtung Applied ITS (AITS)

31000	Integriertes praktisches Studiensemester
31500	Berufsfertigkeit

2.16 7. Semester Vertiefungsrichtung Applied ITS (AITS)

32300	IT-GRC
32400	IT-Sicherheitsmanagement
32500	Mobile und Cloud Forensik
32200	Wahlpflichtmodule 2 (WPM 2)
51000	Bachelor-Thesis

3 Qualifikationsziel-Modul-Matrix

Modul-Nr.	Modulbezeichnung	Summe der Unterstützungspun	Technische Sicherheit	Sicherer Entwurf und Entwicklung	Organisatorische Sicherheit	Gesellschaft und Sicherheit	Informatik Allgemein	Moderne Technologien	Ingenieurmäßige Fach- und Methodenkompetenz	Analytische Systeme	Abstraktes Denkvermögen
	Qualifikationsziel (QuZ)										
11000	Mathematik I	11	1	1	1	1	1	1	2	1	2
11500	Einführung Informatik	4	1				2		1		
12000	Programmierung 1	4	1	1		1	1				
12500	Einführung IT Security	10	2	1	2	2	1	1	1		
13000	Einführung offensive Security-Methoden	7	1	1	1	1	1	1		1	
13500	Digitale Logik	7	1	1			1		2		2
14000	Mathematik 2	8	0	1	0	1	1	1	1	1	2
14500	Programmierung 2	6		1			2	1	2		
15000	Betriebssysteme	3	1				1	1			
15500	Kryptologie 1	8	0	1	0	1	1	2	0	1	2
16500	Formale Grundlagen	7	0	1	0	0	2	1	0	1	2
16600	Web-Anwendungen 1	4	1	2			1				
21000	Sichere Datenbanken	6	2	2	1	1					
21100	Betriebswirtschaftslehre und Management	6			1	1				2	2
21200	Netzwerke	7	2				1	2	2		
21300	Rechnertechnik	8	1	2			1		2		2
21400	Kryptologie 2	9	2	2	1	1	1				2
21500	Algorithmik	11	0	1	0	1	2	1	2	2	2
22000	Web-Anwendungen 2	5		2			1	1	1		
22100	Wirtschafts- und IT-Recht	2			1	1					
22200	Betriebssicherheit	3	1				1	0			1
22300	Software Engineering	7	2	2		1	1		1		
22400	Cybersecurity	11	2	2	2	2		2			1
22500	Reverse Engineering	8		2		2		2		2	
	Qualifikationsziel (QuZ)										
Modul-Nr.	**Modulbezeichnung**	Summe der Unterstützungspun	Technische Sicherheit	Sicherer Entwurf und Entwicklung	Organisatorische Sicherheit	Gesellschaft und Sicherheit	Informatik Allgemein	Moderne Technologien	Ingenieurmäßige Fach- und Methodenkompetenz	Analytische Systeme	Abstraktes Denkvermögen
22600	Netzwerk- und Systemsicherheit	10	2	2	1	1		2	1		1
23000	Projektmanagement	4		1	1		1	1			
23100	Unternehmenskonzepte/Digitale Fabrik	6	1	1				2	2		
23200	Verteilte Systeme (Technik)	4					1	2			1
23300	Intelligente Lernende Systeme	8	1			1	1	1	2	1	1
23500	Projektstudium	9	1	1	1	1	1	1	1	1	1
23600	Datenbanken 2	11	1	1	0	0	2	2	1	2	2
23700	GUI Development	6		1			1	2	2		
23800	Softwarearchitektur	9	1	1	0	0	2	2	1		2
23900	Big Data	7		2			1	2		2	
24000	IT-Management	7			1	1	1	1		1	2
24100	Consulting	5					1	1		1	2
24200	E-Business	5					1	1		1	2
24300	Digitale Forensik	13	2	2	2	2	1	1	2	1	
24400	Offensive Sicherheitsmethoden	12	2	2	2	2		1	2	1	
31000	Integriertes praktisches Studiensemester	9	0	1	2	0	1	2	2	1	0
31500	Berufsfertigkeit	8	1	1	1	1		1	1	1	1
32000	Simulationstechnik	3		1				1	1		
32100	Mobile Systeme und Cloud	7	1	1			1	2	2		
32300	IT-GRC	8	1		2	2	1	1			1
32400	IT-Sicherheitsmanagement	10	1	1	2	2		2	2		
32500	Mobile und Cloud Forensik	12	2	2	2	2	1	1	2		
51000	Bachelor-Thesis	9	1	1	1	1	1	1	1	1	1

Technische Sicherheit: ... sind in der Lage Sicherheitsrisiken, sowie die Wirkungsweise von Angriffen und Schutzmaßnahmen zu verstehen und sind zur Auswahl und Anwendung von geeigneten Sicherheitstechniken befähigt;
Sicherer Entwurf und Entwicklung : ... sind in der Lage Systeme sowie Anwendungen zu analysieren, entwerfen, entwickeln und pflegen, sodass sie den heutigen Maßstäben an die Sicherheit gerecht werden;
Organisatorische Sicherheit: ... sind in der Lage das erforderliche IT-Sicherheitsniveau für unterschiedliche Bereiche eines Unternehmens festzustellen, die einschlägigen Sicherheitsstrategien zu bestimmen und die daraus resultierenden Sicherheitsmaßnahmen einzuleiten;
Gesellschaft und Sicherheit: ... sind sich ihrer Verantwortung gegenüber Individuen und der Gesellschaft beim Umgang mit Sicherheitsrelevanten Informationen und Sicherheitsmethoden bewusst
Informatik Allgemein: ...können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen
Moderne Technologien: ...sind in der Lage, die Trends in der Entwicklung moderner Informationstechnologien in Bezug auf einen bestimmten Anwendungsbedarf zu verfolgen
ingenieurmäßige Fach- und Methodenkompetenz : ...besitzen eine ingenieurmäßige Fach- und Methodenkompetenz mit tiefgehendem Informatikwissen (Algorithmen, Programmierung, Softwareentwicklung, Betriebssysteme und Netzwerke, verteilte Systeme, IT-Security etc.) ergänzt mit ingenieur- und wirtschaftswissenschaftlichem Grundlagenwissen
Analytische Systeme: können Unternehmensdaten extrahieren, konsolidieren und für die Auswertung in geeigneten Kennzahlensystemen bzw. für Recherche / Mustererkennung aufbereiten
Neuartige Geschäftsmodelle: ... verfügen über Kenntnisse zur Konzeption neuer Geschäftsmodelle, die auf modernen Informations- und Kommunikationstechnologien beruhen (E-Business, Mobile-Business, Industrie 4.0)

4 Studiengangs-Kompetenzmatrix

	Kompetenzen	Fachkompetenz					Personale Kompetenz					
		Wissen		Fertigkeiten			Sozialkompetenz			Selbständigkeit		
	Ausprägung	Tiefe	Breite	Instrumentelle Fertigkeiten	systemische Fertigkeiten	Beurteilungs-fähigkeit	Team-/Führungs-fähigkeit	Mitgestaltung	Kommunikation	Eigenständigkeit / Verantwortung	Reflexivität	Lernkompetenz
11000	Mathematik I	6	5	6	5				6	6		6
11500	Einführung Informatik	5	6	5	5	5					5	5
12000	Programmierung 1	6	6	6	6				5	6		
12500	Einführung IT Security	5	6	6	5	6			6			6
13000	Einführung offensive Security-Methoden		6		6	6			6	6	6	
13500	Digitale Logik	6		6								5
14000	Mathematik 2	6	6		6			5		6		
14500	Programmierung 2	5	6	5	5	5					4	4
15000	Betriebssysteme	6		6			6			6		
15500	Kryptologie 1	6	5	6				5		6		
16500	Formale Grundlagen	6	6		6			5		6		
16600	Web-Anwendungen 1	6		6						6		
21000	Sichere Datenbanken	6		6			6			6		
21100	Betriebswirtschaftslehre und Management	5	6	6			5		6	5		
21200	Netzwerke	6		6					6	5		
21300	Rechnertechnik	6		6								4
21400	Kryptologie 2	6				6				6		
21500	Algorithmik	6	5	6					5			6
22000	Web-Anwendungen 2	6		6	6		6				6	
22100	Wirtschafts- und IT-Recht	6	6	6						6		
22200	Betriebssicherheit	5	6			5			4			
22300	Software Engineering	6	6									6
22400	Cybersecurity	6	6	6					6	6	6	6
22500	Reverse Engineering	6		6					6	6		
22600	Netzwerk- und Systemsicherheit	6			6				6			6
23000	Projektmanagement	5	6	5				5	5	6		
23100	Unternehmenskonzepte/ Digitale Fabrik	6	5	6			6	6	6	6		

	Kompetenzen	Fachkompetenz					Personale Kompetenz					
		Wissen		Fertigkeiten			Sozialkompetenz			Selbständigkeit		
	Ausprägung	Tiefe	Breite	Instrumentelle Fertigkeiten	systemische Fertigkeiten	Beurteilungs-fähigkeit	Team-/Führungs-fähigkeit	Mitgestaltung	Kommunikation	Eigenständigkeit / Verantwortung	Reflexivität	Lernkompetenz
23200	Verteilte Systeme (Technik)	5	6	6					6	6		
23300	Intelligente Lernende Systeme	6	6	6					6	6		6
23400	WPM1	6	6	6						6		
23500	Projektstudium		6		6		6			6		
23600	Datenbanken 2	6		6	6							
23700	GUI Development	6	6	6	6	6			6	6		6
23800	Softwarearchitektur	6		6						6		
23900	Big Data	6	6	6								
24000	IT-Management	6		6	6		6		6	6		
24100	IT-Consulting	6		6	6		6		6	6		
24200	E-Business	6		6	6		6		6	6		
24300	Digitale Forensik	6	6	6	6	6	6			6		6
24400	Offensive Sicherheitsmethoden	6	6	6	6	6			6		6	
31000	Integriertes praktisches Studiensemester	6	5	6				6		6		
31500	Berufsfertigkeit				6			6		6		
32000	Simulationstechnik	6			6					6		
32100	Mobile Systeme und Cloud	6	6	6	6	6					6	6
32200	WPM2											
32300	IT-GRC	6		6			6			6	6	
32400	IT-Sicherheitsmanagement	6	6	6		6			6		6	
32500	Mobile und Cloud Forensik	6	6	6	6	6			6	6		6
51000	Bachelor-Thesis	6			6				6	6		

5 Modulbeschreibungen

5.1 1. Semester

5.1.1 11000 – Mathematik 1

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Mathematik 1						
Kennnummer 11000	**Workload** 150	**Modulart** P	**Studiensemester** 1. Semester		**Dauer** 1 Semester	**Häufigkeit** WS und SS
1	**Lehrveranstaltung(en)** LV11005 Vorlesung Mathematik I + Übungen		**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** Vorlesung und Übungen Mathematik 1: 4 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Tiefes Verständnis der grundlegenden Begriffe und Konzepte aus der Logik, Analysis und linearen Algebra sowie deren Zusammenhänge *[Wissen, 6]* Breites Wissen der für Anwendungen relevanten Begriffe und Konzepte aus der Logik, Analysis und linearen Algebra *[Wissen, 6]* *Kompetenz Fertigkeiten* Beherrschung grundlegender Methoden aus der Analysis und linearen Algebra zur Lösung technischer Probleme und zum Verständnis darauf aufbauender Vorlesungen *[Instrumentelle Fertigkeiten, 6]* Fähigkeit Mathematik als Sprache zur präzisen Formulierung technischer/informatischer Problemstellungen systemisch hinsichtlich Generierung von Neuem einzusetzen *[Systemische Fertigkeiten, 5]* *Sozialkompetenz* Fähigkeit logische und quantitative Sachverhalte in einer präzisen logisch-mathematischen Sprachen zu kommunizieren und zu argumentieren *[Kommunikation, 6]* *Selbstständigkeit* Fähigkeit neue quantitative Sachverhalte mit Hilfe der beschriebenen Fertigkeiten eigenständig und eigenverantwortlich zu analysieren *[Eigenständigkeit/Verantwortung, 6]* Fähigkeit sich selbständig neue, weiterführende bzw. noch nicht explizit behandelte Konzepte und Verfahren aus der mathematisch-wissenschaftlichen Literatur anzueignen *[Lernkompetenz, 6]*					

4	**Inhalte*:*** (1) Mathematische Grundlagen: Mengen, Relationen, Funktionen, Aussagen, Logik, Definitionen, Sätze, Beweise (2) Analysis: - Körper der reellen und komplexen Zahlen - Funktionen und Funktionsklassen: Polynome, rationale Funktionen, Potenz-/Wurzel-/Exponential-/Logarithmus- und trigonometrische Funktionen - Grenzwerte von Folgen, Reihen und Funktionen, Stetigkeit - Differenzialrechnung, Ableitungen, Satz von Taylor - Integralrechnung und Integrationstechniken - Funktionen f:R^n-->R^m, partielle Differentiation (3) Lineare Algebra und Analytische Geometrie: - Geraden und Ebenen; Vektorrechnung im R^n - Lineare Gleichungssysteme, Determinanten - Lineare Abbildungen, Matrizen, Koordinatentransformation, Projektionen, Eigenwerte, Eigenvektoren
	Empfohlene Literaturangaben: Teschl G., Teschl S.: Mathematik für Informatiker - Band 1 (Diskrete Mathematik und lineare Algebra) und Band 2 (Analysis und Statistik), Springer Verlag L. Papula: Mathematik für Ingenieure und Naturwissenschaftler, mehrbändiges Standardwerk, Vieweg P. Minorski: Aufgabensammlung der höheren Mathematik, Fachbuchverlag Leipzig W. Preuß: Mathematik für Informatiker, Fachbuchverlag Leipzig M. Kofler, G. Bitsch, M. Komma: „Maple“, Addison-Wesley
5	**Teilnahmevoraussetzungen:** Grundlagen der Mathematik auf dem Niveau der Fachhochschulreife
6	**Prüfungsformen***:* Klausur 90 min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Klausur
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik
9	***Modulverantwortliche(r):*** Prof. Dr. Andreas Knoblauch Dozenten: Prof. Dr. Andreas Knoblauch, Prof. Dr. Walter Hower, Prof. Dr. Joachim Gerlach, Prof. Dr. Tobias Häberlein, Dieter Kriesell
10	***Optionale Informationen:*** Empfohlener Zeitaufwand: - Summe: 150 h

	- Vorlesung: 60 h - Vor- und Nachbereitung der Vorlesung: 30 h - Bearbeitung von Übungsaufgaben: 30 h - Prüfungsvorbereitung und Prüfung: 30 h

5.1.2 11500 – Einführung Informatik

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Einführung Informatik					
Kennnummer 11500	**Workload** 150	**Modulart** P	**Studiensemester** 1. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)** Vorlesung und Übungen Einführung Informatik	**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5

2	**Lehrform(en) / SWS:** Vorlesung: 2 SWS Praktikum: 2 SWS
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Sie kennen die in der Informatik verwendeten Zahlensysteme und Zeichentabellen und können diese den elementaren Datentypen gängiger Programmiersprachen zuordnen. Sie kennen die wichtigsten Shellbefehle einer ausgewählten Linux-Shell, sowie reguläre Ausdrücke und Umgebungsvariablen. Sie kennen die wichtigsten Sprachelemente zum Aufbau von Shell-Skripten. Sie kennen die Begriffe Compiler / Interpreter. Sie kennen die wichtigsten Adressierungssysteme und Grundprinzipien von Rechnernetzen. Die Studierenden kennen die Grundprinzipien des Aufbaus eines Rechners. *[Wissen, 6]*
	Kompetenz Fertigkeiten Die Studierenden können abgegrenzte Problemstellungen auf Betriebssystem-Ebene mit Kommandozeilenbefehlen und Shell-Scripten umsetzen. Sie können mit einfachen Compiler-Aufrufen umgehen. *[Instrumentelle Fertigkeiten, 5]* Sie können Betriebssystembefehle auch auf kleinere, für sie neue Problemstellungen anwenden. *[Systemische Fertigkeiten, 5]* Sie können die richtige Anwendung verschiedener Datentypen beurteilen. Sie können die Wirkungsweise komplexerer Befehlsverkettungen einschätzen und beurteilen. Sie sind auch in der Lage, zu beurteilen, für welche Probleme eine Shell-Sprache vorzugsweise verwendet wird, und für welche Probleme andere Sprachen besser geeignet sind. *[Beurteilungsfähigkeit, 5]*
	Sozialkompetenz Lernergebnisbeschreibung mit einer bestimmten Kompetenz /Kompetenzausprägung wählen /Niveaustufe wählen

	Selbstständigkeit Die Studierenden sind in der Lage, zu erkennen, wenn die bislang gelernten Befehlsstrukturen für eine Problemstellung nicht ausreichen und sind in der Lage, sich hier Neues anzueignen. *[Reflexivität, 5]* Sie sind in der Lage, sich auch für sie neue Shell-Sprachen und Befehlsumgebungen auf der Kommandozeile schnell anzueignen. *[Lernkompetenz, 5]*
4	**Inhalte***:* Zahlendarstellung, Zeichendarstellung (ASCII-/Unicode-Tabellen) Benutzung eines Betriebssystems am Beispiel Linux: Dateisysteme, Nutzerberechtigungen, Prozesse, einfache Shell-Kommandos, Wildcards und reguläre Ausdrücke, Umgebungsvariablen Einführung in die Shell-Programmierung mit einfachen Kontrollstrukturen Automatisierung abgegrenzter Aufgaben auf Betriebssystemebene über Shell-Skripte Compilierte Programmiersprachen vs. Interpretierte Programmiersprachen Prinzipien Rechnernetze, Schichtenmodelle, MAC-Adressen, IP-Adressen Prinzipien Rechneraufbau
	Empfohlene Literaturangaben: Grundlagen der Informatik, H. Herold et al., Pearson, 2017 Shell-Programmierung. Das umfassende Handbuch, J. Wolf et al., Rheinwerk-Verlag, 2019 Rechnerarchitektur, A.S. Tanenbaum, Pearson, 2014. Computernetzwerke, A.S. Tanenbaum, Pearson, 2012.
5	**Teilnahmevoraussetzungen:** Voraussetzungen für die Teilnahme beschreiben; Außerdem beschreiben, wie sich der Studierende vorbereiten kann (u.a. Literaturangaben, Lehr- und Lernprogramme)
6	**Prüfungsformen***:* Modul 11505: Klausur 90 min., benotet Modul 11510: Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Klausur Bestehen des Praktikums
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. Ute Matecki Dozent(in): Prof. Dr. Ute Matecki
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.1.3 12000 – Programmierung 1

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Programmierung 1						
Kennnummer 12000	**Workload** 180	**Modulart** P	**Studiensemester** 1. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** LV12005 Vorlesung Programmierung 1 LV12010 Praktikum Programmierung 1	**Sprache** Deutsch	**Kontakt-zeit** 6 SWS / 180 h	**Selbst-studium** 157,5 h	**Credits (ECTS)** 7,5	
2	**Lehrform(en) / SWS:** 12005 Vorlesung: 15x4 = 60 SWS 12010 Praktikum: 15x2 = 30 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Den Studierenden ist die Syntax der vorgestellten Programmiersprache klar und ihnen ist bewusst, in welchen Situationen man welche der vorgestellten Programmierkonstrukte am sinnvollsten einsetzt und sie haben die Bedeutung aller Befehle und Progammierkonstrukte verstanden *[Wissen, 6]* *Kompetenz Fertigkeiten* Die Studierenden sind in der Lage, Problemstellungen in einer Weise zu abstrahieren, die es erlaubt einen Lösungsansatz angemessen zu formalisieren und eine Lösung in der notwendigen Allgemeinheit zu erstellen *[Instrumentelle Fertigkeiten, 6]* Die Studierenden sind in der Lage die erworbenen Kenntnisse auch auf völlig neue Problemstellungen sinnvoll anzuwenden und sind in der Lage von den in der Vorlesung und im Praktikum behandelten Beispielen zu abstrahieren und sich so neue Programmiersprachen schnell anzueignen. *[Systemische Fertigkeiten, 6]* Die Studierenden sind in der Lage einfache kleinere Anwendungs- und Softwaresysteme neu zu entwickeln. *[Instrumentelle Fertigkeiten, 6]* *Sozialkompetenz* /Niveaustufe wählen Durch die Art der Abnahme der im Praktikum erarbeiteten Lösungen werden erste Kompetenzen in Präsentation und Dokumentation erworben *[Kommunikation, 5]* *Selbstständigkeit* Durch die verwendete Didaktik in Praktika und Vorlesung werden die Studierenden zu eigenverantwortlichem Handeln, Zeitmanagement und Selbstorganisation angehalten /Kompetenzausprägung wählen *[Eigenständigkeit/Verantwortung, 6]*					

4	**Inhalte*:*** Verwendet wird die Programmiersprache Python. • Grundlagen der Imperativen Programmierung: Ausdrücke, Zuweisungen, Schleifen, Bedingungen, Variablen, Funktionen, Einfache Datentypen, Zusammengesetzte Datentypen. • Grundlagen der Objekt-Orientierten Programmierung: Kapselung, Information Hiding, Klassen, Objekte, Methoden Überladung, Vererbung, Exceptions. • Grundlagen der Funktionalen Programmierung: Lambda-Ausdrücke, Funktionen höherer Ordnung, map-Funktion, filter-Funktion, reduce-Funktion, enumerate, zip, List Comprehensions, Numerical Python • Sonstiges: Entwicklungsumgebungen (Verschiedene Editoren wie emacs, vi), Python-Interpreter-Umgebungen, IPython Notebooks,
	Empfohlene Literaturangaben: Tobias Häberlein: Informatik: Eine praktische Einführung mit Bash und Python (De Gruyter Studium), 2016 Dusty Philliphs: Python 3 Object Oriented Programming. Harness the power of Python 3 objects. Packt publishing, 2010.
5	**Teilnahmevoraussetzungen:** keine
6	**Prüfungsformen***:* Klausur 120 min. Laborarbeit La
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Benotete und unbenotete Leistungen; die studienbegleitenden Prüfungen, auf deren Grundlage Leistungspunkte erworben werden, sollen beschrieben sein. Sofern Module Prüfungsvorleistungen vorsehen (Semesterarbeiten, Exkursionsberichte, Hausarbeiten u.a.), müssen diese nach Art und Umfang beschrieben sein
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik
9	***Modulverantwortliche(r):*** Prof. Dr. Tobias Häberlein Dozenten: Prof. Dr. Tobias Häberlein
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.1.4 12500 – Einführung IT Security

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Einführung IT Security						
Kennnummer 12500	**Workload** 150	**Modulart** P	**Studiensemester** 1. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Vorlesung & Übungen Einführung IT Security	**Sprache** Deutsch (deutsches und englisches Literatur-studium erforderlich)	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 150 h	**Credits (ECTS)** 5	
2	**Lehrform(en) / SWS:** Vorlesung/Übungen: 4 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Tiefes Verständnis der grundlegenden Begriffe und Konzepte der IT Security sowie deren Zusammenspiel mit anderen Informatikteilgebieten *[Wissen, 5]* Breites Wissen der für den sicheren Betrieb von IT Systemen notwendigen Grundlagen, Infrastruktur und Anwendungen *[Wissen, 6]*					
	Kompetenz Fertigkeiten Fähigkeit Sicherheitsrisiken des IT Betriebs und die Sicherheit von Verschlüsselungsverfahren einzuschätzen und zu bewerten *[Beurteilungsfähigkeit, 6]* Fähigkeit Angriffe auf die IT Sicherheit in der Praxis zu erkennen und Lösungen zu deren Abwehr zu erarbeiten *[Systemische Fertigkeiten, 5]* Fähigkeit einfache IT Systeme sicher zu konfigurieren und zu betreiben und dabei IT Sicherheitsmaßnahmen umzusetzen *[Instrumentelle Fertigkeiten, 6]*					
	Sozialkompetenz Fähigkeit im Bereich der Soft-, Hardware- und Organisatorischen IT Sicherheit mit Experten sowie mit Fachabteilungen präzisen kommunizieren und zu argumentieren *[Kommunikation, 6]*					
	Selbstständigkeit Fähigkeit sich selbständig neue, weiterführende bzw. noch nicht explizit behandelte Konzepte und Verfahren aus der wissenschaftlichen IT Security Literatur anzueignen *[Lernkompetenz, 6]*					
4	**Inhalte*:*** Vorlesung & Übungen Ziele und Begriffe der Informationssicherheit					

	• Grundlegende Begriffe der Informationssicherheit • Schutzziele, Schwachstellen, Bedrohungen, Angriffe • Angriffs- und Angreifer Typen • Risikobetrachtung, Risikobewertung und Handlungsalternativen • Aktuelle Entwicklungen Bedrohungslage, Maßnahmen, Kosten, Arbeitsmarkt • Inzident Taxonomie • Grundlagen Sicherheit als Prozess, Sicherheitsinfrastruktur, Sicherheitsrichtlinien • Sicherheitslücken in Anwendungen • Bedrohungen aus dem Internet und Gegenmaßnahmen • Kryptografische Verfahren und Algorithmen im Überblick • Grundprinzipien der Digitalen Signaturen & Zertifizierung Datensicherung, Datenwiederherstellung und Datenlöschung im Überblick
	Empfohlene Literaturangaben: Schmeh, K.: Kryptografie, dpunkt Verlag, 5. Auflage, Wiley, 2013 Biskup, J.: Security in Computing Systems, Springer, 2010 Schwenk, J,: Sicherheit und Kryptographie im Internet, Springer, 2014 Kappes, M.: Netzwerk- und Datensicherheit, Springer,2013 Eckert, C.: IT-Sicherheit, Oldenbourg Wissenschaftsverlag, München, 2018 Pohlmann, N.: Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung, Springer, 2019
5	**Teilnahmevoraussetzungen:** keine
6	**Prüfungsformen***:* Klausur 90 min, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Klausur
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): (n.n.), Prof. Holger Morgenstern Dozent(in): Tim Maier
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.1.5 13000 – Einführung offensive Security-Methoden

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Einführung offensive Security-Methoden						
Kennnummer 13000	**Workload** 75	**Modulart** P	**Studiensemester** 1. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Vorlesung/Seminar Einführung offensive Security-Methoden	**Sprache** Deutsch	**Kontakt-zeit** 2 SWS / 30 h	**Selbst-studium** 45 h	**Credits (ECTS)** 2,5	
2	**Lehrform(en) / SWS:** Vorlesung & Seminar: 2 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Breites Wissen über Grundlagen offensiver Sicherheitstest / PEN Test *[Wissen, 6]*					
	Kompetenz Fertigkeiten Können Grundlagen, Methoden und Werkzeuge offensiver ITS auf IT Systeme und Organisationen anwenden *[Systemische Fertigkeiten, 6]* Sind in der Lage die Wirkung von offensiven Methoden auf Sicherheitssysteme in technischer, menschlicher und organisatorischer Sicht zu beurteilen *[Beurteilungsfähigkeit, 6]*					
	Sozialkompetenz Studierende können komplexe offensive Sicherheitsmethoden mit einem Fachpublikum diskutieren *[Kommunikation, 6]*					
	Selbstständigkeit Eigenständiges wissenschaftliches Erschließen aktueller Anwendungen offensiver Sicherheitsmethoden *[Eigenständigkeit/Verantwortung, 6]* Reflexion und Bewusstsein über ethische Grenzen und Auswirkungen offensiver Methoden *[Reflexivität, 6]*					
4	**Inhalte*:*** Vorlesung & Seminar • Motivation offensiver Sicherheitsmethoden • Rechtliche und moralische Grundlagen • Ablauf von Penetrationstests (Testvorbereitung, Informationsbeschaffung, Zielanalyse, Angriff, Dokumentation und Abschlussgespräch) Referate zu Themen wie: • Anatomie von erfolgreichen Angriffen • Beispiele schwerwiegender Sicherheitslücken • Scanning und Datenbeschaffung • Buffer Overflows und deren Ausnutzung					

	• Offensive Werkzeuge (Exploit Toolkits, WLAN Cracking, Web-Exploits) • Passwörter und Passwort Cracking • Social Engineering
	Empfohlene Literaturangaben: Institute for Security and Ipen Methodologies, Open Source Security Testing Methodology Manual (OSSTM) Online: www.isecom.org/osstmm/ C. Hadnagy, Social Engineering: The Art of Human Hacking Wechselnde Online-Literatur für den Referatsteil
5	**Teilnahmevoraussetzungen:** keine
6	**Prüfungsformen***:* Referat (15 min), benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertetes Referat
8	***Verwendbarkeit des Moduls:*** IT Security
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): (n.n.), Prof. Holger Morgenstern Dozent(in): Dufner
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.1.6 13500 – Digitale Logik

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Digitale Logik						
Kennnummer 13500	**Work-load** 150	**Modulart** P	**Studiensemester** 1. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** LV 13505 Vorlesung Digitale Logik		**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** Vorlesung, Umfang 15 x 4 = 60 SWS					

3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Kenntnis und Verständnis der Darstellung und Verarbeitung von Information in digitalen Rechnersystemen, der mathematischen Grundlagen zur Beschreibung und Optimierung von Verarbeitungsschritten in digitalen Rechnersystemen, sowie der schaltungstechnischen Realisierung von Verarbeitungsabläufen. *[Wissen, 6]*
	Kompetenz Fertigkeiten Fähigkeit zur Anwendung von Verfahren der binären Darstellung und Verarbeitung von Daten, von Codierungsverfahren, von Regeln und Verfahren der booleschen Algebra, sowie von Verfahren zur Umsetzung gegebener Problemstellungen in schaltungstechnische Lösungen in Form von Schaltnetzen oder Schaltwerken. *[Instrumentelle Fertigkeiten, 6]*
	Sozialkompetenz
	Selbstständigkeit Transfer der Vorlesungsinhalte in die praktische Anwendung zur selbständigen Lösung von Problemstellungen. *[Lernkompetenz, 5]*
4	**Inhalte*:*** Teil-1: Einführung in Digitale Rechnersysteme - Vom Abakus zum Supercomputer Teil-2: Grundlagen der Digitalen Datenverarbeitung - Grundlagen der Digitaltechnik - Zahlendarstellung und Codes - Boolesche Algebra Teil-3: Digitale Schaltungstechnik - Kombinatorische Schaltungen - Sequentielle Schaltungen - Entwurf digitaler Schaltungen heute
	Empfohlene Literaturangaben: - Hoffmann D.W.: Grundlagen der Technischen Informatik. Carl Hanser Verlag. - Siemers C., Sikora A.: Taschenbuch Digitaltechnik. Carl Hanser Verlag. - Fricke K.: Digitaltechnik. Vieweg+Teubner Verlag. - Gehrke W., Winzker M., Urbanski K., Woitowitz R.: Digitaltechnik. Springer Vieweg Verlag.
5	**Teilnahmevoraussetzungen:**
6	**Prüfungsformen***:* Klausur 90 Minuten, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur
8	***Verwendbarkeit des Moduls:*** Technische Informatik, IT Security

9	***Modulverantwortliche(r):*** Prof. Dr. Joachim Gerlach Dozenten: Prof. Dr. Joachim Gerlach
10	***Optionale Informationen:***

5.2 2. Semester

5.2.1 14000 – Mathematik 2

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Mathematik 2						
Kennnummer 14000	**Workload** 150 h	**Modulart** P	**Studiensemester** 2		**Dauer** 1 Semester	**Häufigkeit** WS und SS
1	**Lehrveranstaltung(en)** Mathematik 2, Vorlesung + Übungen		**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** Vorlesung + Übungen: 4 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* mathematische Sachverhalte einordnen, Abstraktions-Vermögen schärfen *[Wissen, 6]* *Kompetenz Fertigkeiten* Zähl-Probleme systematisch angehen und lösen *[Systemische Fertigkeiten, 6]* *Sozialkompetenz* sich in einer Lern-Gruppe ziel-orientiert verhalten *[Mitgestaltung, 5]* *Selbstständigkeit* hohe Eigen-Motivation anstreben und hochhalten *[Eigenständigkeit/Verantwortung, 6]*						
4	**Inhalte:** Fundamentales: Natürliche Zahlen, Funktionen, Relationen; Mengen: Operationen, Endliche Mengen, Abzählbarkeit und Überabzählbarkeit; Kombinatorik: Grundlegende Zähl-Techniken, Ein-/Ausschluss, Rekurrenz-Relation, Fakultät, Permutation, Binomialkoeffizient, Binom. Lehrsatz, Kombination, Permutations-Koeffizient, Variation, Stirling-Zahlen 1. und 2. Art, Bell-Zahlen; Zahlen-Theorie: modulare Arithmetik, Primfaktor-Zerlegung; Wahrscheinlichkeits-Rechnung: allgemein, bedingt; Dichte, Verteilung, Erwartungswert, Varianz *Empfohlene Literaturangaben:* A. Arnold, I. Guessarian: Mathématiques pour l'informatique; 4e édition, Dunod, 2005, 978-2-100-49230-5 R. A. Beeler: How to Count: An Introduction to Combinatorics and Its Applications – A problem-based approach to learning Combinatorics; Springer International Publ. Switzerland,						

	2015, 978-3-319-13843-5 (hardcover), 10.1007/978-3-319-13844-2 (DOI) J. Buchmann: Einführung in die Kryptographie; 6. Auflage, Springer Spektrum, 2016, 978-3-642-39774-5 (Papier), 10.1007/978-3-642-39775-2 (DOI) R. L. Graham, D. E. Knuth, O. Patashnik: Concrete Mathematics: A Foundation for Computer Science; 2nd edition, 20th printing, Pearson / Addison-Wesley, 2006,978-0-201-55802-9 W. Hower: Diskrete Mathematik – Grundlage der Informatik; 2. Aufl., De Gruyter Studium, 2021 W. Hower: Informatik-Bausteine – Eine komprimierte Einführung; 10.1007/978-3-658-01280-9 (DOI), 978-3-658-01279-3 (Softcover), Springer Nature Vieweg Fachmedien International Publishing, 2019
5	**Teilnahmevoraussetzungen:** - empfohlen: Mathe-1
6	**Prüfungsformen***:* Klausur, 90 Min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** schriftl. Prüfung
8	***Verwendbarkeit des Moduls:*** alle Informatik-Studiengänge
9	***Modulverantwortlicher:*** Prof. Dr. W. Hower Dozenten: Prof. Dr. W. Hower, Prof. Dr. A. Knoblauch, Prof. Dr. J. Gerlach
10	***Optionale Informationen:*** Informatik-Mathe-Allgemeinbildung

5.2.2 14500 – Programmierung 2

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 12.03.20

Modul: Programmierung 2						
Kennnummer 14500	**Workload** 225	**Modulart** P	**Studiensemester** 2. Semester		**Dauer** 1 Semester	**Häufigkeit** WS und SS
1	**Lehrveranstaltung(en)** Vorlesung und Übungen Programmierung 2 Praktikum Programmierung 2		**Sprache** Deutsch, bei Bedarf Englisch (muss vor Semester-beginn geäußert werden)	**Kontakt-zeit** 6 SWS / 90 h	**Selbst-studium** 135h	**Credits (ECTS)** 7,5
2	**Lehrform(en) / SWS:**					

	Vorlesung und Übungen: 4 SWS Praktikum: 2 SWS
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen die typischen Sprachparadigmen der Programmiersprachen Java, C und C++ *[Wissen, 6]*
	Kompetenz Fertigkeiten Die Studierenden sind in der Lage, abgegrenzte Problemstellungen algorithmisch und strukturell mit objektorientierten und imperativen Bestandteilen der Programmiersprachen Java, C und C++ umzusetzen. *[Instrumentelle Fertigkeiten, 5]* Die Studierenden sind in der Lage, auch kleinere, für sie neue Problemstellungen mit den objektorientierten und imperativen Bestandteilen der o.g. Sprachen umzusetzen. *[Systemische Fertigkeiten, 5]* Die Studierenden sind in der Lage, programmiertechnische Lösungen in den o.g. Sprachen für abgegrenzte Problemstellungen zu bewerten. *[Beurteilungsfähigkeit, 5]*
	Sozialkompetenz Lernergebnisbeschreibung mit einer bestimmten Kompetenz /Kompetenzausprägung wählen /Niveaustufe wählen
	Selbstständigkeit Die Studierenden sind in der Lage, zu erkennen, wenn die bisher gelernten Mittel für weitergefasste Problemstellungen nicht reichen und sich weitere Inhalte der o.g. Sprachen (z.B. weitere API-Klassen) anzueignen. *[Reflexivität, 4]* Die Studierenden sind in der Lage, auch andere Programmiersprachen ähnlicher Struktur selbstständig zu lernen und auf ähnliche Problemstellungen wie die behandelten anzuwenden. *[Lernkompetenz, 4]*
4	**Inhalte*:*** Besonderheiten der Programmiersprachen Java und C/C++ im Vergleich zu Python Der Kompilationsprozess in Java bzw. C/C++ Referenztypen in Java bzw. C/C++ (Call-by-value vs. Call-by-Reference) Grundlegenden Sprachelemente von Java und C/C++ Klassen und Objekte UML Klassendiagramme Strings in Java bzw. C/C++ Das Vererbungskonzept in Java bzw. C++ Die STL in C++ Exception Handling Schnittstellen Generische Einheiten Dateien und Streams
	Empfohlene Literaturangaben:

	Ullenboom, Chr.: Java ist auch eine Insel, Rheinwerk Verlag, 14. Auflage, 2018 Goll, J., Heinisch, C.: Java als erste Programmiersprache, Springer Vieweg, 8. Auflage, 2016 http://docs.oracle.com/javase/tutorial/ https://docs.oracle.com/en/java/javase/13/ https://www.uni-trier.de/fileadmin/urt/doku/java/v80/java8.pdf ANSI C, Grundlagen der Programmierung, Herdt-Verlag, 2015 ANSI C++, Grundlagen der Programmierung, Herdt-Verlag, 2018
5	**Teilnahmevoraussetzungen:** Empfehlenswert: - Einführung Informatik - Programmierung 1
6	**Prüfungsformen***:* Klausur 120 min., benotet Praktische Arbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandenes Praktikum Bestandene Klausur
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. German Nemirovski, Prof. Dr. Ute Matecki, Prof. Dr. Thomas Eppler Dozent(in): Prof. Dr. German Nemirovski, Prof. Dr. Ute Matecki, Prof. Dr. Thomas Eppler
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.2.3 15000 – Betriebssysteme und Netzwerke

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Betriebssysteme und Netzwerke						
15000	**Workload** 150 h	**Modulart** P	**Studiensemester** 2	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Vorlesung & Übungen Betriebssysteme und Netzwerke Praktikum Betriebssysteme und Netzwerke	**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90	**Credits (ECTS)** 5	

Version	Erstellt/geändert von Ammann/am 12.10.2020	Dokument	Freigabe am/von	Gültig ab WS 2020/21
1.0		Modulhandbuch_IT_Sec_fin		

2	**Lehrform(en) / SWS:** Vorlesung & Übungen: 3 SWS Praktikum: 1 SWS
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen die wichtigsten Eigenschaften von Betriebssystemen und Netzwerken *[Wissen, 6]*
	Kompetenz Fertigkeiten Die Studierenden können - Einfache Analyse von Arbeitsplatzrechnern - Administration von Windows-Rechnern - Administration von Unix-Rechnern - Einfache Sicherheits-Policies umsetzen - Netzwerke aufbauen und analysieren - Router und Switches konfigurieren - Netzwerkverkehr analysieren *[Systemische Fertigkeiten, 6]*
	Sozialkompetenz Die Studierenden sind in der Lage im Team komplexe Aufgaben zu lösen. *[Team-/Führungsfähigkeit, 6]*
	Selbstständigkeit Die Studierenden lernen selbständig ein Netzwerk zu konfigurieren *[Eigenständigkeit/Verantwortung, 6]*
4	**Inhalte*:*** Linux: Dateisystem, Prozesse, Userverwaltung, Paketverwaltung, Netzwerk, SSH Microsoft: Prozesse, Threads, Memory, DLL, HyperThreading, Registry, Services, Handles, MSDN, Driver, Netzwerk, Befehle, PowerShell, Active Directory Netzwerke: Schichtenmodelle (ISO/OSI und TCP/IP) ISO/OSI Schicht 1 und 2: Übersicht ISO/OSI Schicht 3: Routing, IP Funktionalität, ICMP, IPv6, ARP, RARPISO/OSI Schicht 4: UDP und TCP, Stau- und Flusskontrolle, zuverlässige KommunikationISO/OSI Schicht 7: Anwendungsprotokolle, DNS, DHCP
	Empfohlene Literaturangaben: Andrew S. Tanenbaum: Moderne Betriebssysteme. München u.a.: Pearson Studium, 2009.Glatz, E.: Betriebssysteme : Grundlagen, Konzepte, Systemprogrammierung. Heidelberg: dpunkt, 2006.Andrew S. Tanenbaum: Computernetzwerke, Pearson-Verlag, 3. Auflage, 2000Douglas E. Comer: Computernetzwerke, Pearson-Verlag, 2001Kurose J und Ross K.: Computernetzwerke : der Top-Down-Ansatz Pearson Verlag, 2008
5	**Teilnahmevoraussetzungen:** -

6	**Prüfungsformen***:* Klausur 90 min., benotet Praktische Arbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Am Ende des Semesters ist eine 90 minütige schriftliche Prüfung zu schreiben. Während des Semesters sind mehrere Praktikumsaufgaben zu bearbeiten.
8	***Verwendbarkeit des Moduls:*** IT-Security, Technische Informatik Wirtschaftsinformatik
9	***Modulverantwortliche(r):*** Prof. Dr. Thomas Eppler Dozenten: Prof. Dr. Thomas Eppler
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.2.4 15500 – Kryptologie 1

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Kryptologie 1						
Kennnummer 15500	**Workload** 150	**Modulart** P	**Studiensemester** 2. Semester	**Dauer** 1 Semester		**Häufigkeit** WS und SS
1	**Lehrveranstaltung(en)** Vorlesung + Übung Mathemat. Kryptologie Vorlesung + Übung Angewandte Kryptologie		**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** 15910 Vorlesung + Übung Mathematische Kryptologie: 2 SWS 15920 Vorlesung + Übung Angewandte Kryptologie: 2 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Zahlen-Systeme bewerten, Nicht-Primzahl-Test durchführen *[Wissen, 6]* *Kompetenz Fertigkeiten* Verschlüsselungs-Verfahren einordnen *[Instrumentelle Fertigkeiten, 6]* *Sozialkompetenz*					

	sich in einer Lern-Gruppe ziel-orientiert verhalten *[Mitgestaltung, 5]*
	Selbstständigkeit hohe Eigen-Motivation anstreben und hochhalten *[Eigenständigkeit/Verantwortung, 6]*
4	**Inhalte*:*** Zahlen-Systeme, Ring-Strukturen, Kleiner Satz von Euler-Fermat; symmetrische und asymmetrische Verschlüsselungs-Verfahren, Integrität, Authentifizierung, Hash-Funktionen
	Empfohlene Literaturangaben: Albrecht Beutelspacher, Jörg Schwenk, Klaus-Dieter Wolfenstetter: Moderne Verfahren der Kryptographie – Von RSA zu Zero-Knowledge; 8. Auflage, Springer Spektrum, 2015, 978-3-8348-1927-7 (Papier), 10.1007/978-3-8348-2322-9 (DOI) Johannes Buchmann: Einführung in die Kryptographie; 6. Auflage, Springer Spektrum, 2016, 978-3-642-39774-5 (Papier), 10.1007/978-3-642-39775-2 (DOI) Walter Hower: Diskrete Mathematik – Grundlage der Informatik; 2. Auflage, De Gruyter Studium, 2021 Walter Hower: Informatik-Bausteine – Eine komprimierte Einführung; 10.1007/978-3-658-01280-9 (DOI), 978-3-658-01279-3 (Softcover), Springer Nature Vieweg Fachmedien International Publishing, 2019
5	Teilnahmevoraussetzungen: - empfohlen: Mathe-1, Einführung IT Security
6	**Prüfungsformen***:* je 1 Klausur (Mathematische + Angewandte Krypto) à 45 min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** schriftl. Prüfungen
8	***Verwendbarkeit des Moduls:*** IT Security
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. Walter Hower Dozent(in): Prof. Dr. Walter Hower, Prof. Dr. Tobias Häberlein
10	***Optionale Informationen:*** empfohlene Voraussetzung für Kryptologie 2

5.2.5 16000 – Web-Anwendungen 1

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

<table>
<tr><td colspan="7">Modul: Web-Anwendungen 1</td></tr>
<tr><td colspan="2">Kennnummer
16000</td><td>Workload
75</td><td>Modulart
P</td><td colspan="2">Studiensemester
2. Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung & Übungen Web-Anwendungen 1
Praktikum Web-Anwendungen 1</td><td>Sprache
Deutsch, bei Bedarf Englisch (muss vor Semester-beginn geäußert werden)</td><td>Kontakt-zeit
2 SWS / 30 h</td><td>Selbst-studium
45 h</td><td>Credits (ECTS)
2,5</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung & Übungen: 1 SWS
Praktikum: 1 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen typische Merkmale von Web-Anwendungen, die Grundlage von HTML, XHTML, von CSS, von JavaScript und JQuery
[Wissen, 6]
Kompetenz Fertigkeiten
Die Studierenden sind in der Lage die Anforderungen eines Kunden in Bezug auf die Struktur einer einfachen Webseite zu verstehen und umzusetzen. [Instrumentelle Fertigkeiten, 6]
Sozialkompetenz
Selbstständigkeit
Die Studierenden sind in der Lage größere technischen Aufgaben, deren Bearbeitung auch mehrere Tage in Anspruch nimmt, verantwortungsvoll zu erfüllen, realistische Ziele zu definieren und diese konsequent zu verfolgen.
[Eigenständigkeit/Verantwortung, 6]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Vorlesung und Praktikum
• Typische Merkmale von responsiven modernen Web-Seiten
• HTTP-Protokoll
• die Grundlage der HTML, XHTML
• die Grundlagen von CSS</td></tr>
</table>

	• die Grundlagen von JavaScript • JavaScript und CSS Frameworks am Beispiel von JQuery und Bootsraps
	Empfohlene Literaturangaben: Jürgen Wolf, HTML5 und CSS3 : das umfassende Handbuch, Rheinwerk Computing; Auflage: 2, 2016, ISBN: 3836241587 Kai Günster, Schrödinger lernt HTML5, CSS3 und JavaScript: Das etwas andere Fachbuch, Rheinwerk Computing, 2016, ISBN: 3836242575 Philipp Ackermann JavaScript: Das umfassende Handbuch für Einsteiger, Fortgeschrittene und Profis, Rheinwerk Computing, 2016, ISBN: 3836238381 https://www.w3schools.com/
5	**Teilnahmevoraussetzungen:** Zulassung zu einem der Informatik-Studiengänge BSc. an der HS Albstadt Sigmaringen
6	**Prüfungsformen***:* Studienarbeit benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Studienarbeit
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. German Nemirovski Dozent(in): Prof. Dr. German Nemirovski
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.2.6 16500 – Formale Grundlagen

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Formale Grundlagen					
Kennnummer 16500	**Workload** 150	**Modulart** P	**Studiensemester** 2. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)** Vorlesung + Seminar Formale Grundlagen	**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5

2	**Lehrform(en) / SWS:** Vorlesung + Seminar: 4 SWS
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Komplexitäts-, Sprach- und Automaten-Theorie nutzen; Trennung der berechenbaren von den unberechenbaren Problemen vornehmen *[Wissen, 6]* *Kompetenz Fertigkeiten* mathem. Strukturen beweisen, berechenbare Probl. einordnen *[Systemische Fertigkeiten, 6]* *Sozialkompetenz* sich in einer Lern-Gruppe ziel-orientiert verhalten *[Mitgestaltung, 5]* *Selbstständigkeit* hohe Eigen-Motivation anstreben und hochhalten *[Eigenständigkeit/Verantwortung, 6]*
4	**Inhalte*:*** informatik-basierte mathematische Strukturen, Komplexitäts-Theorie, Sprach-Klassen mit Chomsky-Hierarchie, Automaten-Theorie, prinzipielle Berechnungsgrenzen, Unberechenbarkeit *Empfohlene Literaturangaben:* M. J. Atallah, M. Blanton (eds.): Algorithms and Theory of Computation Handbook; 2nd edition, Vol. 1: General Concepts and Techniques, 978-1-13811-393-0 (paperback), 2017, Volume 2: Special Topics and Techniques, 978-1-58488-820-8 (hardback), 2010, Chapman & Hall / CRC / Taylor & Francis J. E. Hopcroft, R. Motwani, J. D. Ullman: Introduction to Automata Theory, Languages, and Computation; 3rd, new international, edition, Pearson, 2014, 978-1-2920-3905-3 / 978-1-2920-5015-7 (paperback), 978-1-2920-5616-6 (eBook). Einführung in Automatentheorie, Formale Sprachen und Berechenbarkeit; 3., aktualisierte Aufl., Pearson Studium, 2011, 978-3-86–894082-4 (gedruckt), 978-3-86–326509-0 (elektronisch) W. Hower: Diskrete Mathematik – Grundlage der Informatik; 2. Aufl., De Gruyter Studium, 2021 W. Hower: Informatik-Bausteine – Eine komprimierte Einführung; 10.1007/978-3-658-01280-9 (DOI), 978-3-658-01279-3 (Softcover), Springer Nature Vieweg Fachmedien International Publishing, 2019 J. Hromkovič: Theoretische Informatik - Formale Sprachen, Berechenbarkeit, Komplexitätstheorie, Algorithmik, Kommunikation und Kryptographie; 5. Auflage,

	Springer Vieweg Fachmedien, 2014, 978-3-658-06432-7 (softcover), 10.1007/978-3-658-06433-4 (DOI) H. R. Lewis, C. H. Papadimitriou: Elements of the Theory of Computation; 2nd, international, edition, Pearson, 1998, 978-0-13262-478-7 (hardback), 978-0-13272-741-9 C. H. Papadimitriou, K. Steiglitz: Combinatorial Optimization: Algorithms and Complexity; 2nd edition, Dover, 1998, 978-0-486-40258-1 P. Pudlák: Logical Foundations of Mathematics and Computational Complexity – A Gentle Introduction; Springer International Publishing Switzerland, 2013, 978-3-319-3426-8-9 (softcover), 978-3-319-0011-8-0 (hardcover), 10.1007/978-3-319-0011-9-7 (DOI) A. Singh: Elements of Computation Theory; Springer-Verlag, London, 2009, 978-1-4471-6142-4 (soft), 978-1-84882-496-6 (hard), 10.1007/978-1-84882-497-3 (DOI) International Journal of Foundations of Computer Science; World Scientific, 0129-0541 (print), 1793-6373 (online)
5	**Teilnahmevoraussetzungen:** - empfohlen: Mathe-1, parallel Mathe-2
6	**Prüfungsformen***:* Klausur, 90 Min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** schriftl. Prüfung
8	***Verwendbarkeit des Moduls:*** IT Security
9	***Modulverantwortlicher:*** Prof. Dr. Walter Hower Dozent: Prof. Dr. Walter Hower
10	***Optionale Informationen:*** theoretische Fundierung

5.3 3. Semester

5.3.1 21000 – Sichere Datenbanken

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Sichere Datenbanken						
Kennnummer 21000	**Workload** 225	**Modulart** P	**Studiensemester** 3. Semester		**Dauer** 1 Semester	**Häufigkeit** WS und SS
1	**Lehrveranstaltung(en)** Vorlesung & Übungen Datenbanken Grundlagen Praktikum Datenbanken Grundlagen Vorlesung & Übungen Sicherheit der Datenbanken Praktikum Datenbanken Sicherheit der Datenbanken		**Sprache** Deutsch, bei Bedarf Englisch (muss vor Semester-beginn geäußert werden)	**Kontakt-zeit** 6 SWS / 90 h	**Selbst-studium** 135 h	**Credits (ECTS)** 7,5
2	**Lehrform(en) / SWS:** Vorlesung DB Grundlagen: 3 SWS Praktikum DB Grundlagen: 1 SWS Vorlesung Sicherheit der DB: 1 SWS Praktikum Sicherheit der DB: 1 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen - die grundlegende Arbeitsweise von Transaktionssystemen im Sinne des ACID-Paradigmas - die grundlegenden Techniken der Datenmodellierung sowie den prinzipiellen Aufbau und die Arbeitsweise von Datenbanksystemen - die Implementierungstechniken zur Formulierung komplexer Anfragen auf Basis eines (objekt-) relationalen Datenbanksystems in SQL - die Verwendung von Metadaten beim Aufbau (komplexer) Datenbank-Anfragen - Abstraktionstechniken und deren Anwendung bei der Implementierung von persistenten Anwendungsobjekten (z.B. in JDBC) - die Grundlagen der Datenbanksicherheit (Sichten, Zugriffsrechte, Datenschutz) -die Gefahren beim Umgang mit Daten und Datenbanken (Speichern von Passwörtern, Ausführung von Code *[Wissen, 6]* *Kompetenz Fertigkeiten* Die Studierenden können - gegebene Aufgabenstellungen aus dem Bereich der Wirtschaftsinformatik, der					

	Technischen Informatik und der IT-Security zu analysieren und als Datenmodell für den Einsatz von Datenbankanwendungen darzustellen•ein Datenbankschema in SQL zu formulieren und auf der Basis eines gegebenen Datenbanksystems zu realisieren - repräsentative Anwendungsszenarien in SQL zu formulieren und darzustellen - einfache und komplexe Datenbankanfragen auf Basis des (objekt-) relationalen Datenmodells zu formulieren - Integritätsbedingungen zu formulieren und durch SQL auszudrücken - Datenbankprozeduren und Trigger zu implementieren - Zugriffsrechte und Sichten zu verwenden, um einen sicheren Zugriff durch mehrere Parteien zu gewährleisten - Die Vorgänge in einer Datenbank nachvollziehen und nach Sicherheitsgesichtspunkten bewerten (Auditing) *[Instrumentelle Fertigkeiten, 6]*
	Sozialkompetenz Die Studierenden sind in der Lage im Team komplexe Aufgaben zu lösen. *[Team-/Führungsfähigkeit, 6]*
	Selbstständigkeit Die Studierenden lernen im Rahmen des Praktikums eine größere Aufgabe selbständig oder in kleineren Teams zu bearbeiten. *[Eigenständigkeit/Verantwortung, 6]*
4	**Inhalte*:*** Vorlesung, Übungen und Praktikum - das Entity-Relationship-Modell - Normalformenlehre - die Datenbanksprache SQL - Einführung in die Spracheinbettung von SQL in Java und Python - Methoden zur Implementierung von Datensicherungs- und Recovery-Maßnahmen - Modellierung von Zugriffsbeschränkungen, Rechtemodellen, Sicherungen, Benutzerrechten, Rollen, Protokolldateien - Verschlüsselte Datenbanken und Schutz von Datenbanksystemen - Auditing von Datenbanken
	Empfohlene Literaturangaben: Alfons Kemper, Andre Eickler: Datenbanksysteme: Eine Einführung (De Gruyter Studium) (Deutsch) Taschenbuch – 25. September 2015
5	**Teilnahmevoraussetzungen:** --
6	**Prüfungsformen***:* Klausur 120 min, benotet Praktische Arbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:***

	Am Ende des Semesters ist eine 120 minütige schriftliche Prüfung zu schreiben. Während des Semesters sind mehrere Praktikumsaufgaben zu bearbeiten.
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. Thomas Eppler Dozent(in): Prof. Dr. Thomas Eppler
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.3.2 21100 – Betriebswirtschaftslehre und Management

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Betriebswirtschaftslehre und Management					
Kennnummer **21100**	**Workload** 75 h	**Modulart** P	**Studiensemester** 3	**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)** Vorlesung & Übungen Betriebswirtschaftslehre und Management	**Sprache** Deutsch	**Kontakt-zeit** 2 SWS / 30 h	**Selbst-studium** 45 h	**Credits (ECTS)** 2,5
2	**Lehrform(en) / SWS:** Vorlesung & Übungen: 2 SWS				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden verstehen grundlegende betriebswirtschaftliche Zusammenhänge, betriebswirtschaftliche Unternehmensziele sowie die wesentlichen Schritte zur Umsetzung und Verfolgung dieser Ziele. Sie kennen die Aufgaben und wirtschaftlichen Fragestellungen der jeweiligen betrieblichen Funktionen in Unternehmen. Die Studierenden kennen die bekanntesten Rechtsformen von Unternehmen und betriebswirtschaftliche Kriterien zur Auswahl spezifischer Rechtsformen. *[Wissen, 6]* Lernergebnisbeschreibung einer bestimmten Kompetenz z.B. Fachwissen mit Niveaustufe /Niveaustufe wählen				
	Kompetenz Fertigkeiten Die Studierenden • arbeiten mit Methoden der Unternehmensführung und wenden Wissen an, das Ihnen erlaubt interdisziplinäre Fragestellungen zu analysieren, adäquate Entscheidungskriterien herauszuarbeiten sowie Vorgehensweisen zur Beantwortung der aufgeworfenen Fragestellungen zu entwickeln.				

	• können Wirkungen operativer unternehmerischer Entscheidungen auf die Ergebnisse des Unternehmens und sein gesellschaftliches Umfeld aufzeigen. *[Instrumentelle Fertigkeiten, 6]*
	Sozialkompetenz Sind in der Lage Fallstudien in einem Team zu bearbeiten und die Teamarbeit selbst zu organisieren. [Team-/Führungsfähigkeit, /Kompetenzausprägung wählen *5]* Beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen *[Kommunikation, 6]*
	Selbstständigkeit Können Problemstellungen erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen; *[Eigenständigkeit/Verantwortung, 5]*
4	**Inhalte***:* • *Betriebswirtschaftliche Grundbegriffe und Grundtatbestände* • *Rechtsformwahl und Unternehmensverfassung* • *Kooperation und Konzentration von Unternehmen* • *Planen, Entscheiden und Kontrollieren* • *Die Organisationsentscheidungen* • *Grundlagen des externen Rechnungswesens*
	Empfohlene Literaturangaben: Schmalen, H.; Pechtl, H., Grundlagen und Probleme der Betriebswirtschaft, 15. Auflage, Schäffer Poeschel, 2013 Bernecker, M.: Grundlagen der Betriebswirtschaftslehre: BWL, 4. Auflage, Johanna Verlag, 2011 Hopfenbeck, W.: Allgemeine Betriebswirtschafts- und Managementlehre, o. A., o. V., 2002 Jung, H.: Allgemeine BWL, 12. Auflage, Oldenbourg Verlag, 2010 Schierenbeck, H.; Wöhle, C.: Grundzüge der Betriebswirtschaftslehre, 17. Auflage, Oldenbourg Verlag, 2008 Thommen, J.-P.; Achleitner, A.-K.: Allgemeine BWL -Umfassende Einführung aus management-orientierter Sicht, 7. Auflage, Gabler Verlag, 2012 Wöhe, G.: Einführung in die allgemeine BWL, 25. Auflage, Vahlen Verlag, 2013
5	**Teilnahmevoraussetzungen:** Zulassung zu einem der Informatik-Studiengänge BSc. an der HS Albstadt Sigmaringen
6	**Prüfungsformen***:* Klausur 60 min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur
8	***Verwendbarkeit des Moduls:*** Wirtschaftsinformatik

9	***Modulverantwortliche(r):*** Prof. Dr. Philipp Lindenmayer Dozenten: Prof. Dr. Philipp Lindenmayer
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.3.3 21200 – Netzwerke

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

<table>
<tr><td colspan="7">Modul: Netzwerke</td></tr>
<tr><td colspan="2">Kennnummer
21200</td><td>Workload
150</td><td>Modulart
P</td><td colspan="2">Studiensemester
3. Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung & Übungen Netzwerke
Praktikum Netzwerke</td><td>Sprache
Deutsch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
90 h</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung: 3 SWS
Praktikum: 1 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Kennen den Aufbau und dir Bedeutung den wichtigsten Netzwerkprotokolle [Wissen, 6]</td></tr>
<tr><td></td><td colspan="6">Kompetenz Fertigkeiten
Die Studierenden sind in der Lage Netzwerkkonfigurationen zu analysieren und zu konzeptionieren. Die Studierenden können Netzwerkverkehr aufzeichnen und analysieren. Die Studierenden können programmtechnisch Netzwerkverbindungen nutzen. [Instrumentelle Fertigkeiten, 6]</td></tr>
<tr><td></td><td colspan="6">Sozialkompetenz
Die Studierenden sind in der Lage, sich mittels dem spezifischen Vokabular auszudrücken, sich verständlich zu machen und andere zu verstehen [Kommunikation, 6]</td></tr>
<tr><td></td><td colspan="6">Selbstständigkeit</td></tr>
</table>

	Die Studierenden sind in der Lage größere Aufgaben, deren Bearbeitung auch mehrere Tage in Anspruch nimmt, verantwortungsvoll zu erfüllen, realistische Ziele zu definieren und diese konsequent zu verfolgen *[Eigenständigkeit/Verantwortung, 5]*
4	**Inhalte*:*** Grundlagen der Netzwerkkommunikation • Kommunikationsmodelle • Netzwerktopologien und Schichtenmodelle (ISO/OSI und TCP/IP) • Aufbau von Kommunikationsprotokollen und vernetzten Systemen Kommunikationsprotokolle des TCP/IP Protokoll-Stacks • Bitübertragungsschicht: Übertragungs- und Codierungsarten, Leitungscodes, Multiplexing • Sicherungsschicht: Rahmenerkennung, Ethernet, Token Ring, Spanning Tree, WLAN, Leitungscodes und Modulation • Netzwerkschicht: Routing, IP Funktionalität, ICMP, IPv6, ARP, RARP, DHCP, etc. • Transportschicht: UDP und TCP, Stau- und Flusskontrolle, zuverlässige Kommunikation • Anwendungsprotokolle, DNS, Socket Programmierung Netzwerkpraxis und Socket Programmierung • Konfiguration von Netzwerkprotokollen unter Linux • Analyse von Netzwerkprotokollen mit tcpdump und Wireshark • Entwurf und Umsetzung einer Client-Server Anwendung in C • Entwurf und Umsetzung eines HTTP/1.0 Webservers in C
	Empfohlene Literaturangaben: Kurose J. und Ross K.: Computernetzwerke : der Top-Down-Ansatz Pearson Verlag, 2008 Andrew S. Tanenbaum: Computernetzwerke, Pearson-Verlag, 3. Auflage, 2000
5	**Teilnahmevoraussetzungen:** Voraussetzungen für die Teilnahme beschreiben; Außerdem beschreiben, wie sich der Studierende vorbereiten kann (u.a. Literaturangaben, Lehr- und Lernprogramme)
6	**Prüfungsformen***:* Klausur 90 min, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Benotete und unbenotete Leistungen; die studienbegleitenden Prüfungen, auf deren Grundlage Leistungspunkte erworben werden, sollen beschrieben sein. Sofern Module Prüfungsvorleistungen vorsehen (Semesterarbeiten, Exkursionsberichte, Hausarbeiten u.a.), müssen diese nach Art und Umfang beschrieben sein
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik
9	***Modulverantwortliche(r)*** Modulverantwortliche(r): Prof. Morgenstern, Prof. Dr. Rieger Dozent(in):
10	***Optionale Informationen:***

	Studiengangsspezifische, zusätzliche Informationen zum Modul

5.3.4 21300 – Rechnertechnik

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Rechnertechnik						
Kennnummer 21300	**Work-load** 150	**Modulart** P	**Studiensemester** 3. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** LV 21305 Vorlesung Rechnertechnik LV 21310 Praktikum Rechnertechnik	**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5	
2	**Lehrform(en) / SWS:** Vorlesung, Umfang 15 x 2 = 30 SWS Praktikum, Umfang 15 x 2 = 30 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Konzeptionelles Verständnis des strukturellen Aufbaus und der Funktionsweise digitaler Rechnersysteme. Programmierung von Mikroprozessoren in Assembler und Hardware-nahem C. Verständnis für die Sicherheit von Rechnersystemen und Schwachstellen/Angriffsszenarien auf Hardware-naher Ebene. *[Wissen, 6]* *Kompetenz Fertigkeiten* Fähigkeit zum Verstehen von Abläufen in Mikroprozessor-Systemen und zur Programmierung von Mikroprozessoren in Assembler und Hardware-nahem C. *[Instrumentelle Fertigkeiten, 6]* *Sozialkompetenz* *Selbstständigkeit* Transfer der Vorlesungsinhalte in die praktische Anwendung zur selbständigen Lösung von Problemstellungen. Selbständige Umsetzung von Aufgabenstellungen in Lösungsverfahren in Form von Assembler- oder C-Programmen. *[Lernkompetenz, 4]*						
4	**Inhalte*:*** Vorlesung: - Geschichtliche Entwicklung der Mikroprozessortechnik Teil-1: Programmierung von Mikroprozessorsystemen - Grundlagen der Assemblerprogrammierung - Unterprogrammtechniken - Synchronisation & Interrupt-Handling - Hardware-nahe Programmierung in Assembler und C Praktikum: - Programmieren eines Mikroprozessors in Assembler auf Basis eines					

	Befehlssatzemulators - Programmieren eines Mikroprozessors in Assembler und Hardware-nahem C auf Basis eines Einplatinencomputers
	Empfohlene Literaturangaben: - Patterson D.A., Hennessy J.L.: Computer Organization and Design. Morgan Kaufmann. - Bode A., Karl W., Ungerer T.: Rechnerorganisation und -entwurf. Spektrum Akad. Verlag. - Wüst K.: Mikroprozessortechnik. Vieweg+Teubner Verlag. - Beierlein T., Hagenbruch O.: Taschenbuch Mikroprozessortechnik. Carl Hanser Verlag.
5	**Teilnahmevoraussetzungen:** Digitale Logik (Grundlagen der digitalen Schaltungstechnik) Programmierung 2 (Grundlagen der Programmierung, Programmentwicklung in C)
6	**Prüfungsformen***:* Vorlesung: Klausur 90 Minuten, benotet Praktikum: Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Vorlesung: Bestandene Klausur Praktikum: Abgaben/Abnahmen der Praktikumsaufgaben, bestandener Abschlusstest
8	***Verwendbarkeit des Moduls:*** Technische Informatik, IT Security
9	***Modulverantwortliche(r):*** Prof. Dr. Joachim Gerlach Dozenten: Prof. Dr. Joachim Gerlach
10	***Optionale Informationen:*** Modul besitzt im Studiengang TI StuPo-Version 17.2. die Ausprägung 4+2 SWS und im Studiengang ITS StuPo-Version 17.2. die Ausprägung 2+2 SWS. Der Vorlesungsteil beinhaltet bei TI zwei Hauptteile (Programmierung + Technische Grundlagen) und bei ITS einen Hauptteil (Programmierung).

5.3.5 21400 – Kryptologie 2

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Kryptologie 2					
Kennnummer	**Workload**	**Modulart**	**Studiensemester**	**Dauer**	**Häufigkeit**
21400	225	P	3. Semester	1 Semester	WS und SS

1	**Lehrveranstaltung(en)** Vorlesung & Übungen Kryptologie 2 Praktikum Kryptologie 2	**Sprache** Deutsch (deutsches und englisches Literatur-studium erforderlich)	**Kontakt-zeit** 6 SWS / 225 h	**Selbst-studium** 157,5 h	**Credits (ECTS)** 7,5
2	**Lehrform(en) / SWS:** Vorlesung: 4 SWS Praktikum: 2 SWS				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden sind in der Lage das Feld der Kryptologie auch mathematisch zu durchdringen und die vorgestellten Verfahren logisch korrekt und präzise in der Sprache der Mathematik zu fassen. *[Wissen, 6]* *Kompetenz Fertigkeiten* Die Studierenden sind in der Lage die betrachteten Verfahren anzuwenden, gegeneinander abzuwägen, einfache Sicherheitsbetrachtungen anzustellen. *[Beurteilungsfähigkeit, 6]* *Sozialkompetenz* Lernergebnisbeschreibung mit einer bestimmten Kompetenz /Kompetenzausprägung wählen /Niveaustufe wählen *Selbstständigkeit* Zudem sind die Studierenden in der Lage, die wichtigsten Verfahren selbst zu implementieren und diese Implementierungen mit dem bisher erworbenen Wissen der Programmierung, Softwareentwicklung, Mathematik und Algorithmik zu verbinden *[Eigenständigkeit/Verantwortung, 6]*				
4	**Inhalte*:*** • Klassische Verfahrungen der Kryptographie • Symmetrische Verfahren (DES, AES) • Differentielle und Lineare Attacken • Seitenkanalattacken • Endliche Körper und GF(pq) • Betriebsmodi • Kryptographisch sichere Zufallszahlengeneratoren • Hashing • Primzahlen und Primzahltests • Chinesischer Restsatz • Asymmetrische Kryptographie • RSA • Modulare Exponentiation und effiziente Berechnung mit dem chinesischen Restsatz • Perfekt Forward Secrecy • Digitale Zertifikate und Zertifizierungsstellen				

	• Diffie-Hellman • ElGamal • Elliptische Kurven und ECDH-RSA • Blockchain und digitale Währungen
	Empfohlene Literaturangaben: Schmeh: Kryptografie: Verfahren, Protokolle, Infrastrukturen Beutelspacher, Schwenk, Wolfenstetter: Moderne Verfahren der Kryptographie: Von RSA zu Zero-Knowledge, Verlag: Springer Spektrum, Auflage: 8, 2015 Avi Kak: Computer and Network Security, Purdue University, 2017. Paar und Pelzl, Kryptografie verständlich https://www.springer.com/de/book/9783662492963 Buchmann, Einführung in die Kryptograhie https://www.springer.com/de/book/9783642397745
5	**Teilnahmevoraussetzungen:** Krypto 1
6	**Prüfungsformen***:* Klausur 120 min, benotet Laborarbeit unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Benotete und unbenotete Leistungen; die studienbegleitenden Prüfungen, auf deren Grundlage Leistungspunkte erworben werden, sollen beschrieben sein. Sofern Module Prüfungsvorleistungen vorsehen (Semesterarbeiten, Exkursionsberichte, Hausarbeiten u.a.), müssen diese nach Art und Umfang beschrieben sein
8	***Verwendbarkeit des Moduls:*** IT Security
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. Tobias Häberlein Dozent(in): Prof. Dr. Tobias Häberlein
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.3.6 21500 – Algorithmik

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Algorithmik					
Kennnummer 21500	**Workload** 75	**Modulart** P	**Studiensemester** 3. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)** Vorlesung + Übungen Algorithmik	**Sprache** Deutsch	**Kontakt-zeit** 2 SWS / 30 h	**Selbst-studium** 45 h	**Credits (ECTS)** 2,5

2 Lehrform(en) / SWS:
Vorlesung + Übungen: 2 SWS

3 Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen

Größenordnung der Laufzeit von Algorithmen abschätzen *[Wissen, 6]*

Kompetenz Fertigkeiten

Standard-Berechnungsverfahren anwenden *[Instrumentelle Fertigkeiten, 6]*

Sozialkompetenz

.. /Kompetenzausprägung wählen *nicht relevant*

Selbstständigkeit

Selbstständige Reflexion über Einsatz und Laufzeit von Algorithmen in verschiedenen Situationen *[Reflexivität, 6]*

4 Inhalte:

- O-Notation
- Rekursion
- Sortieren (Insertion Sort, Quicksort, Merge Sort)
- Suchalgorithmen (Hashing, Search Trees, Tries. Skip Lists, Bloomfilter)
- Graph-Algorithmen (Tiefensuche, Breitensuche, Kürzeste Wege)
- Python-Code zu Algorithmen

Empfohlene Literaturangaben:

Anany Levitin: Introduction to The Design and Analysis of Algorithms, 3rd (internat.) edition, Pearson Higher Education, 2012, 978-0-273-76411-3; eBook: 978-1-2920-1411-1, 2014

T. H. Cormen, C. E. Leiserson, R. L. Rivest, C. Stein: Introduction to Algorithms, 3rd (internat.) edition, MIT Press, 2009, ISBN 978-0-262-53305-8

Tobias Häberlein: Eine praktische Einführung in die Informatik mit Bash und Python, De Gruyter,

	2012 Tobias Häberlein: Praktische Algorithmik mit Python, De Gruyter, 2012 Walter Hower: Diskrete Mathematik – Grundlage der Informatik, 2. Auflage, De Gruyter Studium, 2021 Walter Hower: Informatik-Bausteine – Eine komprimierte Einführung, 10.1007/978-3-658-01280-9 (DOI), 978-3-658-01279-3 (Softcover), Springer Nature Vieweg Fachmedien International Publishing, 2019 Kurt Mehlhorn: Effiziente Algorithmen, Teubner, 1977, ISBN 9783519023432 Kurt Mehlhorn, Peter Sanders: Algorithmen und Datenstrukturen, eXamen.press/Springer, 2011, 978-3-642-05471-6 Markus Nebel, Sebastian Wild: Entwurf und Analyse von Algorithmen – Eine Einführung in die Algorithmik mit Java, 978-3-658-21154-7 (Print), https://doi.org/10.1007/978-3-658-21155-4 (DOI), Springer Nature Vieweg Fachmedien, Wiesbaden, 2., vollst. überarbeitete, Aufl., 2018; Buch-Reihe Studienbücher Informatik, 2522-0640 (paper), 2522-0659 (el.) R. Sedgewick: Algorithmen in Java, 3. Auflage, Pearson Studium, München, 2003; 978-3-8273-7072-3
5	**Teilnahmevoraussetzungen**: - empfohlen: Mathe- und Prog.-2
6	**Prüfungsformen***:* Klausur, 60 Min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** schriftl. Prüfung
8	***Verwendbarkeit des Moduls:*** alle Informatik-Studiengänge
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. Tobias Häberlein, Prof. Dr. Walter Hower Dozent(in): Prof. Dr. Tobias Häberlein, Prof. Dr. Walter Hower
10	***Optionale Informationen:*** Informatik-Allgemeinbildung

5.4 4. Semester

5.4.1 22000 – Web-Anwendungen 2

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 13.10.20

Modul: Web-Anwendungen 2						
Kennnummer 22000	**Work-load** 150	**Modulart** P	**Studiensemester** 4. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Vorlesung & Übungen Web-Anwendungen 2 Praktikum Web-Anwendungen	**Sprache** Deutsch, bei Bedarf Englisch (muss vor Semester-beginn geäußert werden)	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5	
2	**Lehrform(en) / SWS:** Vorlesung & Übungen: 3 SWS Praktikum: 1 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Studierenden kennen typische Merkmale von Web-Basierten Anwendungen, darunter die Eigenschaften der Protokolle, die Kommunikationsmodelle Client-Server, Subscription-Notifikation, Client- und Server-Seitige asynchrone Datenverarbeitung, den Funktionsprinzip von (REST-) Web Services, gängige Schwachstellen in Web Anwendungen und wie diese ausgenutzt werden können, die Schutzmaßnahmen zu den genannten Schwachstellen, ein der Authentication Verfahren *[Wissen, 6]* *Kompetenz Fertigkeiten* Die Studierenden können Konzeption und Design einer Web-Anwendung selbständig und einem Team durchzuführen, Web Anwendungen mithilfe einer ihnen vertrauten Technologie und einem der gängigen IDE, wie WebStorm oder Visual Studio entwickeln, und umfassend testen. *[Instrumentelle Fertigkeiten, 6]* Die Studierenden sind in der Lage nach einen Bedarf eines Anwendungsgebiet zu analysieren und dementsprechend ein Konzept einer Web Anwendung zu entwickeln, die den Bedarf erfüllen würde; das Konzept einer Zielgruppe gerecht zu präsentieren um diese Zielgruppe für eigene Idee zu gewinnen. *[Systemische Fertigkeiten, 6]* *Sozialkompetenz* Sind in der Lage komplexe Aufgaben in einem Team zu bearbeiten, die Teamarbeit zu organisieren und die Rollen effektiv zu verteilen *[Team-/Führungsfähigkeit, 6]*					

	Selbstständigkeit Die Studierenden können Ergebnisse eigener Tätigkeit im Bezug auf die gesetzten Ziele aber auch im Anbetracht der vorhandenen Ressourcen kritisch betrachten und ggf. Verbesserungen oder Ergänzungen eigenständig einzuführen, falls die Zielsetzung nicht im vollen Umfang erfüllt ist. *[Reflexivität, 6]*
4	**Inhalte*:*** Vorlesung: HTTP-Protokoll, Grundlagen von REST-Services, JSON als Mediation-Protokoll, Node JS /Express als Serverseitige Technologie, Web Sockets, Konfiguration, Testing und Deployment von Web Anwendung, Schwachstellen und die Prüfmethodik für die Client- und Server-Seite. Labor: Konzeption und Entwicklung einer Web Anwendung mithilfe von den o.g. Techniken.
	Empfohlene Literaturangaben: Philipp Ackermann JavaScript: Das umfassende Handbuch für Einsteiger, Fortgeschrittene und Profis, Rheinwerk Computing, 2016, ISBN: 3836238381 Levinson, Deborah, and Todd Belton. Build Your First Web App: Learn to Build Web Applications from Scratch. Sterling Swift Pub Co, 2017 D'mello, Bruno Joseph, Mithun Satheesh, and Jason Krol. Web Development with MongoDB and Node: Build fast web applications for handling any kind of data. Packt Publishing Ltd, 2017. Marshall, Joseph. Hands-On Bug Hunting for Penetration Testers: A practical guide to help ethical hackers discover web application security flaws. Packt Publishing Ltd, 2018.
5	**Teilnahmevoraussetzungen:** Kenntnisse und Praktische Erfahrung für die gängigen Web-Client-Techniken: HTML, CSS, JavsScript
6	**Prüfungsformen***:* Klausur 90 min, benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandenen Klausur und Laborarbeit
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. German Nemirovski Dozent(in): Prof. Dr. German Nemirovski
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.4.2 22100 – Wirtschafts- und IT-Recht

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Wirtschafts- und IT-Recht						
Kennnummer 22100	**Work-load** 150	**Modulart** P	**Studiensemester** 4. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Vorlesung & Übungen Wirtschafts- und IT-Recht Vorlesung & Übungen Datenschutz und Urheberrecht	**Sprache** Deutsch, bei Bedarf Englisch (muss vor Semester-beginn geäußert werden)	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5	
2	**Lehrform(en) / SWS:** Vorlesung: 4 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Nach erfolgreichem Abschluss des Moduls kennen die Studierenden die wesentlichen nationalen und internationalen Rechtsgrundlagen und Rahmenbedingungen des IT-Rechtes; die Lizenzmodell, die rechtlichen Grundlagen zum Datenschutzrechts; die rechtlichen Grundlagen zum Internet- und Telekommunikationsrecht; *[Wissen, 6]* *Kompetenz Fertigkeiten* Die Studierende sind in der Lage wichtige rechtliche Sachverhalte relevante zur Erstellung und zum Betrieb eines IT-Produktes, z.B. einer Internet-Seite bei einem produktiven Einsatz in einem Unternehmen zu berücksichtigen: neben allgemeinen Inhalten wie Rechtsanwendung im Internet und Verletzung von Schutzrechten, Fragen zu e-Commerce, Fernabsatz, Vertragsschluss im Internet, Sicherheit im Internet, Datenschutz und die Urheberrechtlichen Fragestellungen *[Instrumentelle Fertigkeiten, 6]* *Selbstständigkeit* Die Studierenden lernen durch die integrierten Übungen ihren Lernerfolg einzuschätzen und ggf. die Verbesserungsmaßnahmen zu ergreifen. *[Eigenständigkeit/Verantwortung, 6]*					
4	**Inhalte*:*** Der mit Hilfe des Internets bewerkstelligte elektronische Geschäftsverkehr wirft eine Fülle von Rechtsfragen auf. Im ersten Zugang wird die Stellung und Einordnung des					

	sogenannten Internetrechts in das Gesamtrechtssystem und sein Verhältnis zum Medienrecht dargestellt. Nach dieser Grundlegung werden internetrechtsspezifische Problemfelder beim Einsatz des Internets als betriebliches Präsentations-, Marketing- und Vertriebsinstrument erörtert. Aus der Vielzahl möglicher Themenbereiche seien genannt: • Vertragsrecht • Domänenrecht • Redaktionelle Gestaltung von Webseiten • Schutz des Inhalts von Webseiten • Verantwortung für den Inhalt von Webseiten • Verbraucherschutz beim „B2C“Geschäft • Internetauktionen und „Powershopping“ • Zahlung im und per Internet • Signaturrecht • Grenzüberschreitender elektronischer Geschäftsverkehr • Steuerrechtliche Fragen des elektronischen Geschäftsverkehrs
	Empfohlene Literaturangaben: Philipp Ackermann JavaScript: Das umfassende Handbuch für Einsteiger, Fortgeschrittene und Profis, Rheinwerk Computing, 2016, ISBN: 3836238381 Alexander Salvanos, Professionell entwickeln mit Java EE 7: Das umfassende Handbuch, Galileo Computing, 2014, ISBN: 3836220040 Beyer, Jörg; Weimer (Lahn); Schulten, Lars: Servlets & JSP von Kopf bis Fuß, O'Reilly, Köln, 2009 Stuttard, Dafydd, and Marcus Pinto. The web application hacker's handbook: finding and exploiting security flaws. John Wiley & Sons, 2011. Shostack, Adam. Threat modeling: Designing for security. John Wiley & Sons, 2014. https://tomcat.apache.org/ https://www.w3schools.com/
5	**Teilnahmevoraussetzungen:** Voraussetzungen für die Teilnahme beschreiben; Außerdem beschreiben, wie sich der Studierende vorbereiten kann (u.a. Literaturangaben, Lehr- und Lernprogramme)
6	**Prüfungsformen***:* Modul 221505: Klausur 90 min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur
8	***Verwendbarkeit des Moduls:*** IT Security
9	***Modulverantwortliche(r):***

	Modulverantwortliche(r): Prof. Dr. German Nemirovski Dozent(in): N.N.
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.4.3 22200 – Betriebssicherheit

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Betriebssicherheit						
Kennnummer 22200	**Work-load** 150	**Modulart** P	**Studiensemester** 4. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** LV 22205 Vorlesung Betriebssicherheit LV 22210 Praktikum Betriebssicherheit	**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5	
2	**Lehrform(en) / SWS:** Vorlesung mit Übungen, Umfang 15x4 = 60 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Sensibilisierung bezüglich Systeme, welche Sicherheitsanforderungen haben. *[Wissen, 6]* *Kompetenz Fertigkeiten* Bestimmung von Ausfallwahrscheinlichkeiten und Zuverlässigkeit. Programmierung von Bäumen und Graphen zur Wahrscheinlichkeitsbestimmung von Ausfällen. *[Beurteilungsfähigkeit, 5]* *Sozialkompetenz* Diskussionsfähigkeit mit Studierenden über Bewertung von Risiken. *[Kommunikation, 4]* *Selbstständigkeit* Kein Schwerpunkt					
4	**Inhalte*:*** Normen und Standards: IEC 61508, funktionale Sicherheit sicherheitsbezogener Systeme; ISO 26262 (automotive spezifische Sicherheitsnorm), IEC 61511 (Prozessindustrie). Sichere Programmierung von Software. Grundlagen: Fehler, Ausfälle, Risiko- und Zuverlässigkeitsanalyse, Sicherheitsfunktion, Sicherheitsintegritätslevel (SIL), Begriffe und Definitionen aus Sicherheit und					

	Zuverlässigkeit Modelle und Verfahren: Risikomatrix, Risikograph, Fehlerbaumanalyse, Ereignisbaumanalyse, Zuverlässigkeitsanalyse. Simulationstechniken mit Markov.
	Empfohlene Literaturangaben: Börcsök, J.: Funktionale Sicherheit, VDE Verlag, 4. akt. Auflage, 2014. V. Gebhardt et. al., Funktionale Sicherheit nach ISO 26262, dpunkt.verlag Peter Löw et. al., Funktionale Sicherheit in der Praxis, dpunkt.verlag Gehlen, P.: Sicherheitsfibel zur Maschinensicherheit, VDE Verlag 2013. Halang, W.A.; Konakovsky, R.M.: Sicherheitsgerichtete Echtzeitsysteme, Springer Verlag, 2. Akt. Auflage, 2013
5	**Teilnahmevoraussetzungen:** Der Studierende muss die Programmiersprache Python beherrschen (Modul Programmieren). Er muss in der Lage sein, Wahrscheinlichkeiten mit mathematischen Methoden zu berechnen (Modul Mathematik). Rekursionen bei der Programmierung sind notwendig.
6	**Prüfungsformen***:* Betriebssicherheit: Klausur 90 min., benotet Prakt. Betriebssicherheit: Laborarbeit unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Der Studierende soll in der Lage sein, Bäume und Graphen zu programmieren und rekursiv Berechnungen durchzuführen. Der Studierende soll benennen können welche Maßnahmen es gibt, Softwarecode funktional sicher zu entwerfen. Der Studierende soll wissen, welche Normen angewendet werden soll, um sichere Systeme zu entwickeln. Der Studierende soll Methoden anwenden können, um Wahrscheinlichkeiten von Ausfällen zu berechnen.
8	***Verwendbarkeit des Moduls:*** Technische Informatik, IT-Security
9	***Modulverantwortliche(r):*** Prof. Dr. Derk Rembold Dozenten: Prof. Dr. Derk Rembold
10	***Optionale Informationen:*** keine

5.4.4 22300 – Software Engineering

Version	Erstellt/geändert von Ammann/am 12.10.2020	Dokument	Freigabe am/von	Gültig ab WS 2020/21
1.0		Modulhandbuch_IT_Sec_fin		

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Software Engineering						
Kennnummer 22300	**Workload** 75	**Modulart** P	**Studiensemester** 4. Semester		**Dauer** 1 Semester	**Häufigkeit** WS und SS
1	**Lehrveranstaltung(en)** Software Engineering		**Sprache** Deutsch (deutsches und englisches Literatur-studium erforderlich)	**Kontakt-zeit** 4 SWS / 30 h	**Selbst-studium** 45 h	**Credits (ECTS)** 2,5
2	**Lehrform(en) / SWS:** Vorlesung und Übungen: 2 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen die wichtigsten Verfahrensmodelle der Softwareentwicklung sowie die Agile Prozesse. Sie Kenne die Methoden für die Anforderungsanalyse und Softwareentwurf. Sind mir den wichtigsten Architektur-Ansätzen Vertraut. Sie könnenmit den wesentlichen Diagrammformaten der UML umgehen, nämlich: Use Cases, Klassendiagrammen, und Sequenzdiagrammen. Sie kenne die Grundsätze von OOP und kennen die gängig Versionierung und Testing-Tools und -Methoden. *[Wissen, 6]* *Selbstständigkeit* Die Studierenden lernen durch die integrierten Übungen ihren Lernerfolg einzuschätzen und ggf. die Verbesserungsmaßnahmen zu ergreifen. *[Lernkompetenz, 6]* **Inhalte*:*** Software Prozesse Agile Software Entwicklung Dev Ops -Konzept Anforderungsanalyse: Use Cases uns User Stories, Kanban board Entwurf: Architekturtypen, OOP Proviples, UML, Grundsätze der Funktionale Programmierung Implementierung: Testen, Versionieren, Clean Code, Continuous Delivery *Empfohlene Literaturangaben:* Christine Rupp und die SOPHISTen, Requirements-Engineering und -Management: Aus der Praxis von klassisch bis agil, HAnser Verlag, 2014, ISBN: 3446438939					

	Jochen Ludewig, Horst Lichter, Software Engineering: Grundlagen, Menschen, Prozesse, Techniken, dpunkt Verlag, 2013, ISBN: 3864900921 Robert C., Clean Coder: Verhaltensregeln für professionelle Programmierer, mitp, 2014, ISBN: 3826696956 Hay, D.: Requirements Analysis: From Business Views to Architecture. Prentice Hall, 1st edition, 2011, ISBN-13: 978-0132762007 van Lamsweerde, A.: Requirements Engineering: Desktop Edition: From System Goals to UML Models to Software Specification. John Wiley & Sons; 1. Auflage, 2009, ISBN-13: 978-0470012703 https://maven.apache.org/ https://git-scm.com/
4	**Teilnahmevoraussetzungen:** Programmierkenntnisse in mindesten einer Programmiersprache, Grundlagen der Web-Entwiclung
	Prüfungsformen*:* Modulprüfung 22305: Klausur 60 min, benotet
5	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur
6	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik
7	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. German Nemirovski Dozent(in): Prof. Dr. German Nemirovski
8	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul
9	
10	

5.4.5 22400 – Cybersecurity

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.2020

Version	Erstellt/geändert von Ammann/am 12.10.2020	Dokument	Freigabe am/von	Gültig ab WS 2020/21
1.0		Modulhandbuch_IT_Sec_fin		

Modul: Cybersecurity						
Kennnummer 22400	**Workload** 150	**Modulart** P	**Studiensemester** 4. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Vorlesung & Seminar Cybersecurity Praktikum Cybersecurity	**Sprache** Deutsch, bei Bedarf Englisch (muss vor Semester-beginn geäußert werden), deutsches und englisches Literatur-studium erforderlich	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90h	**Credits (ECTS)** 5	
2	**Lehrform(en) / SWS:** Vorlesung & Seminar: 3 SWS Praktikum: 1 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Tiefe und breite Kenntnis die systematischen Grundlagen der IT Sicherheit in den Bereichen Sicherheitsmanagement und Modelle, Identifikation, Authentifizierung, Authorisierung, Betriebssystem-, Datenbank-, Software- und Websicherheit *[Wissen, 6]* Breite Kenntnis aktueller praktischer Probleme und Lösungsstrategien der Cybersicherheit *[Wissen, 6]* *Kompetenz Fertigkeiten* Fähigkeit Grundlagen und Konzepte der IT Security praktisch auf verschiedensten Bereichen des Cyberspace anzuwenden *[Instrumentelle Fertigkeiten, 6]* *Sozialkompetenz* Fähigkeit aktuelle, komplexe Probleme und Lösungen der Cybersecurity einem Fachpublikum überzeugend zu präsentieren und kontrovers zu diskutieren *[Kommunikation, 6]* *Selbstständigkeit* Fähigkeit ein aktuelles, komplexes Fachthema nach wissenschaftlichen Standards selbstständig zu erschließen *[Eigenständigkeit/Verantwortung, 6]* Fähigkeit aktuelle praktische sowie wissenschaftliche Cybersecuritythemen ethisch und gesellschaftliche zu reflektieren *[Reflexivität, 6]*					

	Fähigkeit geeignete Literatur im wissenschaftlichen Print- und Preprintbereich zu einem aktuellen Cybersecurityproblem zu recherchieren und auszuwählen *[Lernkompetenz, 6]*
4	**Inhalte*:*** Vorlesung, Seminar und Praktikum • Sicherheitsmanagement • Identifikation und Authentifizierung • Zugriffskontrolle • Referenzmonitore • Betriebssystemsicherheit • Datenbanksicherheit • Softwaresicherheit • Sicherheitsmodelle • Websicherheit • Aktuelle Sicherheitsthemen • Cyber-Security-Ethics
	Empfohlene Literaturangaben: Gollmann, D.: Computer Security, 3. Auflage, Wiley, 2012 Tavani, H.T.: Ethics and Technology, 4. Auflage, Wiley, 2013 Biskup, J.: Security in Computing Systems, Springer, 2010Schwenk, J,: Sicherheit und Kryptographie im Internet, Springer, 2014 Eckert, C.: IT-Sicherheit, Oldenbourg Wissenschaftsverlag, München, 2019 Stückelberger, Duggal: Cyber Ethics 4.0 – Serving Humanity with Values, Globalethics.net, 2018
5	**Teilnahmevoraussetzungen:** keine empfohlen Inhalte der Module 12500 Einführung IT Security, 15500 Kryptologie 1, 21400 Kryptologie 2, 21200 Netzwerke
6	**Prüfungsformen***:* Referat 20 min, benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Mit mindestens 4.0 bewertetes Referat im Seminar erfolgreiche Teilnahme am Praktikum
8	***Verwendbarkeit des Moduls:*** IT Security
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Holger Morgenstern Dozent(in): Prof. Holger Morgenstern
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.4.6 22500 – Reverse Engineering

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Version	Erstellt/geändert von Ammann/am 12.10.2020	Dokument	Freigabe am/von	Gültig ab WS 2020/21
1.0		Modulhandbuch_IT_Sec_fin		

Modul: Reverse Engineering						
Kennnummer 22500	**Workload** 75	**Modulart** P	**Studiensemester** 4. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Vorlesung & Übungen Reverse Engineering	**Sprache** Deutsch	**Kontakt-zeit** 2 SWS / 30 h	**Selbst-studium** 45 h	**Credits (ECTS)** 2,5	
2	**Lehrform(en) / SWS:** Vorlesung und Übungen: 2 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen die für das Reverse Engineering wichtigen Merkmale der prozessorarchitektur und der Assemblersprache. *[Wissen, 6]* *Kompetenz Fertigkeiten* Die Studierenden sind in der Lage, ausführbare Programme mittels der Verhaltensanalyse, der statichscen und der dynamischen Codeanalyse zu analysieren. *[Instrumentelle Fertigkeiten, 6]* *Sozialkompetenz* Die Studierenden sind in der Lage, sich mittels dem spezifischen Vokabular auszudrücken, sich verständlich zu machen und andere zu verstehen *[Kommunikation, 6]* *Selbstständigkeit* Die Studierenden sind in der Lage, sich mittels dem spezifischen Vokabular auszudrücken, sich verständlich zu machen und andere zu verstehen *[Eigenständigkeit/Verantwortung, 6]*					
4	**Inhalte***:* • Grundlagen der Analyse von Schadsoftware • Prozessorarchitekturen: x86, x64 • Assemblersprache • Compiler-Konstrukte auf Assembler-Ebene • Disassemblierung und Debugging von Code auf Assemblerebene • Analysemethoden und Werkzeuge • Windows Grundlagen: Speicherbild von Prozessen, Formate von ausführbaren Programmen. Laden und Ausführen von Programmen • Programmiertechniken von Malware: Code-Verschleierung, Emulation, Erkennung von Virtualisierung oder Debuggern • Statische und dynamische Analyse von Schadsoftware für die Windows-Plattform • Schutzmechanismen von audführbaren Programmen und deren Überwindung • Verhaltensanlyse von ausführbaren Programmen • Reverse Engineering von Python-basierter Malware					

	Empfohlene Literaturangaben: Eldad Eilam: Reversing: Secrets of Reverse Engineering, John Wiley & Sons, 2005 Michael Sikorski, Andrew Honig: Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press, 2012 Bruce Dang, Alexandre Gazet, Elias Bachaalany, Sebastien Josse: Practical Reverse Engineering, John Wiley & Sons, 2014
5	**Teilnahmevoraussetzungen:** Kenntnisse in einer Programmiersprache und in Rechnertechnik
6	**Prüfungsformen***:* Klausur 60 min, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur
8	***Verwendbarkeit des Moduls:*** IT Security
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. Martin Rieger Dozent(in): Prof. Dr. Martin Rieger
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.4.7 22600 – Netzwerk- und Systemsicherheit

Studiengang: IT Security
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Netzwerk- und Systemsicherheit						
Kennnummer 22600	**Workload** 150	**Modulart** P	**Studiensemester** 4. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Vorlesung & Übungen Netzwerk- und Systemsicherheit Praktikum Netzwerk- und Systemsicherheit	**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90h	**Credits (ECTS)** 5	
2	**Lehrform(en) / SWS:** Vorlesung und Übungen: 3 SWS Praktikum: 1 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:**					

	Kompetenz Wissen • Die Studierenden kennen den aktuellen Forschungsstand ausgewählter Forschungsbereiche in der Netzwerksicherheit *[Wissen, 6]*
	Die Studierenden können Forschungsfragestellungen der Netzwerksicherheit mit geeigneten Mechanismen und Methoden in Verbindung setzen und diese zur Bearbeitung der Fragestellung anwenden *[Systemische Fertigkeiten, 6]*
	Sozialkompetenz Die Studierenden sind in der Lage, sich mittels dem spezifischen Vokabular auszudrücken, sich verständlich zu machen und andere zu verstehen *[Kommunikation, 6]*
	Selbstständigkeit Die Studierenden sind in der Lage komplexe Fragestellungen, deren Bearbeitung auch tiefere Recherche erfordert, zu durchdringen und zur Lösung bekannte Ansätze weiterzuentwickelnd *[Lernkompetenz, 6]*
4	**Inhalte*:*** Die Vorlesung gliedert sich in drei Teile auf, die z.T. zeitlich überlappend durchgeführt werden: 1. Wiederholung und Vertiefung der Grundlagen und fortgeschrittenen Aspekte der Netzwerksicherheit. Dieser Teil wird im Rahmen einer Vorlesung absolviert und dient dazu Informatik Studenten ohne spezifischen IT Security Hintergrund die Grundlagen für die Bearbeitung des Referats und des Projekts zu vermitteln. 2. Ausarbeitung eines Referats über ein aktuelles Thema der Netzwerksicherheit (basierend auf aktuellen Konferenz- oder Journal Veröffentlichungen aus dem Bereich der Netzwerksicherheit). Dieser Teil dient dazu, an einem konkreten Beispiel den Aufbau einer wissenschaftlichen Arbeit zu erarbeiten und diese zu bewerten. Die Referate werden im Peer-Review Prozess von jeweils zwei Kommilitonen korrigiert und ähnlich zu einem Konferenzformat gehalten (1-tägige Blockveranstaltung). 3. Bearbeitung eines eigenen Projekts zu einer ausgewählten Forschungsfragestellung aus dem Bereich der Netzwerk- und Internetsicherheit. Dabei werden sowohl Ingenieursmethoden als auch analytische Methoden verwendet um die Fragestellung zu beantworten. Die Projektbearbeitung schließt mit einem Vortrag über die Ergebnisse ab (erneut im Konferenz-Format als Blockveranstaltung). Hier sollen selbständig wissenschaftliche Fragestellungen bearbeitet werden. Beispiele für die zu behandelnden Themen • Sicherheit moderner Kommunikationsprotokolle (HTTP/2, QUIC, P2P Protokolle, etc.) • Aktuelle Angriffe gegen Kommunikationsprotokolle • Protokolle zur Erreichung spezifischer Sicherheitsziele (Vertraulichkeit, Integrität, Verfügbarkeit, Anonymität, Pseudonymität) • Authentifikations- und Authorisierungsprotokolle • Sicherheit im industriellen Umfeld (Fertigung, Steuerung) • Analyse von Kommunikationsdaten zur Erkennung von Sicherheitsproblemen • Analyse verschlüsselter Verbindungen zur Klassifikation von Verkehr • Analyse von Log- Einträgen und anderweitig erfassten Ereignissen zur Erkennung und Klassifikation von Angriffen

	Empfohlene Literaturangaben: G. Schäfer, M. Roßberg: Netzsicherheit, 2. Auflage, dpunkt Verlag, 2014 C. Eckert: IT-Sicherheit, Konzepte-Verfahren-Protokolle, Oldenbourg-Verlag, 2011 R. Anderson, Security Engineering, Wiley, 2009 B. Schneier: Applied Cryptography. Protocols, Algorithms, and Source Code in C. Wiley, New York 1996.
5	**Teilnahmevoraussetzungen:** Die Studierenden besitzen Kenntnisse, Fertigkeiten und Erfahrungen in • Betriebssysteme • Netzwerke • Netzwerksicherheit • Programmierung in einer Hochsprache und einer Skriptsprache
6	**Prüfungsformen***:* Klausur 90 min, benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Benotete und unbenotete Leistungen; die studienbegleitenden Prüfungen, auf deren Grundlage Leistungspunkte erworben werden, sollen beschrieben sein. Sofern Module Prüfungsvorleistungen vorsehen (Semesterarbeiten, Exkursionsberichte, Hausarbeiten u.a.), müssen diese nach Art und Umfang beschrieben sein
8	***Verwendbarkeit des Moduls:*** IT Security
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Morgenstern, Prof. Dr. Rieger Dozent(in):
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.5 5. Semester

5.5.1 23000 – Projektmanagement

Studiengang: IT Security/Technische Informatik/Wirtschaftsinformatik
Semester: WS 2020/21
StuPO-Version: 17.2
Letzte Bearbeitung: 14.10.20

Version	Erstellt/geändert von Ammann/am 12.10.2020	Dokument	Freigabe am/von	Gültig ab WS 2020/21
1.0		Modulhandbuch_IT_Sec_fin		

Modul: Projektmanagement						
Kennnummer 23000	**Work-load** 75	**Modulart** P	**Studiensemester** 5	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Vorlesung Projektmanagement	**Sprache** Deutsch	**Kontakt-zeit** 2 SWS / 30 h	**Selbst-studium** 45 h	**Credits (ECTS)** 2,5	
2	**Lehrform(en) / SWS:** Projektmanagement: VL + Üb Umfang: 15x2 = 30 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Kenntnis über Inhalt von Projektplänen. *[Wissen, 6]* *Kompetenz Fertigkeiten* Erstellung eines Plans aus einer realen Aufgabenstellung. *[Beurteilungsfähigkeit, 6]* *Sozialkompetenz* Erstellung eines Projektplans anfangs im Team, später die Umsetzung in Einzelarbeit. *[Mitgestaltung, 5]* Es gibt Fragestunden bezüglich Aufgabenstellung. Studierende werden aufgefordert, ihre Ideen aus Teilen ihres entwickelten Projektplans zu präsentieren. *[Kommunikation, 5]* *Selbstständigkeit* Ideensammlung für Projektplan darf im Team erfolgen. Die Umsetzung ist allerdings eine Einzelarbeit. *[Eigenständigkeit/Verantwortung, 6]*						
4	**Inhalte*:*** Grundbegriffe und Grundlagen des Projektmanagements. Organisationsformen bei Projekten innerhalb von Firmen. Lebensphasen von Projekten. Projektmanagementformen: Klassisch, Agile. Wissensbereiche des Projektmanagements: Scope, Zeitplanung, Kostenplanung, Risikomanagement, Kommunikationsmanagement, Qualitätsmanagement, etc. Anwendung der Grundlagen an einem Fallbeispiel aus einem Projekt des Dozenten. Erklärung der Funktionsweise von Plagiatserkennung zur Kontrolle der Studienarbeiten. *Empfohlene Literaturangaben:* Skript der Dozenten mit entsprechenden Literaturangaben PMBOK Guide and Standards, Projekt Management Institute						
5	**Teilnahmevoraussetzungen:** Teamfähigkeit, Kommunikationsfähigkeit						
6	**Prüfungsformen***:* **Projektmanagement: Studienarbeit**						

7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Der Studierende sollte in der Lage sein, aus einer realen Aufgabenstellung einen kompletten Projektplan zu erstellen. Teile des Projektplans sind Scope, Kosten, Zeit, Risiken, Qualität etc.
8	***Verwendbarkeit des Moduls:*** Projektstudium
9	***Modulverantwortliche(r): Prof. Dr. Rembold*** Dozenten: Prof. Dr. Derk Rembold
10	***Optionale Informationen:*** keine

5.5.2 23600 – Datenbanken 2

Studiengang: IT Security/Technische Informatik/Wirtschaftsinformatik
StuPO-Version: 17.2

Semester: WS 2020/21

Letzte Bearbeitung: 14.10.20

Modul: Datenbanken 2						
Kennnummer 23600	**Workload** 150 h	**Modulart** P	**Studiensemester** 5		**Dauer** 1 Semester	**Häufigkeit** WS und SS
1	**Lehrveranstaltung(en)** Vorlesung & Übungen Datenbanken 2		**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** Vorlesung & Übungen: 4 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen die Implementierungstechniken zur Formulierung hoch komplexer Anfragen auf Basis eines objekt-relationalen Datenbanksystems in SQL, die wichtigsten Verfahrensweise des „ETL“ (Extract, Transform, Load),die Rolle der Dimension „Zeit“ im Hinblick auf die langfristige Speicherung in einem Data-Warehouse, den Separationsprozess von Daten des operativen Geschäfts gegenüber den (verdichteten) Daten von Data Warehouse-Anfragen, die „Themenorientierung“ im Hinblick auf die Auswertung komplexer Auswertungen sowie deren Abgrenzung zur Prozessorientiertheit operativer Aufgaben *[Wissen, 6]* *Kompetenz Fertigkeiten* Fertigkeiten Die Studierenden sind in der Lage ein Datenmodell für Datawarehouse-Anwendungen zu konzipieren,					

	komplexe Datenbankanfragen auf Basis des (objekt-) relationalen Datenmodells zur Entscheidungs-unterstützung in Bereichen des Controlling oder der Strategischen Unternehmensführung zu formulieren, mehrdimensionale Wissensbasen im Sinne einer OLAP -Architektur aufzubauen, einfache und komplexe Zusammenhänge zu Unternehmensdaten im Sinne eines Business Analytics zu bewerten *[Instrumentelle Fertigkeiten, 6]* Die Studierenden sind fähig Zusammenhänge zwischen nicht antizipierten Daten durch Data Mining-Techniken zu erkennen, Analysen über zeitliche Veränderungen und Entwicklungen in einem Data-Warehouse anzustellen, Data Marts als anwendungsspezifische Data Warehouse-Bereiche aufzubauen, den Integrationsprozess für große, unterschiedlich strukturierte und verteilte Datenbasen hin zu einer vereinheitlichten Datenbasis für komplexe, mehrdimensionale Auswertungen vorzunehmen geeignete Patterns in den verschiedenen Phasen der Software-entwicklung zu erkennen und umzusetzen *[Systemische Fertigkeiten, 6]*
	Sozialkompetenz -- /Kompetenzausprägung wählen*:* nicht relevant
	Selbstständigkeit /Kompetenzausprägung wählen *]*
4	**Inhalte*:*** Bewertung operativer und analytischer Datenbanken Konzeption von Datenmodellen für Data Warehouses Anwendung von Optimierungstechniken für sehr große Datenbanken Anwendung multidimensionaler Auswertungen Implementierung verteilter Transaktionen auf Basis eines TP-Monitor-basierenden Applikationsservers Aufbau und Arbeitsweise von In-memory-Datenbanken am Beispiel SAP/HANA bzw. Oracle 18g Kurzer Überblick des Modulinhalts bzw. der Inhalte der Lehrveranstaltungen
	Empfohlene Literaturangaben: https://docs.oracle.com/cd/B28359_01/server.111/b28310/ds_txns001.htm#ADMIN12211 https://docs.oracle.com/cd/B19306_01/server.102/b14231/ds_txns.htm Farkisch, Kiumars: Data-Warehouse-Systeme kompakt, Xpers.press, 2011 Bauer, A.; Günzel, H.: Data-Warehouse-Systeme: Architektur, Entwicklung, Anwendung, dpunkt, 2008 Holten, R.: Entwicklung einer Modellierungstechnik für Data Warehouse -Fachkonzepte, Proc. MobIS Fachtagung, Münster, 2000 Kempfer, H.-G.; Mehanna, W., Unger, C.: Business Intelligence – Grundlagen und praktische Anwendungen, Vieweg, 2. Auflage, 2006 https://2bm.com/sap-s-4hana-always-on-business-functions/

	Müller, R.M, Lenz, H.-J.: Business Analytics, Springer Vieweg 2013 Kaiser, C.: Business Intelligence 2.0, Springer Gabler, 2012 Kemper, H.-G., Baars, H., Mehanna, W.: Business Intelligence -Grundlagen und praktische Anwendungen, 3. Ausgabe, Springer Vieweg 2010Klein, A., Gräf, J.: Reporting und Business Intelligence, Haufe 2014 http://www.oracle.com/technetwork/database/features/storage/database-11gr2-managing-storage-whi-131523.pdf
5	**Teilnahmevoraussetzungen:** Zulassung zu einem der Informatik-Studiengänge BSc. an der HS Albstadt Sigmaringen Profunde Kenntnisse auf in vorbereitenden Veranstaltungen des Grundstudiums der Studiengänge Wirtschaftsinformatik/IT-Security bzw. Technische Informatik, beispielsweise 12000 Programmierung 1,14500 Programmierung 2, 15000 Betriebssysteme und Netzwerke 1, 21000 Datenbanken 1 Voraussetzungen für die Teilnahme beschreiben; Außerdem beschreiben, wie sich der Studierende vorbereiten kann (u.a. Literaturangaben, Lehr- und Lernprogramme)
6	**Prüfungsformen***:* Mündliche Prüfung, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreiche Teilnahme an der mündlichen Prüfung
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik Wahlrichtung: Application Development
9	***Modulverantwortliche(r):*** Prof. Dr. J. Röhrle Dozent: Prof. Dr. J. Röhrle
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.5.3 23700 – GUI-Development (Graphical User Interface-Development)

Studiengang: IT Security/Technische Informatik/Wirtschaftsinformatik
Semester: WS 2020/21
StuPO-Version: 17.2
Letzte Bearbeitung: 13.03.2020

Modul: GUI-Development (Graphical User Interface-Development)					
Kennnummer 23700	**Work-load** 150 h	**Modulart** P	**Studiensemester** 5	**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)**	**Sprache** Deutsch	**Kontakt-zeit**	**Selbst-studium** 90 h	**Credits (ECTS)** 5

	Vorlesung & Übungen GUI-Development Praktikum GUI-Development		4 SWS / 60 h		
2	**Lehrform(en) / SWS:** Vorlesung & Übungen: 3 SWS Praktikum: 1 SWS				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen die unterschiedlichen Entwurfs-paradigmen für Desktop-, Web- und Mobile GUIs (ergonomische Sicht). Sie kennen die verschiedenen MVC-Architekturen für Desktop- und mobile Applikationen, sowie Event-Verarbeitungsmechanismen. Sie kennen Aufbau und Funktionsweise typischer Widgets für Desktop-Anwendungen, sowie für für mobile Anwendungen (beispielsweise Android) *[Wissen, 6]* *Kompetenz Fertigkeiten* Die Studierenden sind in der Lage, eigenständig komplexere Workflows in Form von Desktop-GUIs und in Form mobiler GUIs auf Basis von gegebenen Nutzer-Anforderungen zu entwickeln. Sie können gängige Prozessmodelle in der Softwareentwicklung für die GUI-Entwicklung anwenden und andere Regelwerke (z. B. StyleGuides) im Software-entwicklungsprozess adäquat an die gegebene Situation anpassen und anwenden Sie können geeignete Patterns in den verschiedenen Phasen der Software-entwicklung erkennen und umsetzen *[Instrumentelle Fertigkeiten, 6]* Die Studierenden sind in der Lage, auch für sie neue Problemstellungen in Workflows abzubilden und als Desktop-GUI oder mobile GUI umzusetzen. *[Systemische Fertigkeiten, 6]* Die Studierenden können softwaretechnische Lösungen im Umfeld der GUI-Entwicklung architektonisch und codetechnisch beurteilen und einordnen. *[Beurteilungsfähigkeit, 6]* *Sozialkompetenz* Die Studierenden können in Absprache mit Kunden GUIs mit ansprechender Usability und UX für bestimmte Zielgruppen umsetzen. *[Kommunikation, 6]* *Selbstständigkeit* Die Studierenden sind in der Lage, sich im sehr schnelllebigen Umfeld der GUI-Entwicklung selbstständig auf neue Technologien und Frameworks einzustellen und sich diese rasch und selbstständig anzueignen. *[Reflexivität, 6]* Sie sind in der Lage, sich auch weitere Frameworks im GUI-Umfeld, sowie weitere Widget-Sets eigenständig anzueignen. *[Lernkompetenz, 6]*				
4	**Inhalte*:***				

	Ergonomische Sicht / Anwendersicht der GUI-Entwicklung: Usability und User-Experience Arten von GUIs Entwurfsparadigmen für GUIs (Ergonomische Sicht) Verschiedene aktuelle StyleGuides Unterschiede Desktop-Oberflächen, Web-Oberflächen, Mobile Anwendungen Widgets, Widget-Sets Weiterführung und Verallgemeinerung von GUI-Architekturen: verschiedene MVC-Umsetzungen, Thread-Aufteilung, Eventmodelle Entwicklung von Desktop-GUIs mit einem ausgewählten Widget-Set/Framework Entwicklung mobiler GUIs mit einem ausgewählten Framework
	Empfohlene Literaturangaben: *Eclipse rcp (rich client platform) - tutorial. L. Vogel, https://www.vogella.com/tutorials/EclipseRCP/article.html, 2020.* *UX-Methoden praxisnah erklärt. J. Jacobsen et al., Rheinwerk, 2019* *Android Studio 3.5 Development Essentials - Java Edition: Developing Android 10 (Q) Apps Using Android Studio 3.5, Java and Android Jetpack. N. Smyth, Payload-Verlag, 2019* *Material design. developer.android.com, https://material.io/design/introduction/, 2020* *Homepage der eclipse foundation. Eclipse Foundation, http://www.eclipse.org, 2020.* *Mobile Design Patterns Gallery: UI Patterns for Smartphone Apps, T. Neil, O'Reilly, 2014* *Designing the User Interface, B. Shneiderman, Addison-Wesley, 2013* *Lehrbuch der Softwaretechnik: Entwurf, Implementierung, Installation und Betrieb. H. Balzert, Spektrum Akademischer Verlag, 3. Aufl., 2012.*
5	**Teilnahmevoraussetzungen:** Empfohlen: Programmierung 1 und 2
6	**Prüfungsformen***:* GUI-Development: Klausur Praktikum GUI-Development: Laborarbeit (unbenotet)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur, Bestandenes Praktikum
8	***Verwendbarkeit des Moduls:***

	IT Security, Technische Informatik, Wirtschaftsinformatik Wahlrichtung: Application Development Wahlpflichtfach für die anderen Vertiefungsrichtungen
9	***Modulverantwortliche(r):*** Prof. Dr. Ute Matecki Dozent: Prof. Dr. Ute Matecki
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.5.4 23800 – Softwarearchitektur

Studiengang: IT Security/Technische Informatik/Wirtschaftsinformatik
Semester: WS 2020/21
StuPO-Version: 17.2
Letzte Bearbeitung: 14.10.20

Modul: Softwarearchitektur						
Kennnummer 23800	**Work-load** 150 h	**Modulart** P	**Studiensemester** 5	**Dauer** 1 Semester		**Häufigkeit** WS und SS
1	**Lehrveranstaltung(en)** Vorlesung Software-Architektur Praktikum Software-Architektur		**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** Vorlesung & Übungen: 3 SWS Praktikum: 1 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen die Bedeutung und Notwendigkeit der Betrachtung und Entwicklung von Software-Architekturen für komplexe Software-Produkte, wichtige Architekturmuster und –Stile, Techniken zur Implementierung komponentenbasierter Software-Entwicklung auf Basis von Applikationsservern *[Wissen, 6]*					
	Kompetenz Fertigkeiten Die Studierenden sind in der Lage Komponenten im Sinne einer Applikationsserver-orientierten Architektur zu entwerfen und zu implementieren, verteilte Transaktionsarchitekturen zu entwerfen und zu implementieren,					

	verschiedene Frontend- und Backend-Architekturen zu entwickeln und zu implementieren *[Instrumentelle Fertigkeiten, 6]*
	Selbstständigkeit Die Studierenden sind fähig selbständig komplexere Aufgabenstellungen im Sinne einer komponentenorientierten Software-Architektur zu modellieren und umzusetzen *[Eigenständigkeit/Verantwortung, 6]*
4	**Inhalte*:*** Aufbau eines komponentenorientierten, TP-Monitor-basierten Applikationsservers Implementierung komplexer (Datenbank-) Anwendungen auf Basis der Java Persistence Architektur
	Empfohlene Literaturangaben: https://www.tutorialspoint.com/software_architecture_design/component_based_architecture.htm Syperski, C.: Component Software: Beyond Object-Oriented Programming (Addison-Wesley Component Software), 2011 Andresen, A.: Komponentenbasierte Softwareentwicklung mit MDA, UML 2 und XML. Hanser, 2. Auflage, 2004,ISBN-13: 978-3446229150 Eilebrecht, K., Starke, G.: Patterns kompakt: Entwurfsmuster für effektive Software-Entwicklung. Spektrum Akademischer Verlag, 3. Auflage, 2010, ISBN-13: 978-3827425256 Erl, T.: SOA: Design Patterns. Prentice Hall International, 2008, ISBN-13: 978-0136135166Erl, T.: SOA: Entwurfsprinzipien für service-orientierte Architektur. Addison-Wesley, 2008, ISBN-13: 978-3827326515 Fowler, M. et al.: Patterns of Enterprise Application Architecture. mitp, 2003, ISBN-13: 978-3826613784 Gamma et al.: Entwurfsmuster: Elemente wiederverwendbarer objektorientierter Software. Addison-Wesley, Neuauflage, 2010, ISBN-13: 978-3827330437 Gharbi, M.: Basiswissen für Softwarearchitekten: Aus- und Weiterbildung nach iSAQB-Standard zum Certified Professional for Software Architecture - Foundation Level. dpunkt.verlag, 1. Auflage, 2012, ISBN-13: 978-3898647915
5	Teilnahmevoraussetzungen: Zulassung zu einem der Informatik-Studiengänge BSc. an der HS Albstadt Sigmaringen Profunde Kenntnisse auf in vorbereitenden Veranstaltungen des Grundstudiums der Studiengänge Wirtschaftsinformatik/IT-Security bzw. Technische Informatik, beispielsweise 12000 Programmierung 1,14500 Programmierung 2, 15000 Betriebssysteme und Netzwerke 1, 21000 Datenbanken 1
6	**Prüfungsformen***:* Mündliche Prüfung, Dauer 20 min., benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreiche Teilnahme an der mündlichen Prüfung

8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik Wahlrichtung: Application Development
9	***Modulverantwortliche(r):*** Prof. Dr. Jörg Röhrle Dozent: Prof. Dr. Jörg Röhrle
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.5.5 23100 – Unternehmenskonzepte / Digitale Fabrik

Studiengang: IT Security/Technische Informatik/Wirtschaftsinformatik
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Unternehmenskonzepte / Digitale Fabrik						
Kennnummer 23100	**Work-load** 150	**Modulart** P	**Studiensemester** 5	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Unternehmenskonzepte / Digitale Fabrik	**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5	
2	**Lehrform(en) / SWS:** Unternehmenskonzepte / Digitale Fabrik: Vorlesung, Umfang: 15x4 = 60 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Entwicklung eines Konzepts und Systems aus dem Bereich Industrie 4.0 über Fachbereichsgrenzen hinweg. *[Wissen, 6]* *Kompetenz Fertigkeiten* Der Studierende programmiert Schnittstellen für ein ERP, um Informationen daraus weiterzuverarbeiten. Es werden Protokolle angewendet (MQTT, OPCUA), um Informationen aus dem ERP weiter zu verteilen *[Instrumentelle Fertigkeiten, 3]* *Sozialkompetenz* Teams bekommen Aufgabenstellung, die während des Semesters bearbeitet werden. *[Team-/Führungsfähigkeit, 6]*						

	Jedes Teammitglied bekommt innerhalb des Teams eine Aufgabe gestellt, welcher im Laufe des Semesters in ein Produkt integriert wird. *[Mitgestaltung, 6]* Jede Woche findet ein Meeting statt, bei dem der Status kommuniziert wird und die weiteren Schritte geplant werden. *[Kommunikation, 6]*
	Selbstständigkeit Teams organisieren sich selbst, und erstellen eigenständig Projektpläne. *[Eigenständigkeit/Verantwortung, 6]*
4	**Inhalte*:*** Steuerung der digitalen Fabrik Komponenten der digitalen Fabrik, u.a. Steuerungen für Maschinen und Anlagen, Sensoren und Aktoren, Netzwerke und Busse, Informations- und Kommunikationssysteme, Mensch-Maschine Schnittstellen, Autoidentifikation. Unternehmenskonzepte Methoden um Planungsprozesse zu beschleunigen und Kosten zu senken, Vermeidung von Planungsfehlern und Prozesssicherung durch geeignete Simulationsverfahren, Beherrschung komplexer Produkt- und Prozessstrukturen, Standardisierung von Methoden und Prozessen, Schnittstellen zwischen virtuellen Modelle und realen Prozessen Interaktion, Kommunikation und Datenaustausch zwischen den Produktionskomponenten und Produkten, Anpassung der Betriebsorganisation an die Erfordernisse der digitalen Fabrik, lernende und selbstoptimierende Organisation,
	Empfohlene Literaturangaben: VDI-Richtlinie 4499, Blatt 1: Digitale Fabrik – Grundlagen, VDI-Gesellschaft Fördertechnik Materialfluss Logistik, 2008, Schack, R.: Methodik zur bewertungsorientierten Skalierung der Digitalen Fabrik, Kühn, W.: Fabriksimulation für Produktionsplaner, Bullinger, H.-J.: Einführung in das Technologiemanagement, B.G. Teubner Verlag, Stuttgart. Kühn, W.: Fabriksimulation für Produktionsplaner, Bullinger, H.-J.: Einführung in das Technologiemanagement, B.G. Teubner Verlag, Stuttgart.
5	**Teilnahmevoraussetzungen:** Keine. Hilfreich sind jedoch Grundkenntnisse der Betriebsabläufe
6	**Prüfungsformen***:* **Unternehmenskonzepte / Digitale Fabrik: Präsentation 15 min., Mündliche Prüfung 20 min., benotet**
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Der Studierende soll in der Lage sein, ein technisches Projekt aus dem Bereich Industrie 4.0 zu planen und zu bearbeiten. Teil des Projekts soll der Zugriff von Informationen aus ERP enthalten. Ein weiterer Teil soll die Verarbeitung der Informationen und die Steuerung eines industriellen Prozesses enthalten.

8	***Verwendbarkeit des Moduls:*** PM in B.Eng. Technische Informatik (CPS) PM in B.Eng. IT-Security (CPS) PM in B.Eng. Wirtschaftsinformatik (CPS) Wahlrichtung: Cyber-Physical Systems
9	***Modulverantwortliche(r):*** Prof. Dr. Derk Rembold, Bernd Stauss Dozenten: Prof. Dr. Derk Rembold, Prof. Dr. Bernd Stauss
10	***Optionale Informationen:*** Dieses Fach ist insbesondere für Studierende der Wirtschaftsinformatik interessant, da es hier um den Einsatz von ERP geht und es viele Informationen aus ERP Systeme zu verarbeiten gilt.

5.5.6 23200 – Verteilte Systeme (Technik)

Studiengang: IT Security/Technische Informatik/Wirtschaftsinformatik
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Verteilte Systeme (Technik)						
Kennnummer 23200	**Work-load** 150 h	**Modulart** P	**Studiensemester** 5	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Vorlesung Verteilte Systeme (Technik) Praktikum Verteilte Systeme (Technik)	**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5	
2	**Lehrform(en) / SWS:** Unternehmenskonzepte / Digitale Fabrik: Vorlesung, Umfang: 15x4 = 60 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Dem Studierenden sind Systeme und Methoden zur Verteilung von Informationen über Rechnergrenzen hinweg bekannt. *[Wissen, 6]*					
	Kompetenz Fertigkeiten Der Studierende kann verschiedene Kommunikationssysteme anwenden und beispielhaft an verteilten Rechnersystemen austesten. *[Instrumentelle Fertigkeiten, 6]*					
	Sozialkompetenz Der Studierende ist in der Lage technische Probleme bei der Umsetzung zu kommunizieren und Hilfestellungen zu erfragen. *[Kommunikation, 6]*					

	Selbstständigkeit Aufgaben werden vergeben und diese werden bis Semesterende bearbeitet. *[Eigenständigkeit/Verantwortung, 6]*
4	**Inhalte*:*** Vorlesung & Übungen Clouddienste: SaaS, PaaS, IaaS Verteilte Software: REST, SOAP, OPCUA, MQTT etc. Softwareorchestrierung: Docker Dienste: Namensdienst, Transaktionsdienst, Zeitdienst und Sicherheitsdienst Softwaremuster für verteilte Systeme: Einsatz, Struktur, Verhalten, Entwurf, Konstruktion, Varianten der Muster Client-Dispatcher-Server, Forward-Receiver, Proxy, Observer, Layers, Broker, Model-View-Controller. Vernetzte Systeme in Fahrzeugen: CAN: Protokoll, Kommunikationsmatrix LIN: Protokoll, Architektur, Botschaften, Schedule FlexRay: Protokoll, Architektur Praktikum Realisierung eines REST Servers Realisierung einer MQTT Applikation Einsatz von Docker beim REST Server und MQTT Applikation
	Empfohlene Literaturangaben: Buschmann, F. u.a.: Pattern - Oriented Software Architecture: A System of Patterns; Zimmermann, W.; Schmidgall, R.: Bussysteme in der Fahrzeugtechnik, Protokolle und Standards, 2. Vieweg. Reißenweber, B.: Feldbussysteme zur industriellen Kommunikation, Oldenbourg Industrieverlag München.
5	**Teilnahmevoraussetzungen:** Programmierkenntnisse in Python oder C++.
6	**Prüfungsformen***:* Verteilte Systeme (Technik): Klausur 90 min., benotet Prakt. Verteilte Systeme (Technik): Laborarbeit unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Der Studierende muss in der Lage sein, verteilte Software Produkte und ihre Einsatzgebiete zu benennen. Er soll Softwaremuster kennen, und verteilte Software selbst programmieren. Busprotokolle, eingesetzt in Fahrzeugen, müssen benannt und erklärt werden können.
8	***Verwendbarkeit des Moduls:*** PM in B.Eng. Technische Informatik (CPS) PM in B.Eng. IT-Security (CPS) PM in B.Eng. Wirtschaftsinformatik (CPS) Wahlrichtung: Cyber-Physical Systems
9	***Modulverantwortliche(r):***

	Prof. Dr. Derk Rembold Dozenten: Prof. Dr. Derk Rembold
10	***Optionale Informationen:*** keine

5.5.7 23300 – Intelligente Lernende Systeme

Studiengang: IT Security/Technische Informatik/Wirtschaftsinformatik
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Intelligente Lernende Systeme						
Kennnummer 23300	**Work-load** 150	**Modulart** P	**Studiensemester** 5	**Dauer** 1 Semester		**Häufigkeit** WS und SS
1	**Lehrveranstaltung(en)** Intelligente Lernende Systeme		**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** Vorlesung, Umfang 15x3 = 45 SWS Praktikum, Umfang 15x1 = 15 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Breite und tiefe Kenntnisse der grundlegenden Begriffe, Konzepte und Verfahren im Bereich Künstliche Intelligenz und Maschinelles Lernen *[Wissen, 6]* *Kompetenz Fertigkeiten* Beherrschung der Anwendung von Methoden und Verfahren der Künstlichen Intelligenz und des Maschinellen Lernens zur Implementierung intelligenter Lernender Systeme *[Instrumentelle Fertigkeiten, 6]* *Sozialkompetenz* Fähigkeit Sachverhalte im Bereich der Künstlichen Intelligenz und des Maschinellen Lernens präzise zu kommunizieren und darüber zu argumentieren *[Kommunikation, 6]* *Selbstständigkeit* Fähigkeit sich selbständig neue, weiterführende bzw. noch nicht explizit behandelte Konzepte und Verfahren im Bereich der Künstlicher Intelligenz und des Maschinellen Lernens anzueignen *[Lernkompetenz, 6]*						

	Fähigkeit Sachverhalte im Bereich der Künstlicher Intelligenz und des Maschinellen Lernens mit Hilfe der beschriebenen Fertigkeiten eigenständig und eigenverantwortlich zu analysieren und zu beurteilen *[Eigenständigkeit/Verantwortung, 6]*
4	**Inhalte*:*** (1) Intelligente Steuerung und Planung: Methoden aus der Künstlichen Intelligenz, Modelle von Intelligenten Agenten, Diskrete Zustandsraumbeschreibung, A*-Algorithmus, Dynamisches Programmieren (2) Konzepte und Methoden des Maschinellen Lernens: Fehlerfunktion, Lernen durch Minimieren des Fehlers, Modell-Evaluation und -Selektion; Lineare Modelle für Regression und Klassifikation, Neuronale Netze, Backpropagation Algorithmus, Deep Learning, Reinforcement Learning, Clustering, Merkmalsextraktion (3) Kognitive Architekturen: Technische und biologische Systeme, Autonomes Lernen von Zustandsräumen und Situationserkennern
	Empfohlene Literaturangaben: Russell S., Norvig, P.: Künstliche Intelligenz, Pearson; Ertel W.: Grundkurs Künstliche Intelligenz, Springer-Vieweg; Bishop, C: Pattern recognition and machine learning, Springer; S.Raschka: Python Machine Learning. Packt Publishing; W.McKinney: Python for Data Analysis. O'Reilly. F.Chollet: Deep Learning mit Python.
5	**Teilnahmevoraussetzungen:** Grundlagen Mathematik: Mathematik 1 + 2 Grundlagen Programmieren in Python: Programmieren 1 + 2
6	**Prüfungsformen***:* Klausur, 90 min., benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** - Bestehen der Klausur - Bestehen des Praktikums (durch Abgabe von Praktikumsausarbeitungen)
8	***Verwendbarkeit des Moduls:*** PM in B.Eng. Technische Informatik (CPS) PM in B.Eng. IT-Security (CPS) PM in B.Eng. Wirtschaftsinformatik (CPS) Wahlrichtung: Cyber-Physical Systems
9	***Modulverantwortliche(r):*** Prof. Dr. Andreas Knoblauch Dozenten: Prof. Dr. Andreas Knoblauch, Prof. Dr. Walter Hower
10	***Optionale Informationen:***

	Empfohlener Zeitaufwand: - Summe: 150 h - Vorlesung: 15 x 3 = 45 h - Vor- und Nachbereitung der Vorlesung: 30 h - Bearbeitung von Übungsaufgaben: 15h - Praktikum: 15 x 1 = 15 h - Vor- und Nachbereitung des Praktikums: 25h - Prüfungsvorbereitung und Prüfung: 20 h

5.5.8 23900 – Big Data

Studiengang: IT Security/Technische Informatik/Wirtschaftsinformatik
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

<table>
<tr><td colspan="7">Modul: Big Data</td></tr>
<tr><td colspan="2">Kennnummer
23900</td><td>Work-load
75 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
5</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung & Übungen Big Data</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
2 SWS / 30 h</td><td>Selbst-studium
45 h</td><td>Credits (ECTS)
2,5</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung & Übungen: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden
- kennen Systeme und Techniken für die parallele Datenverarbeitung
- kennen die Aufgabenstellungen aus dem Themengebiet von Big Data [Wissen, 6]</td></tr>
<tr><td></td><td colspan="7">Kompetenz Fertigkeiten
Die Studierenden wissen welche BigDatasysteme es gibt und wie ein BigDatasystem aufgebaut ist. [Instrumentelle Fertigkeiten, 6]</td></tr>
<tr><td></td><td colspan="7">Sozialkompetenz
Lernergebnisbeschreibung mit einer bestimmten Kompetenz /Kompetenzausprägung wählen /Niveaustufe wählen</td></tr>
<tr><td></td><td colspan="7">Selbstständigkeit
Lernergebnisbeschreibung mit einer bestimmten Kompetenz /Kompetenzausprägung wählen /Niveaustufe wählen</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:</td></tr>
</table>

	- Überblick zu No-SQL-Datenbanken - Überblick zu Graphendatenbanken - Architekturen für verteiltes und paralleles Datenmanagement und Datenverteilung - Verteilte Anfragebearbeitung - Clustering, Map Reduce, YARN, Tez - Verteilte Datenbanken - Vertikale/horizontale Fragmentierung - Fragmentierungstransparenz - Transaktionskontrolle - Frameworks für Skalierung und Parallelisierung der Datenzugriffe am Beispiel von Apache Hadoop, Spark und verteilten RDBMS
	Empfohlene Literaturangaben: Ramon Wartala: Hadoop: Zuverlässige, verteilte und skalierbare Big-Data-Anwendungen, Open Source PressEdward Capriolo, Dean Wampler, Jason Rutherglen: Programming Hive, O'ReillyTom White. Hadoop. The definitive Guide, O' ReillyUni Hildesheim: MySQL Cluster, http://www.uni-hildesheim.de/rz/DOC/mysql_refman-5.1-de.html/ndbcluster.htmlArun C. Murthy; Vinod Kumar Vavilapalli; Doug Eadline; Joseph Niemiec; Jeff Markham: Apache Hadoop (YARN), Pearson, 2014
5	**Teilnahmevoraussetzungen:** Voraussetzungen für die Teilnahme beschreiben; Außerdem beschreiben, wie sich der Studierende vorbereiten kann (u.a. Literaturangaben, Lehr- und Lernprogramme)
6	**Prüfungsformen***:* Klausur 60 min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Benotete und unbenotete Leistungen; die studienbegleitenden Prüfungen, auf deren Grundlage Leistungspunkte erworben werden, sollen beschrieben sein. Sofern Module Prüfungsvorleistungen vorsehen (Semesterarbeiten, Exkursionsberichte, Hausarbeiten u.a.), müssen diese nach Art und Umfang beschrieben sein
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik Wahlrichtung: IT-Management
9	***Modulverantwortliche(r):*** Prof. Dr. Thomas Eppler Dozent: Prof. Dr. Thomas Eppler
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.5.9 24000 – IT-Management

Studiengang: IT Security/Technische Informatik/Wirtschaftsinformatik
Semester: WS 2020/21
StuPO-Version: 17.2
Letzte Bearbeitung: 14.10.20

Modul: IT-Management

Version	Erstellt/geändert von Ammann/am 12.10.2020	Dokument	Freigabe am/von	Gültig ab WS 2020/21
1.0		Modulhandbuch_IT_Sec_fin		

Kennnummer **24000**	**Workload** 150 h	**Modulart** P	**Studiensemester** 5	**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)** Vorlesung & Übungen IT-Management	**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5

2 **Lehrform(en) / SWS:**
Vorlesung & Übungen: 4 SWS

3 **Lernergebnisse (learning outcomes), Kompetenzen:**

Kompetenz Wissen

Die Studierenden
- kennen die Historie und Prinzipien von Unternehmensstrategien
- kennen Zielstellung, Zielgruppen und den Aufbau von IT-Strategien
- kennen Methoden und Verfahren der IT-Planung und das Zusammenwirken mit den Interessengruppen der Unternehmung (interne und externe Stakeholder)
- kennen Instrumente zur Planung, Steuerung und Kontrolle von IT-Bereichen im Unternehmen
- kennen innovative Geschäftsmodelle der Plattformökonomie aus Sicht der IT

[Wissen, 6]

Kompetenz Fertigkeiten

Die Studierenden
- können den Einsatz der Informationstechnologie im Kontext der strategischen Ausrichtung des Unternehmens bewerten und einordnen
- sind in der Lage, systematisch und methodisch Geschäftsmodelle und Unternehmensstrategien zu konzipieren
- können IT-Strategien systematisch und methodisch – im Kontext der Unternehmensstrategie – entwickeln
- können die Herausforderungen des IT-Management auf der gesamten organisatorischen Unternehmensebene beschreiben
- können die Auswirkungen von Digitalisierung und speziell der Plattformökonomie auf das IT-Management skizzieren
- beherrschen die differenzierte Einordnung von IT-Sicherheit und IT-Governance, Risk and Compliance Management (IT-GRC) in den Kontext des IT-Managements

[Instrumentelle Fertigkeiten, 6]

Die Studierenden
- *können in umfangreichen, realitätsnahen Fallstudien die Unternehmenssituation analysieren, strategische Aspekte vor dem Hintergrund von Branche sowie Unternehmensumwelt bewerten, die Herausforderungen für IT-Organisationen und das IT-Management systematisieren*
- *können weiterhin – durch zielgerichtete Abstraktionstechniken – Grundzüge von IT-Strategien und Maßnahmenkataloge für das IT-Management entwickeln*

[Systemische Fertigkeiten, 6]

Sozialkompetenz

	Die Studierenden sind in der Lage, die komplexen Fallstudien zum IT-Management in einem Team zu bearbeiten und die Teamarbeit selbst zu organisieren *[Team-/Führungsfähigkeit, 6]* *Zielgruppenorientierter Einsatz von Präsentationsmethoden und Dokumentationstechniken [Kommunikation, 6]*
	Selbstständigkeit Die Studierenden können tiefergehende Problemstellungen auch in komplexen Fallstudien erkennen, methodisch bearbeiten, lösungs- sowie kontextbezogen recherchieren, auf das Wesentliche im Managementkontext abstrahieren und zielgerichtet lösen *[Eigenständigkeit/Verantwortung, 6]*
4	**Inhalte*:*** Die Vorlesung vermittelt Kenntnisse in der Entwicklung von IT-Strategien im Kontext von Unternehmensstrategien und dem IT-Management in der Bandbreite organisatorischer, technologischer, personeller und kaufmännischer Aspekte: • Begriffssysteme für Strategie- und Managementlehre • Entwicklung von Unternehmensstrategien • Konzeption von IT-Strategien • Referenzmodelle für das IT-Management • IT-Reifegradmodelle • Interessengruppen (Stakeholder) und interne sowie externe Kunden • Aufgaben und Verantwortung des Chief Information Officer (CIO) und des IT-Managements • Business Alignment und Business Enabling • IT-Sicherheit • IT Governance, Risk and Compliance Management (IT-GRC) • IT-Service- und Prozessmanagement • IT-Ressourcenmanagement • IT-Partnermanagement: Relationship Management und Sourcing-Strategien • IT-Projekt- und Projektportfoliomanagement • IT-Planung und IT-Controlling • Umgang mit Schatten-IT • Innovative Geschäftsmodelle in der Plattformökonomie aus Sicht der IT
	Empfohlene Literaturangaben: Hofmann, J./Schmidt, W.: Masterkurs IT-Management - Grundlagen,Umsetzung und erfolgreiche Praxis für Studenten und Praktiker. 2. Auflage, Vieweg und Teubner, 2010 Tiemeyer, E.: Handbuch IT-Management: Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, 7. Auflage, Hanser Verlag, 2020 Friedrich, K./Malik, F./Seiwert, L.: Das große 1x1 der Erfolgsstrategie: EKS® – Die Strategie für die neue Wirtschaft, 25. Auflage, Gabal, 2009 Oswald G./Krcmar, H.: Digitale Transformation: Fallbeispiele und Branchenanalysen (Informationsmanagement und digitale Transformation), Springer Gabler, 2018 Krcmar, H.: Informationsmanagement, 6. Auflage, Springer, 2015 Resch, O.: Einführung in das IT-Management - Grundlagen, Umsetzung, Best Practice,

	4. Auflage, Erich Schmidt Verlag, 2016 Hermann, Ulrich: Digitalisierung im Industrieunternehmen: Die Chancen der digitalen Ökonomie der Dinge erkennen, entwickeln und erfolgreich umsetzen, Apprimus, 2019 Zimmermann, S.: Der Umgang mit Schatten-IT in Unternehmen: Eine Methode zum Management intransparenter Informationstechnologie Hanschke, I.: Strategisches Management der IT-Landschaft: Ein praktischer Leitfacen für das Enterprise Architecture Management, 3. Auflage, Hanser Verlag, 2013 Kersten, H./Klett, G./Reuter, J./Schröder, K.-W.: IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Controls, 4. Auflage, Springer Vieweg, 2019 Sowa, A.: „Management der Informationssicherheit: Kontrolle und Optimierung“, Springer Vieweg, 2017
5	**Teilnahmevoraussetzungen:** Entweder Wahl der Studienwahlrichtung „IT-Management” im Rahmen der Studiengänge Wirtschaftsinformatik, IT Security und Technische Informatik oder Wahl als Wahlpflichtmodul
6	**Prüfungsformen***:* Klausur 90 min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreiches Bestehen der Klausur
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik Wahlrichtung: IT-Management
9	***Modulverantwortliche(r):*** Prof. Dr. Nils Herda Dozent: Prof. Dr. Nils Herda
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.5.10 24100 – IT-Consulting

Studiengang: IT Security/Technische Informatik/Wirtschaftsinformatik
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: IT-Consulting						
Kennnummer 24100	**Workload** 150 h	**Modulart** P	**Studiensemester** 5		**Dauer** 1 Semester	**Häufigkeit** WS und SS
1	**Lehrveranstaltung(en)** Vorlesung & Übungen IT-Consulting		**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:**					

	Vorlesung & Übungen: 4 SWS
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden • kennen Zielstellung und Aufgaben der Unternehmensberatung • kennen die Beratungsleistung im Kontext strategischer Initiativen im Unternehmen • kennen die Problemlösung als originäre Beratungsleistung, speziell im Kontext der Informationstechnologie • kennen Strategieberatung auf Unternehmens- sowie Geschäftsbereichsebene • kennen typische Fragestellungen des IT-Consulting • beherrschen den Lösungsansatz über ein umfangreiches Portfolio an betriebswirtschaftlichen sowie informationstechnischen Methoden und Lösungsansätzen • kennen Methoden zur Analyse und Definition von Geschäftsmodellen sowie bewährte Geschäftsmodellmuster • kennen die Herausforderungen der digitalen Transformation für Unternehmen und die relevanten Fragestellungen im Zeitalter der Digitalisierung • kennen moderne Technologien und Arbeitsformen • kennen betriebswirtschaftliche Analyse-, Bewertungs- und Entscheidungsverfahren *[Wissen, 6]*
	Kompetenz Fertigkeiten Die Studierenden • können das IT-Consulting systematisieren und den Einsatz der Informationstechnologie im Kontext der strategischen Ausrichtung des Unternehmens bewerten und einordnen • sind in der Lage, systematisch und methodisch Geschäftsmodelle zu analysieren, bewerten und zu konzipieren • können die relevanten Grundkonzepte für die Durchführung von Beratungsprojekten (wie Lernkurven, Business Rengineering, ABC-Analysen, Produktlebenszyklus, Just-In-Time etc.) auswählen und systematisch anwenden • können die relevanten Methoden und Analysewerkzeuge für die Durchführung von Beratungsprojekten (4C-Konzept, Five-Forces-Modell, SWOT-Analyse, Marketing-Mix, Portfolioanalyse: Boston-Consulting-Group-Matrix, Wertschöpfungskette, Businessplan etc.) auswählen und systematisch anwenden • können die relevanten Analyse- und Beschreibungskonzepte für Geschäftsmodelle im digitalen Kontext der Plattformökonomie (Business Model Canvas, Value Proposition Canvas, Persona Design, Lean Startup: Lean Canvas) auswählen und systematisch anwenden • beherrschen das grundlegende Instrumentarium des IT-Consulting (Strategisches IT-Architekturmanagement, strategisches IT-Prozessmanagement, Auswahl von Anwendungssystemen, Optimierung von IT-Organisationsstrukturen, IT-Projekt- und Portfoliomanagement, IT-Anforderungsmanagement, IT-Servicemanagement, Identifikation von Schatten-IT etc.) *[Instrumentelle Fertigkeiten, 6]*

	Die Studierenden • *können in umfangreichen, realitätsnahen Fallstudien die Problemstellungen identifizieren, analysieren und bewerten sowie methodische Lösungsansätze umsetzen* • *können weiterhin – durch zielgerichtete Abstraktionstechniken – die methodischen Lösungsansätze strukturiert systematisieren und den Lösungsweg vor einer definierten Zielgruppe verteidigen* *[Systemische Fertigkeiten, 6]*
	Sozialkompetenz Die Studierenden sind in der Lage, die in Form einer Fallstudie definierten Aufgaben des IT-Consulting in einem Team zu bearbeiten und die Teamarbeit selbst zu organisieren *[Team-/Führungsfähigkeit, 6]* *Zielgruppenorientierter Einsatz von Präsentationsmethoden und Dokumentationstechniken [Kommunikation, 6]*
	Selbstständigkeit Die Studierenden können Problemstellungen auch in komplexen Fallstudien erkennen, methodisch bearbeiten, lösungs- sowie kontextbezogen recherchieren, auf das Wesentliche im Managementkontext abstrahieren, zielgerichtet lösen und präsentieren *[Eigenständigkeit/Verantwortung, 6]*
4	**Inhalte*:*** Die Vorlesung vermittelt Kenntnisse in der Unternehmensberatung, speziell im Kontext der Informationstechnologie und neuerer Entwicklungen der Digitalisierung: • Grundlagen der Unternehmensberatung • Systematisierung von Unternehmensberatungen • Beratungsleistungen im Kontext strategischer Initiativen • Problemlösung als originäre Beratungsleistung • Sinnstiftung als derivative Beratungsleistung • Strategieberatung auf Unternehmens- und Geschäftsbereichsebene • Grundlagen des IT-Consulting • Einsatz moderner Technologien und Technikfolgenabschätzung • Digitalisierung: Prinzipien, Erfolgsfaktoren und Technikeinsatz • Digitale Plattformökonomie • Ökonomische, organisatorische und technologische Grundkonzepte • Fortgeschrittene Methoden und Analysewerkzeuge • Vernetztes Problemlösen • Bearbeitung realitätsnaher Fallstudien
	Empfohlene Literaturangaben: *Fink, D.: Strategische Unternehmensberatung, 1. Auflage, Vahlen, 2009* *Hartenstein, M./Billing, F./Schawel, C./Grein, M.: Der Weg in die Unternehmensberatung: Consulting Case Studies erfolgreich bearbeiten, 12. Auflage, Springer Gabler, 2015* *Tiemeyer, E.: Handbuch IT-Management: Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, 6. Auflage, Hanser, 2017* *Niedereichholz, C.: Unternehmensberatung: Band 1: Beratungsmarketing und*

	Auftragsakquisition, 5. Auflage, Oldenbourg, 2010 *Niedereichholz, C.: Unternehmensberatung: Band 2: Auftragsdurchführung und Qualitätssicherung, 6. Auflage, Oldenbourg, 2012* *Mangiapane, M./Büchler, R.: Modernes IT-Management: Methodische Kombination von IT-Strategie und IT-Reifegrademodell, Springer Vieweg, 2015* *Camenzind, A./Fueglistaller, U.: Strategisches Denken in KMU und die Lehren von Clausewitz, Verlag Neue Zürcher Zeitung, 2014* *Simon, H./Von der Gathen, A.: Das große Handbuch der Strategieinstrumente: Werkzeuge für eine erfolgreiche Unternehmensführung, 2. Auflage, Campus, 2010* *Dörner, D.: Die Logik des Misslingens: Strategisches Denken in komplexen Situationen, 11. Auflage, rororo, 2012* *Vester, F.: Die Kunst vernetzt zu denken: Ideen und Werkzeuge für einen neuen Umgang mit Komplexität: Ein Bericht an den Club of Rome, DVA, 2019* *Hermann, Ulrich: Digitalisierung im Industrieunternehmen: Die Chancen der digitalen Ökonomie der Dinge erkennen, entwickeln und erfolgreich umsetzen, Apprimus, 2019* *Osterwald, A./Pigneur, Y.: Business Model Generation: Ein Handbuch für Visionäre, Spielveränderer und Herausforderer, campus, 2011* *Osterwald, A./Pigneur, Y./Bernarda, G./Smith, A.: Value Proposition Design: Entwickeln Sie Produkte und Services, die Ihre Kunden wirklich wollen, campus, 2015* *Maurya, A.: Running Lean: Das How-to für erfolgreiche Innovstionen, O'Reilly, 2013* *Gärtner, C./Heinrich. C. (Hrsg.): Fallstudien zur Digitalen Transformation: Case Studies für die Lehre und praktische Anwendung, Springer Gabler, 2017* *Von Engelhardt, S./Petzold, S. (Hrsg.): Das Geschäftsmodell-Toolbox für digitale Ökosysteme, Campus, 2019* *Gassmann, O./Frankenberger, K./Csik, M.: Geschäftsmodelle entwickeln: 55 innovative Konzepte mit dem St. Galler Business Model Navigator, 2. Auflage, 2017* *Hoffmeister, C.: Digitale Geschäftsmodelle richtig einschätzen, Hanser, 2013* *Srnicek, N.: Plattform-Kapitalismus, Hamburger Edition, 2018* *Jaekel: Die Macht der digitalen Plattformen: Wegweiser im Zeitalter einer expandierenden Digitalsphäre und künstlicher Intelligenz, Springer Vieweg, 2017* *Parker, G. G./Van Alstyne, M.W./Choudary, S. P.: Die Plattform-Revolution im E-Commerce: Von Airbnb, Uber, PayPal und Co. lernen: Wie neue Plattform-Geschäftsmodelle die Wirtschaft verändern, mitp, 2017* *Clement, R./Schreiber, D./Bossauer, P./Pakusch, C.: Internet-Ökonomie: Grundlagen und Fallbeispiele der digitalen und vernetzten Wirtschaft, 4. Auflage, Springer Gabler, 2020*
5	**Teilnahmevoraussetzungen:** Entweder Wahl der Studienwahlrichtung „IT-Management" im Rahmen der Studiengänge Wirtschaftsinformatik, IT Security und Technische Informatik oder Wahl als Wahlpflichtmodul
6	**Prüfungsformen***:* Klausur 90 min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreiches Bestehen der Klausur
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik Wahlrichtung: IT-Management

9	***Modulverantwortliche(r):*** Prof. Dr. Nils Herda Dozent: Prof. Dr. Nils Herda
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.5.11 24200 – E-Business

Studiengang: IT Security/Technische Informatik/Wirtschaftsinformatik
StuPO-Version: 17.2

Semester: WS 2020/21

Letzte Bearbeitung: 14.10.20

Modul: E-Business					
Kennnummer 24200	**Workload** 75 h	**Modulart** P	**Studiensemester** 5	**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)** Vorlesung & Übungen E-Business	**Sprache** Deutsch	**Kontakt-zeit** 2 SWS / 30 h	**Selbst-studium** 45 h	**Credits (ECTS)** 2,5
2	**Lehrform(en) / SWS:** Vorlesung & Übungen: 2 SWS				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden • kennen die Grundlagen des E-Business • kennen Systeme, Prozesse und Prinzipien des elektronischen Verkaufs (E-Shops), des elektronischen Einkaufs (E-Procurement), des elektronischen Handels (E-Marketplace) sowie elektronischer Kontaktnetzwerke (E-Communities) • kennen die betriebliche elektronische Kooperation (E-Company) • kennen die Systematisierung von Verkaufskanälen in Geschäftsmodellen des E-Business (Multi-Channel-, Omni-Channel- und Cross-Channel-Modelle) • kennen digitale Geschäftsmodelle im Kontext von E-Business und Digitaler Plattformökonomie *[Wissen, 6]*				
	Kompetenz Fertigkeiten Die Studierenden • können Geschäftsmodelle im Kontext von E-Business und Digitaler Plattformökonomie beschreiben und analysieren • können die betrieblich und gesellschaftlich relevanten E-Communities systematisieren, einordnen und unter kommerziellen Gesichtspunkten bewerten • können die Digitale Plattformökonomie darstellen, bewerten und kommerzielle				

	Vertreter systematisch einordnen • können E-Business vor dem Hintergrund der kommerziellen Bedeutung für Unternehmen und die Digitale Plattformökonomie im Kontext ökonomischer, strategischer, volkswirtschaftlicher, sozialer, moralischer und unternehmerischer Sichten qualifizieren *[Instrumentelle Fertigkeiten, 6]* Die Studierenden • können in umfangreichen, realitätsnahen Fallstudien die Herausforderungen von Unternehmen im E-Business analysieren, bewerten und in Bezug auf digitale Vertriebskanäle systematisch und methodisch weiterentwickeln • können systematisch und methodisch digitale Geschäftsmodelle entwickeln • können weiterhin – durch zielgerichtete Abstraktionstechniken – Grundzüge von IT-Strategien und Maßnahmenkataloge für das IT-Management entwickeln *[Systemische Fertigkeiten, 6]*
	Sozialkompetenz Die Studierenden sind in der Lage, die komplexen Fallstudien zum E-Business in einem Team zu bearbeiten und die Teamarbeit selbst zu organisieren *[Team-Führungsfähigkeit, 6]* *Zielgruppenorientierter Einsatz von Präsentationsmethoden und Dokumentationstechniken* *[Kommunikation, 6]*
	Selbstständigkeit Die Studierenden können tiefergehende Problemstellungen auch in komplexen Fallstudien erkennen, methodisch bearbeiten, lösungs- sowie kontextbezogen recherchieren, auf das Wesentliche im Managementkontext abstrahieren und zielgerichtet lösen *[Eigenständigkeit/Verantwortung, 6]*
4	**Inhalte*:*** Die Vorlesung vermittelt Kenntnisse im E-Business – speziell im Kontext betrieblicher Unternehmungen, die vor den Herausforderungen der digitalen Transformation stehen: • Grundlagen des E-Business • Elektronischer Verkauf (E-Shops) • Elektronischer Einkauf (E-Procurement) • Elektronischer Handel (E-Marketplace) • Elektronische Kontaktnetzwerke (E-Communities) • Elektronische Kooperation (E-Company) • Verkaufskanäle im E-Business (Multi-Channel-, Omni-Channel- und Cross-Channel-Modelle) • Digitale Plattformökonomie und E-Business • Geschäftsmodelle im E-Business
	Empfohlene Literaturangaben: Kollmann, T.: E-Business: Grundlagen elektronischer Geschäftsprozesse in der Digitalen Wirtschaft, 7. Auflage, Springer Gabler, 2019

	Kollmann, T.: E-Business kompakt: Grundlagen elektronischer Geschäftsprozesse in der Digitalen Wirtschaft mit über 70 Fallbeispielen, Springer Gabler, 2019 Wirtz, E.: Electronic Business, 6. Auflage, Springer Verlag, 2018 Hermann, Ulrich: Digitalisierung im Industrieunternehmen: Die Chancen der digitalen Ökonomie der Dinge erkennen, entwickeln und erfolgreich umsetzen, Apprimus, 2019 Osterwald, A./Pigneur, Y.: Business Model Generation: Ein Handbuch für Visionäre, Spielveränderer und Herausforderer, campus, 2011 Osterwald, A./Pigneur, Y./Bernarda, G./Smith, A.: Value Proposition Design: Entwickeln Sie Produkte und Services, die Ihre Kunden wirklich wollen, campus, 2015 Maurya, A.: Running Lean: Das How-to für erfolgreiche Innovstionen, O'Reilly, 2013 Gärtner, C./Heinrich. C. (Hrsg.): Fallstudien zur Digitalen Transformation: Case Studies für die Lehre und praktische Anwendung, Springer Gabler, 2017 Von Engelhardt, S./Petzold, S. (Hrsg.): Das Geschäftsmodell-Toolbox für digitale Ökosysteme, Campus, 2019 Gassmann, O./Frankenberger, K./Csik, M.: Geschäftsmodelle entwickeln: 55 innovative Konzepte mit dem St. Galler Business Model Navigator, 2. Auflage, 2017 Hoffmeister, C.: Digitale Geschäftsmodelle richtig einschätzen, Hanser, 2013 Srnicek, N.: Plattform-Kapitalismus, Hamburger Edition, 2018 Jaekel: Die Macht der digitalen Plattformen: Wegweiser im Zeitalter einer expandierenden Digitalsphäre und künstlicher Intelligenz, Springer Vieweg, 2017 Parker, G. G./Van Alstyne, M.W./Choudary, S. P.: Die Plattform-Revolution im E-Commerce: Von Airbnb, Uber, PayPal und Co. lernen: Wie neue Plattform-Geschäftsmodelle die Wirtschaft verändern, mitp, 2017 Clement, R./Schreiber, D./Bossauer, P./Pakusch, C.: Internet-Ökonomie: Grundlagen und Fallbeispiele der digitalen und vernetzten Wirtschaft, 4. Auflage, Springer Gabler, 2020
5	**Teilnahmevoraussetzungen:** Entweder Wahl der Studienwahlrichtung „IT-Management" im Rahmen der Studiengänge Wirtschaftsinformatik, IT Security und Technische Informatik oder Wahl als Wahlpflichtmodul Die Lehrveranstaltung „13500 Einführung E-Business" (1. Semester) ist für das Verständnis hilfreich, aber nicht zwingend erforderlich, da der zu vermittelnde Lehrstoff über die angegebenen Lehrmaterialien abgedeckt ist
6	**Prüfungsformen***:* Klausur 60 min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreiches Bestehen der Klausur
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik Wahlrichtung: IT-Management
9	***Modulverantwortliche(r):*** Prof. Dr. Nils Herda Dozent: Prof. Dr. Nils Herda
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.5.12 24300 – Digitale Forensik

Studiengang: IT Security/Technische Informatik/Wirtschaftsinformatik
StuPO-Version: 17.2

Semester: WS 2020/21

Letzte Bearbeitung: 12.10.2020

<table>
<tr><td colspan="8">Modul: Digitale Forensik</td></tr>
<tr><td colspan="2">Kennnummer
24300</td><td>Workload
150 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
5</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung & Übungen Digitale Forensik</td><td>Sprache
Deutsch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
90 h</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung & Übungen: 4 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Breite Kenntnis forensischer Methoden im Allgemeinen und spezialisiert in der Digitalen Forensik [Wissen, 6]
Tiefe Kenntnis forensischer Prinzipien angewandt auf den Bereich der digitalen Spuren [Wissen, 6]
Kompetenz Fertigkeiten
Breites Spektrum an digitalforensischen Methoden zur Sicherung und Analyse digitaler Spuren [Instrumentelle Fertigkeiten, 6]
Sind in der Lage Möglichkeiten und Grenzen der erlernten forensischen Methoden und Werkzeuge einzuschätzen und diese zu erweitern bzw. neue Skripte/Werkzeuge zu entwickeln [Systemische Fertigkeiten, 6]
Können die Relevanz gesicherter und analysierter digitaler Spuren hinsichtlich ihrer Relevanz auf die juristischen Fragestellungen beurteilen [Beurteilungsfähigkeit, 6]
Sozialkompetenz
Können ein forensisches Ermittlungsteam leiten und die fachlichen Ermittlungsaufgaben im Team verteilt lösen [Team-/Führungsfähigkeit, 6]
Selbstständigkeit
Können juristischen/forensische Aufgabenstellungen eigenständig analysieren, in technische Aufgabenstellungen und zurück übertragen und ihre Untersuchungsprozesse entsprechend gestalten [Eigenständigkeit/Verantwortung, 6]</td></tr>
</table>

	Notwendige neue / angepasste forensische Methoden und Werkzeuge können eigenständig erschlossen werden *[Lernkompetenz, 6]*
4	**Inhalte*:*** Vorlesung & Übungen • Einführung in forensische Wissenschaften im Allgemeinen und die Digitale Forensik im Speziellen • Methodische Fundierung der digitalen Forensik, Einbettung in die klassische analoge Forensik • Forensische Prinzipien bei der Sicherung und Analyse digitaler Spuren • Dokumentation und Präsentation forensischer Untersuchungen (intern und vor Gericht) • Praktische Anwendungen in verschiedenen Teilbereichen der digitalen Forensik (z.B. Datenträgerforensik, Anwendungsforensik, Digitale Forensik Mobiler Geräte)
	Empfohlene Literaturangaben: Dewald, A., Freiling, F.: Forensische Informatik, 2. Auflage, Books on Demand, 2015 Casey, E.: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3. Auflage, Academic Press, 2011 Carrier, B.: File Syste, Forensic Analysis, Addison Wesley, 2005 Geschonneck, A.: Computer-Forensik (iX Edition): Computerstraftaten erkennen, ermitteln, aufklären, dpunkt.verlag, 2014 Hayes, D.: A Practical Guide to Computer Forensics Investigations, Pearson, 2014
5	**Teilnahmevoraussetzungen:** keine empfohlen: Inhalte der Module 12500 Einführung IT Security, 15000 Betriebssysteme, 21200 Netzwerke
6	**Prüfungsformen***:* Referat 20 min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewerteter Vortrag (mdl. Verteidigung eines forensischen Gutachtens)
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik Wahlrichtung: Applied IT Security
9	***Modulverantwortliche(r):*** Prof. Holger Morgenstern Dozent: Prof. Holger Morgenstern
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.5.13 24400 – Offensive Sicherheitsmethoden

Studiengang: Technische Informatik
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 12.10.2020

Modul: Offensive Sicherheitsmethoden					
Kennnummer 24400	**Workload** 225 h	**Modulart** P	**Studiensemester** 5	**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)** Vorlesung & Übungen Offensive Sicherheitsmethoden Praktikum Offensive Sicherheitsmethoden	**Sprache** Deutsch (deutsches und englisches Literatur-studium erforderlich)	**Kontakt-zeit** 6 SWS / 90 h	**Selbst-studium** 135 h	**Credits (ECTS)** 7,5
2	**Lehrform(en) / SWS:** Vorlesung & Übungen: 4 SWS Praktikum: 2 SWS				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Breites Wissen über offensive Methoden der IT Sicherheit inkl. PEN Tests, CIA Angriffe auf Systeme, Netzwerke und Kommunikationskanäle *[Wissen, 6]* Tiefe Kenntnisse aktueller offensiver Werkzeuge und Frameworks, u.a. aktuelles Metasploit *[Wissen, 6]* *Kompetenz Fertigkeiten* Sind in der Lage mittels umfangreicher und vielfältiger offensiver Methoden und Werkzeuge in geschützte IT Systeme einzudringen *[Instrumentelle Fertigkeiten, 6]* Sind in der Lage neue offensive Werkzeuge und Skripte zu entwickeln und anzuwenden *[Systemische Fertigkeiten, 6]* Studierende sind in der Lage das Sicherheitsniveaus aus den Ergebnissen offensiver Sicherheitstests zu beurteilen *[Beurteilungsfähigkeit, 6]* *Sozialkompetenz* Neue Methoden und Techniken im Bereich offensiver Sicherheitsmethoden werden mit einem Fachpublikum diskutiert *[Kommunikation, 6]* *Selbstständigkeit* Reflexion und Bewusstsein über rechtliche und ethische Rahmenbedingungen und Auswirkungen offensiver Methoden *[Reflexivität, 6]*				
4	**Inhalte:** Vorlesung & Übungen • Offensive Methoden und ihre Ziele im Kontext der IT Sicherheit				

	• Rechtliche und Ethische Rahmenbedingungen • Grundlagen, Rahmenbedingungen und Ziele von Penetrationstests • Angriffe auf die Vertraulichkeit, Integrität oder Verfügbarkeit von o Übertragungskanälen o Netzwerken o Betriebssystemen o Anwendungen o Hardwarekomponenten o Web-Anwendungen o Funksystemen • Finden von Schwachstellen durch Fuzzing und Codeanalyse Praktikum Die in der Vorlesung behandelten Punkte werden im Praktikum innerhalb eines isolierten Netzwerks praktisch erprobt. Dabei werden aktuelle Werkzeuge und Systeme aus dem Penetrationstest- und Systemanalysebereich wie z.B. Burp Suite, Nmap und das Metasploit Framework angewandt.
	Empfohlene Literaturangaben: Kim, P.: The Hacker Playbook 2, A practical Guide to Penetration Testing, Secure Planet LLC, 2015 Hadnagy, C.: Social Engineering, The Art of Human Hacking, Wiley Publishing Inc., 2011 Stuttard D.: The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Auflage 2, John Wiley & Sons, 2011 Erickson, J.: Hacking, The Art of Exploitation, No Starch Press, 2008 Messner, M.: Metasploit: Das Handbuch zum Penetration-Testing Framework, dpunkt.Verlag, 2015
5	**Teilnahmevoraussetzungen:** keine empfohlen: Inhalte der Module Einführung ITS, Betriebssysteme, Netzwerke, Web-basierte Anwendungen
6	**Prüfungsformen***:* Klausur 120 min., benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur erfolgreiche Teilnahme am Praktikum
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik Wahlrichtung: Applied IT Security
9	***Modulverantwortliche(r):*** (n.n.), Prof. Holger Morgenstern Dozent: LB
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.5.14 23400 – Wahlpflichtmodul 1 (WPM 1)

Studiengang: Technische Informatik
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Wahlpflichtmodul 1						
Kennnummer 23400	**Workload** 150 h	**Modulart** P	**Studiensemester** 5	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Wahlpflichtmodul gem WPM-Katalog	**Sprache** Deutsch (deutsches und englisches Literatur-studium erforderlich)	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5	
2	**Lehrform(en) / SWS:** Vorlesung: 4 SWS (gesamt) Eine Aufteilung in mehrere Teilmoduleinheiten ist möglich.					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden wenden ihr im Studium erlangtes Wissen auf den jeweiligen Bereich an. Die Studierenden können sich darüber hinaus in angemessener Zeit neue Inhalte aneignen und diese geeignet strukturieren und didaktisch aufbereiten *[Wissen, 6]* *Kompetenz Fertigkeiten* Die Studierenden sind in Lage Konzepte und Methoden zu abstrahieren und auf neue Anwendungsfelder zu übertragen. *[Instrumentelle Fertigkeiten, 6]* *Sozialkompetenz* Die Lernergebnisse sind abhängig vom jeweiligen WPM *Selbstständigkeit* Studierende können die Lehrinhalte selbständig aufarbeiten und strukturiert wiedergeben. Sie sind in der Lage Aufgaben im vorgegeben Zeitrahmen zu bearbeiten *[Eigenständigkeit/Verantwortung, 6]*					
4	**Inhalte*:*** Die Wahlpflichtmodule dienen einerseits der weiteren Vertiefung in den einzelnen Studienschwerpunkten und runden andererseits das Studienangebot mit praxisnahen Inhalten ab. Dies geschieht zum einen in Vorbereitung auf die spätere Berufsfertigkeit als auch im Hinblick auf ein sich anschließendes Masterstudium. Zur Wahl stehen die im jeweiligen Semester gem. WPM-Katalog angebotenen Module im Umfang von jeweils 2,5 bzw. 5ECTS. *Empfohlene Literaturangaben:* Es wird auf die Modulbeschreibungen im jeweils gültigen WPM-Katalog verwiesen					

5	**Teilnahmevoraussetzungen:** Für die Teilnahme gelten keine über die in der Studien- und Prüfungsordnung festgelegten hinausgehenden Voraussetzungen.
6	**Prüfungsformen***:* Es gelten die im WPM-Katalog für das jeweilige Modul angekündigten Prüfungsformen
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreiche Teilnahme an der Modul(teil)prüfung
8	***Verwendbarkeit des Moduls:*** CSP, AD, ITM, ITS
9	***Modulverantwortliche(r):*** Prof. Dr. Bernd Stauß Dozenten: gem. WPM-Katalog
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.5.15 23500 – Projektstudium

Studiengang: Technische Informatik **Semester**: WS 2020/21
StuPO-Version: 17.2 **Letzte Bearbeitung**: 14.10.20

Modul: Projektstudium					
Kennnummer 23500	**Workload** 225 h	**Modulart** P	**Studiensemester** 5	**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)** Projektstudium Projekt Projekt Studium Seminar	**Sprache** Deutsch und/oder Englisch	**Kontakt-zeit** 6 SWS / 90 h	**Selbst-studium** 135 h	**Credits (ECTS)** 7,5
2	**Lehrform(en) / SWS:** Projekt: 4 SWS Seminar: 2 SWS				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen die zentralen Konzepte des (IT-) Projektmanagements, sowie Strukturen und Abläufe *[Wissen, 6]* *Kompetenz Fertigkeiten* Die Kursteilnehmer sind in der Lage einen Projektauftrag ihres Klienten strukturiert zu erfassen und dabei die adressierten Anforderungen (Lasten) als auch die zu erbringende Leistung (Pflichten) gegenüberzustellen. Die Studierenden konzipieren eigenständig Lösungsansätze und stimmen diese mit den Dozenten ab. Ziel ist die				

	Realisierung der Konzepte und die Auslieferung einer protypischen Lösung *[Systemische Fertigkeiten, 6]*
	Sozialkompetenz Das Projektteam legt die Aufbaustrukturen selbst fest und wendet diese während des Projektes konsequent an. Konfliktsituationen werden in den Seminaren aufgearbeitet wobei der Dozent moderierend unterstützt. *[Team-/Führungsfähigkeit, 6]*
	Selbstständigkeit Die Kursteilnehmer organisieren sich in Abstimmung mit dem Dozenten selbst und legen auch die Art des Projektmanagements fest. In wöchentlichen Seminarterminen werden (Zwischen-)Ergebnisse vorgestellt und diskutiert und der weitere Projektverlauf abgestimmt. *[Eigenständigkeit/Verantwortung, 6]*
4	**Inhalte*:*** Eigenständige Bearbeitung eines realen Problems aus dem Studienbereich von der Problemanalyse bis zur marktfähigen Lösung im Projektteam • Coaching des Projektteams durch den Dozenten
	Empfohlene Literaturangaben: Hindel, B. et al.: Basiswissen Software Projektmanagement. Dpunkt ISBN 3898642305Katzenbach, J. R., Smith, D. K.: The Wisdom of Teams. Creating the High-Performance Organization. Harvard Business School Press, ISBN 0875843670 Lessel, W.: Projektmanagement, Cornelsen, ISBN 3589219033 Schreckeneder, B. C.: Projektcontrolling. Projekte über-wachen, bewerten, präsentieren. Haufe, ISBN 344805349XWeitere projektspezifische Literatur wird vom Dozenten zum Beginn des Projekts benannt bzw. von den Studierenden ermittelt
5	**Teilnahmevoraussetzungen:** Hilfreich sind Kentnisse aus dem Projektmanagement
6	**Prüfungsformen***:* Praktische Arbeiten, benotet Hausarbeit, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Die Studierenden fertigen am Ende des Projektes eine Hausarbeit an, die die wesentlichen Erkenntnisse und Ergebnisse aus dem Projektstudium strukturiert wiedergibt. Die Ergebnisse sind in Kurzform (Präsentation) auch den Studierenden des 4, und 5. Semesters vorzustellen.
8	***Verwendbarkeit des Moduls:*** Alle Vertiefungsrichtungen des 5. Semesters (Applied IT Security, Cyber Physical Systems, Apllication Development, IT Management)
9	***Modulverantwortliche(r):*** Prof. Dr. Bernd Stauß Dozenten: Professoren der Fakultät
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.6 6. Semester

5.6.1 31000 – Integriertes Praktisches Studiensemester

Studiengang: Technische Informatik
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.2020

Modul: Integriertes praktisches Studiensemester					
Kennnummer 31000	**Workload** 750	**Modulart** P	**Studiensemester** 6. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)** Ausbildung in der Praxis	**Sprache** Deutsch	**Kontakt-zeit** 720 h	**Selbst-studium** 30 h	**Credits (ECTS)** 25

2	**Lehrform(en) / SWS:** Ausbildung in der Praxis: 95 Präsenz-Tage im Betrieb
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* *praktisch relevante Aufgabenstellung(en) bearbeiten [Wissen, 6]* /Niveaustufe wählen *Kompetenz Fertigkeiten* zielorientiert arbeiten *[Instrumentelle Fertigkeiten, 6]* *Sozialkompetenz* Team-Ziele mitverantwortlich unterstützen *[Mitgestaltung, 6]* *Selbstständigkeit* selbstständig im eigenen fachlichen Bereich wirken *[Eigenständigkeit/Verantwortung, 6]*
4	**Inhalte*:*** konkrete betriebliche Projekte planen, entwickeln und realisieren sowie Praxis-Bericht verfassen *Empfohlene Literaturangaben:* Torsten Czenskowsky, Bernd Rethmeier, Norbert Zdrowomyslaw: Praxissemester und Praktika im Studium – Qualifikation durch Berufserfahrung; Cornelsen Lehrbuch, 2001, 978-3464498071 Daniela Mayrshofer, Hubertus A. Kröger: Prozesskompetenz in der Projektarbeit; 4. Auflage, Edition Windmühle, Feldhaus Verlag, 2011, 978-3937444734
5	**Teilnahmevoraussetzungen:** lfd. StuPO
6	**Prüfungsformen***:* Praxisbericht, unbenotet

7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** pünktliche Bereitstellung des Praxis-Berichts
8	***Verwendbarkeit des Moduls:*** alle Informatik-Studiengänge
9	***Modulverantwortlicher:*** Modulverantwortlicher: Prof. Dr. Walter Hower Dozent/in: Studiengang-Praktikantenamts-Leiter/in
10	***Optionale Informationen:*** von der Praxisstelle bestätigte Aktivitäten

5.6.2 31500 – Berufsfertigkeit

Studiengang: Technische Informatik **Semester**: WS 2020/21
StuPO-Version: 17.2 **Letzte Bearbeitung**: 14.10.20

Modul: Berufsfertigkeit						
Kennnummer 31500	**Workload** 150	**Modulart** P	**Studiensemester** 6. Semester		**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)** a. Vorbereitende Blockveranstaltug b. Nachbereitende Blockveranstaltug	**Sprache** Deutsch (deutsches und englisches Literatur-studium erforderlich)	**Kontakt-zeit** Präsenz 150 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** Vorbereitende Blockveranstaltung Nachbereitende Blockveranstaltung				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Lernergebnisbeschreibung einer bestimmten Kompetenz z.B. Fachwissen mit Niveaustufe /Niveaustufe wählen				
	Kompetenz Fertigkeiten Die Studierenden sind in der Lage, • sich persönliche Ziele zu setzen und Methoden zu deren Erreichung anzuwenden • sich an gemeinsame Absprachen zu halten und selbständig zu arbeiten • sich im zwischenmenschlichen Bereich vorbildlich zu verhalten • Andere mit ihrer Persönlichkeit, ihren Werten und ihrem Verhalten zu achten				

	• sich in ethischen Verhalten an durch Vernunft geprägtes Handeln zu orientieren • über sich und ihr Verhalten zu anderen nachzudenken [Systemische Fertigkeiten, 6]
	Sozialkompetenz Die Studierenden kennen - Kriterien zu einer erfolgreichen Teamarbeit - Methoden zur Eigenmotivation und Bewertung ihres beruflichen Leistungsvermögens - die Bedeutung ihres Verhaltens bzgl. der Selbsteinschätzung und möglicher Fremdbewertungen - die Anforderungen einer leistungsorientierten Gesellschaft [Mitgestaltung, 6]
	Selbstständigkeit Die Studierenden sind in der Lage komplexe Aufgabenstellungen selbständig zu bearbeiten [Eigenständigkeit/Verantwortung, 6]
4	**Inhalte*:*** Kurzer Überblick des Modulinhalts bzw. der Inhalte der Lehrveranstaltungen
	Empfohlene Literaturangaben: Deutsches Institut f. Erwachsenenbildung, Deutsches Institut f. Internationale Pädagogische Forschung, Institut f. Entwicklungs-planung u. Strukturforschung: ProfilPASS - Gelernt ist gelernt: Dokumentation eigener Kompetenzen und des persönlichen Bildungswegs. Bertelsmann, 2006, ISBN-13: 978-3763935154 Duarte, N., Heymann-Reder; D.: slide:ology: Oder die Kunst, brillante Präsentationen zu entwickeln. O'Reilly, 2009, ISBN-13: 978-3897219397 Fischer-Epe, M., Epe, C.: Selbstcoaching:: Hintergrundwissen, Anregungen und Übungen zur persönlichen Entwicklung. Rororo, 3. Auflage, 2007, ISBN-13: 978-3499622830 Fischer-Epe, M., Epe, C.: Stark im Beruf, erfolgreich im Leben. Persönliche Entwicklung und Selbst-Coaching. Anaconda, 2010, ISBN-13: 978-3866475076 Haeske, U.: Pocket Business: Team- und Konfliktmanagement: Teams erfolgreich leiten - Konflikte konstruktiv lösen. Cornelsen Verlag Scriptor, 3. Auflage, 2008, ISBN-13: 978-3589234097 Hüsgen, M.: Projektteams: Das Sechs-Ebenen-Modell zur Selbstreflexion im Team - Instrument und Einsatz. Vandenhoeck & Ruprecht, 2005, ISBN-13: 978-3525451526 Jackman, A.: Ziele setzen, Ziele erreichen. Edition Xxl, 2008, ISBN-13: 978-3897362741 Janson, S.: Selbstorganisation und Zeitmanagement: Mit Praxistipps und Checklisten. Redline Wirtschaftsverlag, 2007, ISBN-13: 978-3636014153 Langmaack, B: Soziale Kompetenz: Verhalten steuert den Erfolg. Beltz, 2004, ISBN-13: 978-3407857835

	Meier, R., Bremke, P.: Qualitätsmanagement. GABAL-Verlag, 2008, ISBN-13: 978-3897498372 Meifert, M.T., Ulrich, D.: Strategische Personalentwicklung: Ein Programm in acht Etappen. Springer, 2. Auflage, 2010, ISBN-13: 978-3642043994 Seiwert, L.: Noch mehr Zeit für das Wesentliche: Zeitmanagement neu entdecken. Goldmann Verlag, 2009, ISBN-13: 978-3442170593 Thom, N., Zaugg, R.J.: Moderne Personalentwicklung: Mitarbeiterpotenziale erkennen, entwickeln und fördern. Gabler, 3. Auflage, 2008, ISBN-13: 978-3834910608 Wedmann-Tosuner, W.: Berufsfeld Management-Assistenz. Der Weg nach oben. Fachliche und persönliche Kompetenz. Walhalla U. Praetoria, 2002, ISBN-13: 978-3802946226 Weiß, J., Kirchner, I.: Selbstcoaching. Persönliche Power und Kompetenz gewinnen. Heyne, 2001, ISBN-13: 978-345319047
5	**Teilnahmevoraussetzungen:** Voraussetzungen für die Teilnahme beschreiben; Außerdem beschreiben, wie sich der Studierende vorbereiten kann (u.a. Literaturangaben, Lehr- und Lernprogramme)
6	**Prüfungsformen***:* Praktische Arbeiten, benotet Referate: Dauer je 20 min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene PA Bestandene Referat
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. Nemirovski Dozent(in):
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.7 7. Semester

5.7.1 32300 – IT-GRC

Studiengang: Technische Informatik
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

<table>
<tr><td colspan="7">Modul: IT-GRC (IT-Governance, Risk & compliance)</td></tr>
<tr><td colspan="2">Kennnummer
32300</td><td>Workload
150 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
7</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung & Übungen IT-GRC</td><td>Sprache
Deutsch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
90 h</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung & Übungen: 4 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden
• kennen die wirtschaftliche, rechtliche und ethische Motivation für Governance, Risk and Compliance Management (GRC)
• können GRC systematisieren und jeweils die Disziplinen Corporate Governance, Risikomanagement und Compliance Management systematisieren und beschreiben
• kennen methodische Modelle für GRC
• kennen den methodischen Zusammenhang zwischen GRC und IT-GRC
• kennen Aufgaben, Zielstellung und Pflichten von Wirtschaftsprüfung, IT-Prüfung und IT-Revision im Kontext von IT-GRC
• kennen Aufgaben, Zielstellung und Pflichten des Chief Information Officer (CIO) sowie des IT-Managements im Kontext von IT-GRC
• kennen die Herausforderungen betrieblicher Unternehmen im Kontext der Digitalisierung, Industrie 4.0 und Plattformökonomie im Kontext von IT-GRC
• kennen aktuelle Forschungsprojekte
[Wissen, 6]

Kompetenz Fertigkeiten
Die Studierenden
• können in umfangreichen, realitätsnahen Fallstudien die Unternehmenssituation analysieren, Herausforderungen in Bezug auf IT-GRC vor dem Hintergrund von Branche sowie Unternehmensumwelt bewerten sowie die Herausforderungen für IT-Organisationen und das IT-Management systematisieren
• können weiterhin – durch zielgerichtete Abstraktionstechniken – Grundzüge von IT-</td></tr>
</table>

	GRC-Reifegraden sowie -Maßnahmenkatalogen für das IT-Management entwickeln *[Instrumentelle Fertigkeiten, 6]*
	Sozialkompetenz Sind in der Lage, die komplexen Fallstudien zu IT-GRC in einem Team zu bearbeiten und die Teamarbeit selbst zu organisieren *[Team-/Führungsfähigkeit, 6]*
	Selbstständigkeit Die Studierenden können tiefergehende Problemstellungen auch in komplexen Fallstudien erkennen, methodisch bearbeiten, lösungs- sowie kontextbezogen recherchieren, auf das Wesentliche im Managementkontext abstrahieren und zielgerichtet lösen *[Eigenständigkeit/Verantwortung, 6]* Die Studierenden erlernen die Fähigkeit, aus Sicht unterschiedlicher Stakeholder und in unterschiedlichen Rollen eine konkrete Unternehmenssituation zu analysieren, zu reflektieren und zu bewerten. Der informationstechnologische Hintergrund der Studierenden wird ergänzt um rechtliche, organisatorische, technologische Aspekte, so dass sie die richtigen Schlussfolgerungen aus einer kritischen Prüfungsperspektive ziehen und zielgerichtete Maßnahmen entwickeln können. *[Reflexivität, 6]*
4	**Inhalte*:*** Die Vorlesung vermittelt Kenntnisse in der Entwicklung von IT-Strategien im Kontext von Unternehmensstrategien und dem IT-Management in der Bandbreite rechtlicher, organisatorischer, technologischer und personeller Aspekte: • Begriffssystem für IT Governance, Risk and Compliance Management • Zusammenhang zwischen GRC und IT-GRC • Unternehmerische Fallbeispiele für Bedeutung und Motivation • Corporate Governance und Corporate Governance-Systeme • Risikomanagement und Risikomanagementsysteme • Compliance und Compliance-Management-Systeme • Reifegradmodelle für den betrieblichen Einsatz • IT-GRC als ganzheitlicher methodischer Ansatz • IT-GRC aus Sicht von Wirtschaftsprüfung • IT-GRC aus Sicht der IT-Revision und IT-Prüfung • IT-GRC im Kontext von IT Security und Cyber Security • IT-GRC im Kontext betrieblicher Resilienz • IT-GRC im Kontext von Daten, Datenschutz und Cloud Computing • IT-GRC im Kontext der Forschung (Industrial Data Space) • IT-GRC im Kontext von Digitalisierung, Industrie 4.0 und digitaler Plattformökonomie
	Empfohlene Literaturangaben: *Knoll, M.: Praxisorientiertes IT-Risikomanagement: Konzeption, Implementierung und Überprüfung, 2. Auflage, dpunkt, 2019* *Nestler, D./Modi, J. (Hrsg.: Institut der Wirtschaftsprüfer in Deutschland e.V.):*

	Leitfaden IT-Compliance: Anforderungen, Chancen und Umsetzungsmöglichkeiten, IDW, 2020. *Klotz, M.: IT-Compliance: Ein Überblick, 1. Auflage, dpunkt, 2009* *Rath, M.; Sponholz, R.: IT-Compliance – Erfolgreiches Management regulatorischer Anforderungen, o. A., Erich Schmidt, 2009* *Sowa, A./Duscha, P./Schreiber, S.: IT-Revision, IT-Audit und IT-Compliance: Neue Ansätze für die IT-Prüfung, Springer Vieweg, 2019* *Kersten, H.; Klett, G.: Der IT Security Manager: Aktuelles Praxiswissen für IT Security Manager und IT-Sicherheitsbeauftragte in Unternehmen und Behörden, 4. Auflage, Springer Vieweg, 2015* *Johannsen, W./Goeken, M.: Referenzmodelle für IT-Governance: Methodische Unterstützung der Unternehmens-IT mit COBIT, ITIL & Co, dpunkt., 2010* *Pohlmann, N.: Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung, Springer Vieweg, 2019* *Schulz, T: Cybersicherheit: für vernetzte Anwendungen in der Industrie 4.0, Vogel, 2019*
5	**Teilnahmevoraussetzungen:** Entweder Wahl der Studienwahlrichtungen „IT-Management" oder „Application Management" im Rahmen der Studiengänge Wirtschaftsinformatik, IT Security und Technische Informatik oder Wahl als Wahlpflichtmodul
6	**Prüfungsformen***:* Klausur, 90 min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreiches Bestehen der Klausur
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik Wahlrichtung: Application Development, IT-Management
9	***Modulverantwortliche(r):*** Prof. Dr. Nils Herda Dozent: Prof. Dr. Nils Herda
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.7.2 32100 – Mobile Systeme und Cloud

Studiengang: Technische Informatik **Semester**: WS 2020/21
StuPO-Version: 17.2 **Letzte Bearbeitung**: 13.03.2020

Modul: Mobile Systeme und Cloud					
Kennnummer **32100**	**Workload** 150 h	**Modulart** P	**Studiensemester** 7	**Dauer** 1 Semester	**Häufigkeit** WS und SS

Version	Erstellt/geändert von Ammann/am 12.10.2020	Dokument	Freigabe am/von	Gültig ab WS 2020/21
1.0		Modulhandbuch_IT_Sec_fin		

1	**Lehrveranstaltung(en)** Vorlesung & Übungen Mobile Systeme und Cloud. Praktikum Mobile Systeme und Cloud		**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** Vorlesung & Übungen: 3 SWS Praktikum: 1 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen die Besonderheiten mobiler Endgeräte (incl. Sensoren), Netzwerke und Protokolle. Sie kennen aktuelle Architekturen, APIs und Deploymentmöglichkeiten mobiler Applikationen (beispielsweise unter Android) Sie kennen Cloud-Einsatzszenarien und Service-Modelle aus Kundensicht, sowie Betriebsszenarien von CloudServices aus Anbietersicht. Sie kennen Cloud-Architekturen und Softwarelösungen für Cloud-Einsatzszenarien *[Wissen, 6]* *Kompetenz Fertigkeiten* Die Studierenden sind in der Lage, eigenständig mobileApplikationen (incl. anzusprechender Sensoren) zu spezifizieren. Sie sind in der Lage, mobile Systeme nach vorgegebener/selbst erstellter Spezifikation zu entwickeln und zu testen. Sie können mobile Systeme für den Endanwender bereitstellen (Deployment). Sie können außerdem Einsatzszenarien für Cloud Anwendungen verstehen und für Kunden entwickeln. Die Studierenden können Cloud-Service-Modelle (aus Anbietersicht) spezifizieren und entwickeln. *[Instrumentelle Fertigkeiten,* 6] Die Studierenden sind in der Lage, auch für sie neue Problemstellungen im Umfeld mobiler Anwendungen und Cloud-Servicemodelle zu lösen. *[Systemische Fertigkeiten, 6]* Die Studierenden im Umfeld Mobile & Cloud architektonisch und codetechnisch beurteilen und einordnen. *[Beurteilungsfähigkeit, 6]* *Sozialkompetenz* Geben Sie alle Inhalte ein, die wiederholt werden sollen – einschließlich anderer Inhaltssteuerelemente. Sie können auch dieses Steuerelement um Tabellenzeilen herum einfügen, um Teile einer Tabelle zu wiederholen. *Selbstständigkeit* Die Studierenden sind in der Lage, sich im sehr schnelllebigen Umfeld mobiler Systeme und Cloud-Systeme selbstständig auf neue Technologien und Frameworks einzustellen und sich diese rasch und selbstständig anzueignen. *[Reflexivität, 6]* Sie sind in der Lage, sich auch weitere Frameworks im Cloud-Umfeld, sowie im Bereich mobiler Anwendungen eigenständig anzueignen. *[Lernkompetenz, 6]*					
4	**Inhalte***:* - Besondere Anforderungen an mobile Anwendungen (Kundensicht und Anbietersicht) - Mobile Endgeräte, Sensoren mobiler Endgeräte					

	- Arten Mobiler Anwendungen (Apps) - Aktuelle mobile Betriebssysteme - Aktuelle Entwicklungswerkzeuge, Frameworks und APIs für mobile Applikationen - Architekturparadigmen für die Entwicklung mobiler Anwendungen - Besondere Anforderungen an Cloud-Einsatzszenarien und Betriebsszenarien (Kundensicht und Anbietersicht) - Cloud-Einsatz-Arten, Cloud-Service-Modelle und Cloud-Architekturen (Private, Public, Hybrid Clouds, SaaS,PaaS,IaaS, HaaS) - Cloud-Management (Service Level Agreements, LifeCycle, Betrieb, Kosten- und Risikomanagement) Exemplarische Betrachtung aktueller Cloud-Lösungen
	Empfohlene Literaturangaben: *Mobile Computing. K. Zeppenfeld et al., W3L GmbH* *Android 7. T. Künneth, Rheinwerk Verlag* *IaaS mit OpenStack. T. Beiter et al., d.punkt Verlag* *Die Logik des Mißlingens, D. Dörner, rororo* *Das E-Commerce-Buch, A. Graf et al., dfv-Mediengruppe*
5	**Teilnahmevoraussetzungen:** Empfohlen: Programmierung 1 und 2
6	**Prüfungsformen***:* GUI-Development: Klausur Praktikum GUI-Development: Laborarbeit (unbenotet)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur, Bestandenes Praktikum
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik Wahlrichtung: Application Development Wahlpflichtfach für die anderen Vertiefungsrichtungen
9	***Modulverantwortliche(r):*** Prof. Dr. Ute Matecki Dozent: Prof. Dr. Ute Matecki
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.7.3 32000 – Simulationstechnik

Studiengang: Technische Informatik
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Simulationstechnik						
Kennnummer 32000	**Workload** 150	**Modulart** P	**Studiensemester** 7. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Vorlesung 3 SWS Praktikum: 1 SWS	**Sprache** Deutsch	**Kontakt-zeit** 4 SWS/ 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5	
2	**Lehrform(en) / SWS:** Vorlesung & Übungen Simulationstechnik Praktikum Simulationstechnik					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen: - die grundlegende Vorgehensweise und die Parameter zur Planung der Fertigungsressourcen in realen und in virtuellen Systemen. - die Analyse von Prozessen für Simulationszwecke und Methoden der Prozessmodellierung. - die Informationsmodelle der Simulation. - grundelemente und Algorithmen zur Modellbildung der objekt- und ereignisorientierten Simulation. - Störgrößenverarbeitung in Simulationssystemen. - Bewertungsverfahren für Simulationsmodelle *[Wissen, 6]* *Kompetenz Fertigkeiten* Die Studierenden können: - Betriebs- und Produktionsstrukturen analysieren und die zur Simulation erforderlichen Parameter erfassen. - die Methoden der Modellbildung anwenden und Simulationsmodelle entwerfen, erstellen, erweiterte Algorithmen hinzufügen. ☐Simulationsmodelle optimieren nach den Kriterien: minimale Durchlaufzeit, maximale Kapazitätsauslastung, minimale Puffergrößen, maximale Flexibilität - Verfahren und Algorithmen anwenden die geeignet sind um Simulationsaufgaben in komplexe Modelle zu überführen und damit zielgerichtet ingenieurmäßig zu arbeiten. ☐Modellierverfahren bewerten und evaluieren und die geeigneten Methoden zur Lösung der Probleme auswählen und anwenden. Dazu gehört auch die Analyse von Simulationsaufgaben nach technischen und ökonomischen Gesichtspunkten. *[Systemische Fertigkeiten, 6]* *Sozialkompetenz* - /Kompetenzausprägung wählen /Niveaustufe wählen *Selbstständigkeit*					

	Die Studierenden sind fähig: - logisch und abstrakt zu denken. - technisch/organisatorische Prozesse in Simulationsmodelle zu überführen und daraus Vorhersagen für die Praxis abzuleiten. - die Praxisrelevanz der erlernten Methoden und Prinzipien zu erkennen und diese zielgerichtet zur Lösung von Ingenieurproblemen anzuwenden. *[Eigenständigkeit/Verantwortung, 6]*
4	**Inhalte***:* Die grundlegende Vorgehensweise und die Parameter zur Planung der Fertigungsressourcen in realen und in virtuellen Systemen Analyse von Prozessen und Abläufen Parameterermittlung und -erfassung zur Modellierung für die Simulation. Methoden der Prozessmodellierung, Grundelemente, Algorithmen und Modellbildung zur objekt- und ereignisorientierten Simulation Störgrößenverarbeitung (Verteilfunktionen) in Simulationssystemen Modellbildungstheorie, Systemarchitekturen, Informationsmodelle der Simulation virtuelle Erprobung, Rapid Prototyping (Verfahren, Schnittstellen), virtuelle und reale Prozessketten, Managementkonzepte für virtuelle Entwicklungs- und Produktionsstrukturen. ☐ Bewertung von Simulationsmodellen (technisch und ökonomisch).
	Empfohlene Literaturangaben: Spur, G., Krause, F.-L.: Das virtuelle Produkt, Hanser Verlag, München. Bangsow, S.: Fertigungssimulationen mit Plant Simulation und SimTalk. Anwendung und Programmierung mit Beispielen und Lösungen, Hanser Verlag, München. Eley, M.: Simulation in der Logistik. Eine Einführung in die Erstellung ereignisdiskreter Modelle unter Verwendung des Werkzeuges "Plant Simulation", Springer Verlag, Berlin,New York Hehenberger, P.: Computerunterstützte Fertigung. Eine kompakte Einführung. 1. Aufl.,: Springer Verlag, Berlin, New York. Kramer, U.; Neculau, M.: Simulationstechnik. Hanser Verlag, München. Liebl, F.: Simulation. Problemorientierte Einführung, 2. Aufl., Oldenburg Verlag,

	München, Wien. Sauerbier, T.: Theorie und Praxis von Simulationssystemen. Eine Einführung für Ingenieure und Informatiker, mit Programmbeispielen und Projekten aus der Technik. Vieweg Verlag, Braunschweig, Wiesbaden
5	**Teilnahmevoraussetzungen:** Voraussetzungen für die Teilnahme beschreiben; Außerdem beschreiben, wie sich der Studierende vorbereiten kann (u.a. Literaturangaben, Lehr- und Lernprogramme)
6	**Prüfungsformen***:* Klausur, 90 min., benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Benotete und unbenotete Leistungen; die studienbegleitenden Prüfungen, auf deren Grundlage Leistungspunkte erworben werden, sollen beschrieben sein. Sofern Module Prüfungsvorleistungen vorsehen (Semesterarbeiten, Exkursionsberichte, Hausarbeiten u.a.), müssen diese nach Art und Umfang beschrieben sein
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wahlrichtung Cyber-Physical Systems
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. Eppler Dozent(in):
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.7.4 32400 – IT-Sicherheitsmanagement

Studiengang: Technische Informatik **Semester**: WS 2020/21
StuPO-Version: 17.2 **Letzte Bearbeitung**: 14.10.20

Modul: IT-Sicherheitsmanagement						
Kennnummer **32400**	**Workload** 75 h	**Modulart** P	**Studiensemester** 7		**Dauer** 1 Semester	**Häufigkeit** WS und SS
1	**Lehrveranstaltung(en)** Vorlesung & Übungen IT-Sicherheitsmanagement	**Sprache** Deutsch (deutsches und englisches Literatur-studium erforderlich)	**Kontakt-zeit** 2 SWS / 30 h	**Selbst-studium** 45 h	**Credits (ECTS)** 2,5	
2	**Lehrform(en) / SWS:** Vorlesung & Übungen: 2 SWS					

3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Breites Wissen über Grundlagen und Bedeutung des IT Sicherheitsmanagements *[Wissen, 6]* Tiefe Kenntnis relevanter Normen und Regulatorien im Bereich IT Sicherheitsmanagement *[Wissen, 6]*
	Kompetenz Fertigkeiten Studierende beherrschen ein breites Spektrum an Methoden und Werkzeugen für die Konzeption und Implementierung eines ISM *[Instrumentelle Fertigkeiten, 6]* Studierende sind in der Lage das IT Sicherheitsniveau einer Organisation auf organisatorischer Ebene zu bewerten und mittels ISM zu verbessern *[Beurteilungsfähigkeit, 6]*
	Sozialkompetenz Fachspezifika und aktuelle Regulatorien können sowohl einem Fachpublikum diskutiert als auch den Fachabteilungen verständlich vermittelt werden *[Kommunikation, 6]*
	Selbstständigkeit Das Sicherheitsniveau und Sicherheitsrisiken der Unternehmens IT können hinsichtlich des rechtlichen und ethischen Rahmens kritisch reflektiert werden. *[Reflexivität, 6]*
4	**Inhalte*:*** Vorlesung & Übungen: • Grundlagen und Bedeutung des ITSicherheitsmanagements • Gesetzliche Anforderungen • IT-Sicherheitsstandards • Prozess „IT-Sicherheitsmanagement“ • IT-Sicherheitsmanagement nach BSI-Grundschutzbe • Normen und Zertifizierung • Organisatorische Aspekte
	Empfohlene Literaturangaben: Hofmann, Schmidt: Masterkurs IT-Management, 2. Auflage, Springer, 2010 Grünendahl, Steinbacher u.a.: Das IT-Gesetz: Compliance in der IT-Sicherheit, 2. Auflage, Springer, 2012 Kersten, Reuter u.a.: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, 4. Auflage, Springer, 2013 Müller, K.-R.: IT-Sicherheit mit System, 4. Auflage, Springer, 2011 Pelzl, J.: e-security 4.0 – Sicherheitsmanagement für das Internet der Dinge, aus: Beherrschbarkeit von Cyber Security, Big Data und Cloud Computing - Tagungsband zur dritten EIT ICT Labs-Konferenz zur IT-Sicherheit, Springer, 2014 Kersten, H.; Klett, G.: Der IT Security Manager: Expertenwissen für jeden IT Security Manager - Von namhaften Autoren praxisnah vermittelt, 2. Auflage, Springer, 2012
5	**Teilnahmevoraussetzungen:** keine empfohlen: Inhalte der Module Einführung ITS, Betriebswirtschaftslehre und Management

6	**Prüfungsformen***:* Klausur, 60 min.,benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik Wahlrichtung: Applied IT-Security
9	***Modulverantwortliche(r):*** (n.n.), Prof. Holger Morgenstern Dozent: LB
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.7.5 32500 – Mobile und Cloud Forensik

Studiengang: Technische Informatik
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.2020

Modul: Mobile und Cloud Forensik					
Kennnummer 32500	**Workload** 75	**Modulart** P	**Studiensemester** 7. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS (falls Wahlrichtung Applied IT-Security zustande kommt)

1	**Lehrveranstaltung(en)** Vorlesung Mobile und Cloud Forensik	**Sprache** Deutsch (deutsches und englisches Literaturstudium erforderlich)	**Kontakt-zeit** 2 SWS/ 30 h	**Selbst-studium** 45 h	**Credits (ECTS)** 2,5
2	**Lehrform(en) / SWS:** Vorlesung & Übungen: 2 SWS				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Breite Kenntnis forensischer Methoden spezialisiert in der Digitalen Forensik im Mobile- und Cloud Bereich *[Wissen, 6]*				

	Tiefe Kenntnis forensischer Prinzipien angewandt auf den Bereich der digitalen Spuren im Mobile- und Cloud Bereich [Wissen, 6]
	Kompetenz Fertigkeiten Breites Spektrum an digitalforensischen Methoden zur Sicherung und Analyse digitaler Spuren im Mobile- und Cloud Bereich *[Instrumentelle Fertigkeiten, 6]* Sind in der Lage Möglichkeiten und Grenzen der erlernten forensischen Methoden und Werkzeuge einzuschätzen und diese zu erweitern bzw. neue Skripte/Werkzeuge zu entwickeln *[Systemische Fertigkeiten, 6]* Können die Relevanz gesicherter und analysierter digitaler Spuren hinsichtlich ihrer Relevanz auf die juristischen Fragestellungen beurteilen *[Beurteilungsfähigkeit, 6]*
	Sozialkompetenz Können forensische Ermittlungen im Mobile- und Cloud Bereich durchführen und vor Gericht vertreten *[Kommunikation, 6]*
	Selbstständigkeit Können juristischen/forensische Aufgabenstellungen eigenständig analysieren, in technische Aufgabenstellungen und zurück übertragen und ihre Untersuchungsprozesse entsprechend gestalten *[Eigenständigkeit/Verantwortung, 6]* Notwendige neue / angepasste forensische Methoden und Werkzeuge können eigenständig erschlossen werden *[Lernkompetenz, 6]*
4	**Inhalte*:*** Vorlesung & Übungen • Digitale Forensik im Kontext mobiler Endgeräte (Smartphones, Navigationsgeräte, etc.) • Besonderheiten im Bereich der forensischen Sicherung und Analyse von mobilen Endgeräten (Betriebssysteme, Dateisysteme, Datenformate, Zugriffsmöglichkeiten und Einschränkungen) • Digitale Forensik im Kontext des Cloudcomputings • Besonderheiten im Bereich der forensischen Sicherung und Analyse von Cloud-Systemen (Architekturen, Service- und Organisationsmodelle, Vertrauensmodelle, Zugriffsmöglichkeiten und Einschränkungen) • Praktische Anwendungen und Übungen im Bereich Digitalen Forensik mobiler Endgeräte und Cloud-Systeme
	Empfohlene Literaturangaben: Bommisetty, Tamma, Mahalik: Practical Mobile Forensics, Packt Publishing, 2014 Quick, Martini, Choo: Cloud Storage Forensics, Syngress Media, 2014 Dewald, A., Freiling, F.: Forensische Informatik, 2. Auflage, Books on Demand, 2015 Casey, E.: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3. Auflage, Academic Press, 2011 Carrier, B.: File System Forensic Analysis, Addison Wesley, 2005 Geschonneck, A.: Computer-Forensik (iX Edition): Computerstraftaten erkennen,

	ermitteln, aufklären, dpunkt.verlag, 2014 Hayes, D.: A Practical Guide to Computer Forensics Investigations, Pearson, 2014
5	**Teilnahmevoraussetzungen:** keine empfohlen: Inhalte der Module Einführung ITS, Betriebssysteme, Netzwerke, Digitale Forensik
6	**Prüfungsformen***:* Klausur, 60 min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik, Wahlrichtung Applied IT-Security
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Holger Morgenstern Dozent(in): Prof. Dr. Fein
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.7.6 32200 – Wahlpflichtmodul 2 (WPM 2)

Studiengang: Technische Informatik
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.20

Modul: Wahlpflichtmodul 2						
Kennnummer 32200	**Workload** 150 h	**Modulart** P	**Studiensemester** 7		**Dauer** 1 Semester	**Häufigkeit** WS und SS
1	**Lehrveranstaltung(en)** Wahlpflichtmodul gem WPM-Katalog		**Sprache** Deutsch (deutsches und englisches Literatur-studium erforderlich)	**Kontakt -zeit** 4 SWS / 60 h	**Selbst-studium** 90 h	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** Vorlesung: 4 SWS (gesamt) Eine Aufteilung in mehrere Teilmoduleinheiten ist möglich.					

3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden wenden ihr im Studium erlangtes Wissen auf den jeweiligen Bereich an. Die Studierenden können sich darüber hinaus in angemessener Zeit neue Inhalte aneignen und diese geeignet strukturieren und didaktisch aufbereiten *[Wissen, 6]*
	Kompetenz Fertigkeiten Die Studierenden sind in Lage Konzepte und Methoden zu abstrahieren und auf neue Anwendungsfelder zu übertragen. *[Instrumentelle Fertigkeiten, 6]*
	Sozialkompetenz Die Lernergebnisse sind abhängig vom jeweiligen WPM
	Selbstständigkeit Studierende können die Lehrinhalte selbständig aufarbeiten und strukturiert wiedergeben. Sie sind in der Lage Aufgaben im vorgegeben Zeitrahmen zu bearbeiten *[Eigenständigkeit/Verantwortung, 6]*
4	**Inhalte*:*** Die Wahlpflichtmodule dienen einerseits der weiteren Vertiefung in den einzelnen Studienschwerpunkten und runden andererseits das Studienangebot mit praxisnahen Inhalten ab. Dies geschieht zum einen in Vorbereitung auf die spätere Berufsfertigkeit als auch im Hinblick auf ein sich anschließendes Masterstudium. Zur Wahl stehen die im jeweiligen Semester gem. WPM-Katalog angebotenen Module im Umfang von jeweils 2,5 bzw. 5ECTS.
	Empfohlene Literaturangaben: Es wird auf die Modulbeschreibungen im jeweils gültigen WPM-Katalog verwiesen
5	**Teilnahmevoraussetzungen:** Für die Teilnahme gelten keine über die in der Studien- und Prüfungsordnung festgelegten hinausgehenden Voraussetzungen.
6	**Prüfungsformen***:* Es gelten die im WPM-Katalog für das jeweilige Modul angekündigten Prüfungsformen
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreiche Teilnahme an der Modul(teil)prüfung
8	***Verwendbarkeit des Moduls:*** CSP, AD, ITM, ITS
9	***Modulverantwortliche(r):*** Prof. Dr. Bernd Stauß Dozenten: gem. WPM-Katalog
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

5.7.7 51000 – Bachelor-Thesis

Studiengang: Technische Informatik
StuPO-Version: 17.2

Semester: WS 2020/21
Letzte Bearbeitung: 14.10.202019

Modul: Bachelor-Thesis						
Kennnummer 51000	**Workload** 450	**Modulart** P	**Studiensemester** 7. Semester	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Bachelor Thesis	**Sprache** Deutsch und/oder Englisch	**Kontakt-zeit** 5 h Präsenz (Bachelor-Thesis 4 h, Mündliche Bachelor-prüfung 1 h)	**Selbst-studium** 445 h	**Credits (ECTS)** 15 (Bachelor-Thesis 12, Bachelor-prüfung 3)	
2	**Lehrform(en) / SWS:** Betreute Eigenarbeit					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden sind in der Lage, sich in ein Themengebiet einzuarbeiten, neue Inhalte zu strukturieren und einzuordnen *[Wissen, 6]* *Kompetenz Fertigkeiten* Die Studierenden können für die Wissenschaft und Praxis relevante Fragestellungen in Bezug auf die im Studium erworbenen Kenntnisse und der in der Praxis erworbenen Kenntnisse selbständig und systematisch bearbeiten. *[Systemische Fertigkeiten, 6]* *Sozialkompetenz* Die Studierenden sind fähig, das Ergebnis einer komplexen Fragestellung für Fachkollegen verständlich zu formulieren und darzustellen. *[Kommunikation, 6]* *Selbstständigkeit* Die Studierenden bearbeiten ein ihnen vorgegebenes Thema eigenständig in Abstimmung mit den Betreuern der Thesis *[Eigenständigkeit/Verantwortung, 6]*					
4	**Inhalte*:*** Die Bachelor-Thesis soll zeigen, dass innerhalb einer vorgegebenen Frist ein Problem aus einem Fachgebiet des gewählten Studiengangs selbstständig nach wissenschaftlichen Methoden bearbeitet werden kann. *Empfohlene Literaturangaben:* Bachelor-Arbeit, deren Quellen und ggf. ausgewählte Literatur in Absprache mit den Prüfern					
5	**Teilnahmevoraussetzungen:** Die Ausgabe des Themas der Bachelor-Thesis erfolgt frühestens, wenn alle Modul- bzw. Modulteilprüfungen, die den ersten fünf Semestern zugeordnet sind, bestanden sind					

	und der Studierende seit mindestens einem Semester an der Hochschule Albstadt-Sigmaringen immatrikuliert ist.
6	**Prüfungsformen***:* Bachelor-Thesis: benotet Mündliche Bachelorprüfung: max. 45 min., davon Referat 30 min. Referat und mündliche Prüfung werden gemeinsam benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Mit der Ausgabe des Themas für die Bachelor-Thesis muss die Anmeldung der Arbeit erfolgen. Das Thema muss innerhalb eines Zeitraums von 3 Monaten bearbeitet werden. Die Thesis muss fristgerecht beim Prüfungssekretariat abgeben werden. Bei der Abgabe ist schriftlich zu versichern, dass die Arbeit – bei einer Gruppenarbeit der entsprechend gekennzeichnete Anteil der Arbeit – selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt wurden. Die Ergebnisse der Arbeit sind in einem Referat im Rahmen einer mündlichen Prüfung vorzustellen.
8	***Verwendbarkeit des Moduls:*** IT Security, Technische Informatik, Wirtschaftsinformatik
9	***Modulverantwortliche(r):*** Modulverantwortliche(r): Prof. Dr. Walter Hower, Prof. Dr. Bernd Stauß
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul